US009686193C1

(12) **EX PARTE REEXAMINATION CERTIFICATE** (11840th)

United States Patent
Moore

(10) **Number: US 9,686,193 C1**
(45) **Certificate Issued: May 5, 2021**

(54) **FILTERING NETWORK DATA TRANSFERS**

(71) Applicant: **Centripetal Networks, Inc.**, Herndon, VA (US)

(72) Inventor: **Sean Moore**, Hollis, NH (US)

(73) Assignee: **Centripetal Networks, Inc.**

Reexamination Request:
No. 90/014,476, Mar. 19, 2020

Reexamination Certificate for:
Patent No.: **9,686,193**
Issued: **Jun. 20, 2017**
Appl. No.: **14/625,486**
Filed: **Feb. 18, 2015**

Related U.S. Application Data

(63) Continuation of application No. 13/795,822, filed on Mar. 12, 2013, now Pat. No. 9,124,552.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04L 12/741 (2013.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1466*** (2013.01); ***H04L 45/74*** (2013.01); ***H04L 63/0254*** (2013.01); ***H04L 63/0263*** (2013.01); ***H04L 67/02*** (2013.01); ***H04L 69/22*** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

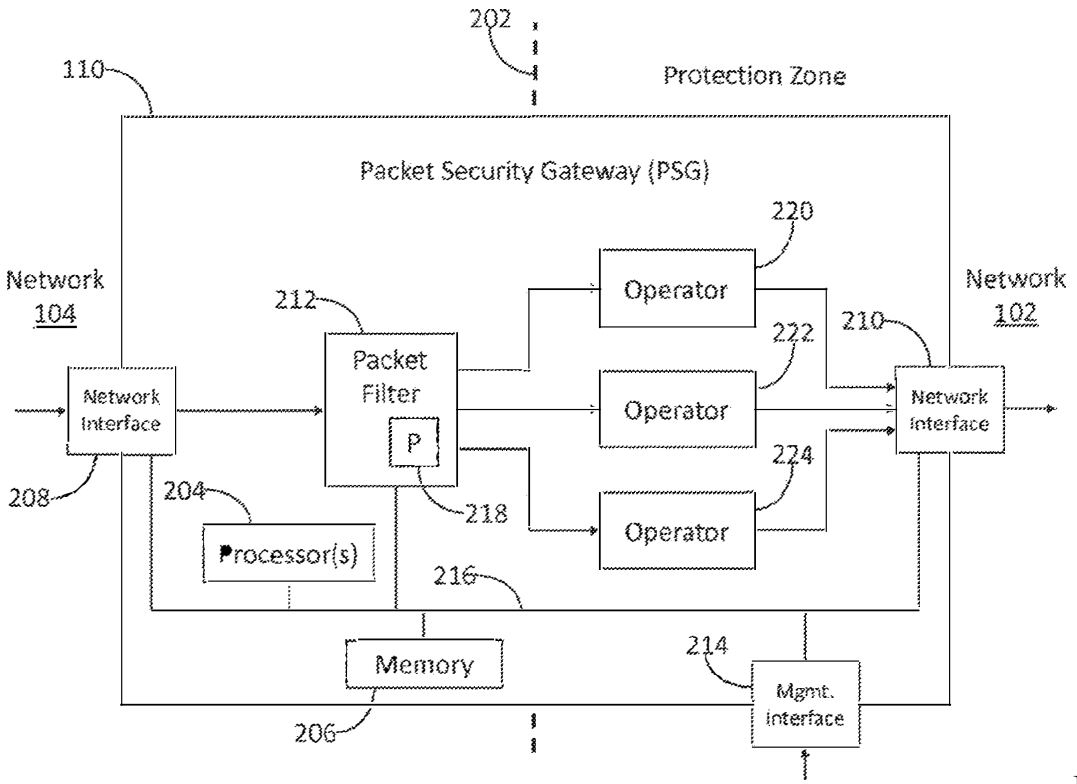
(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/014,476, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner — Minh Nguyen

(57) **ABSTRACT**

Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding, to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.



PAN EX1085
PAN v. Centripetal
IPR2023-01353
Page 00001

EX PARTE REEXAMINATION CERTIFICATE

NO AMENDMENTS HAVE BEEN MADE TO THE PATENT

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **1-20** is confirmed.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,476	03/19/2020	9686193	E4720-00206	1013

31013 7590 04/07/2021

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER
NGUYEN, MINH T

ART UNIT	PAPER NUMBER
3991	

MAIL DATE	DELIVERY MODE
04/07/2021	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

DUANE MORRIS LLP
505 9TH STREET N.W.
SUITE 1000
WASHINGTON, DC 20004

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,476* .

PATENT UNDER REEXAMINATION *9686193* .

ART UNIT *3991* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Notice of Intent to Issue Ex Parte Reexamination Certificate	**Control No.** 90/014,476	**Patent Under Reexamination** 9686193	
	Examiner Minh T Nguyen	**Art Unit** 3991	**AIA Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☑ Prosecution on the merits is (or remains) closed in this *ex parte* reexamination proceeding. This proceeding is subject to reopening at the initiative of the Office or upon petition. *Cf.* 37 CFR 1.313(a). A Certificate will be issued in view of
   (a) ☑ Patent owner's communication(s) filed: 01/25/2021.
   (b) ☐ Patent owner's failure to file an appropriate timely response to the Office action mailed: _____.
   (c) ☐ Patent owner's failure to timely file an Appeal Brief (37 CFR 41.31).
   (d) ☐ The decision on appeal by the ☐ Board of Patent Appeals and Interferences ☐ Court dated _____
   (e) ☐ Other: _____.
2. The Reexamination Certificate will indicate the following:
   (a) Change in the Specification: ☐ Yes ☑ No
   (b) Change in the Drawing(s): ☐ Yes ☑ No
   (c) Status of the Claim(s):
      (1) Patent claim(s) confirmed: 1-20.
      (2) Patent claim(s) amended (including dependent on amended claim(s)): _____
      (3) Patent claim(s) canceled: _____.
      (4) Newly presented claim(s) patentable: _____.
      (5) Newly presented canceled claims: _____.
      (6) Patent claim(s) ☐ previously ☐ currently disclaimed: _____
      (7) Patent claim(s) not subject to reexamination: _____.
3. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
4. ☑ Note the attached statement of reasons for patentability and/or confirmation. Any comments considered necessary by patent owner regarding reasons for patentability and/or confirmation must be submitted promptly to avoid processing delays. Such submission(s) should be labeled: "Comments On Statement of Reasons for Patentability and/or Confirmation."
5. ☐ Note attached NOTICE OF REFERENCES CITED (PTO-892).
6. ☐ Note attached LIST OF REFERENCES CITED (PTO/SB/08 or PTO/SB/08 substitute).
7. ☐ The drawing correction request filed on _____ is: ☐approved ☐disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐None of the certified copies have
   ☐been received.
   ☐not been received.
   ☐been filed in Application No. _____.
   ☐been filed in reexamination Control No. _____.
   ☐been received by the International Bureau in PCT Application No. _____.

   * Certified copies not received: _____.
9. ☐ Note attached Examiner's Amendment.
10. ☐ Note attached Interview Summary (PTO-474).
11. ☐ Other: _____.

All correspondence relating to this reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

cc: Requester (if third party requester)

Notice of Intent to Issue Ex Parte Reexamination Certificate

Pertinent Prosecution History

Ex-Parte Reexamination has been requested for claims 18-19 of United States Patent Number 9,686,193 to Moore ("the 193 patent"), entitled "*Filtering Network Data Transfers*" by a third party requester ("the Requester").

The Office notified the patent owner "PO" of the filing date for reexamination is March 19, 2020.

On May 01, 2020, the Office issued a decision granting ex parte reexamination order ("May 2020 Order").

The Office issued a non-final office action on September 23, 2020 ("Sep. 2020 Non Final OA") following the May 2020 Order.

On January 25, 2021, PO filed an amendment/arguments ("Jan 2021 PO Response") in response to the March 2020 Non Final OA.

The PO requested an Interview on February 24, 2021 ("Feb. 24, 2021 Interview") to further discuss about issues raised in the Sep. 2020 Non Final OA.

The following is a Notice of Intent to Issue Office action in response to the Jan. 2021 PO Response and the Feb. 2021 Interview.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Statement of Reasons for Patentability and/or Confirmation

Claims 1-20 are confirmed.

Claim 18 is confirmed because the prior art of record fails to disclose or render obvious a system which includes a series of filtering steps recited in the claim especially, steps of applying "a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer" and "a second operator configured to forward packets not associated with the particular type of data transfer toward the third network" as recited in the claim.

It appears that Sourcefire is capable of performing each individual step recited in the claim by programming. However, the examiner agrees with the PO's argument that Sourcefire does not disclose a filtering process which includes a series of steps recited in the claim and a POSITA would unlikely to be motivated to apply a first operator to drop packets associated with a particular type of transfer and a second operator to forward packets not associated with a particular type of data transfer toward a third network as recited in the claim. In view of the objective indicia of non-obviousness presented in the record, the examiner agrees to withdraw the rejection based on obviousness.

Claims 1-17 and 19-20 are confirmed for the same reason discussed in claim 18.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Communication with the USPTO

All correspondence relating to this inter partes reexamination proceeding should be directed:

By Mail to: Mail Stop Supplemental Examination
Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at https://efs.uspto.gov/efile/myportal/efs-registered. EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act

on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Notice Re Patent Owner's Correspondence Address

Effective May 16, 2007, 37 CFR 1.33(c) has been revised to provide that:

The patent owner's correspondence address for all communications in an ex parte reexamination or an inter partes reexamination is designated as the correspondence address of the patent.

Revisions and Technical Corrections Affecting Requirements for Ex Parte and Inter Partes Reexamination, 72 FR 18892 (April 16, 2007)(Final Rule)

The correspondence address for any pending reexamination proceeding not having the same correspondence address as that of the patent is, by way of this revision to 37 CFR 1.33(c), automatically changed to that of the patent file as of the effective date.

This change is effective for any reexamination proceeding which is pending before the Office as of May 16, 2007, including the present reexamination proceeding, and to any reexamination proceeding which is filed after that date.

Parties are to take this change into account when filing papers, and direct communications accordingly.

In the event the patent owner's correspondence address listed in the papers (record) for the present proceeding is different from the correspondence address of the patent, it is strongly encouraged that the patent owner affirmatively file a Notification of Change of Correspondence Address in the reexamination proceeding and/or the patent (depending on which address patent owner desires), to conform the address of the proceeding with that of the patent and to clarify the record as to which address should be used for correspondence.

Telephone Numbers for reexamination inquiries:

Reexamination Practice	(571) 272-7703
Central Reexam Unit (CRU)	(571) 272-7705
Reexamination Facsimile Transmission No.	(571) 273-9900

Any inquiry concerning this communication or earlier communication from the Examiner, or as to the status of the proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/Minh Nguyen/
Primary Examiner
571-272-1748
CRU, AU 3991

Conferees:
/Tuan H. Nguyen/
Primary Examiner
CRU, AU 3991

/TIMOTHY M SPEER/
Supervisory Patent Examiner, Art Unit 3991

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Ex Parte* Reexamination of		U.S. Patent No. 9,686,193
Control No.:	90/014,476	Group Art Unit: 3991
Filed:	March 19, 2020	Confirmation No.: 1013
Patent Owner:	Centripetal Networks, Inc.	Examiner: Minh T. Nguyen
For U.S. Patent No.:	9,686,193 – FILTERING NETWORK DATA TRANSFERS	

Submitted Electronically

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

INTERVIEW SUMMARY

Examiner Nguyen,

Centripetal and its undersigned attorney thanks the Examiner and his supervisors for the courtesies extended during the interview conducted on February 24, 2020. During the interview, the attendees discussed the following:

I. THE DIFFERENCES BETWEEN THE '193 AND '552 PATENTS

During the interview, Centripetal described the differences between the claims of the '193 Patent, which the Board found patentable in IPR2018-01559, and the claims of the '552 Patent, which the Board found unpatentable in IPR2018-01436.

The first broad distinction between the claims of the '193 and '552 discussed during the interview is that the "operator" claimed in the '193 Patent is "configured to drop packets associated with the particular type of data transfer" while the '552 Patent includes no such requirement. The attendees also discussed that the '193 Patent is directed to preventing data exfiltration, targeting communications leaving a first network and bound for different (second and third) networks. The claim language relevant to these differences are emphasized below:

'193 Patent	**'552 Patent**
1. A method comprising:	1. A method, comprising:
receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;	at a computing device comprising at least one processor, a memory, and a communication interface: receiving, via the communication interface, a plurality of hypertext transfer protocol secure (HTTPS) packets;
responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, **wherein the data indicates that the first portion of packets is destined for the second network**:	responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet filtering rule stored in the memory,
applying, by the computing system and to each packet in the first portion of packets, ***a*** first operator, specified by the one or more packet-filtering rules, **configured to drop packets associated with the particular type of data transfer**; and	applying, by the at least one processor, an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations; and

dropping, by the computing system, each packet in first portion of packets; and	responsive to a determination by the at least one processor that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations, applying, by the at least one processor, at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination
responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network:	
applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator **configured to forward packets not associated with the particular type of data transfer toward the third network**; and	
forwarding, by the computing system, each packet in the second portion of packets toward the third network.	

On this topic, Centripetal also discussed the Board's Institution Decision in IPR2018-01559, which found that the '193 Patent Claims patentable ***after*** it instituted trial in IPR2018-01436. That is, after it determined that the Sourcefire reference disclosed the "operator" recited in the '552 Patent it determined that Sourcefire did not disclose the "operator" recited in the '193 Patent. In particular, the Board determined in IPR2018-01559 that Sourcefire does not disclose an ***operator*** distinct from a packet-filtering rule, that is ***configured to drop packets associated with a particular type of data transfer***. As shown above, this language does not appear in the

'552 Patent Claims, and the Board focused on this language in declining to institute IPR of the '193 Patent.

With respect to the exfiltration elements, the parties discussed that the Office Action's focus on whether Sourcefire ***could be*** modified to reach the claims is contrary to the law. The correct question is whether a POSITA ***would have been*** motivated to modify Sourcefire. *See Orexo AB v. Actavis Elizabeth LLC*, 903 F.3d 1265, 1272-73 (Fed. Cir. 2018). Sourcefire does not identify exfiltration as a problem and does not disclose or suggest Centripetal's claimed solution to this problem. *See* § III.

II. THERE IS NO SUBSTANTIAL NEW QUESTION OF PATENTABILITY

During the interview, the attendees also discussed the fact that for an SNQ to be present, "the teaching of the (prior art) patents and printed publications is such that a reasonable examiner would consider the teaching to be important in deciding whether or not the claim is patentable; and (B) the ***same question of patentability*** as to the claim has not been decided by the Office in an earlier concluded examination or review of the patent." MPEP § 2242 (II)(A). In this case, the Board already decided the "same question of patentability" in an earlier concluded examination of the '193 Patent. The proceedings in IPR2018-01559 are a "concluded examination" because it was "contested Office proceeding which has been concluded and which involved the patent." MPEP § 2242 (I) (emphasis added). The attendees also discussed the related issue of 35 U.S.C. § 325(d). Since there can be no substantial new question of patentability, the ex parte reexamination should be terminated.

III. OBJECTIVE INDICIA OF NONOBVIOUSNESS

The attendees also discussed objective indicia of nonobviousness during the interview. In particular, the attendees discussed that there was a long-felt need for a solution to the exfiltration problem because exfiltrations are typically facilitated by using ***popular network data transfer protocols***, such as the Hypertext Transfer Protocol (HTTP). Because of this fact, prior attempts by others to prevent data exfiltration were often too coarse or overbroad (such as blocking all HTTP traffic), resulting in negative impact to the subject computer network and ultimately to business operations. The attendees explained how Centripetal solved this problem by (1) analyzing communications between resources on a "first network" and "a second

network," and (2) "applying" a "first operator" to "drop packets associated with the particular type of data transfer." This two-stage process succeeded because it permitted normal business network traffic, like allowing a web browser to download web pages hosted by web servers while still preventing data exfiltrations.

The attendees also discussed the bench trial opinion in the co-pending litigation between Centripetal and Cisco. In that opinion, the Court determined that Cisco copied the '193 Patent, which "provides compelling evidence of nonobviousness." Ex. 2001 at 166 (Court's conclusion of infringement and damages); *id.* at 157 ("Therefore, the fact that Cisco's system mirrors the functionality of the Centripetal patents is compelling evidence that damages should be enhanced for copying.") *id.* at 157 ("The Court **FINDS** that Cisco willfully infringed the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent, therefore enhanced damages are warranted under the evidence."). The evidence of copying is even more relevant here because Cisco made and sold the Sourcefire system and Cisco would not have copied Centripetal's patents if it already had the technology in its possession. As a result, all claims of the '193 Patent should be confirmed patentable. *Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1285 (Fed. Cir. 2000).

Respectfully submitted,

Date: March 16, 2021

/Jeffrey H. Price/
Jeffrey H. Price
Registration No. 69,141
Attorney for Patent Owner
Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, New York 10036
Tel.: (212) 715-9100 | Fax : (212) 715-8000
Customer No. 31013

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,476	03/19/2020	9686193	E4720-00206	1013

31013 7590 02/26/2021

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER
NGUYEN, MINH T

ART UNIT	PAPER NUMBER
3991	

MAIL DATE	DELIVERY MODE
02/26/2021	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Ex Parte Reexamination Interview Summary	Control No. 90/014,476	Patent Under Reexamination 9686193	
	Examiner Minh T Nguyen	Art Unit 3991	AIA (FITF) Status No

All participants (USPTO personnel, patent owner, patent owner's representative):

(1) Minh Nguyen, Timothy Speer, Tuan Nguyen	(3) Sean Moore, Paul More, Paul Andre
(2) Jeffrey Price, Jonathan, James Hannah	(4) ____

Date of Interview: 24 February 2021

Type: a) ☐ Telephonic b) ☑ Video Conference
c) ☐ Personal (copy given to: 1) ☐ patent owner 2) ☐ patent owners representative)

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☑ No.
If Yes, brief description: ____

Agreement with respect to the claims f) ☐ was reached. g) ☐ was not reached. h) ☑ N/A.
Any other agreement(s) are set forth below under "Description of the general nature of what was agreed to..."

Claim(s) discussed: 18-19 .

Identification of prior art discussed: Sourcefire .

Description of the general nature of what was agreed to if an agreement was reached, or any other comments:
See Continuation Sheet .

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims patentable, if available, must be attached. Also, where no copy of the amendments that would render the claims patentable is available, a summary thereof must be attached.)

A FORMAL WRITTEN RESPONSE TO THE LAST OFFICE ACTION MUST INCLUDE PATENT OWNER'S STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. (See MPEP § 2281). IF A RESPONSE TO THE LAST OFFICE ACTION HAS ALREADY BEEN FILED, THEN PATENT OWNER IS GIVEN **ONE MONTH** FROM THIS INTERVIEW DATE TO PROVIDE THE MANDATORY STATEMENT OF THE SUBSTANCE OF THE INTERVIEW
(37 CFR 1.560(b)). THE REQUIREMENT FOR PATENT OWNERS STATEMENT CAN NOT BE WAIVED.
EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).

/Minh Nguyen/ Primary Examiner, CRU, AU 3991	/TUAN H NGUYEN/ Primary Examiner, Art Unit 3991	

cc: Requester (if third party requester)

Continuation of Description of the general nature of what was agreed to if an agreement was reached, or any other comments: We discussed about topics laid out in the attached Interview Agenda. Applicant's representative pointed out differences between claim 18 of the '193 Patent and claim 8 of the parent '552 patent. Further clarifying the term "operator", "data exfiltrations" and explaining his position regarding SNQ.

EXHIBIT 2026

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Ex Parte* Reexamination of		U.S. Patent No. 9,686,193
Control No.:	90/014,476	Group Art Unit: 3991
Filed:	March 19, 2020	Confirmation No.: 1013
Patent Owner:	Centripetal Networks, Inc.	Examiner: Minh T. Nguyen

For U.S. Patent No.: 9,686,193 – FILTERING NETWORK DATA TRANSFERS

Submitted Electronically

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF DR. ALESSANDRO ORSO
IN SUPPORT OF CENTRIPETAL'S RESPONSE TO NON-FINAL OFFICE ACTION

TABLE OF CONTENTS

Page

I. EXPERIENCE AND QUALIFICATIONS 1

A. Curriculum Vitae 1

B. Prior Testimony 4

C. Compensation 4

II. SCOPE OF STUDY AND OPINIONS 4

D. Questions Presented 4

E. Materials Considered 5

III. SUMMARY OF OPINIONS 5

IV. LEGAL STANDARDS 5

F. Claim Construction 5

G. Obviousness 5

V. PERSON OF ORDINARY SKILL IN THE ART 9

VI. BACKGROUND OF CENTRIPETAL PATENTS AND THE STATE OF THE ART 9

VII. Overview of Sourcefire 3D 12

VIII. The '193 Patent is Not Obvious Over Sourcefire 12

A. Claim Interpretation 13

1. "operator… configured to drop packets associated with the particular type of data transfer" 13

H. Sourcefire Does Not Disclose an "operator… configured to drop packets associated with the particular type of data transfer" 14

I. There is No Motivation to Modify Sourcefire to Address Exfiltrations 17

B. Objective Indicia of Nonb Demonstrate Nonobviousness of the Challenged Claims 24

1. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others 24

I, Dr. Alessandro Orso, have been asked by Plaintiff Centripetal Networks, Inc. ("Centripetal") to testify as an expert witness in the above referenced action.

I. EXPERIENCE AND QUALIFICATIONS

A. Curriculum Vitae

1. The details of my education, work experience, research, and publications (including publications authored in the last 10 years) are summarized in my curriculum vitae ("CV") attached hereto as Appendix A of this Report.

2. I am currently a Professor in the School of Computer Science and an Associate Dean in the College of Computing, at the Georgia Institute of Technology (Georgia Tech). I received my MS degree in Electrical Engineering (1995) and my PhD in Computer Science (1999) from Politecnico di Milano, Italy. My main areas of expertise are program analysis, software testing and debugging, computer security, program comprehension, and reverse engineering.

3. Overall, I have been working in the software field for over 25 years. While preparing my MS thesis, in 1994, I worked for one year as the system administrator for a network of 16 public libraries, which involved setting up, connecting, and maintaining a group of Linux servers that were exchanging updates overnight. After getting my MS degree, in 1995, I worked for several months as a free-lance consultant, helping develop IT solutions for companies and performing Linux system installations.

4. Additionally, in my initial years at Georgia Tech, when I was working as a Postdoctoral Fellow, I was in charge of setting up my research group's lab, which involved installing operating systems and software, setting up networks, and configuring routers and firewalls for these networks. In the same period, I became a certified Linux system administrator.

5. During my PhD, I did research in the general area of software testing. My dissertation was about novel techniques for testing systems written using object-oriented

languages. After completing my PhD, in 1999, and before moving to Georgia Tech, I worked for a year as a Postdoctoral Fellow at Politecnico di Milano, where I extended my dissertation work. In the same year, I spent the summer at the University of Illinois at Chicago as a visiting researcher.

6. I joined Georgia Tech in 2000 and worked there in different capacities: Postdoctoral Fellow (2000-2001), Research Scientist (2001-2004), Assistant Professor (2004-2008), Associate Professor with tenure (2008-2014), and Full Professor (2014 to date). From January 2015 to December 2017, I was Associate School Chair for the School of Computer Science, which involved various kinds of administrative responsibilities. Since November 2020, I have been an Associate Dean with the College of Computing at Georgia Tech, which also involves various administrative responsibilities.

7. In 2011, during my sabbatical year, I spent time as a visiting scholar at Politecnico di Milano, Italy (my alma mater), IBM Research, India, University of Lugano, Switzerland, and University of Buenos Aires, Argentina.

8. I have published over 100 refereed conference and journal papers in the general area of computer science. I have received several Distinguished Paper Awards and Best Paper Awards. I also received two Impact Awards, which are given to recognize the impact of research work in retrospect, typically considering the last ten years. I have been invited to give numerous guest lectures, talks, and distinguished lectures about my research. I have received grants to support my research from several major companies and national agencies, including Google, IBM, Microsoft, DARPA, DHS, NSF, and ONR.

9. I have developed and taught several classes on software engineering, for both graduate and undergraduate students. I also developed an on-line class on software engineering that is being offered through the Udacity and edX platforms. My online class is being offered as

part of Georgia Tech's Online MS in both Computer Science and Cybersecurity, and has been offered as part of Georgia Tech's professional education curriculum. My online class has been taken by thousands of students and has been used by several colleagues as teaching material for their software engineering courses.

10. In addition to teaching in the academic context, I also taught a variety of professional education courses in various topics, including software quality, project management, software design, and system administration, to IT professionals in various companies and countries, including Argentina, Italy, Paraguay, South Africa, and United States.

11. I am an expert in the area of computer security. In the last 20 years, I have received multiple grants to support my security-related work from various agencies, including DARPA, DHS, NSF, and ONR, and I have published several well-cited papers about computer security. For example, one line of research that I successfully pursued in my career focuses on analysis and testing of web applications to improve their security. In this context, I developed two new techniques that can detect and prevent injection attacks to web applications. Together the main papers that describe these techniques have been cited over 2,000 times by the scientific community. One of these papers has also recently received a Most Influential Paper Award at the IEEE/ACM International Conference on Automated Software Engineering (ASE 2020). Developing this kind of techniques requires a deep understanding of the concepts, mechanisms, and technologies involved, including computer and network security, multi-tier architectures, databases, JavaScript, SQL, HTML, HTTP and other underlying network protocols.

12. I am active in the software engineering research community in a variety of ways. I served as Program Chair for all the top conferences in my area and regularly serve on Program Boards and Program Committees for these conferences. I also regularly perform peer reviewing

for various journals and for grant proposals submitted for funding to the National Science Foundation and other agencies. I am part of the Steering Committee of the flagship conference in software engineering. I have also served on the Steering Committee for the two main conferences in the area of Software Testing and Program Analysis: The ACM International Symposium on Software Testing and Analysis (ISSTA) and the IEEE International Conference on Software Testing, Verification and Validation (ICST). Finally, I served as Associate Editor of the ACM Transactions on Software Engineering and Methodology.

13. I am a Distinguished Member of the ACM and an IEEE Fellow.

B. Prior Testimony

14. A list of cases in which I have testified at deposition or trial or in written reports during at least the past five years is attached as Appendix A of this Report.

C. Compensation

15. My rate of compensation for my work in this case is $525 per hour plus any direct expenses incurred. My compensation is based solely on the amount of time that I devote to activity related to this case and is in no way affected by any opinions that I render. I receive no other compensation from work on this action. My compensation is not dependent on the outcome of this matter.

II. SCOPE OF STUDY AND OPINIONS

D. Questions Presented

16. I have been asked by counsel for Centripetal to evaluate the Office Action Mailed September 23, 2020, in Reexamination Control No. 90/014,476. In particular, I have been asked to consider whether the asserted claims of the '193 Patent are obvious in view of Sourcefire. My responsive expert opinions are set forth herein.

E. Materials Considered

17. My opinions, expressed herein, are based on information I have reviewed to date including the materials referenced herein and in the exhibits attached to this Report, and are based on my knowledge and experience in the fields of computer and network security.

18. In the process of forming my opinions, I have reviewed and considered numerous documents and items including, but not limited to: the Request filed by Cisco Systems, Inc., including documents cited in the Request, the '193 Patent and its file history, and the Examiner's Non-Final Office Action. A list of the materials I have considered in forming my opinions are cited in this report and attached as Appendix B.

III. SUMMARY OF OPINIONS

19. It is my opinion that all of the asserted claims of the '193 Patent are valid.

IV. LEGAL STANDARDS

20. Counsel for Centripetal has informed me of the following legal standards that I have used as a framework in forming my opinions contained herein.

F. Claim Construction

21. I have been informed that in an *ex parte* reexamination the Patent Office gives claim terms their broadest reasonable interpretation constistent with the specification. I have applied this standard in forming my opinions in this case.

G. Obviousness

22. I have been informed that if a single reference does not contain every limitation of a patent claim, it can only invalidate that claim if it would be obvious when considered in light of other prior art references or devices without viewing the combination with hindsight bias. Only if the differences between the claimed invention and the prior art are such that the claimed invention,

as a whole, would have been obvious to a person having ordinary skill in the art at the time the invention was made without the benefit of hindsight is the claim is invalid.

23. I have been informed that the types of 35 U.S.C. § 102 prior art described above can individually be a basis for invalidating a patent, or these references can be combined to show a patent is invalid as obvious under 35 U.S.C. § 103. I have been informed that the analysis of obviousness involves several factual inquiries including the scope and content of the prior art, the differences between the prior art and the claim, and the level of ordinary skill in the art at the time of the invention.

24. I have been informed that the test for analogous art is very specific. I have been informed that art is non-analogous unless it is: (1) from the same field of endeavor as the claimed invention; or (2) reasonably pertinent to the particular problem faced by the inventor. I have been informed that an art citation that is not from the same field of endeavor as a claimed invention must be "reasonably pertinent" to the problem addressed by the inventor. I have been informed that art is "reasonably pertinent" when it would "logically commend itself" to an inventor's attention in considering his problem. Conversely, I have been informed that when art is directed to a different purpose than a claimed invention, an inventor would have less motivation or occasion to consider it.

25. I have been informed that the fact that prior art references all concern the same field of endeavor is not in itself sufficient rationale for making the combination. Many types of techniques and systems exist in the same field of endeavor. That fact alone would not make it obvious to combine their features. I have been informed that a proper obviousness determination must show reason why a person of ordinary skill in the art would have thought to combine

particular available elements of knowledge, as evidenced by the prior art, to reach the claimed invention.

26. I have been informed that a party seeking to invalidate a patent on obviousness grounds must demonstrate by clear and convincing evidence that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.

27. I have been informed that to establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art.

28. I have been informed that if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious.

29. I have been informed that to determine whether a combination of known elements would have been obvious to a person of ordinary skill in the art at the time of the invention, one must consider the references in their entirety to ascertain whether the disclosures in those references render the combination obvious to such a person.

30. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. Additionally, I understand that a patent is likely to be invalid for obviousness if a person of ordinary skill in the art can implement a predictable variation or if there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. A combination is not obvious, however, where the combination cannot be implemented without undue experimentation or when the motivation to create the combination comes from hindsight.

31. I have been informed that when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill in the art has good reason to pursue the known options within his or her technical grasp. I understand that, if this leads to anticipated success, it is likely the product not of innovation, but rather of ordinary skill and common sense. I have been informed that the fact that a combination was obvious to try might show that the patent claim was obvious.

32. I have been informed that, even when all claim limitations can be found in a combination of prior art references, the fact-finder must consider as part of the obviousness determination not only what the prior art teaches, but whether the prior art teaches away from the claimed invention and whether there is a motivation to combine teachings from separate references in the manner claimed.

33. I have been informed that, in assessing whether a claimed invention is obvious, secondary considerations that may weigh towards the non-obviousness of the invention, including the following, should be considered:

- Whether the claimed invention satisfied a long-felt need;
- Whether the claimed invention was preceded by a history of failures by others to solve a problem or problems solved by such invention;
- Whether the claimed invention achieved a surprising or unexpected result;
- Whether the claimed invention exhibited performance superior to prior art devices and/or methods;
- Whether the claimed invention has achieved commercial success;
- Evidence of industry acquiescence;
- Licenses;
- Whether the claimed invention has been copied;
- Whether the claimed invention was the subject of skepticism by the industry; and
- Whether the prior art taught away from the claimed invention.

V. PERSON OF ORDINARY SKILL IN THE ART

34. I understand that the factors to be considered in determining the level of ordinary skill in the art to be: (1) the educational level of active workers in the field, including the named inventors of the patent; (2) the type of problems encountered in the art; (3) prior art solutions to those problems; (4) the rapidity with which innovations are made; and (5) the sophistication of the technology in the art.

35. Based on my review of the '193 Patent and my consideration of the abovementioned factors, it is my opinion that a person of ordinary skill in the art at the time of the invention of the '193 Patent would be someone with a bachelor's degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field. My opinion would not change if the '193 Patent is found to have a priority date differing from those listed below.

36. I further understand that the priority date of the '193 Patent is no later than March 12, 2013.

VI. BACKGROUND OF CENTRIPETAL PATENTS AND THE STATE OF THE ART

37. As a means to continue its development of innovative cyber security products and solutions, Centripetal submitted and was awarded multiple patents, including the patent involved in this case, the '193 Patent.

38. The '193 Patent generally discloses systems and methods for "filtering network data transfers." '193 Patent at Title. In particular, the '193 Patent discloses exemplary techniques for preventing "[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet)…." '193 Patent at 1:24–25. The exemplary techniques claimed in the '193 Patent involve applying packet-filtering rules specifically crafted to prevent such exfiltrations.

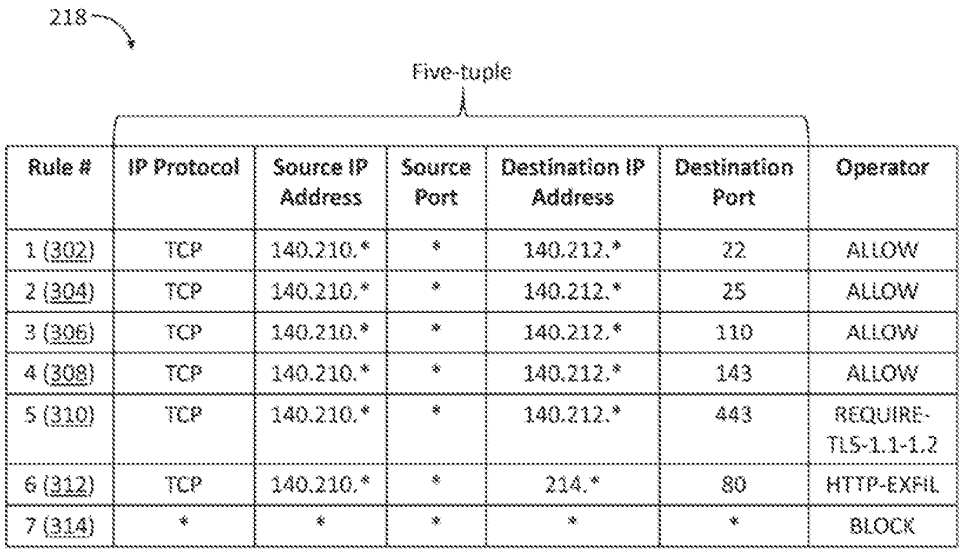
39. In other words, the asserted claims of the '193 Patent recite rules for preventing the transfer of a subset of packets out of the network. These rules involve implementing a two-stage process for filtering traffic:

> Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; **if so, the second stage** may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources.

'193 Patent at 8:45–52 (emphasis added).

40. Thus, the '193 Patent discloses preventing exfiltrations when packets match (1) a particular source and destination criteria (*i.e.* a first and second network, as claimed) and (2) using an operator to determine whether the rule allows for the "particular type of data transfer." Once it is determined that a received packet matches the source/destination criteria, the second stage (that may be performed by the operator recited in the asserted claims) occurs, wherein an operator is applied to drop packets associated with a "particular type of data transfer."

41. Exemplary rules of the type described above and recited in the '193 Patent are described with respect to FIG. 3, wherein each rule "may specify criteria and one or more operators that may be applied to packets associated with (e.g., matching) the specified criteria." '193 Patent at 5:49–52. For example, the claims recite a technique in which a first portion of packets is identified that includes data that "indicates that the first portion of packets [received from the first network] is destined for the second network." For that first portion of packets an operator is applied that is "configured to drop packets associated with the particular type of data transfer." This technique is akin to Rule 6 of FIG. 3, which specifies that an HTTP-EXFIL operator should be applied to packets received from a Source IP Address, 140.210.* (*e.g.* a first network), destined for a Destination IP Address, 214.* (*e.g.* a second network) and may be used to block a particular type of data transfer:



Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

'193 Patent at FIG. 3.

42. The HTTP-EXFIL operator disclosed in the '193 Patent is one example of a type of operator. An example of an HTTP-EXFIL operator is shown below:

```
Operator HTTP-EXFIL(ip-packet):
    Inspect app-pkt(ip-packet) match GET return ALLOW;
    Inspect app-pkt(ip-packet) match POST return BLOCK;
    Inspect app-pkt(ip-packet) match PUT return BLOCK;
    Inspect app-pkt(ip-packet) match DELETE return BLOCK;
    Inspect app-pkt(ip-packet) match CONNECT return BLOCK;
    Return BLOCK;
End Operator HTTP-EXFIL;
```

'193 Patent at 7:51–59.

43. However, rather than only operating on HTTP such as those in the HTTP-EXFIL operator, the operators recited in the challenged claims more broadly encompass any "particular type of data transfer," including types of data transfers associated with communications protocols other than HTTP and HTTPS. This technique furthers one of the goals of the '193 Patent, which

is to "prevent exfiltrations that are mediated by other data transfer protocols besides HTTP and HTTPS." '193 Patent at 8:61–62.

VII. OVERVIEW OF SOURCEFIRE 3D

44. Sourcefire 3D is a system of components that provide "real-time network intelligence for real-time network defense." Sourcefire Manual at 32. The system operates via network appliances referred to as "3D sensors" that are capable of running an intrusion prevention system (IPS), which "monitor your network for attacks that might affect the availability, integrity, or confidentiality of hosts on the network." Sourcefire Manual at 33-34. 3D sensors that are licensed to use IPS "include a set of intrusion rules developed by the Sourcefire Vulnerability Research Team (VRT)." Sourcefire Manual at 34.

45. An intrusion rule used by a 3D sensor with the IPS component is not a network-threat-indicator based rule, but rather "a specified set of keywords and arguments… that detects attempts to exploit vulnerabilities on your network by analyzing network traffic to check if it matches the criteria in the rule." Sourcefire Manual at 761. IPS compares traffic against the conditions specified in each rule, and if the traffic matches all the conditions specified in a rule, the rule triggers. Sourcefire Manual at 761. When a 3D sensor device identifies a possible intrusion, "it generates an intrusion event, which is a record of the date, time, the type of exploit, and contextual information about the source of the attack and its target." Sourcefire Manual at 35.

46. Sourcefire 3D has previously been considered in *inter partes* reviews IPR2018-1559, which affirmed the validity of the '193 Patent over Sourcefire 3D. Ex. 1067. I have reviewed IPR2018-01559. Notably IPR2018-01559 addresses the exact reference at issue in this reexamination. I also note that the Request makes the same exact arguments that were rejected by the PTAB in denying institution of the IPR.

VIII. THE '193 PATENT IS NOT OBVIOUS OVER SOURCEFIRE

A. Claim Interpretation

1. "operator… configured to drop packets associated with the particular type of data transfer" and "second operator configured to forward packets not associated with the particular type of data transfer"

47. Each of the independent claims of the '193 Patent recites an "operator… configured to drop packets associated with the particular type of data transfer" and a "second operator configure to forward packets not associated with the particular type of data transfer." Two exemplary operators of the type recited in the claims of the '193 Patent are reproduced below:

HTTP-EXFIL Operator	REQUIRE-TLS-1.1-1.2 Operator
Operator HTTP-EXFIL(ip-packet): Inspect app-pkt(ip-packet) match GET return ALLOW; Inspect app-pkt(ip-packet) match POST return BLOCK; Inspect app-pkt(ip-packet) match PUT return BLOCK; Inspect app-pkt(ip-packet) match DELETE return BLOCK; Inspect app-pkt(ip-packet) match CONNECT return BLOCK; Return BLOCK; End Operator HTTP-EXFIL;	Operator REQUIRE-TLS-1.1-1.2(ip-packet): Inspect app-pkt(ip-packet) match 1.0 return BLOCK; Inspect app-pkt(ip-packet) match 1.1 return ALLOW; Inspect app-pkt(ip-packet) match 1.2 return ALLOW; Return BLOCK; End Operator REQUIRE-TLS-1.1-1.2;

See '193 Patent at 7:51–59; 8:21–26. Consistent with the plain language of the claims, the HTTP-EXFIL Operator and the REQUIRE-TLS-1.1-1.2 Operator is each configured to drop packets associated with a particular type of data transfer.

48. Notably, the claims of the '193 Patent require two operator which are distinct from the rules themselves.

49. Notably, the claims of the '193 Patent differ from the claims of the '552 Patent in a critical manner. Specifically, unlike the operator of the '552 Patent claims, the operator recited in the claims of the '193 Patent must "be configured to drop packets associated with the particular type of data transfer." *Compare* '552 Patent at Claim 1 *with* '193 Patent at Claim 1. Unlike the '193 Patent claims, there is no requirement in the '552 Patent claims that the operator itself must be configured to drop packets. Rather, the only requirement in the '552 Patent is that the operator ***specifies*** application-header-field-value criteria and a packet transformation function. In addition,

the '552 Patent does not require a second operator that is configured to forward packets not associated with the particular type of data transfer.

50. In denying institution of *inter partes* review in IPR2018-01559, the Board focused on this crucial claim language. Ex. 1067 at 9 ("This first operator is ***configured to drop*** packets associated with the type of data transfer that the recited packet-filtering rules are configured to prevent."); *id.* at 10–11 (contrasting an ***operator*** that is configured to drop packets with a ***rule*** that drops packets); *id.* at 11 (finding that an operator is distinct from the rule because an operator may be associated with multiple rules); *id.* at 12 (finding that the rules and operators are "distinct," and the operator performs "one or more functions on the packets").

51. For the foregoing reasons, and consistent with the Board's Institution Decision in IPR2018-01559, the "operator" term of the '193 Patent is distinct from the "operator" term claimed in the '552 Patent because it is "configured to drop packets associated with the particular type of data transfer."

H. Sourcefire Does Not Disclose an "operator… configured to drop packets associated with the particular type of data transfer" or "a second operator configured to forward packets not associated with the particular type of data transfer"

52. The '193 Patent teaches and claims, responsive to a determination that a first portion of packets is destined for the second network, applying an operator that specified by the packet-filtering rules that is "configured to drop packets associated with the particular type of data transfer" as well as a second operator that forwards packets not associated with the particular type of data transfer. *See, e.g.*, '193 Patent at 8:10-17 ("Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication. *See also id.* at 8:53–65.

53. Indded, the '193 Patent introduced the concept of applying an operator that is applied after a packet filter rule determines whether certain criteria have been met. Id. at 2:24–29. There are simply no such rules or operators in Sourcefire.

54. In the Office Action, the Examiner states:

> As discussed above, a first operator in this case is a "drop operator" which can be used to drop packets that meet the criteria. The following are examples regarding HTTP method PUT criteria, FTP command of PORT criteria and ssl_version criteria.

Office Action at 11. As a preliminary matter, it is unclear what disclosure from Sourcefire the Examiner points to as a "drop operator" because there is no citation to Sourcefire accompanying the Examiner's statement. *Id.* And as the Board previously determined, and a text search of Sourcefire confirms, Sourcefire does not disclose anything called a "drop operator." IPR2018-01559 at 10.

55. I presume that the Examiner is referring to Sourcefire's "Rule Action." *See* Office Action at 7 (citing Sourcefire at 358–359); *see also* Sourcefire at 764–765. But the "Rule Action" is part of the rule itself and not part of any operator specified by the rule. *See* Sourcefire at 765 ("Each rule header includes a parameter that specifies the action the system takes when a packet triggers a rule."). Thus, the rule itself is configured to drop packets, not any operator specified by the rule, so the Rule Action fails to satisfy the Board's conception of what the term "first operator" means in the context of the '193 Patent, which is specified by but ***distinct from*** the packet-filtering rule. *See* § VII.A.1, *supra*.

56. Nor is Sourcefire's "Rule Action" "configured to drop packets **associated with the particular type of data transfer**," as recited in each independent claim of the '193 Patent. Rather than specifying an operator "configured to drop packets associated with the particular type of data transfer, the rule itself specifies the "patterns that a packet's payload must match to trigger the

rule" and the rule's ***Rule Action*** drops the packet without applying any additional operator. Sourcefire at 762-765 ("Each rule header includes a parameter that specifies the action the system takes when a packet triggers a rule."). Sourcefire neither teaches nor suggests a separate operator, like the explaray HTTP-EXFIL operator associated with Rule 6 of FIG.3, which is "configured to drop packets associated with [a] particular type of data transfer." *See* '193 Patent, Claim 1 and Fig. 3.

218

Five-tuple

Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

57. In contrast to Sourcefire, in Rule 6 (which is consistent with the claim language), the rule specifies the criteria a packet must match in order to determine whether to apply a separate "operator," which is in turn "configured to drop packets associated with the particular type of data transfer."

58. In other words, Sourcefire is ***not*** capable of applying "a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular

type of data transfer." There is simply no functionality in Sourcefire capable of constructing a rule that specifies "a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer."

59. Accordingly, while the Examiner contends that "[u]sing the rules language, a user could specify the behavior of a rule by combining keywords in the rule," both the behavior and keywords are explicitly within the rule itself and are neither specified nor carried out by an operator distinct from the rule itself, which is "configured to drop packets associated with the particular type of data transfer," as claimed. Office Action at 7. For at least the foregoing reasons, Sourcefire does not teach or suggest "apply[ing]... a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer," as recited in independent claims 1, 8, 18, and 19 of the '193 Patent. Moreoever, there is no disclosure of a second operator that is configured to forward packets not associated with the particular type of dta transfer as recited in independent claims 1, 8, 18, and 19 of the '193 Patent. Claims 2-7, 9-17, and 20, which depend therefrom, are patentable for at least the same reasons.

I. There is No Motivation to Modify Sourcefire to Address Exfiltrations

60. The Examiner concedes that Sourcefire does not explicitly disclose the combination of rules recited in the independent claims of the '193 Patent and states instead that "Sourcefire discloses that different intrusion rules ***could be applied*** to some different portion of the plurality of packets which can be deemed to be a second portion of packets from the first network (source) and destined for a third network (destination different than second network destination)." Office Action at 7. Further, the Examiner suggests that because "Sourcefire provides a very flexible approach for crafting rules that recognize that the same rule criteria can be utilized differently for packets to/from an internal network as compared to an external network" it would have been obvious to construct the particular set of rules and operators recited in the claims of the '193 Patent

and that the claims of the '193 Patent represent nothing more than a "design choice." *See* Office Action at 12–13. I disagree.

61. First, the Examiner's obviousness rationale fails because it focuses on what a POSA could[1] do with the Sourcefire system but does not establish that a POSA ***would*** have been motivated to do it. As discussed above, the claims of the '193 Patent are explicitly drawn to preventing exfiltrations. *See* § VI, *supra*. Sourcefire, on the other hand, is an "Intrusion Prevention System," or "IPS" that allegedly "provides best-in-class ***intrusion*** detection and prevention by harnessing the power of the industry-standard Snort® rules-based detection engine." Sourcefire at 33. It applies ***intrusion*** rules. Sourcefire at 34 ("3D Sensors that are licensed to use IPS include a set of *intrusion rules* developed by the Sourcefire Vulnerability Research Team (VRT)."). The entirety of the 2,123 pages of the Sourcefire reference does not mention exfiltration attacks, disclose any rules or combinations of rules for preventing exfiltration attacks, or suggest any steps that a user might take to prevent exfiltrations.

62. In fact, the very nature of exfiltration attacks would have confounded a POSA reading Sourcefire because Sourcefire "looks for malicious activity, and reports and/or takes actions based on detected malicious activity." Sourcefire at 34. At the time of the invention, however, exfiltrations were difficult to prevent precisely because they did not look like "malicious activity":

> A category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent. A first cause is that many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web, that often appear to an observer (e.g., a conventional cyber defense system) as ***normal network behavior***. A second cause is that typical

[1] As discussed above, a POSA also could not have used Sourcefire to construct packet-filtering rules with the claimed operator. *See* § VII.B.1, *supra*.

> network trust models, such as those used by network firewalls, ***interpret exfiltrations as trusted operations***.

'193 Patent at 1:24–34. Accordingly, Sourcefire manual, which instructs users to implement "intrusion rules" to detect "malicious activity," provides no instruction for how to deal with exfiltrations or motivation to block ***outgoing*** traffic that does not appear to be malicious.

63. The specific set of rules and operators recited in the independent claims of the '193 Patent, as a whole, establish a technique whereby a computing device inspects outgoing packets from a first network to determine whether they are destined for a particular second or third network and applies different operators depending on that determination. *See generally*, '193 Patent, Claims 1, 8, 18, and 19. The reason for this approach is that, because exfiltration attacks are often mediated by "popular network data transfer protocols," simply blocking every packet that utilizes a particular data transfer protocol would not allow users to freely surf the Internet:

> One or more administrators of the secured network may associate such an operator with one or more rules in a network security policy in order to enforce, via the PSG, a Web usage policy that may, for example, allow users to surf (e.g., GET) to one or more web sites attached to the Internet, but may prevent such user(s) from one or more of writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more web sites. For example, administrator(s) may utilize such functionality to prevent one or more exfiltrations (e.g., file transfers containing sensitive information, posting of login credentials (usernames and passwords), etc.) to network nodes (e.g., web sites) that they may not trust.

'193 Patent at 2:43–54. Similarly:

> Returning to the example described above, organization Z may own or operate network 108, and may have allocated network IP addresses 214.0.0.0/8 to network 108. ***Enterprise X may not have a business relationship with organization Z, and may therefore not consider network 108 to be trusted. While enterprise X could simply block all communications to networks that are owned or operated by organizations it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet***. Enterprise X's employees, therefore, could not freely surf the Web, which may restrict the employees' ability to conduct business on behalf of enterprise X. By enforcing sets of rules similar to rule 6 312 that may apply operators like or similar to HTTP-EXFIL, enterprise

> X may enable its employees to freely surf the web and conduct company business, but may prevent one or more cyber attacks (e.g., HTTP-mediated exfiltrations).

'193 Patent at 7:1–37. But Sourcefire fails to teach any approaches for preventing exfiltrations, fails to appreciate the problems known to plague prior attempts to deal with exfiltrations, and certainly does not suggest the solution explicitly recited in the claims of the '193 Patent.

64. I disagree with the Examiner's statement that a POSA understood that it would be important to identify such methods because of certain alleged "vulnerabilities with certain HTTP methods." *Id.* The Examiner cites Sourcefire's disclosure that "rule keywords could be used by the HTTP inspect preprocessor and rules engine to search for matched application-layer content... including the most common HTTP methods of GET, PUT, POST, and CONNECT and *pass* (allow), *alert* (and pass), or *drop* (block) packets based on the results of such searches." Office Action at 8. Respectfully, there is no evidence cited to support the Examiner's statement that there were known vulnerabilities with certain HTTP methods.

65. I presume that the Examiner's statement was based on Cisco's citation to RFC 2616. *See* Request at 60 (citing Ex. 1046, pg. 44). However, in this context "safe" only means that the HTTP GET command, by convention, does not allow any action on the server other than data retrieval. Ex. 2002 at 1 ("An HTTP method is **safe** if it doesn't alter the state of the server. In other words, a method is safe if it leads to a read-only operation."). "Safe" in this context does not mean that the HTTP command is actually safe. Ex. 1046, pg. 44 ("Naturally, it is not possible to ensure that the server does not generate side-effects as a result of performing a GET request; in fact, some dynamic resources consider that a feature."). Nor does this passage mean that there are "vulnerabilities" associated with other "unsafe" HTTP methods, like POST, PUT, and DELETE. *Id.* All "unsafe" means in this context is that these HTTP methods by design effect changes to the server receiving the command. For example, because a POST command entails a "write"

command, it is not "read-only," and is therefore "unsafe." Indeed, far from indicating that there are any "vulnerabilities" associated with certain HTTP commands, RFC 2616 illustrates that HTTP was ***designed*** to include read-only commands, such as GET and HEAD as well as non-read-only commands, such as POST, PUT, and DELETE. Thus, while RFC 2616 suggests making a user aware that they are using a non-read-only command, it certainly does not claim that there are any "vulnerabilities" associated with those commands such that packets associated with the command should be blocked. Ex. 1046, pg. 44.

66. Accordingly, there is no motivation for a POSA to have written a rule to block any of those HTTP methods, let alone explaining ***why*** a POSA would have (1) written a rule to block such HTTP methods for some network traffic and not other network traffic, (2) written the rule to prevent the HTTP method for ***outgoing*** traffic, and (3) written the rule to specify an operator that is configured to drop the packet rather than dropping the packet using the rule itself. Nor does Sourcefire or any other record evidence disclose or suggest any ***basis*** for determining which network traffic should be blocked and which should not for any particular HTTP method. Indeed, it ***could not have been*** obvious to block packets using a particular HTTP method given that the HTTP Method option "does not generate events." Sourcefire at 568.

67. I also disagree that the Examiner's reference to the FTP Bounce attack is evidence that a POSA would have written a rule to block the FTP Port command. Office Action, pg. 8. An FTP Bounce attack involves an attacker sending an FTP "PORT" command to an FTP server containing the network address and the port number of the machine and service being attacked. At this point, the original client can instruct the FTP server to send a file to the service being attacked. Such a file would contain commands relevant to the service being attacked (SMTP, NNTP, etc.)." Ex. 1040, pg. 2. Accordingly, the computer running the service being attacked does

not receive any packets associated with the "PORT" command that a security device can take action upon because it only receives commands "relevant to the service being attacked (SMTP, NNTP, etc.)." Ex. 1040, pg. 2.

68. Rather than block packets associated with FTP "PORT" command as suggested in the Office Action, POSAs knew of three techniques for thwarting Bounce attacks. *First*, it was known to ensure that FTP servers "not open data connections to TCP ports less than 1024" because those ports are associated with well-known services, making them easy to attack. Ex. 1040, pg. 2. *Second*, a POSA could implement "proper file protections" to prevent an attacker from uploading a file to an FTP server and later downloading it to the service being attacked. *Id.* *Third*, the FTP server could disable the "PORT" command entirely. *Id.* None of these options entail applying an operator that blocks packets associated with the FTP "PORT" command, let alone blocking such packets when they are destined for a one network but not another. Further still, the known techniques for thwarting a Bounce attack involved taking action on ***incoming*** requests to an FTP server, not ***outgoing*** requests emanating from a first network and destined for a second or third network. Thus, it was neither known nor obvious at the time of the invention to apply the claimed technique to outgoing packets (*i.e.* packets received from a first network).

69. I also disagree with the Examiner's contention that "[b]ecause security vulnerabilities associated with HTTPS data transfers using or proposing to use TLS 1.0, SSLv2, SSLv3 are widely known, a POSA would be motivated to write appropriate drop rules to identify and block Record Protocol packets that proposed using these particular less secure SSL and TLS types of data transfer from continuing toward their second network destination." Office Action at 9. As with the HTTP method example discussed above, this does not explain ***why*** a POSA would have (1) written a rule to block such types of data traffic for some network traffic and not other

network traffic, (2) written the rule to prevent the data transfer for ***outgoing*** traffic, or (3) written the rule to specify an operator that is configured to drop the packet rather than dropping the packet using the rule itself. In fact, at the time of the invention, it was known ***not to*** simply block traffic using an older TLS/SSL version because the newer protocol versions were not yet deployed:

> The BEAST attack is released to exploit predictable IVs in TLS 1.0. Even though this problem had been fixed in TLS 1.1 released in 2006 and TLS 1.2 in 2008, ***no one actually uses these newer protocol versions***. Browsers will take about 2 more years to deploy TLS 1.2 and servers many years longer. ***We have no choice*** but to rely on browser counter-measures in the meantime. BEAST is the first attack to show how rich browser functionality can be abused to attack cryptography from multiple vantage points. Many similar attacks will follow.

Ex. 1037 at 8 (emphasis added). The '193 Patent solved this problem and has the ability to block potentially vulnerable protocols like TLS1.0 for some network traffic but allowing it for other traffic. And as with the HTTP example discussed above, neither Sourcefire nor any other record evidence discloses or suggests any basis for determining which network traffic should be blocked and which should not for any given TLS/SSL protocol.

70. I also disagree with the Examiner's statement that a POSA could use Sourcefire to block RTP traffic in order "to enforce a security policy prohibiting employees' use of such applications" allegedly because "enterprise networks restrict employees use of high bandwidth applications like streaming media while also avoiding known vulnerabilities posed by such use." Office Action at 9–10. Just like the examples above, this explanation does not explain ***why*** a POSA would have (1) written a rule to block such RTP data transfers for some network traffic and not other network traffic, (2) written the rule to prevent the data transfer for ***outgoing*** traffic, or (3) written the rule to specify an operator that is configured to drop the packet rather than dropping the packet using the rule itself.

71. For at least the foregoing reasons, a POSA would have modified Sourcefire to reach the claims of the '193 Patent.

B. Objective Indicia of Nonb Demonstrate Nonobviousness of the Challenged Claims

1. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others

72. The '193 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to protect against "[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet)." '193 Patent at 1:24-47. Data exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer.

73. The claims of the '193 Patent recite techniques that address this long-felt but unresolved problem of data exfiltrations. The claims of the '193 Patent involve applying "packet-filtering rules" specifically crafted to prevent such exfiltrations. In particular, the claimed invention prevents malicious exfiltrations by (1) detecting communications between two identified resources (i.e., a "first network" and "a second network", as claimed), and (2) "applying" a "first operator" to "drop packets associated with the particular type of data transfer," as claimed. *See* '193 Patent, Claim 1. The claims of the '193 Patent are embodied in Centripetal's CleanINTERNET and RuleGATE products. Ex. 2029 (PTX-1215). The RuleGATE and CleanINTERNET products include the ability to counter these types of exfiltrations and also address insider threats.

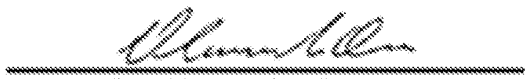
74. Centripetal's inventions unlocked the ability to derive network threat intelligence data (from multiple sources) and "operationalize" cyber threat intelligence (CTI) to proactively protect networks. The claimed invention leveraged CTI by applying operators ("applying… a first

operator… configured to drop packets associated with the particular type of data transfer") to only those packets meeting specified packet header criteria ("responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules") rather than blocking any and all traffic utilizing a particular type of data transfer. '193 Patent at 7:6-10.

75. The '193 Patent explains that such an HTTP-EXFIL operator achieves the solution of stopping exfiltrations. '193 Patent at 7:18-20. The '193 Patent explains that this two-stage process succeeds where traditional, overbroad techniques failed because it enables, for example, the operator to "thus allow a web browser to 'surf the web' (e.g., download web pages hosted by web servers), but [] prevent the web browser from writing files to a web server (e.g., using the PUT method), posting forms (e.g., forms that might contain login credentials, such as usernames or passwords) to a web server (e.g., using the POST method), or otherwise communicating with a web server (e.g., using any HTTP method except GET)." '193 Patent at 7:10-17.

76. Centripetal's solution to the exfiltration thus solved the long-standing problem of how to prevent exfiltrations that are mediated by popular data transfer protocols, demonstrating the nonobviousness of the '193 Patent Claims.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on January 25, 2020, in Atlanta, Georgia.



Dr. Alessandro Orso

APPENDIX A

Alessandro Orso

College of Computing
Georgia Institute of Technology
266 Ferst Drive, Atlanta, GA 30332–0765
+1 (404) 385–2066 (phone)
+1 (404) 385–2295 (fax)
orso@cc.gatech.edu
http://www.cc.gatech.edu/~orso

Main Areas of Expertise

Software engineering, with emphasis on software testing, program analysis, and software security.

Consulting and Advisory Appointments

(I was retained by the underlined parties.)

Ongoing Engagements

1. **Cisco Systems, Inc. v. Centripetal Networks, Inc.**
   - Type of matter: Patent infringement
   - Case No.: 2:18-cv-00094-HCM-LRL
   - Location of court: U.S.D.C. Eastern District of Virginia Norfolk Division
   - Law firm: Kramer Levin Naftalis & Frankel LLP
2. **Finjan, Inc. v. Rapid7, Inc. and Rapid7 LLC**
   - Type of matter: Patent infringement
   - Case No.: 1:18-cv-01519-MN
   - Location of court: U.S.D.C. Northern District of California
   - Law firm: Kramer Levin Naftalis & Frankel LLP
3. **Finjan, Inc. v. Check Point Software Technologies Inc. et al.**
   - Type of matter: Patent infringement
   - Case No.: 3:18-cv-02621-WHO
   - Location of court: U.S.D.C. Northern District of California
   - Law firm: Kramer Levin Naftalis & Frankel LLP
4. **CUPP Cybersecurity LLC, et al. v. Trend Micro, Inc., et al.**
   - Type of matter: Patent infringement
   - Case No.: 3:18-cv-01251-M
   - Location of court: U.S.D.C. Northern District of Texas
   - Law firm: Kramer Levin Naftalis & Frankel LLP
5. **CUPP Cybersecurity LLC, et al. v. Symantec Corp.**
   - Type of matter: Patent infringement
   - Case No.: 19-cv-00298
   - Location of court: U.S.D.C. Northern District of California
   - Law firm: Kramer Levin Naftalis & Frankel LLP

IPR2023-01353 Page 00047

6. **Symantec Corp. v. CUPP Cybersecurity LLC, et al.**
   Type of matter: Patent infringement
   Case No.: 5:18-cv-04720
   Location of court: U.S.D.C. Northern District of California
   Law firm: Kramer Levin Naftalis & Frankel LLP

7. **Finjan, Inc. v. Cisco Systems, Inc.**
   Type of matter: Patent infringement
   Case No.: 17-cv-0072-BLF-SVK
   Location of court: U.S.D.C. Northern District of California
   Law firm: Kramer Levin Naftalis & Frankel LLP

8. **Cisco Systems, Inc. v. Centripetal Networks, Inc.**
   Type of matter: IPR proceedings
   Law firm: Kramer Levin Naftalis & Frankel LLP

9. **Philips Medical Systems Nederland B.V., Philips North America LLC, and Philips Electronics India Ltd. v. TEC Holdings, Inc. f/k/a Transtate Equipment Company, Inc. and Transtate Equipment Company, Inc. f/k/a Transtate Holdings, Inc.**
   Type of matter: Litigation
   Case No.: 1:17-cv-02864-LMM
   Location of court: U.S.D.C. Northern District of Georgia
   Law firm: Reed Smith LLP

10. **Finjan, Inc. v. Juniper Networks, Inc.**
    Type of matter: patent infringement
    Case No.: 3:17-cv-05659-WHA
    Location of court: U.S.D.C. Northern District of California
    Law firm: Kramer Levin Naftalis & Frankel LLP

11. **Finjan, Inc. v. ESET, LLC**
    Type of matter: patent infringement
    Case No.: 3:17-cv-0183-CAB-BGS
    Location of court: U.S.D.C. Southern District of California
    Law firm: Kramer Levin Naftalis & Frankel LLP

Completed Engagements

1. **Typemock, LTD. v. Telerik, Inc.**
   Type of matter: Patent infringement
   Case No.: 1:17-cv-10274-RGS
   Location of court: U.S.D.C. District of Massachusetts Boston Division
   Law firm: Proskauer Rose LLP

2. **Centripetal Networks, Inc. v. Keysight Technologies, Inc. and Ixia**
   Type of matter: patent infringement
   Case No.: 2:17-cv-00383-HCM-LRL
   Location of court: U.S.D.C. Eastern District of Virginia Norfolk Division
   Law firm: Kramer Levin Naftalis & Frankel LLP

3. **Technology for Energy Corporation v. William H. Hardy, Power Measurements, LLC & Power Measurements, Inc.**

Type of matter:	Patent infringement
Case No.:	3:16-cv-00091
Location of court:	U.S.D.C. Eastern District of Tennessee at Knoxville
Law firm:	Bass, Berry & Sims PLC

4. **Finjan, Inc. v. Symantec Corp.**

Type of matter:	patent infringement
Case No.:	3:14-cv-02998-HSG
Location of court:	U.S.D.C. Northern District of California
Law firm:	Kramer Levin Naftalis & Frankel LLP

5. **Sony Corporation v. Pace plc; Pace Americas, LLC; other related companies**

Type of matter:	Patent infringement
Case No.:	1:15-cv-288-SLR-SRF
Location of court:	U.S.D.C. District of Delaware
Law firms:	Andrews Kurth Kenyon LLP Finnegan, Henderson, Farabow, Garrett & Dunner, LLP

6. **Novatel Wireless Solutions, Inc.; Nova Intellectual Solutions v. Franklin Wireless Corp.; ZTE Corp.; ZTE (USA)**

Type of matter:	Patent infringement
Case No.:	3:10-cv-02530-CAB-JMA
Location of court:	U.S.D.C. Southern District of California
Law firm:	Pillsbury LLP

7. **e-Watch, Inc.; e-Watch Corporation v. Apple, Inc.; Blackberry Corporation; Blackberry Limited; HTC America, Inc.; HTC Corporation; Huawei Device Co.; Ltd., Huawei Device USA, Inc.; Kyocera Communications, Inc.; Kyocera International, Inc.; LG Electronics, Inc.; LG Electronics USA, Inc.; LG Electronics MobileComm USA, Inc.; Nokia, Inc.; Microsoft Mobile Oy; Samsung Electronics Co., Ltd.; Samsung Electronics America, Inc.; Sharp Corporation; Sharp Electronics Corporation; Sony Mobile Communications (USA), Inc.; ZTE (USA)**

Type of matter:	Patent infringement
Case No.:	2:13-cv-1061 (LEAD CASE)
Location of court:	U.S.D.C. Eastern District of Texas Marshall Division
Law firm:	Pillsbury LLP

Alessandro Orso

College of Computing
Georgia Institute of Technology
266 Ferst Drive, Atlanta, GA 30332–0765
+1 (404) 385–2066 (phone)
+1 (404) 385–2295 (fax)
orso@cc.gatech.edu
http://www.cc.gatech.edu/~orso

IPR2023-01353 Page 00050

Contents

EDUCATIONAL BACKGROUND 3

EMPLOYMENT HISTORY 3

CURRENT FIELDS OF INTEREST 3

I. TEACHING 4
- A. Courses Taught . . . 4
- B. Continuing Education . . . 5
- C. Curriculum Development . . . 5
- D. Individual Student Guidance . . . 6
- E. Teaching Honors and Awards . . . 9
- F. Other Academic and Teaching Activities . . . 9

II. RESEARCH AND CREATIVE SCHOLARSHIP 11
- A. Theses . . . 11
- B. Published Journal Papers . . . 11
- C. Published Books and Parts of Books . . . 12
- D. Edited Proceedings . . . 12
- E. Conference Presentations (refereed) . . . 12
  - E.1 Invited Keynote Addresses . . . 12
  - E.2 Conference Presentations with Proceedings (refereed) . . . 13
  - E.3 Workshop Presentations with Proceedings (refereed) . . . 22
- F. Other . . . 23
  - F.1 Research Posters . . . 23
  - F.1 Submitted Journal Papers . . . 23
  - F.3 Software . . . 23
- G. Research Proposals and Grants (Principal Investigator) . . . 26
- H. Research Honors and Awards . . . 29

III. SERVICE 31
- A. Professional Activities . . . 31
  - A.1 Membership and Activities in Professional Societies . . . 31
  - A.2 Conference Committee Activities . . . 31
  - A.3 Conferences, Workshops, and External Courses . . . 34
- B. On-campus Georgia Tech Committees . . . 35
- C. Special Assignments at Georgia Tech . . . 36
- D. Member of Ph.D. Examining Committees . . . 36
- E. External Member of Masters Examining Committees . . . 38
- F. Research Project Reviewer . . . 38

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION 40
- A. Invited Conference Session Chairmanships . . . 40
- A. Patents . . . 40
- B. Editorial and Reviewer Work for Technical Journals and Publishers . . . 40

V. OTHER CONTRIBUTIONS 42
- A. Invited Talks . . . 42
- B. Participation in U.S.-Funded Projects . . . 44
- C. Participation in European-Union-Funded Projects . . . 44

IPR2023-01353 Page 00051

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	1999	Politecnico di Milano, Italy	Computer Science
M.S. and B.S.	1995	Politecnico di Milano, Italy	Electrical Engineering (I.T.)

EMPLOYMENT HISTORY

Title	Organization	Years
Professor	College of Computing Georgia Institute of Technology	08/2014–present
Professor and Associate School Chair	College of Computing Georgia Institute of Technology	01/2015–12/2017
Associate Professor	College of Computing Georgia Institute of Technology	08/2008–07/2014
Assistant Professor	College of Computing Georgia Institute of Technology	08/2004–07/2008
Research Scientist II	College of Computing Georgia Institute of Technology	01/2001–08/2004
Postdoctoral Fellow	College of Computing Georgia Institute of Technology	03/2000–01/2001
Visiting Researcher	EECS Department University of Illinois at Chicago	07/1999–10/1999
Research and Teaching Assistant	Department of Electronics and Informatics Politecnico di Milano, Italy	02/1996–07/1999

CURRENT FIELDS OF INTEREST

Software Engineering

My area of research is software engineering, with emphasis on software testing and program analysis. My interests include the development of techniques for improving software reliability, security, and trustworthiness, and the validation of such techniques on real-world systems.

IPR2023-01353 Page 00052

I. TEACHING

A. Courses Taught

Semester/Year	Course	Number of Students	Comments
Spring 2020	CS 6301 Advanced Topics in Software Engineering	56	
Spring 2020	CS 6300 Software Development Process	475	Offered as part of Georgia Tech's OMS-CS
Fall 2019	CS 6300 Software Development Process	461	Offered as part of Georgia Tech's OMS-CS
Summer 2019	CS 6300 Software Development Process	354	Offered as part of Georgia Tech's OMS-CS
Spring 2019	CS 6301 Advanced Topics in Software Engineering	56	
Spring 2019	CS 6300 Software Development Process	426	Offered as part of Georgia Tech's OMS-CS and OMS-CY
Fall 2018	CS 6300 Software Development Process	450	Offered as part of Georgia Tech's OMS-CS
Summer 2018	CS 6300 Software Development Process	200	Offered as part of Georgia Tech's OMS-CS
Spring 2018	CS 6301 Advanced Topics in Software Engineering	40	
Spring 2018	CS 6300 Software Development Process	356	Offered as part of Georgia Tech's OMS-CS
Fall 2017	CS 6300 Software Development Process	361	Offered as part of Georgia Tech's OMS-CS
Summer 2017	CS 6300 Software Development Process	200	Offered as part of Georgia Tech's OMS-CS
Spring 2017	CS 8803 Advanced Software Engineering	32	
Spring 2017	CS 6300 Software Development Process	362	Offered as part of Georgia Tech's OMS-CS
Fall 2016	CS 6300 Software Development Process	361	Offered as part of Georgia Tech's OMS-CS
Summer 2016	CS 6300 Software Development Process	200	Offered as part of Georgia Tech's OMS-CS
Spring 2016	CS 6300 Software Development Process	366	Offered as part of Georgia Tech's OMS-CS
Fall 2015	CS 8803 Advanced Software Engineering	43	
Fall 2015	CS 6300 Software Development Process	317	Offered as part of Georgia Tech's OMS-CS
Summer 2015	CS 6300 Software Development Process	219	Offered as part of Georgia Tech's OMS-CS
Spring 2015	CS 6300 Software Development Process	318	Offered as part of Georgia Tech's OMS-CS
Spring 2015	CS 6300 Software Development Process	16	Offered as part of Georgia Tech's GTPE
Fall 2014	CS 8803 Advanced Software Engineering	17	
Fall 2014	CS 6300 Software Development Process	236	Offered as part of Georgia Tech's OMS-CS

IPR2023-01353 Page 00053

Semester/Year	Course	Number of Students	Comments
Fall 2014	CS 6300 Software Development Process	46	Offered as part of Georgia Tech's GTPE
Summer 2014	CS 6300 Software Development Process	209	Offered as part of Georgia Tech's OMS-CS
Spring 2014	CS 6300 Software Development Process	49 (10 DL)	
Spring 2014	CS 6300 Software Development Process	132	Offered as part of Georgia Tech's OMS-CS
Fall 2012	CS 6300 Software Development Process	43 (6 DL)	
Fall 2011	Testing y Análisis de Software (in Castilian) (Escuela Regional en Tecnologías de la Información y Comunicaciones (ERTIC), Facultad Politécnica de la Universidad Nacional de Asunción (FP-UNA))	36	
Spring 2012	CS 3300 Introduction to Software Engineering	21	
Spring 2012	CS 6300 Software Development Process	43	
Spring 2011	Software Testing and Analysis (Ph.D. course at Università della Svizzera Italiana, Switzerland)	18	
Spring 2011	Software Testing and Analysis (Ph.D. course at Politecnico di Milano, Italy)	14	
Fall 2010	CS 6300 Software Development Process	40	
Fall 2009	CS 4001 Computing and Society	38	
Fall 2009	CS 6300 Software Development Process / CS 4320 Introduction to Software Processes	44	
Fall 2008	CS 3300 Introduction to Software Engineering	25	
Fall 2008	CS 4001 Computing and Society	28	
Summer 2008	CS 3300 Introduction to Software Engineering	13	
Summer 2008	CS 4001 Computing and Society	31	
Summer 2008	Testing y Análisis de Software (in Castilian) (summer school at the University of Buenos Aires, Argentina)	162	
Fall 2007	CS 3300 Introduction to Software Engineering	32	
Fall 2007	CS 6300 Software Development Process / CS 4320 Introduction to Software Processes	58	
Fall 2006	CS 3300 Introduction to Software Engineering	27	
Fall 2006	CS 8803 Software Testing and Analysis	9	Now a regular 6000-level class (CS 6340)
Fall 2005	CS 1322 Computer Science II	165	Sections A1, A2, and A3
Fall 2005	CS 8803 Software Testing and Analysis	25	Now a regular 6000-level class (CS 6340)
Spring 2005	CS 1322 Computer Science II	150	Breakout Sections
Spring 2003	CS 8803 Software Analysis and Testing	9	Co-taught

In addition, prepared and taught lab sections at Politecnico di Milano, Italy, between 1996 and 1999, for the following undergraduate classes: Software Engineering, Foundations of Computer Science I, Foundations of Computer Science II, and Information-Processing Systems. I also developed and taught, from 1997 to 2002, a course on software testing for companies targeted at test managers.

B. Continuing Education

None

C. Curriculum Development

IPR2023-01353 Page 00054

CS 6301 (Advanced Topics in Software Engineering): This is a graduate course in which students study the way software is developed, verified, and deployed in modern companies. Students will get exposed to and become familiar with new tools and technologies used in today's development organizations. The course will also cover cutting edge research techniques to develop better quality software and include guest lecturers from industry that can provide a view from the trenches on what it means to develop software today. Finally, the course involves a semester long project in which teams of students develop the different modules (i.e., web client, mobile client, server, and backend database) of a multi-tier application. By the end of the semester, the students are able to automatically build, deploy, and integrate their modules.

OMS CS 6300 (Software Development Process): This is the OMS version of my CS 6300 on-campus class. Although this class covers the same topics that I cover in my regular CS 6300 course, I had to develop the class from scratch to make is suitable for online delivery. More specifically, the class is based on a "whiteboard animation" paradigm, in which most of the content is presented by writing and sketching on a virtual whiteboard. Moreover, the class content is presented in short segments followed by frequent quizzes, which required me to rethink the whole structure of the course and add a considerable amount of new material. Finally, I had to find creative solutions for presenting topics that require a high level of (synchronous) interaction with the students. I normally teach my lectures on software design, for instance, by having some students design an actual system at the whiteboard and commenting on it as they go, which is clearly not possible in an online, asynchronous setting. What I did was therefore to record, with the help of a colleague, a 45-minute video "skit". In the video, I pretend to help a librarian friend to design an IT system for his library, and my friend makes all the typical mistakes that students tend to make in class. By watching the video, the students can get a similar experience to the one they would get in class doing the exercise themselves.

CS 6340 (Advanced Topics in Software Analysis and Testing): This is a graduate course in which students are exposed to various topics in static and dynamic program analysis and in software testing. The material presented ranges from fundamental principles to the most advanced research topics. Half way through the semester, students pick a project based on one of the topics presented and work on the project until the end of the semester. Projects can be either theoretical or applied and provide students with invaluable research and engineering experience. The course ends with a mini-conference in which students present papers that describe the results of their projects. In 2003, I have co-developed the part of the course on dynamic analysis and developed the part of the course on testing. In 2005, I have revamped the whole class, including updating the topics covered, adding new material, and preparing an extensive set of supporting slides for the course. I have further updated the course with new material in 2006. I presented the course to the CoC Graduate Committee and to the Institute Graduate Committee, which approved it in Summer 2007.

CS 3300 (Introduction to Software Engineering) and CS 6300 (Software Development Process): In 2007 I started teaching CS 3300 and 6300 on a regular basis, and shortly thereafter I took ownership of both classes. I considerably revamped both courses by making a number of changes to their syllabi. First, I removed obsolete material and added new material. For example, the classes now cover test-driven and agile development, which are practices widely used in industry (e.g., at Google) and which were totally neglected in the earlier syllabi. Second, I added a whole new part on novel technologies, in which students are exposed to widely used technologies, such as cloud computing platforms, web application frameworks, configuration management tools, and mobile development environments. (A number of students gave me feedback on how useful they found this part to be when they went for interviews or, more generally, in their job.) Finally, I modified the class projects to make them more stimulating and practically useful. For example, I now have the instructor and the TAs acting as real customers, so that students can better learn what it means to elicit requirements through interaction with actual project stakeholders. For another example, projects now involve the new technologies that we study in class. Also in this case, many students reported that they enjoyed the projects and felt like they learned a good deal by doing them.

D. Individual Student Guidance

1. Ph.D. Students Graduated

Mattia Fazzini: Graduated in Summer 2019, Assistant Professor in the Department of Computer Science & Engineering at University of Minnesota

Qianqian Wang: Graduated in Summer 2019, Software Engineer at Manhattan Associates

IPR2023-01353 Page 00055

Wei Jin: Graduated in Summer 2015, Software Engineer at Google

Shauvik Roy Choudhary: Graduated in Summer 2015, CEO and Co-Founder of MoQuality

James Clause: Graduated in Spring 2011, Associate Professor in the Computer and Information Sciences Department at the University of Delaware, US

William Halfond: Graduated in Spring 2010, Associate Professor with tenure in the Computer Science Department at the University of Southern California, US

Taweesup Apiwattanapong: Graduated in Fall 2007 (co–advised), Researcher at the National Electronics and Computer Technology Center (NECTEC), Thailand

2. Research Scientists and Tech Temp Supervised

Mattia Fazzini: Fall 2012, Spring 2013

Matteo Miraz: Spring 2012

James Clause: Summer 2005

Arjan Seesing: Summer 2005, Fall 2005

3. Ph.D. Students Supervised

Robin Guzniczak: Fall 2018–Present

Ravi Mangal: Spring 2017–Present

Loren Klingman: Spring 2017–Fall 2018

Richard Rutledge: Fall 2016–Present

Farnaz Behrang: Fall 2014–Present

Xiangyu Li: Fall 2013–Present

Juyuan Yang: Spring 2013–Fall 2014

Ikpeme Erete: Fall 2009–Fall 2010

Shauvik Roy Choudhary: Fall 2009–Summer 2015

Dan Zhao: Fall 2009–Fall 2011 (visiting from Hunan University, China)

Saswat Anand: Fall 2004–Fall 2010 (co–advised)

Wei Jin: Fall 2008–Summer 2015

Sarah Clark: Summer 2008–Fall 2008

Hwa-You Hsu: Fall 2006–Fall 2009

James Clause: Summer 2005–Spring 2011

William Halfond: Fall 2004–Fall 2009

Taweesup Apiwattanapong: Spring 2002–Fall 2007 (co–advised)

Yi Zhang: Fall 2003–Fall 2004 (co–advised)

Nanjuan Shi: Fall 2003–Spring 2004 (co–advised)

4. M.S. Projects and Special Problems Students

Harshit Sharma: Spring 2016

Jie Lu: Fall 2013–Fall 2014

Juyuan Yang: Spring 2014–Fall 2014

IPR2023-01353 Page 00056

Niranjanaa Ragupathy: Spring 2013

Noel Go: Spring 2013

Shunmugam Murugan: Fall 2012

Lokesh Balakrishnan: Fall 2012

Jeremy Duvall: Fall 2010–Fall 2013

Romain Jobredeaux: Fall 2010

Hersh Iyer: Spring 2010, Fall 2010

Kunal Thakar: Spring 2009

Satvir Bhatia: Spring 2008, Fall 2008

Mijung Kim: Fall 2008

Pranav Kuber: Fall 2008

Sarang Ozarde: Fall 2008

Shauvik Roy Choudhary: Spring 2008, Fall 2008, Spring 2009

Kunal Thakar: Spring 2008

Farbana Aleen: Fall 2007

Yimin Zhang: Fall 2007

Jeremy Viegas: Spring 2006

Shrinivas Balkrishna Joshi: Fall 2004, Spring 2005, Fall 2005, Spring 2006

Bryan Kennedy: Fall 2003, Spring 2004

Manas Tungare: Fall 2002, Spring 2003

5. Undergraduate Special Problems Students

Shaowei Zhu: Spring 2016

Tommaso Pieroncini: Spring 2016

Jing Hong: Fall 2015

Zixiang Zhu: Spring 2015–Spring 2016

Brian Edmonds: Spring 2014

Crystal Lo: Spring 2014

Nirav Bathia: Spring 2013, Fal 2013

Michael Sambol: Spring 2013

Jorge Villasmil: Fall 2009

Husayn Versee: Spring 2009, Fall 2009, Spring 2010, Fall 2010

Petar Tsankov: Spring 2009, Fall 2009

Quinn Cone: Spring 2009

Jonathan Loesch: Spring 2009

Thomas Smith: Spring 2009

Stephan Prockow: Fall 2007, Spring 2008, Spring 2009
(Supported by a President's Undergraduate Research Award in Spring 2008)

William Cray: Fall 2007, Spring 2008
(Supported by a President's Undergraduate Research Award in Spring 2008)

IPR2023-01353 Page 00057

Conroy Whitney: Fall 2007

Matthew Wood: Fall 2006, Spring 2007
(Supported by a President's Undergraduate Research Award in Spring 2007 and winner of the 2007 UROC Research Symposium)

Matthew Ordonez: Fall 2004, Spring 2005, Summer 2005
(Supported by a President's Undergraduate Research Award in Spring 2005)

Carlo Tambuatco: Spring 2005

Anil Jagdish Chawla: Spring 2003, Fall 2003, Spring 2004

Mahesh Balakrishnan: Fall 2002, Spring 2003
(Supported by a President's Undergraduate Research Award in Fall 2002)

Anup Rao: Spring 2002

Rebecca Hutchinson: Summer 2001 (co-advised)
(CRA-W Distributed Mentor Project)

Kathleen Repine: Summer 2001 (co-advised)
(CRA-W Distributed Mentor Project)

E. Teaching Honors and Awards

1. Hesburgh Award Teaching Fellow, Georgia Tech, 2017
2. Class of 1940 Course Survey Teaching Effectiveness Award, Georgia Tech, 2015.
3. Most Influential Faculty Member, selected by Anil Jagdish Chawla, Dean's Honor Graduate, 2004.

F. Other Academic and Teaching Activities

1. Attended the invitational Dagstuhl seminar on Program Repair. Dagstuhl, Germany, January 2017.
2. Attended several IFIP WG 2.4 Meetings (Stellenbosch, South Africa; Victoria, Canada; Vadstena, Sweden).
3. Attended the invitational Workshop on the Future of Debugging. Mysore, India, February-March 2012.
4. Attended the invitational Dagstuhl seminar on Fault Prediction, Localization, and Repair. Dagstuhl, Germany, February 2013.
5. Panelist at the IEEE International Conference on Software Testing for a panel on the future of software testing, March 2011.
6. Attended the invitational Dagstuhl seminar on Self-Repairing Programs. Dagstuhl, Germany, February 2011.
7. Attended the invitational Microsoft Think Tank meeting at Microsoft Research, Bellevue, WA, November 2009.
8. Attended, as a member of the Independent Evaluation Team, the site visit for the DARPA Application Community program, Phase II. Boston, MA, September 2009.
9. Visited IBM Research, New Delhi, India, August 2009.
10. Attended the invitational Dagstuhl seminar on Web Application Security. Dagstuhl, Germany, March 2009.
11. Attended, as a member of the Independent Evaluation Team, the site visit for the DARPA Application Community program, Phase II. Boston, MA, March 2009.

IPR2023-01353 Page 00058

12. Attended, as a member of the Independent Evaluation Team, the Kick-off Meeting for the DARPA Application Community program, Phase II. Boston, MA, December 2008.

13. Attended, as a member of the Independent Evaluation Team, the Red Team Exercises for the DARPA Application Community program. Menlo Park, CA and Boston, MA, February 2008.

14. Panelist at the ASE International Workshop on Living with Uncertainties (IWLU 2007).

15. Attended, as a member of the Independent Evaluation Team, the site visits for the DARPA Application Community program. Boston, MA and Menlo Park, CA, March 2007.

16. Attended, as a member of the Independent Evaluation Team, the PI meeting of the DARPA Application Community program. Arlington, VA, January 2007.

17. Attended, as a member of the Independent Evaluation Team, the kick-off meeting of the DARPA Application Community program. Arlington, VA, July 2006.

18. Attended DHS-ARPA Cyber Security PI meeting. Washington, D.C., August 2006.

19. Attended, as a member of the Independent Evaluation Team, the kick-off meeting of the DARPA Application Community program. Arlington, VA, July 2006.

20. Attended the 2nd DARPA-sponsored Information Science and Technology (ISAT) invitational study on "Trustable Deployed Adaptive Systems." SRI International, Menlo Park, CA, March 2006.

21. Attended the 1st DARPA-sponsored Information Science and Technology (ISAT) invitational study on "Trustable Deployed Adaptive Systems." Carnegie Mellon University, Pittsburgh, PA, February 2006.

22. Attended DHS-ARPA Cyber Security PI meeting. SRI International, Menlo Park, CA, January 2006.

23. Volunteered for the CoCeasar Palace initiative at Georgia Tech. Spring 2006.

24. Attended the ARO-HS ARPA invitational Malware Detection Workshop. SRI International, Arlington, VA, August 2005.

25. Attended DHS-ARPA Cyber Security PI meeting. SRI International, Arlington, VA, August 2005.

26. Session chair and session organizer for Georgia Tech's Technology Symposium. February 2005.

27. Given a presentation about opportunities in CS for high-school minority students in the context of Cool Computing@GT's Diversity Fair. February 2005.

28. Volunteered for the CoCeasar Palace initiative at Georgia Tech. Spring 2005.

29. Attended the DARPA invitational Application Communities Workshop. Schafer Corporation, Arlington, VA, October 2004.

30. Attended the 2004 NSF Information Technology Research Grantee Meeting (ITR PI Meeting). Crystal City, VA, June 2004.

31. Attended the New Software Engineering Faculty Symposium (NSEFS). Portland, OR, May 2003.

32. Member of the jury for the UROC (Undergraduate Research Opportunities in Computing) contest, to award the best undergraduate research project, 2002–2004.

33. Instructor for bi-annual tutorial on software testing and analysis (which I developed) for industrial developers and quality-assurance managers, 1996–2002.

IPR2023-01353 Page 00059

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Theses

Ph.D. Thesis

Integration Testing of Object-Oriented Software
Date Completed: February 1999
Advisor: Mauro Pezzè
Tutor: Carlo Ghezzi
University: Politecnico di Milano, Italy

Master's Thesis

Customizable Notations for Kernel Formalisms
Date Completed: May 1995
Advisors: Mauro Pezzè
University: Politecnico di Milano, Italy

B. Published Journal Papers (refereed)

1. W. Jin and A. Orso. Automated Support for Reproducing and Debugging Field Failures. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2015, Volume 24, Issue 4, pages 1–35.

2. D. Zhao, S. Roy Choudhary, and A. Orso. Developing Analysis and Testing Plug-ins for Modern IDEs: An Experience Report. *Software: Practice and Experience*, 2013, Volume 43, Issue 4, pages 465–478.

3. I. Doudalis, J. Clause, G. Venkataramani, M. Prvulovic, and A. Orso. Effective and Efficient Memory Protection Using Dynamic Tainting. *IEEE Transactions on Computers*, 2012, Volume 61, Number 1, pages 87–100.

4. W. Halfond, S. Roy Choudhary, and A. Orso. Improving Penetration Testing through Static and Dynamic Analysis. *Journal of Software Testing, Verification and Reliability (JSTVR)*, 2011, Volume 21, Number 3, pages 195–214.

5. M. Last, G. Luta, A. Orso, A. Porter and S. Young, Pooled ANOVA, *Computational Statistics & Data Analysis*, 2008, Volume 52, Issue 12, pages 5215–5228.

6. W. Halfond, A. Orso, and P. Manolios. WASP: Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation. *IEEE Transactions on Software Engineering (TSE)*, 2008, Volume 34, Number 1, pages 65–81.

7. M. Haran, A. Karr, M. Last, A. Orso, A. Porter, A. Sanil, and S. Fouché. Techniques for Classifying Executions of Deployed Software to Support Software Engineering Tasks. *IEEE Transactions on Software Engineering (TSE)*, 2007, Volume 33, Number 5, pages 287–304.

8. A. Orso, H. Do, G. Rothermel, M. J. Harrold and D. Rosenblum Using Component Metadata to Regression Test Component–based Software. *Journal of Software Testing, Verification and Reliability (JSTVR)*, 2007, Volume 17, Number 2, pages 61–94.

9. T. Apiwattanapong, A. Orso and M. J. Harrold JDiff: A Differencing Technique and Tool for Object–Oriented Programs. *Automated Software Engineering: An International Journal*, 2007, Volume 14, Number 1, pages 3–36.

10. A. Orso, S. Sinha, and M.J. Harrold. Classifying Data Dependence in the Presence of Pointers for Program Comprehension, Testing, and Debugging. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 2004, Volume 13, Number 2, pages 199–239.

11. J. Jones, A. Orso, and M.J. Harrold. Gammatella: Visualizing Program-Execution Data for Deployed Software. *Information Visualization*, 2004, Volume 3, Number 3, pages 173–188.

IPR2023-01353 Page 00060

C. Published Books and Parts of Books

1. A. Orso. Don't Forget the Developers! (and Be Careful with Your Assumptions). *Perspectives on Data Science for Software Engineering (Book Chapter)*, T. Menzies, L. Williams, and T. Zimmermann (Eds.)
(invited paper)

2. N. Medvidovic and A. Orso. Software Analytics Under the Lamppost (or What Star Trek Teaches Us About the Importance of Asking the Right Questions). *Perspectives on Data Science for Software Engineering (Book Chapter)*, T. Menzies, L. Williams, and T. Zimmermann (Eds.)
(invited paper)

3. A. Orso. SQL Injection Attacks. *Encyclopedia of Cryptography and Security,* Springer Science and Business Media LLC, 2010.
(invited paper)

4. W. Halfond and A. Orso. Detection and Prevention of SQL Injection Attacks. *Malware Detection*, Series: Advances in Information Security, Springer, Vol. 27, M. Christodorescu, S. Jha, D. Maughan, D. Song, C. Wang (Eds.), 2007, XII.
(invited paper)

D. Edited Proceedings

1. Proceedings of the ACM-SIGSOFT and IEEE International Conference on Software Engineering (ICSE 2017), Buenos Aires, Argentina, May 2017.

2. Proceedings of the ACM-SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2014), Hong Kong, China, November 2014.

3. Proceedings of the IEEE International Conference on Software Testing, Verification and Validation (ICST 2013), Luxembourg, April 2013.

4. Proceedings of the ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2010). Trento, Italy, July 2010.

5. Proceedings of the Fifth ICSE *Workshop on Dynamic Analysis (WODA 2007).* Minneapolis, MN, USA, May 2007.

6. Proceedings of the Fifth ICSE *Workshop on Dynamic Analysis (WODA 2007).* Minneapolis, MN, USA, May 2007.

7. Proceedings of the Second ICSE Workshop on *Remote Analysis and Measurement of Software Systems (RAMSS 04).* Edinburgh, Scotland, May 2004.

E. Conference Presentations

E.1. Invited Keynote Addresses

1. Software Debugging: Past, Present, and Future. Distinguished lecture in the Department of Computer Science at Virginia Tech, November 2018.

2. Invited talk for the ISSTA 2017 Impact Paper Award, Santa Barbara, CA, USA, July 2017.

3. Software Debugging: Past, Present, and Future. Distinguished lecture in the Special Lecture Series of the Computing Colloquium Seminars, at Imperial College London, UK, June 2017.

IPR2023-01353 Page 00061

4. Software Debugging: Past, Present, and Future. Invited lecture at Politecnico di Milano, Italy, June 2017.
5. Software Debugging: Past, Present, and Future. Distinguished lecture in the ISR Distinguished Speaker Series, University of California, Irvine, March 2017.
6. Software Debugging: Past, Present, and Future. Invited lecture at the Department of Computing at Imperial College London, UK, December 2016.
7. Automated Debugging: Are We There Yet? Distinguished lecture in the Distinguished Lectures Series in Cybersecurity at TU Darmstadt, April 2106.
8. Automated Debugging: Are We There Yet? Invited talk at the CHOOSE forum (yearly meeting of the Swiss Group for Original and Outside-the-box Software Engineering), October 2015.
9. Automated Support for Reproducing and Debugging Field Failures. Distinguished Lecturer at the College of Information and Computer Sciences of UMass Amherst, January 2015.
10. "Automated Debugging: Are We There Yet?". Distinguished Lecture at the University of Luxembourg, Luxembourg, June 2014.
11. Automated Debugging: Are We There Yet? Opening talk at the Dagstuhl Seminar on Fault Prediction, Localization, and Repair, February 2013.
12. In-house Debugging of Field Failures. Keynote talk at the ISSTA Workshop on Dynamic Analysis (WODA 2012), Minneapolis, MN, USA July 2012.
13. Automated Debugging: Are We There Yet? Keynote talk at the ICST Workshop on Testing and Debugging (TeBug 2011), Berlin, Germany, March 2011.
14. Repository Mining and Program Analysis & Testing: Better Together? Keynote talk at the Mining Software Archives workshop, Ascona, Switzerland, March 2010.
15. Improving Application Security through Program Analysis. Invited keynote at the 5th ICSE Workshop on Software Engineering for Secure Systems (SESS 2009), Vancouver, Canada, May 2009.
16. Using Program Analysis to Improve Web Application Security and Reliability. Invited keynote at the ISSTA Workshop on Testing, Analysis and Verification of Web Software (TAV-WEB 2008), Seattle, WA, USA, July 2008.

E.2. Conference Presentations with Proceedings (refereed)

(Note: ASE, ESEC/FSE, FSE, ICSE, ICST, and ISSTA are all top-tier conferences.)

1. Q. Xin, M. Kim, Q. Zhang, and A. Orso Program Debloating via Stochastic Optimization. *Proceedings of the 42nd IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2020) – NIER Track*, Seoul, South Korea, May 2020.
   (29 of the 93 submissions accepted – 31%)
2. F. Behrang and A. Orso. AppTestMigrator: A Tool for Automated Test Migration for Android Apps. *Proceedings of the 42nd IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2013) – Demo Track*, Seoul, South Korea, May 2020.
   (25 of 75 submissions accepted – 33%)
3. R. Rutledge and A. Orso. PG-KLEE: Trading Soundness for Coverage. *Proceedings of the 42nd IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2013) – Demo Track*, Seoul, South Korea, May 2020.
   (25 of 75 submissions accepted – 33%)

4. X. Li and A. Orso. More Accurate Dynamic Slicing for Better Supporting Software Debugging. *Proceedings of the 13th IEEE International Conference on Software Testing, Verification and Validation (ICST 2020)*
(27 of the 114 submissions accepted – 24%)

5. F. Behrang and A. Orso. Test Migration Between Mobile Apps with Similar Functionality. *Proceedings of the 34th IEEE/ACM International Conference on Automated Software Engineering (ASE 2019)*, San Diego, CA, USA, November 2019.
(91 of the 445 submissions accepted – 20%)

6. M. Fazzini, Q. Xin, and A. Orso. Automated API-Usage Update for Android Apps. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2019)*, Beijing, China, July 2019.
(29 of the 145 submissions accepted – 20%)

7. R. Rutledge, S. Park, H. Khan, A. Orso, M. Prvulovic and A. Zajic. Zero-Overhead Path Prediction with Progressive Symbolic Execution. *Proceedings of the 41st IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2019)*, Montreal, Canada, May 2019.
(109 of the 529 submissions accepted – 21%)

8. Q. Wang and A. Orso. [Poster] Mimicking User Behavior to Improve In-House Test Suites. *Poster track of the 41st IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE-Poster 2019)*, Montreal, Canada, May 2019.
(Invited)

9. R. Mangal, A. Nori, and A. Orso. Checking Probabilistic Properties of Neural Networks via Symbolic Methods and Sampling. *Proceedings of the First ICSE Workshop on Testing for Deep Learning and Deep Learning for Testing (DeepTest 2019)*, Montreal, Canada, May 2019.

10. R. Mangal, A. Nori, A. Orso. Robustness of Neural Networks: A Probabilistic and Practical Perspective. *Proceedings of the 41st IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2019) – NIER Track*, Montreal, Canada, May 2019.
(25 of the 92 submissions accepted – 27%)

11. X. Li, M. d'Amorim, and A. Orso. Intent-Preserving Test Repair. *Proceedings of the 12th IEEE International Conference on Software Testing, Verification and Validation (ICST 2019)*
(31 of the 110 submissions accepted – 28%)

12. Y. Ji, S. Lee, M. Fazzini, J. Allen, E. Downing, T. Kim, A. Orso, and W. Lee. Enabling Refinable Cross-Host Attack Investigation with Efficient Data Flow Tagging and Tracking. *Proceedings of the 27th USENIX Security Symposium (USENIX Security 2018)*, Baltimore, MD, USA, August 2018.
(100 of the 524 submissions accepted – 19%)

13. M. Fazzini, M. Prammer, M. d'Amorim, and A. Orso. Automatically Translating Bug Reports into Test Cases for Mobile Apps. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2018)*, Amsterdam, Netherlands, July 2018.
(31 of the 130 submissions accepted – 24%)

14. F. Behrang and A. Orso. Test Migration for Efficient Large-Scale Assessment of Mobile App Coding Assignments. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2018)*, Amsterdam, Netherlands, July 2018.
(31 of the 130 submissions accepted – 24%)

15. F. Behrang, S. Reiss and A. Orso. GUIFetch: Supporting App Design and Development through GUI Search. *Proceedings of the 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems (MobileSoft 2018)*, Gothenburg, Sweden, May 2018. (This paper was presented with an **ACM-SIGSOFT Distinguished Paper Award**.)

16. F. Behrang and A. Orso. [Poster] Automated Test Migration for Mobile Apps. *Poster track of the 40th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE-Poster 2018).* , Gothenburg, Sweden, June 2018.
(Invited)

17. X. Li, S. Zhu, M. d'Amorim, and A. Orso. Enlightened Debugging. *Proceedings of the 40th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2018)*, Gothenburg, Sweden, June 2018.
(105 of the 502 submissions accepted – 21%)

18. Y. Ji, S. Lee, E. Downing, W. Wang, M. Fazzini, T. Kim, A. Orso, and W. Lee. RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking. *Proceedings of the ACM-SIGSAC Conference on Computer and Communications Security (CCS 2017)*
(151 of the 836 submissions accepted – 18%)

19. M. Fazzini and A. Orso. Automated Cross-Platform Inconsistency Detection for Mobile Apps. *Proceedings of the 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE 2017)*
(88 of the 314 submissions accepted – 28%)

20. M. Fazzini, E. Noronha de A. Freitas, S. Roy Choudhary, and A. Orso. Barista: A Technique for Recording, Encoding, and Running Platform Independent Android Tests. *Proceedings of the 10th IEEE International Conference on Software Testing, Verification and Validation (ICST 2017)*
(36 of the 135 submissions accepted – 27%)

21. Behavioral Execution Comparison: Are Tests Representative of Field Behavior? Q. Wang, Y. Brun, and A. Orso. *Proceedings of the 10th IEEE International Conference on Software Testing, Verification and Validation (ICST 2017)*
(36 of the 135 submissions accepted – 27%)

22. W. Jin and A. Orso. Improving Efficiency and Accuracy of Formula-based Debugging. *Proceedings of the 12th Haifa Verification Conference (HVC 2016)*

23. X. Li, M. d'Amorim, and A. Orso. Iterative User-Driven Fault Localization. *Proceedings of the 12th Haifa Verification Conference (HVC 2016)*

24. R. Callan, F. Behrang, M. Prvulovic, A. Zajic, and A. Orso. Zero-Overhead Profiling via EM Emanations. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2016)*
(37 of the 147 submissions accepted – 25%)

25. S. Roy Choudhary, A. Gorla, and A. Orso. Automated Test Input Generation for Android: Are We There Yet?. *Proceedings of the 29th IEEE/ACM International Conference on Automated Software Engineering (ASE 2015)*, Lincoln, NE, USA, 2015.
(60 of the 289 submissions accepted – 21%)

26. F. Behrang, M. Cohen, and A. Orso. Users Beware: Preference Inconsistencies Ahead. *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2015)*, Bergamo, Italy, 2015. (This paper was presented with an **ACM-SIGSOFT Distinguished Paper Award.**)
(74 of the 291 submissions accepted – 25%)

27. Q. Wang, C. Pamin, and A. Orso . An In-Depth Study of IR-Based Fault Localization Techniques. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2015)*, Baltimore, MD, USA, 2015.
(33 of the 119 submissions accepted – 28%)

28. M. Fazzini, P. Saxena, and A. Orso. AutoCSP: Automatically Retrofitting CSP to Web Applications. *Proceedings of the 37th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2015)*, Florence, Italy, May 2015.
(84 of the 452 submissions accepted – 19%)

29. D. Zuddas, W. Jin, F. Pastore, L. Mariani, and A. Orso. Mimic: Locating and Understanding Bugs by Analyzing Mimicked Executions. *Proceedings of the 29th IEEE/ACM International Conference on Automated Software Engineering (ASE 2014)*, Västerås, Sweden, September 2014.

30. A. Orso and G. Rothermel. Software Testing: A Research Travelogue (2000-2014). *Proceedings of the 36th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2014) – FOSE Track*, Hyderabad, India, June 2014.
(invited paper)

31. S. Roy Choudhary, M. Prasad, and A. Orso. Cross-Platform Feature Matching for Web Applications. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2014)*, San Jose, CA, USA, July 2014.
(36 of the 128 submissions accepted – 28%)

32. S. Roy Choudhary, M. Prasad, and A. Orso. X-PERT: A Web Application Testing Tool for Cross-Browser Inconsistency Detection. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2014) – Tool Demonstraction track*, San Jose, CA, USA, July 2014.
(acceptance rate unknown)

33. S. Kaleeswaran, V. Tulsian, A. Kanade, and A. Orso. MintHint: Automated Synthesis of Repair Hints. *Proceedings of the 36th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2014)*, Hyderabad, India, June 2014.
(99 of the 495 submissions accepted – 20%)

34. F. Meshesha Kifetew, W. Jin, R. Tiella, A. Orso, and P. Tonella. Reproducing Field Failures for Programs with Complex Grammar Based Input. *Proceedings of the 7th IEEE International Conference on Software Testing, Verification and Validation (ICST 2014)*, Cleveland, OH, USA, April 2014.
(40 of the 131 submissions accepted – 28%)

35. F. Meshesha Kifetew, W. Jin, R. Tiella, A. Orso, and P. Tonella. SBFR: A Search Based Approach for Reproducing Failures of Programs with Grammar Based Input. `Proceedings of the 28th IEEE/ACM International Conference on Automated Software Engineering (ASE 2013)` [short paper], Palo Alto, CA, USA, November 2013.
(74 of the 317 submissions accepted – 23%)

36. W. Jin and A. Orso. F^3: Fault localization for Field Failures. `Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2013)`, Lugano, Switzerland, July 2013.
(32 of the 124 submissions accepted – 25.8%)

37. S. Roy Choudhary, M. Prasad, and A. Orso. X-PERT: Accurate Identification of Cross-Browser Issues in Web Applications. *Proceedings of the 35th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2013)*, San Francisco, CA, USA, May 2013.
(85 of the 461 submissions accepted – 18%)

38. L. Sales Pinto, S. Sinha, and A. Orso. TestEvol: A Tool for Analyzing Test-Suite Evolution. *Proceedings of the 35th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2013) – Formal research demonstration*, San Francisco, CA, USA, May 2013.
(16 of the 52 submissions accepted – 30%)

39. L. Sales Pinto, S. Sinha, and A. Orso. Understanding Myths and Realities of Test-suite Evolution. *Proceedings of the ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2012)*, Research Triangle Park, NC, USA, November 2012.
(35 of the 196 submissions accepted – 18%)

40. M. Alkhalaf, T. Bultan, S. Roy Choudhary, M. Fazzini, A. Orso and C. Kruegel. ViewPoints: Differential String Analysis for Discovering Client and Server-Side Input Validation Inconsistencies. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2012)*, Minneapolis, MN, USA, July 2012.
(31 of the 108 submissions accepted – 29%)

41. J. Rößler, G. Fraser, A. Zeller and A. Orso, Isolating Failure Causes through Test Case Generation. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2012)*, Minneapolis, MN, USA, July 2012.
(31 of the 108 submissions accepted – 29%)

42. M. Kim, J. Cobb, M.J. Harrold, T. Kurc, A. Orso, J. Saltz, A. Post, K. Malhotra and S. Navathe. Efficient Regression Testing of Ontology-Driven Systems. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2012)*, Minneapolis, MN, USA, July 2012.
(31 of the 108 submissions accepted – 29%)

43. W. Jin and A. Orso. BugRedux: Reproducing Field Failures for In-house Debugging. *Proceedings of the 34th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2012)*, Zurich, Switzerland, June 2012.
(87 of the 408 submissions accepted – 21%)

44. S. Roy Choudhary, M. Prasad, and A. Orso. CrossCheck: Combining Crawling and Differencing to Better Detect Cross-browser Incompatibilities in Web Applications. *Proceedings of the 5th IEEE International Conference on Software Testing, Verification and Validation (ICST 2012)*, Montreal, Canada, April 2012.
(39 of the 145 submissions accepted – 27%)

45. W. Halfond, S. Roy Choudhary, and A. Orso. Improving Penetration Testing through Static and Dynamic Analysis. *Journal of Software Testing, Verification and Reliability (JSTVR)*, 2011, Volume 21, Issue 3, pages 195–214.

46. C. Parnin, A. Orso. Are Automated Debugging Techniques Actually Helping Programmers? *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2011)*, Toronto, Canada, July 2010. (This paper was presented with an **Haifa Verification Conference 2013 Award for the most significant contribution to verification in the past 5 years**.)
(34 of the 121 submissions accepted – 28%)

47. M. Kim, T. Kurc, A. Orso, J. Cobb, M.J. Harrold, A. Post, A. Sharma, and J. Saltz. An Informatics Framework for Testing Data Integrity and Correctness of Federated Biomedical Databases. *Proceedings of the 2011 AMIA Summit on Clinical Research Informatics (CRI 2011)*, San Francisco, CA, USA, March 2011.

48. P. Tsankov, W. Jin, A. Orso, and S. Sinha. Execution Hijacking: Improving Dynamic Analysis by Flying off Course. *Proceedings of the 4th IEEE International Conference on Software Testing, Verification and Validation (ICST 2011)*, Berlin, Germany, March 2011.
(35 of the 166 submissions accepted – 21%)

49. A. Nanda, S. Mani, S. Sinha, M.J. Harrold, and A. Orso. Regression Testing in the Presence of Non-code Changes. *Proceedings of the 4th IEEE International Conference on Software Testing, Verification and Validation (ICST 2011)*, Berlin, Germany, March 2011.
(35 of the 166 submissions accepted – 21%)

50. J. Clause and A. Orso. Camouflage: Automated Anonymization of Field Data. *Proceedings of the 33rd IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2011)*, Waikiki, Honolulu, Hawaii, May 2011.
(52 of the 380 submissions accepted – 14%)

51. A. Orso. Monitoring, Analysis, and Testing of Deployed Software. *Proceedings of the Foundations of Software Engineering (FSE) and NITR&D/SPD Working Conference on the Future of Software Engineering Research (FoSER 2010)*, Santa Fe, NM, USA, November 2010.
(87 of the 139 submissions accepted – 63%)

52. M. Grechanik, J. Jones, A. Orso, and A. van der Hoek. Bridging Gaps between Developers and Testers in Globally-distributed Software Development. *Proceedings of the Foundations of Software Engineering (FSE) and NITR&D/SPD Working Conference on the Future of Software Engineering Research (FoSER 2010)*, Santa Fe, NM, USA, November 2010.
(87 of the 139 submissions accepted – 63%)

53. W. Jin, A. Orso, and T. Xie. BERT: A Tool for Behavioral Regression Testing. *Proceedings of the 18th European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2010) – Formal research demonstration*, Santa Fe, NM, USA, November 2010.
(6 of the 28 submissions accepted – 21%)

54. S. Roy Choudhary, and A. Orso. WebDiff: Automated Identification of Cross-browser Issues in Web Applications. *Proceedings of the 26th IEEE International Conference on Software Maintenance (ICSM 2010)*, Timisoara, Romania, September 2010.
(36 of the 133 submissions accepted – 27%)

55. S. Roy Choudhary, H. Versee, and A. Orso. A Cross-browser Web Application Testing Tool. *26th IEEE International Conference on Software Maintenance (ICSM 2010) – Formal research demonstration*, Timisoara, Romania, September 2010.
(8 of the 11 submissions accepted – 73%)

56. J. Clause and A. Orso. Leakpoint: Pinpointing the Causes of Memory Leaks. *Proceedings of the 32nd IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2010)*, Cape Town, South Africa, May 2010.
(52 of the 380 submissions accepted – 14%)

57. W. Jin, A. Orso, and T. Xie. Automated Behavioral Regression Testing. *Proceedings of the 3rd IEEE International Conference on Software Testing, Verification and Validation (ICST 2010)*, Paris, France, April 2010.
(41 of the 154 submissions accepted – 27%)

58. R. Santelices, A. Orso, and M.J. Harrold. Precisely Detecting Runtime Change Interactions for Evolving Software. *Proceedings of the 3rd IEEE International Conference on Software Testing, Verification and Validation (ICST 2010)*, Paris, France, April 2010.
(41 of the 154 submissions accepted – 27%)

59. J. Clause and A. Orso. PENUMBRA: Automatically Identifying Failure-Relevant Inputs Using Dynamic Tainting. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2009)*, Chicago, Illinois, USA, July 2009, pages 249–260.
(25 of the 93 submissions accepted – 27%)

60. W. Halfond, S. Anand, and A. Orso. Precise Interface Identification to Improve Testing and Analysis of Web Applications. *Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2009)*, Chicago, Illinois, USA, July 2009, pages 285–296. (This paper was presented with an **ACM-SIGSOFT Distinguished Paper Award**.)
(25 of the 93 submissions accepted – 27%)

61. W. Halfond, S.R. Choudhary, and A. Orso. Penetration Testing with Improved Input Vector Identification. *Proceedings of 2nd IEEE International Conference on Software Testing, Verification and Validation (ICST 2009)*, Denver, Colorado, USA, April 2009, pages 346–355. (My student William Halfond was awarded a **Best Presentation Award** at the conference for the presentation of this paper.)
(45 of the 141 submissions accepted – 32%)

62. H.-Y. Hsu and A. Orso. MINTS: A General Framework and Tool for Supporting Test-suite Minimization. *Proceedings of the 31st IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2009)*, Vancouver, Canada, May 2009, pages 419–429.
(50 of the 405 submissions accepted – 12%)

63. W. Halfond and A. Orso. Automated Identification of Interface Mismatches in Web Applications. *Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2008)*, Atlanta, Georgia, USA, November 2008, pages 181–191. (My student William Halfond was awarded a **Best Student Presentation Award** at the conference for the presentation of this paper.)
(31 of the 152 submissions accepted – 20%)

64. Raul Santelices, Pavan Kumar Chittimalli, Taweesup Apiwattanapong, Alessandro Orso, and Mary Jean Harrold. Test-suite Augmentation for Evolving Software. `Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering (ASE 2008)`, L'Aquila, Italy, September 2008. (This paper was presented with the **Best Paper Award** and an **ACM-SIGSOFT Distinguished Paper Award**.)
(34 of 280 submissions accepted – 12%)

65. Hwa-You Hsu, James Jones, and Alessandro Orso. Rapid: Identifying Bug Signatures to Support Debugging Activities. `Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering (ASE 2008)` [short paper], L'Aquila, Italy, September 2008.

66. J. Clause, I. Doudalis, A. Orso, and M. Prvulovic. Effective Memory Protection Using Dynamic Tainting. *Proceedings of the 22nd IEEE and ACM International Conference on Automated Software Engineering (ASE 2007)*, Atlanta, Georgia, USA, November 2007, pages 283–292.
(37 of 270 submissions accepted – 14%)

67. W. Halfond and A. Orso. Improving Test Case Generation for Web Applications Using Automated Interface Discovery. *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2007)*, Dubrovnik, Croatia, September 2007, pages 145–154.
(43 of 251 submissions accepted – 17%)

68. S. Joshi and A. Orso. SCARPE: A Technique and Tool for Selective Record and Replay of Program Executions. *Proceedings of the 23rd IEEE International Conference on Software Maintenance (ICSM 2007)*, Paris, France, October 2007, pages 234–243.
(46 of 214 submission accepted – 21%)

69. J. Clause, W. Li, and A. Orso. Dytan: A Generic Dynamic Taint Analysis Framework. *Proceedings of The ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2007)*, London, United Kingdom, pages 196–206. (This paper was presented with the 2017 **ISSTA Impact Paper Award**.)
(22 of 101 submissions accepted – 22%)

70. J. Clause and A. Orso. A Technique for Enabling and Supporting Debugging of Field Failures. *Proceedings of the 29th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2007)*, Minneapolis, Minnesota, USA, pages 261–270.
(50 of 334 submissions accepted – 15%)

71. S. Anand, A. Orso, and M.J. Harrold. Type-dependence Analysis and Program Transformation for Symbolic Execution. *Proceedings of the 29th IEEE and ACM SIGSOFT International Conference on Software Engineering (TACAS 2007)*, Braga, Portugal, pages 117–133.
(54 of 204 submissions accepted – 26%)

72. W. Halfond, A. Orso, and P. Manolios. Using Positive Tainting and Syntax-Aware Evaluation to Protect Web Applications. *Proceedings of the 14th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2006)*, Portland, Oregon, USA, November 2006, pages 175–185.
(25 of 125 submissions accepted – 20%)

73. W. Halfond and A. Orso. Command-Form Coverage for Testing Database Applications. *Proceedings of the IEEE and ACM International Conference on Automated Software Engineering (ASE 2006)*, Tokyo, Japan, September 2006, pages 69–78.
(22 of 121 submissions accepted – 18%)

74. T. Apiwattanapong, R. Santelices, P. Kumar Chittimalli, A. Orso, and M.J. Harrold. MaTRIX: Maintenance-Oriented Testing Requirements Identifier and Examiner. *Proceedings of the IEEE Conference on "Testing: Academic & Industrial Conference, Practice and Research Techniques" (TAIC PART 2006)*, London, United Kingdom, August 2006, pages 137–146.

75. W. Halfond and A. Orso. Preventing SQL Injection Attacks Using AMNESIA. *Proceedings of the 28th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2006) – Formal Demos track*, Shanghai, China, May 2006, pages 795-798.
(9 of 40 submissions accepted – 22%)

76. J. Viegas, W. Halfond, and A. Orso. A Classification of SQL Injection Attacks and Prevention Techniques. *Proceedings of the IEEE International Symposium on Secure Software Engineering (ISSSE 2006)*, Washington, D.C., USA, March 2006, pages 12–23.

77. W. Halfond and A. Orso. AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks. *Proceedings of the IEEE and ACM International Conference on Automated Software Engineering (ASE 2005)*, Long Beach, California, USA, November 2005, pages 174–183.
(28 of 291 submissions accepted – 10%)

78. M. Haran and A. Karr and A. Orso and A. Porter and A. Sanil. Applying Classification Techniques to Remotely-Collected Program Execution Data. *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2005)*, Lisbon, Portugal, September 2005, pages 146–155.
(32 of 201 submissions accepted – 16%)

79. T. Apiwattanapong, A. Orso, and M.J. Harrold. Efficient and Precise Dynamic Impact Analysis Using Execute-After Sequences. *Proceedings of the 27th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2005)*, St. Louis, MO, USA, May 2005, pages 432–441.
(44 of 313 submissions accepted – 14%)

80. A. Orso, N. Shi, and M.J. Harrold. Scaling Regression Testing to Large Software Systems. *Proceedings of the 12th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2004)*, Newport Beach, CA, USA, November 2004, pages 241–252.
(25 of 169 submissions accepted – 15%)

81. T. Apiwattanapong, A. Orso, and M.J. Harrold. A Differencing Algorithm for Object-oriented Programs. *Proceedings of the 19th IEEE International Conference on Automated Software Engineering (ASE 2004)*, Linz, Austria, September 2004, pages 2–13. (This paper was presented with the **Best Paper Award** and an **ACM-SIGSOFT Distinguished Paper Award**.)
(26 of 183 submissions accepted – 14%)

82. A. Orso, T. Apiwattanapong, J. Law, G. Rothermel, and M.J. Harrold. An Empirical Comparison of Dynamic Impact Analysis Algorithms. *Proceedings of the 26th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2004)*, Edimburgh, Scotland, May 2004.
(59 of 436 submissions accepted – 14%)

83. S. Sinha, A. Orso, and M.J. Harrold. Automated Support for Development, Maintenance, and Testing in the Presence of Implicit Control Flow. *Proceedings of the 26th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2004)*, Edimburgh, Scotland, May 2004.
(59 of 436 submissions accepted – 14%)

84. A. Orso, J. Jones, M.J. Harrold, and J. Stasko. GAMMATELLA: Visualization of Program-Execution Data for Deployed Software. *26th IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2004) – Formal Demos track*, Edinburgh, Scotland, May 2004.

85. A. Orso, T. Apiwattanapong, and M.J. Harrold. Leveraging Field Data for Impact Analysis and Regression Testing. *Proceedings of the 4th European Software Engineering Conference and 10th ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE 2003)*, Helsinki, Finland, September 2003, pages 128–137.
(33 of 168 submissions accepted – 20%)

86. A. Orso, J. Jones, and M.J. Harrold. Visualization of Program-Execution Data for Deployed Software. *Proceedings of the ACM Symposium on Software Visualization*, San Diego, CA, USA, June 2003, pages 67–76. (This paper was presented with an ACM SIGSOFT Distinguished Paper Award.)
(20 of 63 submissions accepted – 29%)

87. V. Martena, A. Orso, and M. Pezzè. Interclass Testing of Object Oriented Software. *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2002)*, IEEE Computer Society, Greenbelt, MD, USA, December 2002, pages 145–154.

88. A. Orso, A. Rao, and M.J. Harrold. A Technique for Dynamic Updating of Java Software. *Proceedings of the IEEE International Conference on Software Maintenance (ICSM 2002)*, IEEE Computer Society, Montreal, Canada, October 2002, pages 649–658.
(129 of 61 submissions accepted – 47%)

89. A. Orso, D. Liang, M.J. Harrold, and R. Lipton. Gamma System: Continuous Evolution of Software after Deployment. *Proceedings of the ACM International Symposium on Software Testing and Analysis (ISSTA 2002)*, Rome, Italy, July 2002, pages 65–69.
(25 of 97 submissions accepted – 26%)

90. A. Orso, M.J. Harrold, D. Rosenblum, G. Rothermel, M.L. Soffa, and H. Do. Using Component Metacontents to Support the Regression Testing of Component-Based Software. *Proceedings of the IEEE International Conference on Software Maintenance (ICSM 2001)*, Florence, Italy, November 2001, pages 716–725.
(68 of 161 submissions accepted – 42%)

91. A. Orso, S. Sinha, and M.J. Harrold. Incremental Slicing Based on Data-Dependences Types. *Proceedings of the IEEE International Conference on Software Maintenance (ICSM 2001)*, Florence, Italy, November 2001, pages 158–167.
(68 of 161 submissions accepted – 42%)

92. M.J. Harrold, J. Jones, T. Li, D. Liang, A. Orso, M. Pennings, S. Sinha, S. Spoon, and A. Gujarathi. Regression Test Selection for Java Software. *Proceedings of the ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2001)*, Tampa Bay, FL, USA, October 2001, pages 312–326.
(27 of 145 submissions accepted – 19%)

93. U. Buy, A. Orso and M. Pezzè. Automated Testing of Classes. *Proceedings of the ACM International Symposium on Software Testing and Analysis (ISSTA 2000)*, Portland, OR, USA, August 2000, pages 39–48.
(17 of 73 submissions accepted – 23%)

94. A. Orso and M. Pezzè. Integration Testing of Procedural Object-Oriented Languages with Polymorphism. *Proceedings of the International Conference on Testing Computer Software (TCS 1999)*, Washington, D.C., USA, June 1999.

95. A. Orso and S. Silva. Open Issues and Research Directions in Object-Oriented Testing. *Proceedings of the Fourth International Conference on Achieving Quality in Software (AQUIS 1998)*, Venice, Italy, January 1998.

96. L. Baresi, A. Orso, and M. Pezzè. Introducing Formal Specification Methods in Industrial Practice. *Proceedings of the Nineteenth IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 1997)*, Boston, MA, USA, May 1997, pages 56–66.

97. L. Baresi, A. Orso, and M. Pezzè. Customizable Notations for Kernel Formalisms. *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 1995)*, IEEE Computer Society, Fort Lauderdale, FL, USA, November 1995, pages 43–52.

E.3. Workshop Presentations with Proceedings (refereed)

1. S. Shamshiri, G. Fraser, P. McMinn, and A. Orso. Search-Based Propagation of Regression Faults in Automated Regression Testing. *Proceedings of the 3rd ICST International Workshop on Regression Testing (Regression 2013)*, Luxembourg, March 2013.

2. I. Erete and A. Orso. Optimizing Constraint Solving to Better Support Symbolic Execution. *Proceedings of the 3rd ICST Workshop on Constraints in Software Testing, Verification, and Analysis (CSTVA 2011)*, Berlin, Germany, March 2011. (This paper was presented with the **Best Paper Award**.)

3. J. Rößler, A. Orso, and A. Zeller. When does my program fail? *Proceedings of the 3rd ICST Workshop on Constraints in Software Testing, Verification, and Analysis (CSTVA 2011)*, Berlin, Germany, March 2011.

4. S.R. Choudhary, and A. Orso. Automated Client-side Monitoring for Web Applications. *Proceedings of the 1st International Workshop on Web Applications Testing (WEBTEST 2009)*, Denver, CO, USA, April 2009.

5. A. Orso and Tao Xie. BERT: BEhavioral Regression Testing. *Proceedings of the Sixth International ISSTA Workshop on Dynamic Analysis (WODA 2008)*, Seattle, WA, USA, July 2008, pages 36–42.
(11 of 23 submissions accepted – 48%)

6. A. Orso, S. Joshi, M. Burger, and A. Zeller. Isolating relevant Component Interactions with JINSI. *Proceedings of the Fourth International ICSE Workshop on Dynamic Analysis (WODA 2006)*, Shanghai, China, May 2006, pages 3–9.
(11 of 18 submissions accepted – 60%)

7. L. Wendehals and A. Orso. Recognizing Behavioral Patterns at Runtime using Finite Automata. *Proceedings of the Fourth International ICSE Workshop on Dynamic Analysis (WODA 2006)*, Shanghai, China, May 2006, pages 33-39.
(11 of 18 submissions accepted – 60%)

8. A. Seesing and A. Orso. InsECTJ: A Generic Instrumentation Framework for Collecting Dynamic Information within Eclipse. *Proceedings of the eclipse Technology eXchange (eTX) Workshop at OOPSLA 2005*, San Diego, USA, October 2005.

9. J. Cook and A. Orso. MonDe: Safe Updating through Monitored Deployment of New Component Versions. *Proceedings of the ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering (PASTE 2005)*, Lisbon, Portugal, September 2005, pages 43–46.

10. Alessandro Orso and Bryan Kennedy. Selective Capture and Replay of Program Executions. *Proceedings of the Third International ICSE Workshop on Dynamic Analysis (WODA 2005)*, St. Louis, MO, USA, May, 2005.

11. William G.J. Halfond and Alessandro Orso. Combining Static Analysis and Runtime Monitoring to Counter SQL-Injection Attacks. *Proceedings of the Third International ICSE Workshop on Dynamic Analysis (WODA 2005)*, St. Louis, MO, USA, May 2005.

12. A. Chawla and A. Orso. A Generic Instrumentation Framework for Collecting Dynamic Information. *Proceedings of the ISSTA Workshop on Empirical Research in Software Testing.*

13. A. Carzaniga and A. Orso. Continuous Remote Analysis for Improving Distributed Systems Performance. *Proceedings of the First ICSE Workshop on Remote Analysis and Measurement of Software Systems (RAMSS 03)*, Portland, OR, USA, May 2003, pages 47–50.

14. J. Bowring, A. Orso, and M.J. Harrold. Monitoring Deployed Software Using Software Tomography. *Proceedings of the ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering (PASTE 2002)*, Charleston, SC, USA, November 2002, pages 2–8.

15. A. Orso, G. Vigna, and M.J. Harrold. MASSA: Mobile Agents Security through Static/Dynamic Analysis. *Proceedings of the ICSE Workshop on Software Engineering and Mobility*, Toronto, Canada, May 2001.

16. A. Orso, S. Sinha, and M.J. Harrold. Effects of Pointers on Data Dependences. *Proceedings of the International Workshop on Program Comprehension (IWPC 2001)*, Toronto, Canada, May 2001, pages 39–49.

17. A. Orso, M.J. Harrold, and D. Rosenblum. Component Metadata for Software Engineering Tasks. *Proceedings of the International Workshop on Engineering Distributed Objects (EDO 2000)*, LNCS Vol. 1999, Springer-Verlag, Davis, CA, USA, November 2000, pages 129–144.

18. U. Buy, C. Ghezzi, A. Orso, M. Pezzè, and M. Valsasna. A Framework for Testing Object-Oriented Components. *Proceedings of the ICSE Workshop on Testing Distributed Component-Based Systems*, Los Angeles, CA, USA, May 1999.

F. Other

F.1. Research Posters

1. M. Kim, J. Cobb, T. Kurc, A. Orso, M.J. Harrold, A. Post, A. Sharma, and J. Saltz. Informatics Support for Data Integrity Testing in Heterogeneous and Dynamic Database Environments. *Proceedings of the 2012 AMIA Summit on Clinical Research Informatics (CRI 2012)*, San Francisco, CA, USA, March 2011.

2. A. Orso, J. Jones, and M.J. Harrold. Visualization of Program-Execution Data for Deployed Software, at the *ACM Symposium on Software Visualization (SOFTVIS 2003)*, San Diego, CA, USA, June 2003.

3. J. Bowring, A. Orso, and M.J. Harrold. Software Tomography – Enabling Continuous Improvement in Software Development, at the *ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2002)*, Charleston, SC, USA, November 2002.

4. M. Balakrishnan, A. Orso, and M.J. Harrold. Dynamic Update of Java Software, at the *Yamacraw Industrial Advisory Board Workshop*, Atlanta, GA, USA, October 2002.

5. A. Orso, D. Liang, and M.J. Harrold. DejaVOO: A Regression Testing Tool for Java Software, at the *ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2001)*, Tampa Bay, Florida, USA, October 2001.

F.1. Submitted Journal Papers

F.3. Software

MintHint: MINTHINT is a novel technique and tool for program repair that is a departure from most of today's approaches. Instead of trying to fully automate program repair, which is often an unachievable goal, MINTHINT performs statistical correlation analysis to identify expressions that are likely to occur in the repaired code and generates, using pattern-matching based synthesis, repair hints from these expressions. Intuitively, these hints suggest how to rectify a faulty statement and help developers find a complete, actual repair. MINTHINT has been released in May 2014 and is freely available from my web page.

F^3: F^3 (Fault localization for Field Failures) is a tool that builds on BUGREDUX (see below) and extends it with automated debugging capabilities. F^3 can thus help developers not only recreate, but also debug field failures. Given an observed field failure, F^3 can synthesize a number of failing and passing executions similar to the observed failure and use these executions, in conjunction with automated fault localization approaches, to help developers identify likely causes of such failure. F^3 has been released in July 2013 and is freely available from my web page.

TestEvol: TESTEVOL is a tool for analyzing test-suite evolution. More precisely, TestEvol facilitates the systematic study of test-suite evolution for Java programs and JUnit test suites. The tool analyzes a sequence of versions of a software system, where a system consists of an application together with its test suite, and allows for studying how the test cases in the test suite evolved when going from one version to the next. TESTEVOL has been released in November 2012 and is freely available from my web page.

BugRedux: BUGREDUX is a general tool for enabling in-house debugging of field failures. BUGREDUX works by (1) collecting data about failing program executions in the field, (2) extracting from the collected execution data sequences of intermediate goals (i.e., statements in the program), and (3) using a symbolic execution technique to synthesize, in house, executions that reach such goals, mimic the observed executions, and reproduce the corresponding failures. The current implementation of BUGREDUX can collect four types of increasingly rich execution data: points of failure, call stacks, call sequences, and complete program traces. To perform symbolic execution, BUGREDUX relies on a suitably modified version of KLEE (`http://klee.llvm.org/`). BUGREDUX has been released in August 2011 and is freely available from my web page.

NIONKA: NIONKA is a tool for execution hijacking. Given a program P and an input I for P, execution hijacking allows for running P with I as input and following a specific path that P would normally not follow under I. By doing so, execution hijacking can expose additional behaviors and benefit different kinds of dynamica analysis. Two versions of the tool are available, one for hijacking of Java programs, and the other for x86 programs. These tools have been released in March 2011 and are freely available from my web page.

BERT: BERT (BEhavioral Regression Testing) is an Eclipse plug-in that implements our automated behavioral regression testing approach. Every time a new version of a program is saved, BERT (1) analyzes the changes between the new and the old version, (2) generates tests for the changed parts, (3) runs the tests on the old and new versions, (4) analyzes and reports to the developers the behavioral differences between the two versions. This tool has been released in November 2010 and is freely available from my web page.

MINTS: MINTS (MINimizer for Test Suites) is a generic framework for supporting test-suite minimization that allows for (1) easily encoding a wide range of test-suite minimization problems, (2) handling problems that involve any number of minimization criteria, and (3) computing optimal solutions to minimization problems by leveraging a number of integer linear programming solvers. This tool has been released in February 2008 and is freely available from my web page.

DYTAN: DYTAN is a general framework for dynamic taint analysis (also known as dynamic information flow analysis) that operates on X86 binaries. DYTAN is flexible and easy to use because it allows for instantiating different flavors of dynamic taint analysis by simply specifying a set of pre-defined options in a configuration file. Although we have not officially released the tool yet, we have pre-released it to several researchers in universities and research labs in the US and in Europe, including researchers at Columbia University, UC Berkeley, and Politecnico di Milano, Italy.

WASP: WASP (Web Application SQL-injection Preventer) is a highly-automated tool against SQL-injection attacks. Unlike AMNESIA, WASP does not require any complex static analysis of the code and provides both conceptual and practical advantages. The conceptual advantages are in the use of (1) positive tainting, which focuses on the identification and marking of trusted, rather than untrusted data, and (2) flexible syntax-aware evaluation, which provides developers with a mechanism to regulate the usage of strings based not only on their source, but also on the syntactical role they play in the final query string. From a practical standpoint, WASP is accurate, efficient, and has only minimal deployment requirements. WASP also incorporates MetaStrings, a library that we developed and that tracks taint information at the character level and accurately maintains markings during string manipulations. *In April 2007, we signed a contract with Reflective for the commercialization of WASP.*

SCARPE: SCARPE is a tool for Selective CApture and Replay of Program Executions. Given a program, the tool lets users (1) select a subsystem, (2) capture at runtime all the interactions between such subsystem and the rest of the program, and (3) replay the recorded interactions on the subsystem in isolation. SCARPE can be used for various applications, including post-mortem dynamic analysis of users' executions, regression testing, and debugging. Although we have not officially released the tool yet, we have pre-released it to several researchers in universities and research labs in the US and in Europe.

AMNESIA: AMNESIA is a tool to detect and prevent SQL-injection attacks. The tool combines conservative static analysis and runtime monitoring to detect and stop illegal queries before they are executed on a database underlying a web application. In its static part, the tool builds a conservative model of the legitimate queries that could be generated by the application. In its dynamic part, the tool inspects the dynamically generated queries for compliance with the statically-built model. Queries that do not comply with the model are stopped and suitably reported. AMNESIA has been evaluated extensively and is currently available on a per-request basis. *So far, we distributed the tool to more than 20 universities and research labs.*

JDiff: JDIFF is a tool for comparing different versions of object-oriented programs that identifies both differences and correspondences between two versions. The technique implemented in the tool is based on a representation that handles object-oriented features and, thus, can capture the behavior of object-oriented programs. In this way, JDIFF can outperform existing tools based on purely syntactic differencing. The tool is currently available on a per-request basis.

DejaVOO: DEJAVOO, developed at Georgia Tech, is a regression test selection tool for Java software. The tool inputs a program P, a set of test cases for P T, and a new version of the program P', and outputs a subset of T T' that contains the test cases to be rerun on P'. T' is computed using static and dynamic program analysis techniques. P and P' are provided in bytecode format and are analyzed using the Java Architecture for Bytecode Analysis (JABA), developed at Georgia Tech. Test cases can be provided in the form of JUnit tests. *The tool is currently available on a per-request basis and is being used by TATA Consulting Services in the context of a funded research project.*

InsECT: INSECT (Instrumentation, Execution, and Coverage Tool) is an infrastructure for selective instrumentation of Java software developed at Georgia Tech. InsECT inputs a program and an instrumentation policy and outputs an instrumented version of the program, generated through bytecode rewriting. The instrumentation policy specifies what parts of the program must be instrumented and what kinds of dynamic information must be collected. Currently, InsECT is integrated into Eclipse and can instrument for statement, edge, call, and exception (throw and catch) coverage, and for statement and call profiling. Dynamic information can be analyzed using the InsECT API or visualized using the InsECT GUI. *Insect is available on the SourceForge site and has been downloaded more than a thousand times.*

Older Software

DUSC: DUSC (Dynamic Updating through Swapping of Classes) is an infrastructure for dynamic, remote updating of Java software developed at Georgia Tech. DUSC produces, for each class C in the system to be updated, a wrapper and an implementation. All interaction of C with the rest of the application occur through the wrapper, so that the implementation of C can be updated with a new version without having to stop the system.

DUSC transforms Java systems in updateable systems automatically, without requiring any interaction with the developer and without any support from the Java Virtual Machine. Moreover, DUSC allows for the updates to be sent through the network, so enabling remote, on-line updating of systems.

CabJava: CABJAVA, developed at Politecnico di Milano, is an editor, analyzer, and simulator for High-Level Time Petri Nets (HLTPNs). The tools consists of three main JavaBeans components connected through a C2 architecture: (1) the graphical editor, in which the user can easily create and edit Petri nets, define and modify their temporal properties, and visualize their simulation; (2) the kernel, which implements the HLTPN semantics; and (3) the executor, which lets the user simulate the behavior of the generated Petri nets. CabJava is available and can be downloaded from my web page.

MeTaEDitor (MTD): MTD, developed at Politecnico di Milano, is a tool that allows for defining high-level semi-formal graphical specification notations in terms of an underlying formal kernel. The tool consists of three modules: (1) the mapping generator, which is a graphical editor that lets the user define the mapping from the high-level notation to the underlying kernel in terms of graph-grammar productions; (2) the translator, which, given a specification in the high-level notation and the user-defined mapping, generates the corresponding kernel-level executable model; and (3) the simulator, which executes the kernel-level model step by step and maps the results of each step back to the high-level specification.

G. Research Proposals and Grants (Principal Investigator)

a. Approved and Funded

1. **Comprehensive System Debloating via Path-Based Learning and Late-Stage OS Composition**
   ONR
   PI: Wenke Lee
   Co-PIs: William Harris (Galois, Inc.), Taesoo Kim (Georgia Tech), Alessandro Orso, Santosh Pande (Georgia Tech)
   Awarded in December 2017, $7,500,000

2. **Creating an Interprocedural Analyst Oriented Data Flow Representation**
   Research contract with Sandia National Labs/Sandia Corporation.
   PI: Alessandro Orso
   Co-PIs: None
   Awarded in December 2017, $48,500

3. **SHF: Medium: Spectral Profiling: Understanding Software Performance without Code Instrumentation**
   NSF CCF/SHF Program
   PI: Alessandro Orso
   Co-PIs: Milos Prvulovic (Georgia Tech) and Alenka Zajic (Georgia Tech)
   Awarded in June 2016, $850,000

4. **CAMELIA: Computational Activity Monitoring by Externally Leveraging Involuntary Analog sSignals**
   DARPA
   PI: Alenka Zajic
   Co-PIs: Alessandro Orso and Milos Prvulovic (Georgia Tech)
   Subcontractor: Matthew Welborn (Northrop Grumman Information Systems)
   Awarded in May 2016, $9,440,000

5. **EAGER: Collaborative Research: Leveraging Graph Databases for Incremental and Scalable Symbolic Analysis and Verification of Web Applications**
   NSF CCF/SHF Program
   PI: Alessandro Orso
   Co-PIs: Wenke Lee (Georgia Tech), Tevfik Bultan (UCSB), Xifeng Yan (UCSB), Corina Pasareanu (CMU Silicon Valley)
   Awarded in September 2015, $249,990 (Georgia Tech's part: $100,000)

6. **THEIA: Tagging and Tracking of Multi-level Host Events for Transparent Computing and Information Assurance**
   DARPA
   PI: Wenke Lee
   Co-PIs: Taesoo Kim (Georgia Tech), Alessandro Orso (Georgia Tech), Simon Chung (Georgia Tech), Albert Brzeczko (GTRI)
   Awarded in March 2015, $4,253,126

7. **Capturing Field Data for Mobile Applications**
   NSF I-Corps Program
   PI: Alessandro Orso
   Co-PIs: None
   Awarded in January 2015, $50,000

8. **CheckDroid: Mobile Application Testing**
   Georgia Research Alliance
   PI: Alessandro Orso
   Co-PIs: None
   Awarded in October 2014, $24,877.29

9. **Quantitative Analysis and Reporting of Potential Covert- and Side-Channel Attacks**
   Air Force Office of Scientific Research
   PI: Milos Prvulovic
   Co-PIs: Alessandro Orso and Alenka Zajic
   Awarded in July 2014, $993,031

10. **Teaching Software Engineering To the Masses with TouchDevelop**
    Microsoft Research Software Engineering Innovation Foundation (SEIF) Award
    PI: Alessandro Orso
    Co-PIs: None
    Awarded in March 2014, $40,000

11. **WebGamma: Post-deployment Quality Assurance for Web Applications**
    Google Research Award
    PI: Alessandro Orso
    Co-PIs: None
    Awarded in August 2013, $49,545

12. **SHF:Small: BugX: In-house Debugging of Field Failures to Improve Software Quality**
    NSF CCF/SHF Program
    PI: Alessandro Orso
    Co-PIs: None
    September 2013–August 2016, $434,999

13. **Differential Cross-Platform Testing of Web Applications**
    Research contract with Fujitsu Laboratories of America, Inc.
    PI: Alessandro Orso
    Co-PIs: None
    Awarded in December 2012, $20,000

14. **SHF: Medium: Collaborative Research: Regression Testing Techniques for Real-world Software Systems**
    NSF CCF/SHF Program
    PI: Alessandro Orso
    Co-PIs: Mary Jean Harrold, Myra Cohen (University of Nebraska, Lincoln)
    July 2012–June 2016, $875,065

15. **Viewpoints: Discovering Client- and Server-side Input Validation Inconsistencies to Improve Web Application Security**
NSF CNS/TC Program
PI: Alessandro Orso
Co-PIs: Tevfik Bultan (UCSB), Christopher Krugel (UCSB)
October 2011–September 2013, $199,994.

16. **Testing of Biomedical Federated Databases**
ACTSI's Biomedical Informatics Program
PI: Alessandro Orso
Co-PI: Mary Jean Harrold
June 2010–May 2013, $340,000.

17. **MEDITA - Multi-layer Enterprise-wide Dynamic Information-flow Tracking & Assurance**
NSF CCF Program
PI: Alessandro Orso
Co-PIs: Nicholas Feamster, Milos Prvulovic
June 2010–May 2013, $969,141.

18. **BERT – BEhavioral Regression Testing**
Microsoft Research Software Engineering Innovation Foundation (SEIF) Award
PI: Alessandro Orso
Co-PIs: None
Awarded in May 2010, $25,000

19. **Designing Tests for Evolving Software Systems (supplemental funding request)**
NSF CCF Program
PI: Alessandro Orso
Co-PIs: None
May 2010–December 2011, $68,086.

20. **Automated Debugging Techniques for Modern Software Systems**
NSF, Software and Hardware Foundations (SHF) Program
PI: Alessandro Orso
Co-PIs: None
July 2009–June 2012, $445,000.

21. **Designing Tests for Evolving Software Systems**
NSF, Science of Design (SoD) Program
PI: Alessandro Orso
Co-PIs: Mary Jean Harrold (Georgia Tech)
Collaborative project with Tao Xie (North Carolina State University)
January 2008–December 2010, $342,000.

22. **Software and Hardware Support for Efficient Monitoring of Program Behavior**
National Science Foundation Award CCF-0541080, Computing Processes and Artifacts (CPA) Program
PI: Alessandro Orso
Co-PIs: Milos Prvulovic (Georgia Tech)
Collaborative project with Yan Solihin (North Carolina State University) and Jonathan Cook (New Mexico State University).
September 2006–August 2009, $350,000.

23. **Preventing SQL Code Injection by Combining Static and Runtime Analysis**
Homeland Security Advanced Research Projects Agency (HSARPA) Contract FA8750-05-2-0214

PI: Alessandro Orso
Co-PIs: Wenke Lee (Georgia Tech)
May 2005–October 2007, $387,069.

24. **REU Extension** for project: GAMMA: Acquiring Accurate Dynamic Field Data Using Lightweight Instrumentation
Extension to National Science Foundation Award CCR-0205422
PI: Alessandro Orso
Co-PIs: None
June 2005–August 2006, $12,000.

25. **DejaVOO – Cost-Effective Regression Testing of Java Software**
IBM Eclipse Innovation Grant and Faculty Award
PI: Alessandro Orso
Co-PIs: None
Awarded in March 2005, $26,700.

26. **Scalable Integration Testing of Object-Oriented Software: An Empirical Research Program**
National Science Foundation Award CCR-0306372, Information Technology Research Program
PI: Mary Jean Harrold (Georgia Tech) Co-PIs: Alessandro Orso
Collaborative project with Gregg Rothermel (Oregon State University).
June 2003–May 2007, $201,146.

27. **GAMMA: Acquiring Accurate Dynamic Field Data Using Lightweight Instrumentation**
National Science Foundation Award CCR-0205422, Information Technology Research Program
PI: Mary Jean Harrold (Georgia Tech)
Co-PIs: Alessandro Orso, Richard Lipton (Georgia Tech), John Stasko (Georgia Tech)
Joint project with Alan F. Karr (National Institute of Statistical Sciences), David S. Notkin (University of Washington), Adam A. Porter (University of Maryland, College Park), and Douglas C. Schmidt (Vanderbilt University).
September 2002–August 2007, $412,000.

H. Research Honors and Awards

1. ISSTA 2017 Impact Paper Award, for the ISSTA 2007 paper "Dytan: A Generic Dynamic Taint Analysis Framework."

2. IBM Haifa Verification Conference 2013 Award for the most significant contribution to testing and verification in the past 5 years, for the ISSTA 2011 paper "Are Automated Debugging Techniques Actually Helping Programmers?" (`https://www.research.ibm.com/haifa/conferences/hvc2013/award.shtml`)

3. 2013 Google Research Award for the project "WebGamma: Post-deployment Quality Assurance for Web Applications".

4. 2014 Microsoft Research Software Engineering Innovation Foundation (SEIF) Award for the project "Teaching Software Engineering To the Masses with TouchDevelop".

5. Nomination for ACM-SIGSOFT Distinguished Paper Award at the *IEEE and ACM SIGSOFT International Conference on Software Engineering (ICSE 2013)*, for paper "X-PERT: Accurate Identification of Cross-Browser Issues in Web Applications." Co-authors: S. Roy Choudhary and M. Prasad. May 2013. (461 submissions.)

6. Nomination for ACM-SIGSOFT Distinguished Paper Award at the *ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2012)*, for paper "Efficient Regression Testing of Ontology-Driven Systems." Co-authors: M. Kim, J. Cobb, M.J. Harrold, T. Kurc, J. Saltz, A. Post, K. Malhotra and S. Navathe. (108 submissions.)

7. Nomination for ACM-SIGSOFT Distinguished Paper Award at the *ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2011)*, for paper "Are Automated Debugging Techniques Actually Helping Programmers?" Co-author: C. Parnin. (121 submissions.)

8. Best Paper Award at the *ICST Workshop on Constraints in Software Testing, Verification and Analysis (CSTVA 2011)*, for paper "Optimizing Constraint Solving to Better Support Symbolic Execution." Co-author: I. Erete. March 2011.

9. 2010 Microsoft Research Software Engineering Innovation Foundation (SEIF) Award for the project "BERT – BEhavioral Regression Testing".

10. ACM-SIGSOFT Distinguished Paper Award at the *ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2009)*, for paper "Precise Interface Identification to Improve Testing and Analysis of Web Applications." Co-authors: W. Halfond and S. Anand. July 2009. (93 submissions.)

11. Best Paper Award at the *23rd IEEE International Conference on Automated Software Engineering (ASE 2008)*, for paper "Test-suite Augmentation for Evolving Software." Co-authors: R. Santelices, P. Kumar Chittimalli, T. Apiwattanapong, A. Orso, and M.J. Harrold. September 2008. (280 submissions.)

12. ACM-SIGSOFT Distinguished Paper Award at the *23rd IEEE International Conference on Automated Software Engineering (ASE 2008)*, for paper "Test-suite Augmentation for Evolving Software." Co-authors: R. Santelices, P. Kumar Chittimalli, T. Apiwattanapong, A. Orso, and M.J. Harrold. September 2008. (280 submissions.)

13. Georgia Institute of Technology College of Computing Outstanding Research Scientist Research Award, 2004.

14. Best Paper Award at the *19th IEEE International Conference on Automated Software Engineering (ASE 2004)*, for paper "A Differencing Algorithm for Object-oriented Programs." Co-authors: T. Apiwattanapong and M.J. Harrold. September 2004. (183 submissions.)

15. ACM-SIGSOFT Distinguished Paper Award at the *19th IEEE International Conference on Automated Software Engineering (ASE 2004)*, for paper "A Differencing Algorithm for Object-oriented Programs." Co-authors: T. Apiwattanapong and M.J. Harrold. September 2004. (183 submissions.)

16. ACM-SIGSOFT Distinguished Paper Award at the *ACM Symposium on Software Visualization*, for paper "Visualization of Program-Execution Data for Deployed Software." Co-authors: J. Jones, and M.J. Harrold. June 2003. (63 submissions.)

III. SERVICE

A. Professional Activities

A.1 Membership and Activities in Professional Societies

1. Senior Member, Association for Computing Machinery (ACM) (also SIGSOFT).
2. Senior Member, Institute of Electrical and Electronics Engineers (IEEE) Computer Society.

A.2 Conference Committee Activities

1. Program Committee Member, 29th ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2020), Los Angeles, USA, July 2020.
2. Program Committee Member, 42nd IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2020), Seoul, South Korea, May 2020.
3. Program Committee Member, 41st IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2019), Montreal, Canada, May 2019.
4. Program Committee Member, 27th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2019), Tallinn, Estonia, August 2019.
5. Program Committee Member, 26th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2018), Lake Buena Vista, Florida, USA, November 2018.
6. Program Committee Member, 27th ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2018), Amsterdam, Netherlands, July 2018.
7. Program Board Member, 40th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2018), Gothenburg, Sweden, May-June 2018.
8. Program Committee Member, Doctoral Symposium of the 26th ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2017), Santa Barbara, CA, USA, July 2017.
9. Program Committee Member, International Symposium on Engineering Secure Software and Systems (ESSoS 2017), July 2017, Bonn, Germany.
10. Program Co-Chair, 39th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2017), Buenos Aires, Argentina, May 2017.
11. Program Board Member, 38th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2016), Austin, Texas, USA, May 2016.
12. Steering Committee Member, ACM and IEEE International Conference on Software Engineering (ICSE), July 2014 to date.
13. Program Committee Member, 35th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2014), Hyderabad, India, June 2013.
14. Member of the Expert Review Panel, 28th IEEE/ACM International Conference on Automated Software Engineering (ASE 2013), Palo Alto, California, USA, November 2013.
15. Program Committee Member, 8th joint meeting of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE 2013), Saint Petersburg, Russia, August 2013.

16. Program Committee Member, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2013), Lugano, Switzerland, July 2013.

17. Program Committee Member, Doctoral Symposium of the 35th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2013), San Francisco, California, USA, May 2013.

18. Program Committee Member, 35th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2013), San Francisco, California, USA, May 2013.

19. Steering Committee Member, IEEE International Conference on Software Testing, Verification and Validation (ICST), April 2013 to date.

20. Program Committee Member, 2nd ETAPS Workshop on Validation Strategies for Software Evolution (VSSE 2013), Rome, Italy, March 2013.

21. Program Committee Member, 20th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2012), Research Triangle Park, North Carolina, USA, November 2012.

22. Program Committee Member, 2nd International ISSTA Workshop on End-to-end Test Script Engineering (ETSE 2012), July 2012.

23. Program Committee Member, 4th ICST International Workshop on Constraints in Software Testing, Verification and Analysis (CSTVA 2012), Montreal, Canada, April 2012.

24. Member of the External Review Committee, ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2012), Tucson, Arizona, USA, October 2012.

25. Member of the Expert Review Panel, 27th IEEE/ACM International Conference on Automated Software Engineering (ASE 2012), Essen, Germany, September 2012.

26. Program Committee Member, International ICSE Workshop on Recommendation Systems for Software Engineering (RSSE 2012), Zurich, Switzerland, June 2012.

27. Program Committee Member, 34th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2012), Zurich, Switzerland, June 2012.

28. Program Committee Member, 50th International Conference on Objects, Models, Components and Patterns (TOOLS Europe 2012), May 2012.

29. Program Committee Member, 50th International Conference on Objects, Models, Components, Patterns. Prague, Czech Republic, May 2012.

30. Program Committee Member, ESEC/FSE 2011 Workshop on Verification, Analysis, and Testing of Service Systems (VATSS 2011), September 2011.

31. Member of the Expert Review Panel, 26th IEEE/ACM International Conference on Automated Software Engineering (ASE 2011), Oread, Lawrence, Kansas, USA, November 2011.

32. Program Committee Member, 2nd International Workshop on Software Engineering for Sensor Network Applications (SESENA 2011), Waikiki, Honolulu, Hawaii, May 2011.

33. Program Committee Member, 1st International Workshop on Developing Tools as Plug-ins (TOPI 2011), Waikiki, Honolulu, Hawaii, May 2011.

34. Judge for the ACM Student Research Competition at ICSE 2011, Waikiki, Honolulu, Hawaii, May 2011.

35. Program Committee Member, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2011), Toronto, Canada, July 2011.

36. Program Committee Member, 4th IEEE International Conference on Software Testing Verification and Validation (ICST), Berlin, Germany, March 2011.

37. Program Committee Member, 32nd International IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2011), Waikiki, Honolulu, Hawaii, May 2011.

38. Program Committee Member, 24th IEEE/ACM International Conference on Automated Software Engineering (ASE 2010), Antwerp, Belgium, September 2010.

39. Program Committee Member, 18th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2010), Santa Fe, New Mexico, USA, November 2010.

40. Program Committee Member, 32nd International IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2010), Cape Town, South Africa, May 2010.

41. Program Committee Member, 24th IEEE/ACM International Conference on Automated Software Engineering (ASE 2009), Auckland, New Zealand, November 2009.

42. Steering Committee Member, Workshop on Software Engineering for Secure Systems (SESS), August 2009 to date.

43. Program Committee Member, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2009), Chicago, Illinois, USA, July 2009.

44. Steering Committee Member, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), July 2009 to date.

45. Program Committee Member, 7th International Workshop on Dynamic Analysis (WODA 2009), Chicago, IL, USA, July 2009.

46. Program Committee Member, IEEE International Conference on Program Comprehension (ICPC 2009), Vancouver, British Columbia, Canada, May 2009.

47. Program Committee Member, 1st International ICST Workshop on Web Testing, Denver, Colorado, USA, April 2009.

48. Program Committee Member, 2nd India Software Engineering Conference (ISEC 2009), Pune, India, February 2009.

49. Program Committee Member, 2nd IEEE International Conference on Software Testing Verification and Validation (ICST), Denver, Colorado, USA, April 2009.

50. Program Committee Member, Doctoral Symposium of 16th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2008), Atlanta, Georgia, USA, September 2008.

51. Program Committee Member, International FSE Workshop on Recommendation Systems for Software Engineering (RSSE 2008), Atlanta, Georgia, USA, November 2008.

52. Program Committee Member, 16th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2008), Atlanta, Georgia, USA, September 2008.

53. Program Committee Member, 1st Working Conference on Mining Software Repositories (MSR 2008), Leipzig, Germany, May 2008.

54. Program Committee Member for the Research Demonstrations track of the 30th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2008), Leipzig, Germany, May 2008.

55. Program Committee Member, 1st IEEE International Conference on Software Testing Verification and Validation (ICST 2008), Lillehammer, Norway, April 2008.

56. Program Committee Member, 22nd IEEE International Conference on Automated Software Engineering (ASE 2007), Atlanta, Georgia, USA, November 2007.

57. Program Committee Member, Joint 11th European Software Engineering Conference and 15th ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE 2007), Dubrovnik, Croatia, September 2007.

58. Program Committee Member, 4th ICSE International Workshop on Dynamic Analysis (WODA 2006), Shanghai, China, May 2006.

59. Program Committee Member, 21th IEEE International Conference on Automated Software Engineering (ASE 2006), Tokyo, Japan, September 2006.

60. Program Committee Member, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2006), Portland, Maine, USA, July 2006.

61. Program Committee Member for the Research Demonstrations track of the 28th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2006), Shanghai, China, May 2006.

62. Program Committee Member for the 4th eclipse Technology eXchange Workshop at OOPSLA 2005 (eTX 2005), San Diego, CA, USA, October 2005.

63. Program Committee Member, 20th IEEE International Conference on Automated Software Engineering (ASE 2005), Long Beach, CA, USA, November 2005.

64. Program Committee Member, Joint 5th European Software Engineering Conference and 13th ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE 2005), Lisbon, Portugal, September 2005.

65. Workshops Committee Member, 27th International IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2005), St. Louis, MO, USA, May 2005.

66. Program Committee Member, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2004), Boston, MA, USA, July 2004.

67. Program Committee Member, 26th International IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2004), Edinburgh, Scotland, May 2004.

68. Program Committee Member, 6th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2000), Tokyo, Japan, September 2000.

69. Program Committee Member, 5th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 1999), Las Vegas, NV, USA, October 1999.

A.3 Conferences, Workshops, and External Courses

1. Awards Chair, 42nd IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2020), Seoul, South Korea, May 2020.

2. Program Co-Chair, 39th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2017), Buenos Aires, Argentina, May 2017.

3. Chair, Doctoral Symposium of the 37th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2015), May 2015.

4. Program Co-Chair, ACM-SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2014), November 2014.

5. Co-organizer, Second Workshop on the Future of Debugging, at the ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2013), July 2013.

6. Co-organizer, 2nd Web Quality Security and Testing (WebQUeST) workshop at the 20th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2012), November 2012.

7. Program Co-Chair, IEEE International Conference on Software Testing, Verification and Validation (ICST 2013), April 2013.

8. Workshop Co-chair for the 34th IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2012), June 2012.

9. Chair, Doctoral Symposium of the 18th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2010), November 2010.

10. Program Chair, ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2010), July 2010.

11. Workshop Co-chair for the joint 12th European Software Engineering Conference and 17th ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE 2009), August 2009.

12. Co-chair, New Ideas and Emerging Results Track at the 31st IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2009), May 2009.

13. Co-organizer, ASE International Workshop on Living with Uncertainties (IWLU 2007), with Marsha Chechik (University of Toronto, Canada), Betty H.C. Cheng (Michigan State University, USA), Alexander Egyed (Teknowledge Corporation, USA), and Kevin Sullivan (University of Virginia, USA).

14. Co-organizer, OOPSLA Eclipse Technology eXchange Workshop (ETX 2007), with Martin Robillard (McGill University, Canada) and Li-Te Cheng (IBM T J Watson Research Center, USA).

15. Co-organizer, ICSE Workshop on Dynamic Analysis (WODA 2007), with Andreas Zeller (Saarland University, Germany), 2007.

16. Program co-chair, ICSE 2007 Posters and Demonstrations track, with Elisabetta Di Nitto (Politecnico di Milano, Italy).

17. Co-organizer, OOPSLA Eclipse Technology eXchange Workshop (ETX 2006), with Martin Robillard (McGill University, Canada) and Michael Burke (IBM T J Watson Research Center, USA).

18. Co-organizer, ISSTA Workshop on Testing and Analysis of Evolving and Deployed Software (TAEDS 2006), with Tao Xie (North Carolina State University, USA), 2006.

19. Co-organizer, Second ICSE Workshop on *Remote Analysis and Measurement of Software Systems (RAMSS)*, with Adam A. Porter (University of Maryland, USA), 2004.

20. Co-organizer, First ICSE Workshop on *Remote Analysis and Measurement of Software Systems (RAMSS)*, with Adam A. Porter (University of Maryland, USA), 2003.

21. Local Arrangements Chair, Third IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 1997), sponsored by IEEE, September 1997, Lake Como, Italy.

B. On-campus Georgia Tech Committees

1. Member, Georgia Tech's Strategic Planning Steering Committee.

2. Chair, Search Committee for the Chair of the School of Computational Science and Engineering in the College of Computing.
3. GT Research Advisory Committee: 2019-to date.
4. Chair, Faculty Recruiting Committee, School of Computer Science, College of Computing. Academic Years 2013 and 2014.
5. Software Engineering/Embedded Software professional Master's working group, Georgia Tech. Academic Year 2013.
6. MOOMS working group, College of Computing. Academic Year 2013. Chair: Kishore Ramachandran.
7. SCS representatives to the CS PhD program committee (with Carsten Schwan). Academic Years 2011 and 2012.
8. CS Ph.D. Program Committee, College of Computing. Academic Year 2010.
9. School Advisory Committee, School of Computer Science, College of Computing. Academic Year 2010.
10. Faculty Recruiting Committee, School of Computer Science, College of Computing. Academic Year 2009.
11. Chair, PhD Task Force, College of Computing. Fall 2008–Spring 2009.
12. Threads Implementation Committee, College of Computing. Academic Years 2004–2005 and 2005–2006.
13. Steering Committee, Core Computing Division (observer), College of Computing. Academic Years 2004–2005.
14. Steering Committee, Computing & Networking Services (CNS), College of Computing. Academic Year 2004–2005.

C. Special Assignments at Georgia Tech

1. School Associate Chair, School of Computer Science, College of Computing, January 2015–December 2017.
2. Co-chair of UROC (Undergraduate Research Opportunities in Computing), College of Computing, 2004–present.
3. Area Coordinator, Software Methodology & Engineering, College of Computing, 2004–2007.

D. Member of Ph.D. Examining Committees

Ph.D. Qualifiers Committees – Georgia Tech

Sangmin Park
College of Computing
Advisor(s): Mary Jean Harrold

Raul Santelices
College of Computing
Advisor(s): Mary Jean Harrold

Chris Parnin
College of Computing
Advisor(s): Spencer Rugaber

George Baah
College of Computing
Advisor(s): Mary Jean Harrold

William Halfond
College of Computing
Advisor(s): Alessandro Orso

Saswat Anand
College of Computing
Advisor(s): Mary Jean Harrold and Alessandro Orso

Christoph Csallner
College of Computing
Advisor: Yannis Smaragdakis

Yi Zhang
College of Computing
Co-advisors: Mary Jean Harrold and Alessandro Orso

Ph.D. Examining Committees – Internal

Byoungyoung Lee
College of Computing
Advisor(s): Taesoo Kim and Wenke Lee

Sangho Lee
College of Computing
Advisor(s): Santosh Pande

Hina Shah
College of Computing
Advisor(s): Mary Jean Harrold and Nancy Nersessian

Chris Parnin
College of Computing
Advisor(s): Spencer Rugaber

George Baah
College of Computing
Advisor(s): Mary Jean Harrold

Saswat Anand
College of Computing
Advisor(s): Mary Jean Harrold

Raul Santelices
College of Computing
Advisor(s): Mary Jean Harrold

James Jones
College of Computing
Advisor: Mary Jean Harrold

Christoph Csallner
College of Computing
Advisor: Yannis Smaragdakis

Mohamed Mansour
College of Computing
Advisor: Karsten Schwan

Ph.D. Examining Committees – External

Tomasz Kuchta
Imperial College London
Title: Enhanced Symbolic Execution for Patch Testing and Document Recovery
Advisors: Cristian Cadar

Casper Svenning Jensen
Aarhus University
Title: Automated Testing of Event-Driven Applications
Advisors: Anders Møller

Qi Dawei
National University of Singapore
Title: Software Regression Localization Via Semantic Analyses
Advisors: Abhik Roychoudhury and Zhenkai Liang

Nadia Alshahwan
University College London
Title: Utilizing Output in Web Application Testing
Advisor: Mark Harman

Ali Mesbah
Delft University of Technology
Title: Ajaxifying Classic Web Applications
Advisor: Arie van Deursen

Murali Krishna Ramanathan
Department of Computer Science, Purdue University
Title: Path-aware Analysis of Program Invariants
Co-advisors: Suresh Jagannathan and Ananth Grama

Christoph Csallner
School of Computer Science, Georgia Tech
Title: Combining Over- and Under-approximating Program Analyses for Automatic Software Testing
Advisor: Yannis Smaragdakis

Matthew Rutherford
Computer Science Department, Univerisity of Colorado at Boulder
Title: Adequacy Criteria for System-Level Testing of Distributed Applications
Co-advisors: Alex Wolf and Antonio Carzaniga

E. External Member of Masters Examining Committees

None.

E. Consulting and Advisory Appointments

1. Member of the Independent Evaluation Team for the DARPA Application Community program, May 2006 to May 2010.
2. Member of the Advisory Board of Reflective (http://www.reflectivecorp.com/), January 2006 to date.
3. External member of the DARPA-sponsored Information Science and Technology (ISAT) study on "Trustable Deployed Adaptive Systems," January 2006 to August 2006.

F. Research Project Reviewer

1. National Science Foundation. Panelist for proposal review panel, Spring 2017.
2. National Science Foundation. Panelist for proposal review panel, Spring 2016.
3. National Science Foundation. Panelist for proposal review panel, Fall 2015.
4. National Science Foundation. Panelist for proposal review panel, Spring 2015.
5. National Science Foundation. Panelist for proposal review panel, Fall 2013.
6. National Science Foundation. Panelist for proposal review panel, Spring 2010.
7. National Science Foundation. Panelist for proposal review panel, Fall 2009.
8. National Science Foundation. Panelist for proposal review panel, Spring 2007.
9. National Science Foundation. Panelist for proposal review panel, Fall 2003.
10. NASA/EPSCoR. Research Grant Program Reviewer. April 2003.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Invited Conference Session Chairmanships

1. IEEE International Conference on Automated Software Engineering (ASE 2013).
2. ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2013).
3. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2013).
4. ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2012).
5. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2012).
6. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2011).
7. IEEE International Conference on Software Testing, Verification and Validation (ICST 2011).
8. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2010).
9. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2009).
10. European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2009).
11. ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE 2008).
12. IEEE International Conference on Automated Software Engineering (ASE 2008).
13. IEEE International Conference on Automated Software Engineering (ASE 2007).
14. European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2007).
15. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2007).
16. IEEE and ACM International Conference on Automated Software Engineering (ASE 2006).
17. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2006).
18. IEEE and ACM International Conference on Automated Software Engineering (ASE 2005).
19. European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2005).
20. IEEE and ACM-SIGSOFT International Conference on Software Engineering (ICSE 2004).
21. ACM-SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2004).

A. Patents

1. Title: Methods and Systems for Testing Mobile Applications for Android Mobile Devices
   Patent No.: US10296444B1
   Inventors: S. Roy Choudhary, M. Fazzini, and A. Orso
   Current Assignee: Georgia Tech Research Corp.
   Publication Date: 2019-05-21

B. Editorial and Reviewer Work for Technical Journals and Publishers

1. Editorial work:

   - Associate Editor for IEEE Transactions on Software Engineering (TSE), December 2019 to date.
   - Associate Editor for ACM Transactions on Software Engineering and Methodology (TOSEM), March 2008 to March 2014.
   - Board Member for Elsevier's Information and Software Technology Journal, May 2005 to December 2011.

2. Reviewer for:

   - ACM Transactions on Software Engineering and Methodology (TOSEM).
   - IEEE Transactions on Software Engineering (TSE).
   - Journal of Software Testing, Verification and Reliability (STVR).
   - Automated Software Engineering Journal (ASE).
   - International Journal of Applied Intelligence.
   - Distributed and Parallel Databases.
   - 2004 IEEE International Conference on Software Engineering (ICSE 2004).
   - 2004 ACM International Symposium on Software Testing and Analysis (ISSTA 2004).
   - 2002 IEEE International Conference on Software Engineering (ICSE 2002).
   - 2002 ACM International Symposium on Software Testing and Analysis (ISSTA 2002).
   - 2000 European Conference on Object-Oriented Programming (ECOOP 2000).

V. OTHER CONTRIBUTIONS

A. Invited Talks

1. "Users Beware: Preference Inconsistencies Ahead". Invited Talk at the Innovations in Software Engineering Conference, ISEC 2017, Jaipur, India, January 2017 (together with my student F. Behrang and my collaborator M. Cohen).
2. "Automated Debugging: Are We There Yet?". Meeting of the IFIP WG 2.4 on Software Implementation Technology, Asilomar, CA, USA, February 2014.
3. "Field Failure Reproduction Using Symbolic Execution and Genetic Programming". 30th CREST Open Workshop on Search Based Software Testing (SBST) and Dynamic Symbolic Execution (DSE), University College London, London, UK, January 2014.
4. "Automated Debugging: Are We There Yet?". IMDEA Software Institute, Madrid, Spain, December 2013.
5. "Software Testing and Debugging". Universidad Politecnica de Madrid, Madrid, Spain, December 2013.
6. "Automated Debugging: Are We There Yet?". MSR's Software Engineering Innovation Foundation Workshop, Rio de Janeiro, Brasil, November 2013.
7. "Automated Debugging: Are We There Yet?". Haifa Verification Conference, Haifa, Israel, November 2013 (in connection with the HVC Award).
8. "Automated Debugging: Are We There Yet?". University of Southern California, Los Angeles, CA, September 2013.
9. "Automated Debugging: Are We There Yet?". Google, Santa Monica, CA, September 2013.
10. "In-house Debugging of Field Failures". Coverity, May 2013.
11. "Software Testing and Debugging". Pan American Software Quality Institute, Puntarenas, Costa Rica, July 2013.
12. "How Can I Get My Paper Accepted at a Top SE Conference?" Latin American School on Software Engineering. Rio de Janeiro, Brasil, July 2013.
13. "In-house Debugging of Field Failures". Politecnico di Milano, Italy, Department of Electronics and Informatics, July 2012.
14. "BugRedux: In-house Debugging of Field Failures". 52nd IFIP WG 2.4 Meeting, Vadstena, Sweden, May 2012.
15. "BugRedux: In-house Debugging of Field Failures". Mysore Park Workshop on The Future of Debugging, Mysore, India, February-March 2012.
16. "Testing Evolving Software". First Workshop on Validation Strategies for Software Evolution, Tallin, Estonia. March 2012.
17. "Automated Debugging: Are We There Yet?". UBA – University of Buenos Aires, Buenos Aires, Argentina. November 2011.
18. "Testing and Analysis of Deployed Software". IISc – Indian Institute of Science, Department of Computer Science and Automation, Bangalore, India. August 2011.
19. "Automated Debugging: Are We There Yet?". MSR – Microsoft Research India, Bangalore, India. August 2011.
20. "Testing Modern Evolving Software". TCS – Tata Consultancy Services, Pune, India. August 2011.

21. "Automated Regression Testing of Modified Software". Dagstuhl Seminar on Self-Repairing Programs. February 2011.

22. "Testing Evolving Software". Stellenbosch University. May 2010.

23. "Advanced Debugging Techniques for Modern Software". University of California, Santa Barbara, January 2010.

24. "Improving Web Application Security and Reliability through Program Analysis". IBM Research, India, August 2009.

25. "Improving Web Application Security and Reliability through Program Analysis". Delft University of Technology, June 2009.

26. "Web Application Analysis and Testing". Universität Zürich, Institut für Informatik, September 2008.

27. "Testing y análisis de Web Application (in Castilian)". University of Buenos Aires, Departamento de Computación, July 2008.

28. "Web application analysis and testing". Saarland University, Computer Science Department, June 2008, Saarbrücken, Germany.

29. "Web Application Analysis and Testing". Amazon.com, June 2008, Seattle, WA, USA.

30. "Automated Support for Testing and Maintenance of Exception Handling Constructs". Bellairs workshop On Software Analysis for Recommendation Systems (SARS 2008), McGill University's Bellairs Research Institute, Barbardos, February 2008.

31. "Dynamic Tainting and its Application to Memory Protection". Purdue University, Department of Computer Science, January 2008.

32. "Improving the Security of Web Applications Using Static and Dynamic Analysis". University of Lugano, Switzerland, April 2007.

33. "(Re)Testing Evolving Software". Bellairs workshop On Automated Techniques for Software evolution (BOATSe), McGill University's Bellairs Research Institute, Barbardos, March 2007.

34. "Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation". University of Southern California, Los Angeles, CA, March 2007.

35. "Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation". Google, Santa Monica, CA, March 2007.

36. "Improving SW Quality through Continuous Monitoring". Analysis, and Testing, DARPA-sponsored Information Science and Technology (ISAT) study on "Trustable Deployed Adaptive Systems." Carnegie Mellon University, Pittsburgh, PA, March 2006.

37. "Combining Static Analysis and Runtime Monitoring to Counter SQL-Injection Attacks". ARO-HS ARPA invitational Malware Detection Workshop. SRI International, Arlington, VA, August 2005.

38. "Analysis and Testing of Deployed Software". University of Massachusetts-Amherst, April 2004.

39. "Analysis and Testing of Deployed Software". University of Texas at Austin, Department of Electrical and Computer Engineering, April 2004.

40. "Analysis and Testing of Deployed Software". IBM Research, April 2004.

41. "Analysis and Testing of Deployed Software". Purdue University, Department of Computer Science, March 2004.

42. "Analysis and Testing of Deployed Software". University of California, Irvine, School of Information and Computer Science, March 2004.

43. "Analysis and Testing of Deployed Software". North Carolina State University, Department of Computer Science, February 2004.

44. "Improving Dynamic Analysis through Partial Replay of Users' Executions". Dagstuhl Seminar on Understanding Program Dynamics, December 2003.

45. "Regression Testing of Object-Oriented Software". Politecnico di Milano, Italy, Department of Electronics and Informatics, December 2002.

46. "Regression Test Selection for Java Software". University of Colorado at Boulder, Department of Computer Science, October 2002.

47. "Object-Oriented Testing Techniques". University of Illinois at Chicago, EECS Department, September 1999.

B. Participation in U.S.-Funded Projects

1. National Science Foundation Award 0196145, Experimental Systems Program, Scalable Program-Analysis-Based Testing and Maintenance: Infrastructure and Experimentation. PIs: Mary J. Harrold (Georgia Tech), Adam A. Porter (University of Maryland, College Park), Gregg Rothermel (Oregon State University). December 1999 – August 2003.

C. Participation in European-Union-Funded Projects

1. *TWO*. ESPRIT Project, 1998-2001. Project goal: To develop a tool supporting automatic generation of test cases for both C and C++ systems, based on static analysis techniques.

2. *Promote*. ESSI Project, 1998-2000. Project goal: To redefine the testing process of a big-size company, based on the use of both static and dynamic metrics to forecast the testing effort and the cost-effectiveness of testing strategies.

3. *UseGat*. ESPRIT Project, 1996-1997. Project goal: To demonstrate the suitability and viability of combining structured and formal methods, in particular SA/RT and VDM, to develop real large-scale applications.

4. *IDERS*. ESPRIT Project, 1994-1996. Project goal: To develop methodologies and tools to support the complete visibility of software artifacts, during the whole development cycle, and to design a software process well suited for real-time systems.

APPENDIX B

List of Materials Considered

Exhibit No.	Description
Exhibit-2001	Opinion and Order, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va. Oct. 5, 2020)
Exhibit-2002	Definition of "Safe" [available at https://developer.mozilla.org/en-US/docs/Glossary/safe]
Exhibit-2003	Centripetal's Opening Brief, Appeal No. 20-1635
Exhibit-2004	Cisco's Response Brief, Appeal No. 20-1635
Exhibit-2005	Centripetal's Reply Brief, Appeal No. 20-1635
Exhibit-2006	Cisco's Sourcefire Invalidity Chart
Exhibit-2007	Data Exfiltration: How Data Gets Out [available at https://www.computerworld.com/article/2520483/data-exfiltration--how-data-gets-out.html]

Exhibit-2008	A. Giani et al. , "Detection of Covert Channel Encoding in Network Packet Delays," Tech. Rep. TR2005-536, Department of Computer Science, Dartmouth College, Nov. 2005, http://www.ists.dartmouth.edu/library/149.pdf
Exhibit-2009	Trial Transcript of May 7, 2020, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2010	ESG White Paper – Centripetal Networks Threat Intelligence Gateway, by Tony Palmer (May 2018)
Exhibit-2011	American Banker article, "Top 10 FinTech Companies to Watch," published November 6, 2013
Exhibit-2012	Gartner – Cool Vendors in Security for Technology and Service Providers, 2017, published May 4, 2017
Exhibit-2013	Stanley Chincheck, US Naval Research Laboratory, Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day
Exhibit-2014	Trial Transcript of May 11, 2020, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2015	Cisco Security Analytics, PTX-995, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)

Exhibit-2016	Cisco Enterprise Silicon - Delivering Innovation for Advanced Networking, PTX-1303, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2017	Cisco 1000 Series Integrated Services Routers, PTX-175, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2018	Cisco ASR 1000 Overview, PTX-1313, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2019	Cisco Polaris Software System Functional Specification, PTX-1276, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2020	CiscoCognitive Threat Analytics, PTX-576, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2021	Cisco Catalyst 9000 Switches, PTX-1262, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2022	Network as a Sensor and Encrypted Traffic Analytics Integration, PTX-1280, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2023	Digital Network Architecture for Securing Enterprise Networks, PTX-563, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)

Exhibit-2024	Rapid Threat Containment in SD-Access, PTX-1356, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2025	Cisco Identity Services Engine, PTX-1326, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit 2029	PTX-1215, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2031	CleanINTERNET Components [available at https://www.centripetal.ai/products]
Exhibit-2032	Cisco Ordered To Pay $1.9B In Centripetal Patent Trial, Law360
Exhibit-2033	RuleGATE 2000 Gateway
Exhibit-2036	Email from TK Keanini, PTX-1326, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2037	Network Survivability, Recovery & Reconsitution [available at https://www.sbir.gov/sbirsearch/detail/12493]

EXHIBIT 2027

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Ex Parte* Reexamination of		U.S. Patent No. 9,686,193
Control No.:	90/014,476	Group Art Unit: 3991
Filed:	March 19, 2020	Confirmation No.: 1013
Patent Owner:	Centripetal Networks, Inc.	Examiner: Minh T. Nguyen
For U.S. Patent No.:	9,686,193 – FILTERING NETWORK DATA TRANSFERS	

Submitted Electronically

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF JONATHAN ROGERS
IN SUPPORT OF CENTRIPETAL'S RESPONSE TO NON-FINAL OFFICE ACTION

I, Jonathan Rogers, declare:

1. I am over the age of 18 and make this declaration of my own personal knowledge.

2. I have personal knowledge of the facts stated in this Declaration and can testify competently to those facts. I make this Declaration in support of Centripetal Networks, Inc.'s ("Centripetal") Patent Owner Response.

3. I am currently the Chief Operating Officer (COO) at Centripetal. I am responsible for overseeing all operations of the business, including product and service delivery and solution design to our end customers. I am familiar with Centripetal's licensing practices and assist in the licensing of Centripetal's patented technologies.

4. I joined Centripetal in May 2010 as its fourth employee. Prior to joining Centripetal, I earned a Bachelor's in Electrical Engineering from Boston University, and a Master's in Business with a concentration in finance from the University of Maryland. After graduating from college, I entered the United States Navy and was commissioned as an officer in the Navy. There, I was a part of a Navy security group called Cryptology and Information Warfare that protects naval military communications and exploits adversary communications. I was later stationed as a military officer at the National Security Agency (NSA) working in the National Security Operations Center. After my tour in the Navy, I joined the Central Intelligence Agency and served as a technical intelligence officer in the Directorate of Science & Technology.

5. Centripetal won a series of competitive research & development contracts that were in excess of $1 million to perform the research that eventually led to the patented invention. As one example, Centripetal won a grant from the Department of Homeland Security to perform research into the problem of "enabl[ing] packet filtering devices to rapidly switch between large

security policies which are applied to high-speed packet interfaces." Ex. 2037. This was core to the development of the Centripetal product known as "RuleGATE" and its ability to protect against network infiltrations and exfiltrations.

6. As laid out in our successful award, our technology was critical to a solution that secures the Internet: A network protection service that addresses the problem of network survivability, rapid recovery, and reconstitution during attacks. The technology improved cyber security quality and effectiveness for critical U.S. networks and reduces cyber security costs.

7. Centripetal's patented technologies have garnered interest from and have been copied by other companies. In particular, starting in 2015, there were several meetings between Centripetal and Cisco, including meetings where Centripetal's products were explained and demonstrated. In January 2016, Centripetal and Cisco entered into a nondisclosure agreement to explore the possibilities of (1) jointly selling Centripetal and Cisco products and (2) a strategic investment by Cisco in Centripetal.

8. In February 2016, I, along with several other Centripetal employees, attended a Webex meeting with a group of top-level Cisco technologists. At this meeting, I gave a confidential and highly technical presentation about Centripetal's patented technologies, covering everything from our general technical approach to specific algorithmic techniques. I fielded a number of questions from Cisco's team about Centripetal's patents and proprietary algorithms. No deal was consequentially made between Centripetal and Cisco. It is my understanding that after all of these detailed meetings with Centripetal, Cisco released new version of its products a year and a half later on June 20, 2017, which incorporated Centripetal's patented technologies, including the technology disclosed in the '193 Patent.

9. I understand that, in October 2020, Cisco was found to have willfully infringed Centripetal's patents, including U.S. 9,686,193 Patent that is at issue in this reexamination proceeding. I testified as a witness at this trial and watched the entire trial as a corporate representative. Based on the facts that were elicited during trial, I understand that the judge determined that Cisco deliberately copied Centripetal's technology. Specifically, the judge found that Cisco met with Centripetal to express interest in Centripetal's proprietary technology, then appropriated the information it learned at those meetings and embedded the technology into its own products. The Judge's conclusion was that Cisco "willfully and egregiously" copied Centripetal and that "this was not a close call."

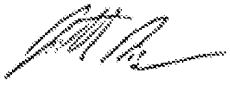
10. It is my understanding that Judge Morgan made the following specific findings of fact related to Cisco's copying of Centripetal products which I personally witnessed as I watched the trial:

- Centripetal's RuleGate product practices the '193 Patent.
- In 2015, Centripetal CEO Stephen Rogers had a meeting with Pavan Reddy, a Cisco employee, where Mr. Rogers disclosed Centripetal product offerings and the effectiveness of their solutions. Mr. Reddy and Mr. Rogers had a follow-up meeting in 2015, where Centripetal provided a demonstration of their system and explained why it was an effective method of cyber defense.
- As a result of these meetings, on January 26, 2016, Centripetal and Cisco entered into a nondisclosure agreement ("NDA"), requiring Cisco to keep Centripetal's confidential, proprietary or non-public information "strictly confidential" and "not use any Information in any manner . . . other than solely in connection with its consideration of" a possible partnership.
- After Cisco executed the NDA, Centripetal, on February 4, 2016, presented in a WebEx meeting detailed, highly sensitive, confidential and proprietary information about its patented technology and products to Cisco, including details of its patented technology for Centripetal's patents, including the '193 Patent. For example, Centripetal detailed how its "patented filter algorithms eliminate the speed and scalability problem," how its "patented system, live update, and correlation

technologies 'automate workflow' and how its "patented" "instant host correlation" conveys "real time analytics."

- After the WebEx meeting, Cisco's Engineer, TK Keanini, who attended the WebEx meeting, wrote an internal email, stating the team should "look at these algorithms" that Centripetal had and "study their [patent] claims."
- The next day, on February 5, 2016, Centripetal's Jonathan Rogers sent an e-mail to Cisco summarizing the WebEx meeting, noting that Cisco "seemed to hone in on our filter technology and algorithms. The algorithms are a significant networking technology with broad application that we've productized for security. There were also a few questions on our patents..."
- There were a number of follow up meetings with Cisco, including a request from Cisco's security architect, Joseph Muniz, who was very interested in Centripetal's patented technology. He requested and received a demonstration of Centripetal's patented RuleGate product, which he described in an online blog that educates Cisco employees entitled "Cool Tool: Centripetal Networks RuleGate – Threat Intelligence Tool," and where he stated, "I found this tool to be a pretty cool new approach to leveraging threat data."
- In November and December 2016, Cisco had several meetings with Oppenheimer about Centripetal, pursuant to Centripetal's engagement with Oppenheimer to evaluate companies who were interested in making a strategic investment in Centripetal. In December 2016, Oppenheimer presented to Cisco additional information about Centripetal, including a list of Centripetal's patents issued at the time, product offerings that practice the patents, and a highly sensitive, detailed technical disclosure which detailed the core RuleGate functionalities covered by the Asserted Patents.
- After all of these detailed meetings with Centripetal, Cisco released its "network of the future" products on June 20, 2017, which incorporated Centripetal's patented technology.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on January 25, 2020 in Portsmouth, NH.



Jonathan Rogers

EXHIBIT 2028

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Ex Parte* Reexamination of		U.S. Patent No. 9,686,193
Control No.:	90/014,476	Group Art Unit: 3991
Filed:	March 19, 2020	Confirmation No.: 1013
Patent Owner:	Centripetal Networks, Inc.	Examiner: Minh T. Nguyen

For U.S. Patent No.: 9,686,193 – FILTERING NETWORK DATA TRANSFERS

Submitted Electronically

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION OF DR. SEAN MOORE
IN SUPPORT OF CENTRIPETAL'S RESPONSE TO NON-FINAL OFFICE ACTION

I, Sean Moore, Ph.D. declare:

1. I am over the age of 18 and make this declaration of my own personal knowledge.

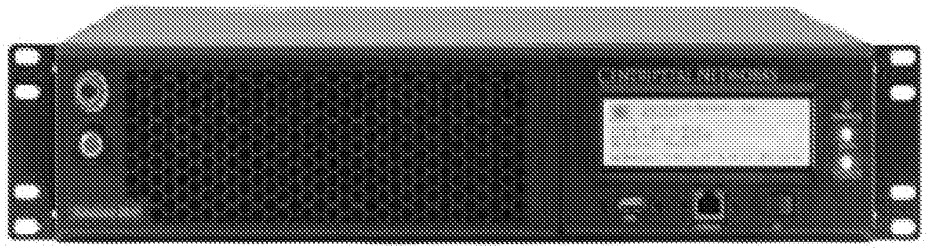
2. Since 2010, I have been Chief Technology Officer ("CTO") at Centripetal Networks, Inc. ("Centripetal"). Before joining Centripetal, I obtained a B.S. degree in Electrical Engineering in 1983, a M.S. degree in Mathematics in 1990, a M.S. degree in Computer Science in 1993, and a Ph.D. in Computer Science in 1994. Prior to starting at Centripetal, I also worked for sixteen (16) years at different companies developing new networking, communications, web and machine learning technologies, including at BBN Technologies.

3. I joined Centripetal (as its third employee) because I wanted to be part of a company whose intent and purpose was to solve the Internet cyber security problem once and for all. Our goal was to improve the security of the Internet via a new disruptive method and approach since existing approaches in the network security space were not working. In particular, Centripetal focuses on solving network security and network protection problems by "operationalizing" cyber threat intelligence (CTI). Our idea was to take cyber threat intelligence and somehow transform it so that it can be applied to live Internet traffic to secure the Internet, by essentially shutting down the cybercriminal communications and their attacks. The step of transforming raw CTI to operationalized CTI has been difficult. We had to develop new mathematics, new algorithms, and new technologies that could apply this operationalized CTI to live Internet traffic to stop cyber-attacks. In the end, Centripetal created a revolutionary network appliance marketed as RuleGATE™ (and other products) that is a CTI enforcement platform and threat intelligence gateway on which these operationalized CTI technologies are built.

4. As CTO, I lead Centripetal's product development, research and development, and intellectual property protection. Centripetal markets and sells a threat intelligence gateway

system that can be deployed to protect a network and that has various components that can be configured to implement a Network Protect System where those components (e.g., RuleGATE described below) are located at network boundaries and are applying dynamic threat intelligence to network traffic. Ex. 2031.

5. Specifically, Centripetal's threat intelligence gateway system includes three components: RuleGATE, Advanced Cyber Threat, and QuickTHREAT. The RuleGATE product component of the system (which is also offered as a security-as-a-service solution under CleanINTERNET), is a high-performance threat intelligence gateway designed to protect networks from a broad array of threats. RuleGATE instances can be inserted in-line at physical or virtual Internet connections and can be deployed in public or private clouds, on virtual infrastructures, and on a variety of platforms and appliances to enforce intelligence-based security policies, detect possible threats, and stop network attacks. A physical RuleGATE appliance is shown below:



Ex. 2033. In particular, the RuleGATE system can observe in-transit packets to recognize and prevent exfiltrations. The Advanced Cyber Threat ("ACT") system collects and manages millions of unique threat indicators from a combination of Centripetal sources and Centripetal partners. Security expertise is distributed to the gateway system in the form of units of threat intelligence. The QuickTHREAT system is a cyber-threat event analytics system that enables, in part, system administrators to view in real-time the active threat environment in their networks.

One way to summarize Centripetal's product offerings is that CleanINTERNET is a network protection service that Centripetal provides its clients using the RuleGATE platform, the ACT system, and the QuickTHREAT user interface.

6. Centripetal's products prevent a category of cyber-attack known as data exfiltration. Data exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer. For example, a cyber-criminal might steal data such as usernames/passwords, personal information, financial data, or corporate trade secrets, and exfiltrate that data out from a computer or network and into their possession. This problem has been known in the industry since at least 2006, and has been discussed in research papers and trade periodicals, but it was still an ongoing problem. *See* Exs. 2007, 2008 (2006 academic paper describing data exfiltrations at length).

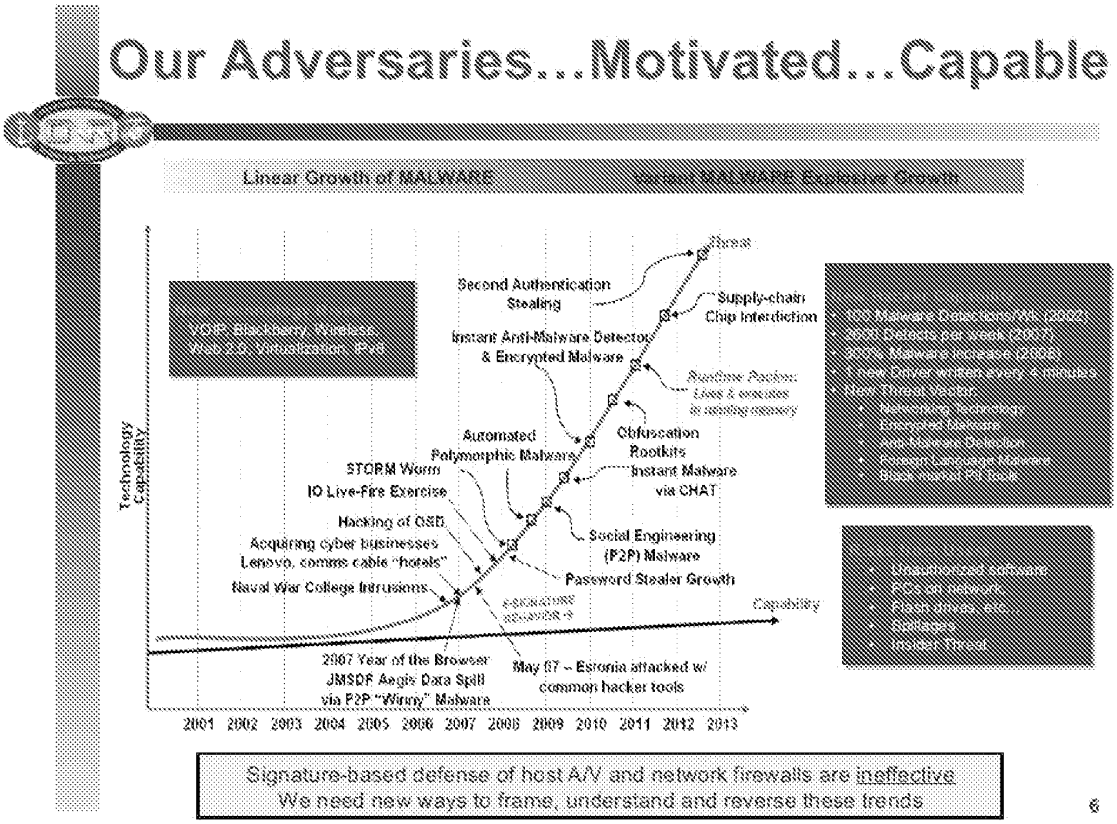
7. We realized that the problem of exfiltrations has been difficult to address because many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the web, that often appear to conventional cyber defense systems as normal network behavior. We also realized that the exfiltration threat was difficult to solve because conventional solutions would block all traffic including legitimate business traffic, which would impede productivity. In addition, conventional cyber defense systems were inadequate and could not scale sufficiently to counter a cyber threat; for example, with respect to traffic volumes, network link speeds, network performance (for example, while still staying within latency and packet loss requirements), network usage policy enforcement, and so forth.

8. With respect to the lack of a sufficiently viable solution, in 2010, the Office of Naval Research announced a program named Proactive Network Defense and Information

Assurance (CND/IA) (Research Opportunity No. 10-004) for funding research into solving the computer network defense program. In connection with this program, the United States Naval Research Laboratory hosted an "Industry Day" event where Stanley Chincheck, the Director for the Navy's Center for High Assurance Computer Systems, explained in a presentation that previous approaches for protecting computer networks could not keep up with changes in the techniques of malware and malicious actors. Ex. 2013 at 5.

9. In particular, a chart found on page 6 of that presentation is illustrative of the Computer Network Defense program as a whole. The chart's horizontal axis is time, demarcated in years (from 2000 through 2013) including years 2010-2013 as projected future time, and the chart's vertical axis represents technological capability. There are two plot graphs in this chart: red and black. The red line represents the technological capability of cyber criminals and the attacks they launch over time. As shown, this graph moves linearally until around the year 2005 or 2006, and then soars, to indicate the explosive (super-linear) growth in the technological capability of cyber criminals. The black line represents the technology capability of computer network defense systems. This graph is nearly horizontal, indicating the flat progress of

conventional network defense systems and their inability to keep up with cyber criminals.



Ex. 2013 at 6. As stated in the yellow box, this chart demonstrated that "[s]ignature-based defense of host A/V and network firewalls are ineffective… we need new ways to frame, understand and reverse these trends." The failure of signature behavior-based systems, such as the ones disclosed in the Sourcefire reference cited by the Examiner, to keep up with emerging threats demanded new solutions. Accordingly, the need for a scalable solution to the problem of exfiltration attacks was recognized by at least 2010.

10. Conventional network defense systems also failed to provide proactive network protection that could scale to larger networks and meet emerging threats. This was recognized in a white paper entitled "Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led Enforcement." Ex. 2010 at 1. In particular, the

ESG Paper recognized that "[t]he promise of cyber threat intelligence (CTI) for cyber-defense has been talked about for years" and that the manual processes most enterprises have in place for using CTI "don't scale well and the forensic focus on security emergencies can cause enterprises to miss out on the benefits of proactive, preventive intelligence-based defense." ESG Paper at 3. The ESG Paper further acknowledged that "[t]he end goal of a threat intelligence program is defense in advance of an event" and identified that "multiple challenges stand in the way of operationalizing threat intelligence in a high performance, and high-fidelity way," including "[l]ack of automation," the inability to use feeds "in a meaningful way to live network traffic and even less frequently applied inline for a protective benefit," and the ability to "turn[] CTI into actionable insight." Ex. 2010 at 4.

11. Centripetal's products, including the RuleGATE and CleanINTERNET products, address this problem of exfiltrations because they provide techniques for filtering data between different networks in a manner that greatly curtails the risk of data exfiltration by detecting the threat earlier and acting in response, if desired, while still preserving the flow of normal legitimate network traffic without disruption. It is my understanding that one reason that traditional cybersecurity solutions were ineffective in preventing the exfiltration of data because they required time-expensive inspection of a collection of multiple packets (sometimes referred to as deep packet inspection and/or signature matching) vs. single packets on significant amounts/volumes of high-speed network traffic. Also, prior attempts by others to prevent data exfiltration were often too coarse or overbroad because they would simply block all traffic to/from a given network, regardless of the actual threat, resulting in negative impact to the subject computer network and ultimately to business operations.

12. Centripetal's products allow for deriving network threat intelligence data (from multiple sources) and "operationalizing" cyber threat intelligence (CTI) for protecting networks. RuleGATE leveraged CTI by applying operators only to those packets meeting specific CTI-derived criteria rather than by blocking any and all traffic. This two-stage process succeeds where traditional, overbroad techniques failed because it permits normal business network traffic, like allowing a web browser to download web pages hosted by web servers, but still prevents data exfiltrations. For example, RuleGATE could check outbound traffic for certain types of data transfers that were directed to threat resources (i.e., exfiltrations) and then block those while allowing data transfers to benign/non-threat resources. This is accomplished by applying particular "operators" to different types of traffic based on the criteria of the packets.

13. The ESG Paper discussed above contains industry praise for Centripetal's innovative products. The ESG Paper discussed above praised Centripetal's Threat Intelligence Gateway (TIG) as having "the highest performance network filter that ESG has tested or seen in action to date." Ex. 2010 at 7. The ESG Paper further lauded Centripetal's TIG ability to "deliver[] more than is possible with firewalls and IPS [e.g., Sourcefire] systems", pointing to Centripetal's RuleGATE and CleanINTERNET products:

> Centripetal Networks' **CleanINTERNET** intelligence-led managed security service using their **RuleGATE** enforcement point provides customized threat intelligence filtering designed to significantly reduce security event volume and workload in the enterprise. Centripetal shields the network and dynamically monitors for advanced threats using intelligence. **Centripetal's goal is nothing less than the transformation of CTI into protective action at scale. Centripetal does this by converting indicators to rules that drive actions** across a risk spectrum, i.e., logging, content capture, mirroring, redirection, shielding, and advanced threat detection.
>
> Simply put, Centripetal delivers more than is possible with firewalls and IPS systems, which aren't designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds. ESG watched as Centripetal

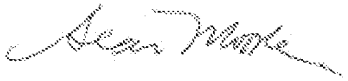
> Networks' Threat Intelligence Gateway solution processed over 140 Gbps of network traffic at wire speed; distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules. Each complex filtering rule contained at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state. With intelligence enforcement there can be **no presumption of insider trust** so traditional filters' state assumptions are invalid.

Ex. 2010 at 7 (emphasis added).

14. Centripetal was recognized as an innovator by trade periodicals and analysts. For example, in May 2017, Gartner published its "Cool Vendors in Security for Technology and Service Providers," praising Centripetal as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds." Ex. 2012 at 5. As described in the Cool Vendors article, Centripetal's QuickThreat Gateway "currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously." *Id.* Centripetal Networks was also named one of American Banker's "Top 10 FinTech Companies to Watch" for 2014 because its Threat Intelligence Gateway, RuleGATE "has the potential to detect and deter rapidly changing cybersecurity threats on the fly." Ex. 2011 at 14.

15. I understand that, in October 2020, Cisco was found to have willfully infringed Centripetal's patents, including U.S. 9,686,193 Patent that is at issue in this reexamination proceeding. Ex. 2032. I testified as a fact witness at this trial. I understand that the judge determined that Cisco deliberately copied Centripetal's technology. Specifically, the judge found that Cisco met with Centripetal to express interest in Centripetal's proprietary technology, then appropriated the information it learned at those meetings and embedded the technology into its own products. Ex. 2032.

16. I have I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on January 25, 2020 in Portsmouth, NH.



Sean Moore

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re *Ex Parte* Reexamination of		U.S. Patent No. 9,686,193
Control No.:	90/014,476	Group Art Unit: 3991
Filed:	March 19, 2020	Confirmation No.: 1013
Patent Owner:	Centripetal Networks, Inc.	Examiner: Minh T. Nguyen

For U.S. Patent No.: 9,686,193 – FILTERING NETWORK DATA TRANSFERS

Submitted Electronically

Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

The following is intended to be fully responsive to the non-final Office Action mailed September 23, 2020.

I. INTRODUCTION

Centripetal Networks Inc. was founded in 2010 with one goal in mind—to solve the Internet security problem once and for all. In order to do this, Centripetal realized a completely different approach was needed than what had been done before, namely including specific techniques to prevent exfiltrations from company resources while ensuring that employees remained productive. Centripetal received numerous patents for its innovations, including U.S. Patent 9,686,193 ("the '193 Patent") which is at issue in this proceeding. A Notice of Intent to Issue a Reexamination Certificate, confirming the patentability of all claims of the '193 Patent, is appropriate for several reasons.

First, the Patent Office already determined that Sourcefire does not disclose an "operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer," as recited in each independent claim of the '193 Patent. *See* Ex. 1067. Thus, not only should this reexamination be terminated because the claims are nonobvious, but it should not have been ordered given that there is no "substantial new question of patentability and the Request violated 35 U.S.C. § 325(d). The claims are also nonobvious because a POSA would not have been motivated to modify Sourcefire to reach the particular exfiltration prevention technique recited in each of the independent claims by which the claimed operator is applied to packets leaving a first network bound for a second while not applying the operator to packets leaving the first network and bound for a third network..

Second, objective indicia confirm the nonobviousness of the '193 Patent. At the time of the invention there was a long-felt need for a solution to the exfiltration problem that did not involve essentially shutting down all Internet traffic. Centripetal solved this problem with its patented exfiltration prevention technique. Further, third-party requester, Cisco Systems, Inc. ("Cisco"), realized that Centripetal had invented something revolutionary and blatantly copied Centripetal's innovations found in the '193 Patent even though Cisco made and sold the Sourcefire system. After a lengthy bench trial in the District Court in the Eastern District of Virginia[1] ("the District Court case"), the Honorable Judge Coke Morgan[2] found as a matter of

[1] *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, Case No. 2:18-cv-00094-HCM-LRL (E.D. Va.).

[2] Judge Morgan is a very experienced judge, who has handled numerous patent cases over his nearly thirty years as a District Court judge.

fact that Cisco copied Centripetal's technology, which "was outlined and detailed to them by disclosure of the patents and multiple technical discussions and demonstrations." Ex. 2001 at 157. Thus, the objective indicia of nonobvious confirm the validity of the claims of the '193 Patent.

II. PREVIOUS PROCEEDINGS

The history of Cisco's unsuccessful challenges to the '193 Patent are extensive. Cisco filed a Petition for *Inter Partes* Review of the '193 Patent in Case No. IPR2018-01559 on August 21, 2018. *See* IPR2018-01559, Paper 1. Following Centripetal's Preliminary Response, the Board denied institution of the Petition, finding that Cisco had not demonstrated a reasonable likelihood that Sourcefire—the same reference cited against the claims in this reexamination—discloses the "operator" claimed in the '193 Patent. *See* IPR2018-01559, Paper 7 at 8–12. Specifically, the Board found that Cisco had not demonstrated that Sourcefire's "drop rules" could be equated with an "operator… configured to drop packets associated with [a] particular type of data transfer." *Id.* at 10–11. The Board also determined, correctly, that "the first operator refers to something other than the recited packet-filtering rule(s) because a different term is used, including within the same claim limitation." *Id.* at 11. After filing a Request for Rehearing, the Board once again found the claims not unpatentable, stating once again that it found Sourcefire's disclosure of "drop rules" inapplicable to the challenged claims. *See* IPR2018-01559, Papers 8 and 9. Because the Board already rejected the equation of "drop rules" and "drop operators" with the claimed "operator… configured to drop packets associated with [a] particular data transfer," the Request which applies the same rationale did not raise an SNQ.

Second, Cisco argued that Claims 18 and 19 of the '193 Patent were obvious over Sourcefire in the parallel District Court case between the parties. Ex. 2006. While Cisco dropped this ground before trial and after receiving Centripetal's expert's rebuttal to the ground of invalidity, Cisco proceeded with what it contended was a stronger invalidity ground at trial. Nonetheless, the District Court still upheld the validity of the '193 Patent claims holding that validity (and infringement) was not a close call. Ex. 2001 at 95–98.

III. SUMMARY OF ARGUMENTS

As explained in detail below, consistent with the Board's prior decision on this exact issue, and supported by the expert declaration of Dr. Alessandro Orso, the Sourcefire manual has no concept of an "operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer" or a "second operator configured to forward packets not associated with the particular type of data transfer."[3] In particular, the '193 Patent discloses an "operator," which is specified by (but separate from) the packet-filtering rule, and it must be "configured to drop packets associated with the particular type of data transfer" and a "second operator" that will "forward packets not associated with the particular type of data transfer."

Nor does Sourcefire disclose or render obvious any techniques for preventing a class of network threats known as "exfiltrations," particularly given that Sourcefire is an ***intrusion*** prevention/identification system, which is a different technology that "looks for malicious activity, and reports and/or takes actions based on detected malicious activity." Sourcefire at 34. Yet the language of the claims, wherein different rules and operators are applied to traffic exiting one network and destined for two different networks, mark the claims as explicitly directed to preventing exfiltrations rather than intrusions. Thus, the claims subject to reexamination are patentable.

Objective indicia of nonobviousness confirm the patentability of the claims subject to reexamination. The techniques disclosed and claimed in the '193 Patent satisfied a long-felt need for a solution to the exfiltration problem, which had flummoxed security experts for years before Centripetal's '193 Patent. Further, after witnessing Centripetal's solution to this long-standing problem, Cisco copied the technology. Specifically, Judge Morgan determined that Cisco had met with Centripetal for two years where Centripetal disclosed its patents and confidential information regarding its patent practicing products to Cisco under a Nondisclosure Agreement. Cisco's internal emails revealed that Cisco copied Centripetal's technology and its patents, even stating that it needed to "study [the] [] claims" of Centripetal's patents, including the '193 Patent. Ex. 2001 at 150. After stringing Centripetal along for years, Cisco abruptly

[3] Notably, an entirely different claim limitation was at issue in IPR2018-01436, regarding the '552 Patent, so Centripetal is not estopped from raising these arguments herein. *See* § VII.A.1, *infra*.

ended the dialog with Centripetal and immediately released a copycat version of Centripetal's products. The Court further found that "Cisco's systems mirrors the functionality of the Centripetal patents" and described in great detail Cisco's copying. Ex. 2001 at 157 (citation omitted). Objective evidence of a long-felt need and Cisco's copying of Centripetal's solution to this need confirm the patentability of the claims subject to reexamination.

Additionally, this reexamination should be terminated because Cisco's challenge does not present an SNQ. This is Cisco's ***third attempt*** to challenge patentability of the '193 Patent with the same prior art. In addition to the unsuccessful validity attack before the District Court, Cisco also presented the same prior art in *inter partes* review proceedings. Cisco has no argument that would justify the upheaval of decisions from Examiner Nguyen, Justice McNamara, Justice Lee, Justice Pinkerton, and District Court Justice Morgan, all of whom confirmed that the validity of the '193 Patent based on the same prior art. In fact, the prior Patent Office proceedings involving the '193 Patent ***preclude*** the finding of a Substantial New Question of Patentability ("SNQ") in this case. In particular, an SNQ cannot be found where the same issue of patentability was already decided in a concluded examination or review of the patent, and the Proceeding in IPR2018-01559 is just such a "concluded examination" because it is a "contested Office proceeding which has been concluded and which involved the patent." MPEP § 2242(I). In that concluded examination, the Office considered and rejected the argument that Sourcefire teaches an "operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer." Ex. 1067 at 8–12. Cisco has not raised any SNQ here, so this reexamination should be terminated.

Similarly, the Request should have been rejected pursuant to 35 U.S.C. § 325(d) under the PTAB's precedential caselaw and should be terminated now. This case squarely implicates § 325(d) because the exact same art was previously presented to the Office. *See* 35 U.S.C. § 325(d) (a reexamination Request may be denied when the same prior art or arguments were previously presented to the Office). There is no indication that the Examiner either considered the Office's precedential opinions concerning § 325(d) or brought any such issues "to the appropriate SPRS or the Director of the CRU." MPEP § 2242.

Finally, Centripetal respectfully files herewith a true and correct copy of the Opening and Reply Briefs filed in its appeal to the Federal Circuit of the Board's Final Written Decisions in IPR2018-01436 and IPR2018-01437. Exhibits 2003 and 2004. This appeal concerns two

patents related to the '193 Patent[4] and raises at least one issue that would be dispositive in this case, *i.e.* whether Sourcefire is a publicly accessible printed publication. *See* Exhibit 2003 at 8–9, 13, and 15–21; Exhibit 2004 at 3–8. Centripetal respectfully preserves and does not waive the arguments made in the Opening Brief in this reexamination.

IV. STATUS

A. Status of Claims

The patent under reexamination, U.S. Patent No. 9,686,193 ("the '193 Patent"), was granted on June 20, 2017, with twenty claims. Cisco sought reexamination of Claims 18 and 19 of the '193 patent. The Decision Granting Ex Parte Reexamination mailed May 1, 2020, found that a substantial new question was raised with respect to Claims 18 and 19.

V. GROUNDS OF REJECTION

The Patent Office recited the following ground for its rejection:

Claims 1–20 of the '193 Patent were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Sourcefire in view of the knowledge of a POSA.

VI. SUMMARY OF THE CLAIMED INVENTION

As a means to continue its development of innovative cyber security products and solutions, Centripetal submitted and was awarded multiple patents, including the patent involved in this case, the '193 Patent. The '193 Patent generally discloses systems and methods for "filtering network data transfers." '193 Patent at Title. In particular, the '193 Patent discloses exemplary techniques for preventing exfiltrations:

> A category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent. A first cause is that many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web, that often appear to an observer (e.g., a conventional cyber defense system) as normal network behavior. A second cause is that typical network trust models, such as those used by network firewalls, interpret exfiltrations as trusted operations.

---

[4] The '193 Patent is a continuation of U.S. Patent 9,124,552 ("the '552 Patent"). *See* '193 Patent at 1:6–10. U.S. Patent No. 9,160,713 ("the '713 Patent) is also a continuation of the '552 Patent. *See* '713 Patent at 1:6–11.

'193 Patent at 1:24–34. As will be demonstrated below, Sourcefire is precisely the type of "conventional cyber defense system[]" distinguished in the '193 Patent, which views exfiltrations "as normal network behavior." '193 Patent at 1:24–34.

Centripetal's solution to the problem involves filtering data transfers ***out of*** a protected network (*i.e.* the "first network" in the challenged claims) and destined for one or more other networks (*i.e.* the second and third claimed networks):

> Enterprise X may desire to prevent cyber attacks (e.g., exfiltrations) from one or more of its networks (e.g., network 104 or 106). Accordingly, it may locate one or more packet security gateways ***at each boundary between its networks and one or more public interconnect networks*** (e.g., network 102), which may be utilized by a cyber criminal, such as organization Z, to attempt to remotely access its networks (e.g., network 104 or 106), and which may, for example, potentially be used to attempt to transfer data from one or more of its networks (e.g., network 104 or 106) to one or more networks affiliated with organization Z (e.g., network 108). For example, packet security gateway 110 may protect network 104 from one or more cyber attacks (e.g., exfiltrations) mediated by network 102 (e.g., the Internet), and packet security gateway 112 may protect network 106 from one or more cyber attacks (e.g., exfiltrations) mediated by network 102.

'193 Patent at 4:21–37 (emphasis added). Consistent with this disclosure, the '193 Patent's claims recite filtering packets received from one network and destined for two other networks, illustrating that the claims are directed to the exfiltration scenario discussed above. *See, e.g.*, '193 Patent at Claim 1 (applying different packet-filtering rules and operators depending on whether packets leaving the first network are destined for the second or third network).

One major problem with preventing exfiltrations is that exfiltrations are typically mediated by commonly used data transfer protocols like HTTP. Thus, in order to allow an employee of an organization to surf the web and conduct company business, the organization cannot simply block all traffic using the particular protocol. Nor is it sufficient to only allow traffic between trusted networks. Rather, the '193 Patent prevents exfiltrations by disallowing certain types of data transfers but only those destined for certain networks which would allow, for example, an employee to continue accessing the Internet but would prevent exfiltrations directed to access protected resources on a company's Intranet:

> Returning to the example described above, organization Z may own or operate network 108, and may have allocated network IP addresses 214.0.0.0/8 to network 108. Enterprise X may not have a business relationship with organization Z, and may therefore not consider network 108 to be trusted. While enterprise X could simply block all communications to networks that are owned or operated by

> organizations it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet. Enterprise X's employees, therefore, could not freely surf the Web, which may restrict the employees' ability to conduct business on behalf of enterprise X. By enforcing sets of rules similar to rule 6 312 that may apply operators like or similar to HTTP-EXFIL, enterprise X may enable its employees to freely surf the web and conduct company business, but may prevent one or more cyber attacks (e.g., HTTP-mediated exfiltrations).

'193 Patent at 7:21-37. These considerations explain why the claims require that different packet-filtering rules and different operators depending on whether traffic leaving the first network is destined for a second network or a third network.

As a concrete example, networks 104 and 106 of FIG. 1 represent networks commonly owned by a single Enterprise, whereas network 108 represents another network such as the Internet. '193 Patent at 4:11–37.

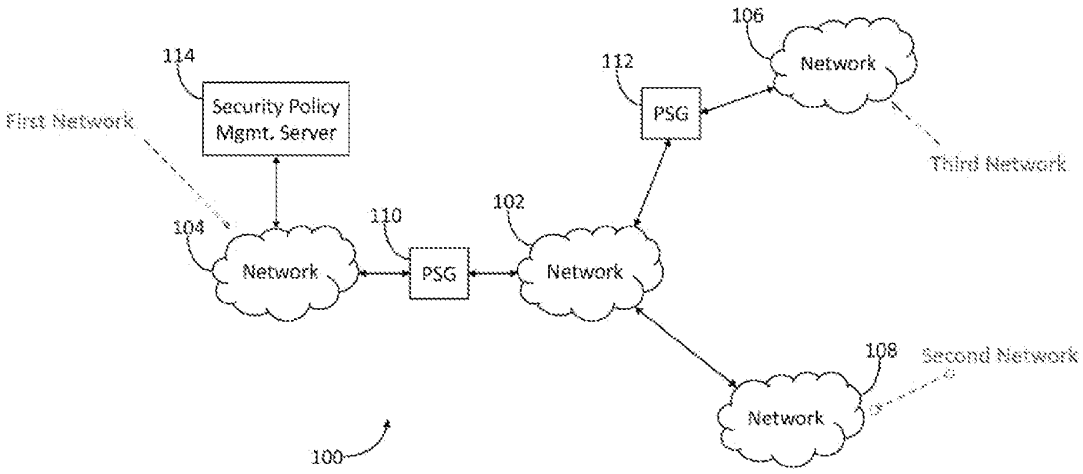
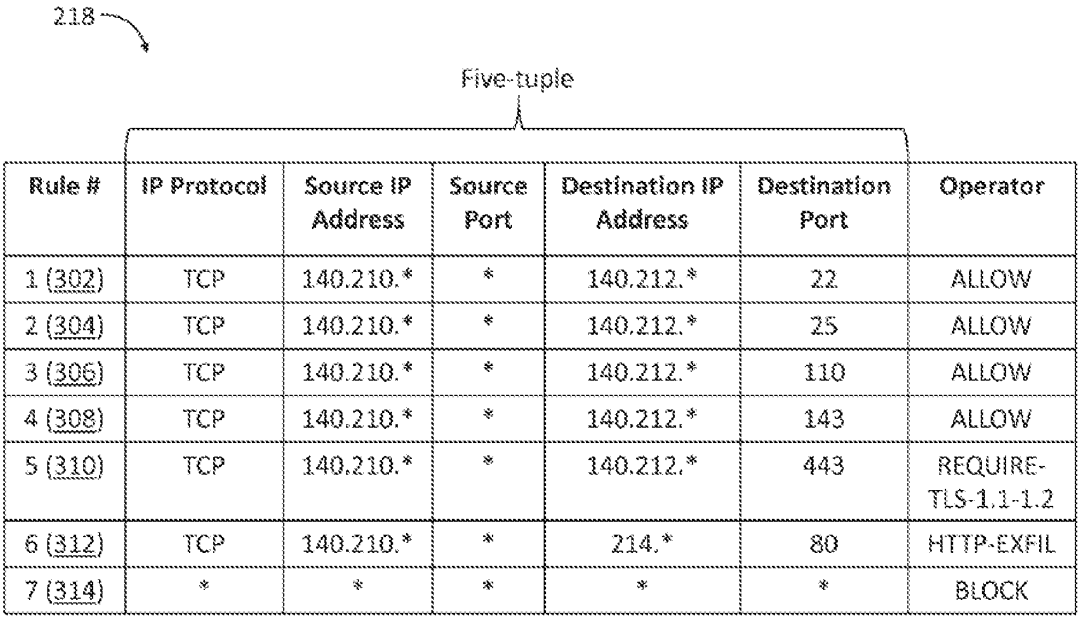


FIG. 1

Declaration of Dr. Alessandro Orso ("Orso Decl.") (Ex. 2026), ¶ 39 (annotating FIG. 1). In the technique recited in the claims of the '193 Patent, a computing device (e.g., PSG 110) receives packets from a first network (*e.g.* Network 104) and applies different packet-filtering rules and operators depending on whether the received packets are destined for the second network (*e.g.* Network 108) or the third network (*e.g.* Network 106). When a packet filtering rule identifies packets received from the first network and destined for the second network that contains protected resources, the computing device applies an operator "configured to drop packets associated with the particular type of data transfer," which will block a cybercriminal from

exfiltrating information from the protected resource. '193 Patent at 7:1–20, Claim 1. On the other hand, when a packet filtering rule identifies packets received from the first network and destined for the third network it does not apply the same operator "configured to drop packets associated with the particular type of data transfer," but rather applies a second operator which will forward the packets. '193 Patent, Claims 18. In this way, an employee will be able to access the Internet and be productive, while the resources of the company are protected from exfiltrations.

This same mapping of the Specification of the '193 Patent to the claims is also disclosed with respect to FIG. 3, reproduced below:



Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

'193 Patent, FIG. 3. In particular, FIG. 3 illustrates 7 different packet-filtering rules. The first six rules are all applicable to packets received from a single (*e.g.* first) network. But depending on the destination (*i.e.* whether the packets are destined for a second network with protected resources with IP address 214.* or a third network with IP address 140.212.* with unprotected resources), the computing device will apply different rules and different operators. Further, this is precisely how it is recited in the claims: the packet-filtering rule, which identifies the packets received from the first network and destined for the second network, specifies an "operator"

which ultimately blocks a packet and a second "operator" that applies to traffic destined to a third network which allows the packet.

The HTTP-EXFIL operator disclosed in the '193 Patent is one example of a type of operator. *See, e.g., id.* at claim 10 (reciting a first operator that is configured to drop packets "responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP POST method"). An example of an HTTP-EXFIL operator is shown below:

```
Operator HTTP-EXFIL(ip-packet):
    Inspect app-pkt(ip-packet) match GET return ALLOW;
    Inspect app-pkt(ip-packet) match POST return BLOCK;
    Inspect app-pkt(ip-packet) match PUT return BLOCK;
    Inspect app-pkt(ip-packet) match DELETE return BLOCK;
    Inspect app-pkt(ip-packet) match CONNECT return BLOCK;
    Return BLOCK;
End Operator HTTP-EXFIL;
```

Id. at 7:51–59. Critically, the HTTP-EXFIL operator, which is specified by, but not part of, a packet-filtering rule is "configured to drop packets associated with the particular type of data transfer." This type of operator is distinct from the Rule Action disclosed in Sourcefire. In particular, Sourcefire's Rule Action, are each part of the packet filtering rule and are not specific to any "particular type of data transfer."

VII. ARGUMENTS

A. Claim Interpretation

1. "operator… configured to drop packets associated with the particular type of data transfer" and "second operator configured to forward packets not associated with the particular type of data transfer"

Each of the independent claims of the '193 Patent recites two "operators," namely an "operator… configured to drop packets associated with the particular type of data transfer" and a "second operator configured to forward packets not associated with the particular type of data transfer." Orso, ¶ 47. Exemplary operators disclosed in the '193 Patent are reproduced below:

HTTP-EXFIL Operator	REQUIRE-TLS-1.1-1.2 Operator
Operator HTTP-EXFIL(ip-packet): Inspect app-pkt(ip-packet) match GET return ALLOW; Inspect app-pkt(ip-packet) match POST return BLOCK; Inspect app-pkt(ip-packet) match PUT return BLOCK; Inspect app-pkt(ip-packet) match DELETE return BLOCK; Inspect app-pkt(ip-packet) match CONNECT return BLOCK; Return BLOCK; End Operator HTTP-EXFIL.	Operator REQUIRE-TLS-1.1-1.2(ip-packet): Inspect app-pkt(ip-packet) match 1.0 return BLOCK; Inspect app-pkt(ip-packet) match 1.1 return ALLOW; Inspect app-pkt(ip-packet) match 1.2 return ALLOW; Return BLOCK; End Operator REQUIRE-TLS-1.1-1.2;

See '193 Patent at 7:51–59; 8:21–26. Consistent with the plain language of the claims, the HTTP-EXFIL Operator and the REQUIRE-TLS-1.1-1.2 Operator is each configured to drop packets associated with a particular type of data transfer. Orso Decl., ¶ 47.

Notably, the claims of the '193 Patent differ from the claims of the '552 Patent, which Cisco relies upon in its request, in a critical manner. Orso Decl., ¶ 49. Specifically, unlike the operator of the '552 Patent claims, the operator recited in the claims of the '193 Patent must "be configured to drop packets associated with the particular type of data transfer" and a second operator must configured to forward packets not associated with the particular type of data transfer. *Compare* '552 Patent at Claim 1 *with* '193 Patent at Claim 1. Unlike the '193 Patent claims, there is no requirement in the '552 Patent claims for two operators, one that must be configured to drop packets and another to forward packets. Instead, the '552 Patent only requires a single operator that ***specifies*** the application-header-field-value criteria and a packet transformation function. Tellingly, Cisco failed to apprise the Office of this critical distinction in the claim language in its Request. *See* Request at 28–34. Accordingly, Centripetal is not estopped from arguing that the Claims of the '193 Patent are valid on this basis.

In denying institution of *inter partes* review in IPR2018-01559, the Board focused on this crucial claim language. Orso Decl., ¶ 50 (citing Ex. 1067 at 9 ("This first operator is ***configured to drop*** packets associated with the type of data transfer that the recited packet-filtering rules are configured to prevent."); *id.* at 10–11 (contrasting an ***operator*** that is configured to drop packets with a ***rule*** that drops packets); *id.* at 11 (finding that an operator is distinct from the rule because an operator may be associated with multiple rules); *id.* at 12 (finding that the rules and operators are "distinct," and the operator performs "one or more functions on the packets")). Accordingly, not only are the claims of the '193 Patentably distinct from the claims of the '552 Patent, the Board has already upheld the patentability of the '193 Patent based on that very distinction.

Moreover, the Board's Final Written Decision in IPR2018-01436 focused precisely on the language of the '552 Patent, which requires only that an "operator" ***specify*** application-layer-header-value criteria and a packet transformation function[5] without the operator itself being "configured to drop packets associated with the particular type of data transfer." Ex. 1058 at 50–51; '193 Patent at Claim 1. The Board did not consider whether Sourcefire disclosed an operator "configured to drop packets associated with the particular type of data transfer" in IPR2018-01436 because that language does not appear in the claims of the '552 Patent.

For the foregoing reasons, and consistent with the Board's Institution Decision in IPR2018-01559, the "operator" term of the '193 Patent is distinct from the "operator" term claimed in the '552 Patent because there is one operator that is "configured to drop packets associated with the particular type of data transfer" and there is a second operator that forward packets that are not associated with the particular type of data transfer.

B. Ground 1 (Claims 1–20)

Sourcefire fails to disclose or suggest "applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer," and a second operator that is configured to forward packets not associated with the particular type of data transfer, as recited in each independent claim of the '193 Patent. It also would not have been obvious to modify Sourcefire in order to prevent the type of exfiltrations targeted by the '193 Patent, let alone to use the specific technique recited in the claims.

1. Sourcefire Does Not Disclose the Claimed Operator

The '193 Patent teaches and claims, responsive to a determination that a first portion of packets is destined for the second network, applying an operator that specified by the packet-filtering rules that is "configured to drop packets associated with the particular type of data transfer." *See, e.g.*, '193 Patent at 8:45-51 ("Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule;

[5] Centripetal is appealing this aspect of the Board's Final Written Decision in IPR2018-01436 and does not waive the issue in the event that the Federal Circuit reverses that decision, but it remains a distinct issue from the one raised here, which is premised on the claim language of the '193 Patent that differs from that of the '552 Patent. *See* Ex. 2003 at 31–34.

if so, the second stage may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources."); *see also id.* at 8:53–65; Orso Decl., ¶ 52.

The '193 Patent does not only disclose a simple packet filtering rule that can block all traffic. Rather, the '193 Patent introduced the concept of a two-stage packet filtering rule that determines if certain criteria is met, and if so, a separate operator is applied that is configured to drop packets associated with a particular type of data transfer...In other words, the relevant claims of the '193 Patent state that the operator is "configured to drop packets associated with [a] particular type of data transfer," and there is no such operator in Sourcefire. Orso Decl., ¶ 53

In the Office Action, the Examiner states:

> As discussed above, a first operator in this case is a "drop operator" which can be used to drop packets that meet the criteria. The following are examples regarding HTTP method PUT criteria, FTP command of PORT criteria and ssl_version criteria.

Office Action at 11. As a preliminary matter, it is unclear what disclosure from Sourcefire the Examiner points to as a "drop operator" because there is no citation to Sourcefire accompanying the Examiner's statement. *Id.* And as the Board previously determined, and a text search of Sourcefire confirms, Sourcefire does not disclose anything called a "drop operator." IPR2018-01559 at 10; Orso Decl., ¶ 54.

Centripetal presumes that the Examiner is referring to Sourcefire's "Rule Action." *See* Office Action at 7 (citing Sourcefire at 358–359); *see also* Sourcefire at 764–765. But the "Rule Action" is part of the rule itself and not part of any operator specified by the rule. *See* Sourcefire at 765 ("Each rule header includes a parameter that specifies the action the system takes when a packet triggers a rule."); Orso Decl., ¶ 55. Thus, the rule itself is configured to drop packets, not any operator specified by the rule, so the Rule Action fails to satisfy the Board's conception of what the term "first operator" means in the context of the '193 Patent, which specified by but ***distinct from*** the packet-filtering rule. *See* § VII.A.1, *supra*. In addition, there is no disclosure in Sourcefire of a second operator that will forward packets that are not associated with the particular type of data transfer.

Nor is Sourcefire's "Rule Action" "configured to drop packets **associated with the particular type of data transfer**," as recited in each independent claim of the '193 Patent. Rather than specifying an operator "configured to drop packets associated with the particular

type of data transfer, the rule itself specifies the "patterns that a packet's payload must match to trigger the rule" and drops the packet without applying any additional operator. Orso Decl., ¶ 56 (citing Sourcefire at 762-765) ("Each rule header includes a parameter that specifies the action the system takes when a packet triggers a rule."). Sourcefire neither teaches nor suggests a separate operator, like the exemplary HTTP-EXFIL operator associated with Rule 6 of FIG.3, which is applied after the criteria of the packet have been met and is "configured to drop packets associated with [a] particular type of data transfer." *See* '193 Patent, Claim 1 and Fig. 3.

218

Five-tuple

Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

In contrast to Sourcefire, in exemplary Rule 6 (which is consistent with the claim language), the rule specifies the criteria a packet must match in order to determine whether to apply a separate "operator," which is in turn "configured to drop packets associated with the particular type of data transfer." Orso Decl., ¶ 57.

In other words, Sourcefire is ***not*** capable of applying "a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer." Orso Decl., ¶ 58. There is simply no functionality in Sourcefire capable of constructing a rule that specifies "a first operator, specified by the one or more packet-filtering

rules, configured to drop packets associated with the particular type of data transfer." And certainly there is no second operator that is configured to forward packets that are not associated with the particular type of data transfer.

Accordingly, while the Examiner contends that "[u]sing the rules language, a user could specify the behavior of a rule by combining keywords in the rule," both the behavior and keywords are explicitly within the rule itself and are neither specified nor carried out by an operator distinct from the rule itself, which is "configured to drop packets associated with the particular type of data transfer," or "forward packets not associated with the particular type of data transfer" as claimed. Orso Decl., ¶ 59 (quoting Office Action at 7). For at least the foregoing reasons, Sourcefire does not teach or suggest "apply[ing]… a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer," or a "second operator configured to forward packets not associated with the particular type of data transfer" as recited in independent claims 1, 8, 18, and 19 of the '193 Patent. Claims 2-7, 9-17, and 20, which depend therefrom, are patentable for at least the same reasons.

2. There is No Motivation to Modify Sourcefire to Address Exfiltrations

The Examiner concedes that Sourcefire does not explicitly disclose the combination of rules recited in the independent claims of the '193 Patent and states instead that "Sourcefire discloses that different intrusion rules ***could be applied*** to some different portion of the plurality of packets which can be deemed to be a second portion of packets from the first network (source) and destined for a third network (destination different than second network destination)." Office Action at 7. Further, the Examiner suggests that because "Sourcefire provides a very flexible approach for crafting rules that recognize that the same rule criteria can be utilized differently for packets to/from an internal network as compared to an external network" it would have been obvious to construct the particular set of rules and operators recited in the claims of the '193 Patent and that the claims of the '193 Patent represent nothing more than a "design choice." *See* Office Action at 12–13. Respectfully, this reasoning is contrary to Federal Circuit precedent and represents an overly simplistic conception of both the Sourcefire reference and the claims of the '193 Patent.

First, the Examiner's obviousness rationale fails as a matter of law because it focuses on what a POSA could[6] do with the Sourcefire system but does not establish that a POSA ***would*** have been motivated to do it. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) ("[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.") (emphasis original); *see also Orexo AB v. Actavis Elizabeth LLC*, 903 F.3d 1265, 1272-73 (Fed. Cir. 2018) (quoting *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984)) ("The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification.").

As discussed above, the claims of the '193 Patent are explicitly drawn to preventing exfiltrations. *See* § VI, *supra*. Sourcefire, on the other hand, is an "Intrusion Prevention System," or "IPS" that allegedly "provides best-in-class ***intrusion*** detection and prevention by harnessing the power of the industry-standard Snort® rules-based detection engine." Sourcefire at 33. It applies ***intrusion*** rules. Sourcefire at 34 ("3D Sensors that are licensed to use IPS include a set of *intrusion rules* developed by the Sourcefire Vulnerability Research Team (VRT)."). The entirety of the 2,123 page Sourcefire reference does not mention exfiltration attacks, disclose any rules or combinations of rules for preventing exfiltration attacks, or suggest any steps that a user might take to prevent exfiltrations. Orso Decl., ¶ 61.

In fact, the very nature of exfiltration attacks would have confounded a POSA reading Sourcefire because Sourcefire "looks for malicious activity, and reports and/or takes actions based on detected malicious activity." Sourcefire at 34. At the time of the invention, however, exfiltrations were difficult to prevent precisely because they did not look like "malicious activity":

> A category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent. A first cause is that many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web, that often appear to an observer (e.g., a conventional cyber defense system) as ***normal network behavior***. A second cause is that typical network trust models, such as those used by network firewalls, ***interpret exfiltrations as trusted operations***.

---

[6] As discussed above, a POSA also could not have used Sourcefire to construct packet-filtering rules with the claimed operator. *See* § VII.B.1, *supra*.

'193 Patent at 1:24–34 (emphasis added). Accordingly, Sourcefire manual, which instructs users to implement "intrusion rules" to detect "malicious activity," provides no instruction for how to deal with exfiltrations or motivation to block ***outgoing*** traffic that does not appear to be malicious. Orso Decl., ¶ 62.

The specific set of rules and operators recited in the independent claims of the '193 Patent, as a whole, establish a technique whereby a computing device inspects outgoing packets from a first network to determine whether they are destined for a particular second or third network and applies different operators depending on that determination. *See generally,* '193 Patent, Claims 1, 8, 18, and 19. The reason for this approach is that, because exfiltration attacks are often mediated by "popular network data transfer protocols," simply blocking every packet that utilizes a particular data transfer protocol would not allow users to freely surf the Internet:

> One or more administrators of the secured network may associate such an operator with one or more rules in a network security policy in order to enforce, via the PSG, a Web usage policy that may, for example, allow users to surf (e.g., GET) to one or more web sites attached to the Internet, but may prevent such user(s) from one or more of writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more web sites. For example, administrator(s) may utilize such functionality to prevent one or more exfiltrations (e.g., file transfers containing sensitive information, posting of login credentials (usernames and passwords), etc.) to network nodes (e.g., web sites) that they may not trust.

Orso Decl., ¶ 63 (citing '193 Patent at 2:43–54). Similarly:

> Returning to the example described above, organization Z may own or operate network 108, and may have allocated network IP addresses 214.0.0.0/8 to network 108. ***Enterprise X may not have a business relationship with organization Z, and may therefore not consider network 108 to be trusted. While enterprise X could simply block all communications to networks that are owned or operated by organizations it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet***. Enterprise X's employees, therefore, could not freely surf the Web, which may restrict the employees' ability to conduct business on behalf of enterprise X. By enforcing sets of rules similar to rule 6 312 that may apply operators like or similar to HTTP-EXFIL, enterprise X may enable its employees to freely surf the web and conduct company business, but may prevent one or more cyber attacks (e.g., HTTP-mediated exfiltrations).

Orso Decl., ¶ 63 (quoting '193 Patent at 7:1–37 (emphasis added)).

But Sourcefire fails to teach any approaches for preventing exfiltrations, fails to appreciate the problems known to plague prior attempts to deal with exfiltrations, and certainly does not suggest the solution explicitly recited in the claims of the '193 Patent. Orso Decl., ¶ 63.

Thus, not only is there no evidence that a POSA at the time would have appreciated the problem of how to handle exfiltrations, but there is also no evidence that a POSA would have found the claimed solution obvious. *See Mintz v. Dietz & Watson, Inc.*, 679 F.3d 1372, 1377–78 (Fed. Cir. 2012) (finding impermissible hindsight where the problem in the prior art does not suggest the problem the invention solves).

Further, the Office Action impermissibly focuses on the obviousness of individual "features" of the claim rather than the claim as a whole, which the Federal Circuit and its predecessor court prohibits:

> As we have observed, it is the emphasis on the obviousness of "features", rather than the claimed telephone system as a whole, that constitutes the flaw in the application of section 103 to the Feil claims. As stated in *In re Shuman*, 361 F.2d 1008, 1012 [] (CCPA 1966):
>
> It is impermissible to first ascertain factually what appellants did and then view the prior art in such a manner as to select from the random facts of that art only those which may be modified and then utilized to reconstruct appellants' invention from such prior art.

Interconnect Planning Corp. v. Feil, 774 F. 2d 1132, 1141 (Fed. Cir. 1985). Reviewing the claims element-by-element and concluding that a POSA ***could have*** reconstructed the claimed invention, as done in the Office Action, represents "the essence of hindsight." *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999).

For example, the Examiner cites Sourcefire's disclosure that "rule keywords could be used by the HTTP inspect preprocessor and rules engine to search for matched application-layer content… including the most common HTTP methods of GET, PUT, POST, and CONNECT and *pass* (allow), *alert* (and pass), or *drop* (block) packets based on the results of such searches." Office Action at 8. The Examiner also contends that a POSA understood that it would be important to identify such methods because of certain alleged "vulnerabilities with certain HTTP methods." *Id.* Respectfully, there is no evidence cited to support the Examiner's statement that there were known vulnerabilities with certain HTTP methods. Orso Decl., ¶ 64.

Centripetal presumes that the Examiner's statement was based on Cisco's citation to RFC 2616. *See* Request at 60 (citing Ex. 1046 at 44). However, in this context "safe" only means that the HTTP GET command, by convention, does not allow any action on the server other than data retrieval. Orso Decl., ¶ 65 (citing Ex. 2002 at 1 ("An HTTP method is **safe** if it doesn't alter

the state of the server. In other words, a method is safe if it leads to a read-only operation."). "Safe" in this context does not mean that the HTTP command is actually safe. Orso Decl., ¶ 65 (Ex. 1046 at 44 ("Naturally, it is not possible to ensure that the server does not generate side-effects as a result of performing a GET request; in fact, some dynamic resources consider that a feature.")). Nor does this passage mean that there are "vulnerabilities" associated with other "unsafe" HTTP methods, like POST, PUT, and DELETE. *Id.* All "unsafe" means in this context is that these HTTP methods by design effect changes to the server receiving the command. Orso Decl., ¶ 65. For example, because a POST command entails a "write" command, it is not "read-only," and is therefore "unsafe." Indeed, far from indicating that there are any "vulnerabilities" associated with certain HTTP commands, RFC 2616 illustrates that HTTP was ***designed*** to include read-only commands, such as GET and HEAD as well as non-read-only commands, such as POST, PUT, and DELETE. Thus, while RFC 2616 suggests making a user aware that they are using a non-read-only command, it certainly does not claim that there are any "vulnerabilities" associated with those commands such that packets associated with the command should be blocked. Orso Decl., ¶ 65 (Ex. 1046 at 44).

Accordingly, there is no motivation for a POSA to have written a rule to block any of those HTTP methods, let alone ***why*** a POSA would have (1) written a rule to block such HTTP methods for some network traffic and not other network traffic, (2) written the rule to prevent the HTTP method for ***outgoing*** traffic, and (3) written the rule to specify an operator that is configured to drop the packet rather than dropping the packet using the rule itself. Nor does Sourcefire or any other record evidence disclose or suggest any ***basis*** for determining which network traffic should be blocked and which should not for any particular HTTP method. Orso Decl., ¶ 66. Indeed, it ***could not have been*** obvious to block packets using a particular HTTP method in Sourecfire given that the HTTP Method option "does not generate events"! Sourcefire at 568.

The Examiner also references the FTP Bounce attack for evidence that a POSA would have written a rule to block the FTP Port command. Office Action, pg. 8. The Examiner's statement is respectfully traversed. An FTP Bounce attack involves an attacker sending an FTP "PORT" command to an FTP server containing the network address and the port number of the machine and service being attacked. At this point, the original client can instruct the FTP server to send a file to the service being attacked. Such a file would contain commands relevant to the

service being attacked (SMTP, NNTP, etc.)." Ex. 1040 at 2. Accordingly, the computer running the service being attacked does not receive any packets associated with the "PORT" command that a security device can take action upon because it only receives commands "relevant to the service being attacked (SMTP, NNTP, etc.)." Orso Decl., ¶ 67; Ex. 1040 at. 2.

Rather than block packets associated with FTP "PORT" command as suggested in the Office Action, POSAs knew of three techniques for thwarting Bounce attacks. *First*, it was known to ensure that FTP servers "not open data connections to TCP ports less than 1024" because those ports are associated with well-known services, making them easy to attack. Orso Decl., ¶ 68; Ex. 1040 at 2. *Second*, a POSA could implement "proper file protections" to prevent an attacker from uploading a file to an FTP server and later downloading it to the service being attacked. *Id.* *Third*, the FTP server could disable the "PORT" command entirely. *Id.* None of these options entail applying an operator that blocks packets associated with the FTP "PORT" command, let alone blocking such packets when they are destined for a one network but not another. Orso Decl., ¶ 68. Further still, the known techniques for thwarting a Bounce attack involved taking action on ***incoming*** requests to an FTP server, not ***outgoing*** requests emanating from a first network and destined for a second or third network. *Id.* Thus, it was neither known nor obvious at the time of the invention to apply the claimed technique to outgoing packets (*i.e.* packets received from a first network).

The Examiner also cites Sourcefire's disclosure that "[b]ecause security vulnerabilities associated with HTTPS data transfers using or proposing to use TLS 1.0, SSLv2, SSLv3 are widely known, a POSA would be motivated to write appropriate drop rules to identify and block Record Protocol packets that proposed using these particular less secure SSL and TLS types of data transfer from continuing toward their second network destination." Office Action at 9. Yet, as with the HTTP method example discussed above, this does not explain ***why*** a POSA would have (1) written a rule to block such types of data traffic for some network traffic and not other network traffic, (2) written the rule to prevent the data transfer for ***outgoing*** traffic, or (3) written the rule to specify an operator that is configured to drop the packet rather than dropping the packet using the rule itself. Orso Decl., ¶ 69. In fact, at the time of the invention, it was known ***not to*** simply block traffic using an older TLS/SSL version because the newer protocol version were not yet deployed:

> The BEAST attack is released to exploit predictable IVs in TLS 1.0. Even though this problem had been fixed in TLS 1.1 released in 2006 and TLS 1.2 in 2008, ***no one actually uses these newer protocol versions***. Browsers will take about 2 more years to deploy TLS 1.2 and servers many years longer. ***We have no choice*** but to rely on browser counter-measures in the meantime. BEAST is the first attack to show how rich browser functionality can be abused to attack cryptography from multiple vantage points. Many similar attacks will follow.

Orso Decl., ¶ 69 (quoting Ex. 1037 at 8). The '193 Patent solved this problem with the ability to block potentially vulnerable protocols like TLS1.0 for some network traffic but allowing it for other traffic. And as with the HTTP example discussed above, neither Sourcefire nor any other record evidence discloses or suggests any basis for determining which network traffic should be blocked and which should not for any given TLS/SSL protocol. Orso Decl., ¶ 69.

The Examiner also states that a POSA could use Sourcefire to block RTP traffic in order "to enforce a security policy prohibiting employees' use of such applications" allegedly because "enterprise networks restrict employees use of high bandwidth applications like streaming media while also avoiding known vulnerabilities posed by such use." Office Action at 9–10. However, just like the examples above, this explanation does not explain ***why*** a POSA would have (1) written a rule to block such RTP data transfers for some network traffic and not other network traffic, (2) written the rule to prevent the data transfer for ***outgoing*** traffic, or (3) written the rule to specify an operator that is configured to drop the packet rather than dropping the packet using the rule itself. Orso Decl., ¶ 70. And again, neither Sourcefire nor any other record evidence discloses or suggests any basis for determining which network traffic should be blocked and which should not for RTP traffic. *Id.*

The Examiner's reliance on a purported "design choice" rationale to bridge the gap between the claims of the '193 Patent also fails. Design choice is applicable where a particular ***claim element*** "presents no novel or unexpected result over" a prior art ***claim element***. *Application of Kuhle*, 526 F. 2d 553, 555 (CCPA 1975). For example, in *Application of Kuhle*, the CCPA found that there was "no novel or unexpected result" associated with replacing the metallic connections of the prior art with a "metallic wrapping." *Id.* On the other hand, the obviousness modification proposed in the Office Action does not involve simply swapping one prior art element for a different but equivalent element that provides "no novel or unexpected result."

Design choice is not an applicable rationale for rejecting claims that define a theretofore unknown solution to an unknown problem simply because individual claim elements could have been reconstructed once the problem and solution were known.[7] Rather than representing a simple "design choice," a POSA only could have arrived at the claimed solution to the exfiltration problem by utilizing very specific features of Sourcefire in a very specific way, like "throwing metaphorical darts at a board". *In re Cyclobenzaprine Hydrochloride Extended Release Capsule Patent Litig.*, 676 F. 3d 1063, 1071 (Fed. Cir. 2012) ("Where, however, a defendant urges an obviousness finding by 'merely throw[ing] metaphorical darts at a board' in hopes of arriving at a successful result, but 'the prior art gave either no indication of which parameters were critical or no direction as to which of many possible choices is likely to be successful,' courts should reject 'hindsight claims of obviousness.'" (citing *In re Kubin*, 561 F.3d 1351, 1359 (Fed. Cir. 2009) (quoting *In re O'Farrell*, 853 F.2d 894, 903 (Fed. Cir. 1988)).).

For at least the foregoing reasons, a POSA would have modified Sourcefire to reach the claims of the '193 Patent.

C. Objective Indicia of Nonb Demonstrate Nonobviousness of the Challenged Claims

In addition to the reasons above, objective evidence demonstrates that Claims 1–20 are not obvious. "Objective evidence relevant to the issue of obviousness must be evaluated by Office personnel. [] Such evidence, sometimes referred to as "secondary considerations," may include evidence of commercial success, long-felt but unsolved needs, failure of others, and unexpected results." MPEP § 2141(II). During the course of the District Court case of the '193 Patent, a significant record of objective evidence, including evidence of long-felt need, industry praise and commercial success for Centripetal's products, and evidence of Cisco's copying of Centripetal's patented technology, was developed demonstrating the non-obviousness of the claims at issue. This significant evidence is presented again independently here to the Patent Office, demonstrating again, the validity of the '193 Patent claims.

---

[7] And even then, Sourcefire was not capable of constructing a rule that specified an "operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer." *See* § VII.B.1, *supra*.

1. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others

The failure of others can result in a strong indication of non-obviousness. *See In re: Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1075 (Fed. Cir. 2012) (reversing district court and finding evidence of unexpected results and long-felt need for those results supported a finding of non-obviousness). Failure of others is also indicative of unexpected results and long-felt need because one of ordinary skill in the art would not reasonably expect the success. *See id; see also Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1382 (Fed. Cir. 1983) (holding that the lack of previous attempts to achieve the results of the invention indicated a lack of long-felt need).

The '193 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to protect against "[a] category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet)." Orso Decl., ¶ 72 (citing '193 Patent at 1:24-47). Data exfiltrations occur when malware and/or malicious actors carry out an unauthorized data transfer from a computer. For example, a cyber criminal might steal data such as usernames/passwords, personal information, financial data, or corporate trade secrets, and exfiltrate that data out from a computer or network and into their possession. Declaration of Dr. Sean Moore ("Moore Decl.") (Ex. 2028), ¶ 6. This problem has been known in the industry since at least 2006, and while it was extensively discussed in research papers and trade periodicals, it was still an ongoing problem. Moore Decl., ¶ 6 (citing Ex. 2007 and Ex. 2008). Centripetal solved this long-felt, unsolved need with its RuleGATE, Advanced Cyber Threat, and QuickTHREAT system components, which practices the '193 Patent. Moore Decl., ¶¶ 5–6.

Centripetal's solution to this long-felt problem began with the recognition that exfiltrations are typically facilitated by using ***popular network data transfer protocols***, such as the Hypertext Transfer Protocol (HTTP). Moore Decl., ¶ 7. Because bad actors on the internet discovered that they could exfiltrate valuable data using popular data transfer protocols rather than explicitly malicious code, traditional signature-based techniques designed to recognize and prevent the transfer of malicious code into a network were not suited to stopping the emerging exfiltration problem. Moore Decl., ¶ 7. Further, because exfiltrations are mediated by popular data transfer protocols, it was also not an option simply to block all traffic utilizing a particular protocol, even when those protocols had a known vulnerability. Moore Decl., ¶ 11.

The claims of the '193 Patent recite techniques that address this long-felt but unresolved problem of data exfiltrations. The claims of the '193 Patent involve applying "packet-filtering rules" specifically crafted to prevent such exfiltrations. Orso Decl., ¶ 73. In particular, the claimed invention prevents malicious exfiltrations by (1) detecting communications between two identified resources (i.e., a "first network" and "a second network", as claimed), and (2) "applying" a "first operator" to "drop packets associated with the particular type of data transfer," as claimed. *See* '193 Patent, Claim 1. The claims of the '193 Patent are embodied in Centripetal's CleanINTERNET and RuleGATE products. The RuleGATE and CleanINTERNET products include the ability to counter these types of exfiltrations and also address insider threats. Orso Decl., ¶ 73.

Centripetal's solution to these problems greatly curtailed the risk of data exfiltration by detecting the threat earlier and acting in response while still preserving the flow of normal network traffic without disruption. In particular, Centripetal recognized that it could employ cyber-threat intelligence ("CTI") to focus its data-transfer-method-based packet filtering on traffic destined for potentially risky hosts on the Internet. Moore Decl., ¶ 11. This two-stage process succeeded where traditional, overbroad techniques failed because it permitted normal business network traffic, like allowing a web browser to download web pages hosted by web servers, while still preventing data exfiltrations. Moore Decl., ¶ 11.

Prior attempts by others to prevent data exfiltration were often too coarse or overbroad (such as blocking all HTTP traffic), resulting in negative impact to the subject computer network and ultimately to business operations. Moore Decl., ¶ 11. But using Centripetal's technique in conjunction with CTI, the '193 Patent could ALLOW packets sent from a first network to a third network and specify additional precautions, like applying the HTTP-EXFIL operator, for packets sent from the first network to a second network. *Id.*; Moore Decl., ¶ 12.

Centripetal's inventions unlocked the ability to derive network threat intelligence data (from multiple sources) and "operationalize" cyber threat intelligence (CTI) to proactively protect networks. The claimed invention leveraged CTI by applying operators ("applying… a first operator… configured to drop packets associated with the particular type of data transfer") to only those packets meeting specified packet header criteria ("responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules") rather than blocking any and all traffic utilizing

a particular type of data transfer. Orso Decl., ¶ 74. The '193 Patent provides the example of "an HTTP-EXFIL operator" that "may allow HTTP packets containing a GET method, but may block HTTP packets containing other HTTP methods (e.g., PUT, POST, CONNECT, etc.)." '193 Patent at 7:6-10.

The '193 Patent explains that such an HTTP-EXFIL operator achieves the solution of stopping exfiltrations "[b]ecause attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data." '193 Patent at 7:18-20. The '193 Patent also explains that this two-stage process succeeds where traditional, overbroad techniques failed because it enables, for example, the operator to "thus allow a web browser to 'surf the web' (e.g., download web pages hosted by web servers), but [] prevent the web browser from writing files to a web server (e.g., using the PUT method), posting forms (e.g., forms that might contain login credentials, such as usernames or passwords) to a web server (e.g., using the POST method), or otherwise communicating with a web server (e.g., using any HTTP method except GET)." '193 Patent at 7:10-18; Orso Decl., ¶ 75.

Centripetal's solution to the exfiltration solved the long-standing problem of how to prevent exfiltrations that are mediated by popular data transfer protocols, demonstrating the nonobviousness of the '193 Patent Claims.

2. Copying

There is no doubt that Cisco copied the '193 Patent and Centripetal's products that practice the '193 Patent. Ex. 2001 at 166. This fact is dispositive of non-obviousness because there is simply no reason for Cisco to copy Centripetal's patented technology if Sourcefire, which Cisco owns, performed the same functionality of the '193 Patent. Because "wholesale copying of the claimed invention" "provides compelling evidence of nonobviousness," all claims of the '193 Patent should be confirmed. *Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1285 (Fed. Cir. 2000).

Cisco's copying of Centripetal's technology began two years before Cisco released a copycat version of Centripetal's technology in Cisco's products. In 2015, Centripetal and Cisco entered into negotiations because Cisco was interested in Centripetal's technology. Declaration of Steven Rogers ("Rogers Decl.") (Ex. 2027), ¶ 7; Ex. 2009 at 190:8-15 ("So in 2015, this is six months after we launched our product, Cisco showed interest in our technology. And we, we gave them many demonstrations, many meetings in 2015. I got three of them demonstrated here.

They were demonstrations that we provided to them. We gave them non-confidential information, our public information. Kind of what we give to potential customers. See if they were interested. They were interested. They wanted to get more information.").

The negotiations results in an NDA being signed in 2016. Rogers Decl., ¶ 7; Ex. 2009 at 190:15-19 ("So in January of 2016 they proposed signing a non-disclosure agreement. And that's what we did. We signed a non-disclosure agreement so we could have a confidential meeting with Cisco and we could provide them with our confidential proprietary information."); *id.* at 193:11-15 ("We then gave them, provided them with a management presentation in 2016. This all under NDA. And it was labeled very sensitive. We gave them the RuleGATE Management Architecture. We actually gave them our architecture under the NDA. We told them about our patents.").

Following execution of the NDA, Centripetal disclosed its propriety technology to Cisco, including its exfiltration technology that is disclosed in the '193 Patent. *Id.* at 190:20-191:2 ("On February 4th, 2016 . . . Centripetal gave Cisco a presentation over WebEx. That's their technology. And in that presentation we gave them a lot of information. We talked about our algorithms, our secret sauce. We talked about our patents. We talked about a lot of our very sensitive information. There were follow-up meetings after that with, once again, senior top executives, and later in February and then again in March."). After two years of discussions, Cisco abruptly ended the discussions, and on June 20, 2017 released a suite of new technologies in its products that included Centripetal's patented technology. Rogers Decl., ¶ 8; Ex. 2009 at 191:10-21 ("At the end of 2016, Cisco said thanks, but no thanks, we're not interested in your technology. Six months later, they launched their Network Intuitive, their brand-new networking system. And all this time they were hitting our website as well. If you look at that bottom red bar below, they hit our website 354 times during this visit, or at least a Cisco IP address did. They visited 1,200 pages, over 1,200 pages from our website, of how we do things. And if you look at the hits of the website and what they downloaded, you'll see there are certain periods where they were very active. A Cisco IP address was hitting our website very actively during certain time periods."); *id.* at 194:5-196:12 (detailing the press release from Cisco dated June 20, 2017 on the development of Encrypted Traffic Analytics and its "revolutionary" nature); *id.* at 194:5-7 ("June 20th, 2017, this was the press releases. 'Cisco unveils a network of the future that can learn, adapt and evolve.'").

After Centripetal learned that Cisco copied Centripetal's technology, Centripetal sued Cisco for patent infringement on February 13, 2018. During the course of that litigation, it became apparent that Cisco's conduct was egregious. Not only did Cisco blatantly rip off Centripetal's technology, internal emails revealed that Cisco also studied Centripetal's patent claims, including the claims of the '193 Patent. Ex. 2034 (PTX-90) (internal Cisco email discussing Centripetal technology); Ex. 2035 (PTX-1064) (internal Cisco email discussing Centripetal technology); Ex. 2036 (PTX-1635) (internal Cisco email discussing Centripetal technology).

Trial began on May 6, 2020 and lasted approximately six weeks. Centripetal presented, and the Court found, that Cisco had embedded Centripetal's technology that is claimed in the '193 Patent in its routers and switches demonstrating a direct nexus between the '193 Patent and Cisco's copying. Ex. 2014 at 433:16-434:1 ("A: For the '193 patent, my opinion was that the accused switches and routers infringe claims 18 and 19 of the '193 patent. Q. And which products are those that infringe? A. That would be the Catalyst switches and the Aggregation Services Routers, or sometimes you'll see them as ASRs and Integrated Services Routers, ISRs. I believe the numbers – and I think we have a slide on this in case I've forgotten any, are the Catalyst switches 9300, 9400, 9500. For the ASR, it's the ASR 1000 series. For the ISR it's also the 1000 series. And then one of the 4000 series. I think that's the ISR one."); Ex. 2001 at 61 ("It is evident to the Court that Cisco lacked this functionality before 2017, yet this infringing functionality is exactly what was embedded in the accused products with the addition of ETA in 2017."); *id.* at 97 ("Not one selection of asserted prior art shows the infringing switch and router functionality was embedded in any of the Cisco products before the '193 Patent's priority date. These conclusions allow the Court to infer that the infringing functionality was added as a result of newly designed versions of the accused products that occurred after March of 2013.").

The facts showed that Cisco deliberately copied the '193 Patent, including its exfiltration technology that uses the claimed "operators" to inspect packets and determine whether the packets are destined for protected resources, and therefore blocked with the appropriate operator, or whether the packets are destined for unprotected resources, such as the Internet, and therefore allowed using another operator. Ex. 2014 at 470:6-551:21 (discussion of PTX-995 (Ex. 2015), PTX-1303 (Ex. 2016), PTX-175 (Ex. 2017), PTX-1313 (Ex. 2018), PTX-1276 (Ex. 2019), PTX-576 (Ex. 2020), PTX-1262 (Ex. 2021), PTX 1280 (Ex. 2022), PTX-563 (Ex. 2023), PTX-1356

(Ex. 2024), PTX-1326 (Ex. 2025) related to Cisco's exfiltration technology and overlap of '193 patent claims 18 and 19 in regard to the exfiltration technology). Further, the facts showed that the '193 Patent was valid because the '193 was not in the prior Cisco systems as Cisco alleged during trial. At the conclusion of trial, the Court found Cisco's infringement of the '193 Patent and the validity of the '193 Patent was "not a close call," determined that Cisco willfully infringed the '193 Patent, and enhanced damages because of Cisco deliberate copying resulting in a judgement with a minimum payment of $2.65 billion and a maximum payment of $3.25 billion. Ex. 2001 at 166 (Court's conclusion of infringement and damages); *id.* at 155 ("The Court **FINDS** that Cisco willfully infringed the '856 Patent, the '176 Patent, the '193 Patent, and the '806 Patent, therefore enhanced damages are warranted under the evidence.").

With regard to copying, the Court found, ***as a matter of fact***, that Cisco deliberately copied Centripetal's '193 Patent and its products that contained the technology claimed in the '193 Patent. Specifically, the Court determined that Cisco willfully infringed and deliberately copied the '193 Patent, portion of which is recited below:

> The facts illustrate that Cisco had pre-suit knowledge of Centripetal's asserted patents. ***First, after signing an NDA, Centripetal presented a detailed PowerPoint presentation to Cisco employees that laid out their patented technology***. PTX-547 at 389-91; Tr. 258:21-25, 260:2-18; 1220:1-1222:25. This meeting was presented by Jonathan Rogers, who testified that, at this meeting, he:
>
> > highlighted the technologies that were patented. We had a number of questions there, and I was offering to have additional discussion on that, as well, if it would be helpful.
>
> Tr. 1227:15-18. Contemporaneous emails sent by Jonathan Rogers to the Cisco team state that he was willing to share more information on the patented technology, as the group asked, "a few questions on our patents." PTX-102. This knowledge of the patents is confirmed by internal emails of Cisco's engineer, TK Keanini, which detailed the type of functionality covered by Centripetal's intellectual property and ***expressing interest in "study[ing] their claims***." PTX-134 at 3; see Tr. 1128:8-1129:5. Moreover, a third-party firm, Oppenheimer, met with Cisco to discuss Centripetal's product offerings that practice the patents, and ***presented a highly sensitive, detailed technical disclosure, which detailed the core RuleGate functionalities covered by the Asserted Patents***. Tr. 1235:11-20, 1237:25-1238:9; 1242:17-1243:11; DTX-1270 at 1, 25-28, 30.

Ex. 2001 at 155–56 (emphasis added).

Similar to the fact pattern in *Arctic Cat Inc. v. Bombardier Recreational Prods., Inc*, 198 F. Supp. 3d 1343, 1350 (S.D. Fla. 2016), *aff'd*, 876 F.3d 1350 (Fed. Cir. 2017), "Cisco had

multiple meetings with Centripetal employees and provided detailed presentations of the patents and their functionality," which demonstrates strong evidence of deliberate copying:

> As detailed in the Court's factual findings, Cisco was provided with demonstrations of the product and confidential information regarding Centripetal's proprietary algorithms. Within a year of these meetings, Cisco released the "network of the future," involving the release of older products embedded with new software ***functionality that was outlined and detailed to them by disclosure of the patents and multiple technical discussions and demonstrations***. The fact that Cisco released products with Centripetal's functionality within a year of these meetings goes ***beyond mere coincidence***. Therefore, the fact that Cisco's system ***mirrors the functionality of the Centripetal patents*** is compelling evidence that damages should be enhanced for copying

Id. at 155–56 (emphasis added).

Further, the Court determined that Cisco had not produced evidence that it "investigated the scope of the patent and formed a good-faith belief that it was invalid or that it was not infringed." *Id.* 155–56. In the end, the facts revealed, and the Court found, that Cisco was privy to detailed discussions and demonstrations of the technology that embodies the '193 Patent, cut off discussions with Centripetal, and released a system that "mirrors the functionality" of the '193 Patent less than a year later. *Id.* (emphasis added). Cisco's copying is dispositive evidence of nonobviousness, particularly because Cisco makes and sells the Sourcefire product and it would not need to copy Centripetal's technology if the technology was already provided in Sourcefire. As such, the '193 Patent claims should be confirmed.

3. Industry Praise

Products embodying the invention claimed in the '193 Patent have received substantial industry praise. Moore Decl., ¶¶ 13–14. In a white paper entitled "Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led Enforcement," an industry research firm named ESG Research praised Centripetal's Threat Intelligence Gateway as having "the highest performance network filter that ESG has tested or seen in action to date." Ex. 2010 at 7; Moore Decl., ¶ 13. The ESG Paper further lauded Centripetal's Threat Intelligence Gateway's ability to "deliver[] more than is possible with firewalls and IPS systems," pointing to Centripetal's RuleGATE and CleanINTERNET products. *Id.*

Centripetal was recognized as an innovator by trade periodicals and analysts. On May 4, 2017, Gartner published its "Cool Vendors in Security for Technology and Service Providers,"

praising Centripetal as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds." Ex. 2012 at 5. As described in the Cool Vendors article, Centripetal's QuickThreat Gateway "currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously." *Id.* Centripetal Networks was also named one of American Banker's "Top 10 FinTech Companies to Watch" for 2014 because its Threat Intelligence Gateway, RuleGATE "has the potential to detect and deter rapidly changing cybersecurity threats on the fly." Ex. 2011 at 14; Morse Decl., ¶ 14.

The evidence of industry praise discussed above is reasonably commensurate with the scope of the claims of the '193 Patent and that there is a nexus between the merits of the claimed invention and the evidence of secondary considerations, as the praise is directed at Centripetal's products which embody the claimed features of the '193 Patent. In fact, the court expressly made a factual finding that Centripetal's RuleGATE product practiced the '193 Patent. Ex. 2001 at 149 ("Centripetal's RuleGate product practices the patents found to be infringing in this case. Centripetal marks its RuleGate product with the patents that it practices.") (citation omitted). Therefore, the praise that Centripetal's products and technology have received from others further demonstrates that the claimed invention of the '193 Patent is not obvious.

D. The Reexamination must be Terminated Because There is no New Substantial Question of Patentability

The reexamination statute does not give requesters license to harass patent owners or waste the Office's resources. *See In re Recreative Techs. Corp.*, 83 F.3d 1394, 1397 (Fed. Cir. 1996) ("However, Congress recognized that this broad purpose must be balanced against the potential for abuse, whereby unwarranted reexaminations can harass the patentee and waste the patent life. The legislative record and the record of the interested public reflect a serious concern that reexamination not create new opportunities for abusive tactics and burdensome procedures."). Cisco's conduct here presents both issues. Cisco's Request constitutes harassment because it follows other unsuccessful attempts by Cisco to invalidate the '193 Patent in District Court and before the Patent Office using the same prior art.

Cisco's Request also wastes the Office's resources, asking it to find a "substantial new question of patentability" where it cannot. In particular, the Request cannot raise an SNQ

because the Patent Office already considered the issues raised in the Request in an earlier review of the '193 Patent:

> A "substantial new question of patentability" is not raised by prior art presented in a reexamination request if the Office has previously considered (in an earlier concluded examination or review of the patent) the same question of patentability as to a patent claim favorable to the patent owner based on the same prior art patents or printed publications. *In re Recreative Technologies*, 83 F.3d 1394 (Fed. Cir. 1996).

MPEP § 2242 (II)(A). In particular, the Patent Office already considered the patentability of the '193 Patent over Sourcefire in IPR2018-01559, which is a "concluded examination" under the Office's definition:

> An earlier concluded examination or review of the patent is: (A) the original examination of the application which matured into the patent; (B) the examination of the patent in a reissue application that has resulted in a reissue of the patent; (C) the examination of the patent in an earlier concluded reexamination or supplemental examination; (D) the review of the patent in an earlier concluded trial by the Patent Trial and Appeal Board, such as a post-grant review, *inter partes* review, or covered business method review of the patent; or (E) ***any other contested Office proceeding which has been concluded and which involved the patent***.

MPEP § 2242 (I) (emphasis added). This definition of "concluded examination" is broad and is ***not*** limited to AIA *trial* proceedings that end in a Final Written Decision. Accordingly, the Office's definition of "concluded examination" encompasses the "Preliminary Proceeding" conducted in IPR2018-01559 because it was a "contested Office proceeding which has been concluded and which involved the patent." *Id.*

The rationale behind this rule is to ensure that substantial new question of patentability (SNQ) will not be found where the request merely questions the prior judgment. *See In re Swanson*, 540 F.3d 1368, 1380 (Fed. Cir. 2008) ("As was true before the amendment, an 'argument already decided by the Office, whether during the original examination or an earlier reexamination' cannot raise a new question of patentability.'"). Yet Cisco's Request does just that, asking the Examiner to question and ultimately overrule the prior findings of the Board.

During the previous proceeding, the Patent Office considered Sourcefire for its alleged teaching of an "operator… configured to drop packets associated with the particular type of data transfer." Specifically, The Board's decision denying institution of *inter partes* review focused on this same claim language. Ex. 1067 at 9 ("This first operator is ***configured to drop*** packets associated with the type of data transfer that the recited packet-filtering rules are configured to

prevent."); *id.* at 10–11 (contrasting an ***operator*** that is configured to drop packets with a ***rule*** that drops packets); *id.* at 11 (finding that an operator is distinct from the rule because an operator may be associated with multiple rules); *id.* at 12 (finding that the rules and operators are "distinct," and the operator performs "one or more functions on the packets"). The ***same*** issue is raised here, precluding the finding of an SNQ.

Because the same question of patentability has already been "decided in an earlier concluded examination of the patent by the Office," an SNQ has not been raised, and the *ex parte* reexamination of the '193 Patent should be terminated.

E. The Reexamination Violates the USPTO's Procedures and Precedent Regarding 35 U.S.C. § 325(d)

The USPTO should also rescind its decision to order reexamination of the '193 Patent pursuant to 35 U.S.C. § 325(d), which provides that the director may reject a reexamination request when "same or substantially the same prior art or arguments previously were presented to the Office." There is no question that Sourcefire was already presented to the Office. *See generally* Ex. 1065. In these circumstances, the Office's policy and precedent require the following two actions:

1. "If the request for reexamination includes issues involving 35 U.S.C. 325(d), ***the examiner must bring such issues to the attention of the appropriate SPRS or the Director of the CRU***." MPEP § 2242(I).
2. A demonstration "that the Office erred in a manner material to the patentability of challenged claims." *Advanced Bionics, LLC, v. Med-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper No. 6 at 7-9 (P.T.A.B. Feb. 13, 2020) (precedential).

The record does not demonstrate that either of these requirements were met prior to issuing the Determination to Order Reexamination or prior to issuing the first Non-Final Office Action. While the ultimate decision of whether to order a reexamination in view of § 325(d) is discretionary, these two preliminary requirements are not.

The legislative history of the America Invents Act ("AIA") demonstrates that Congress passed § 325(d) to address this precise situation, where a Requester seeks ex parte reexamination of issues that it presented in an earlier petition for *inter partes* review:

> The second sentence of section 325(d) complements the protections against abuse of ex parte reexamination that are created by sections 315(e) and 325(e). The estoppels in subsection (e) will prevent inter partes and post-grant review petitioners from seeking ex parte reexamination of issues that were raised or could have been raised in the inter partes or post-grant review. The Office has generally declined to apply estoppel, however, to an issue that is raised in a request for inter partes reexamination if the request was not granted with respect to that issue. Under section 325(d), second sentence, however, the Office could nevertheless ***refuse a subsequent request for ex parte reexamination with respect to such an issue, even if it raises a substantial new question of patentability, because the issue previously was presented to the Office in the petition for inter partes or post-grant review***.

157 CONG. REC. S1376 (daily ed. Mar. 8, 2011) (statement of Sen. Kyl) (emphasis added). Indeed, the standard for determining of whether to reject a request for reexamination under 35 U.S.C § 325(d) differs from the "substantial new question of patentability" standard provided under 35 U.S.C. § 303. Thus, while the SNQ determination "is not precluded by the fact that a patent or printed publication was previously cited by or to the Office or considered by the Office," that issue falls squarely within the ambit of 35 U.S.C. § 325(d).

Importantly, Cisco has provided no justification for filing this request other than that it allegedly presents a "substantial new question of patentability."[8] See Request, pg. 35–36. However, the Office's precedential opinion on § 325(d) requires not only justification when presenting "the same or substantially the same prior art or arguments" but also a demonstration "that the Office erred in a manner material to the patentability of challenged claims." *Advanced Bionics, LLC, v. Med-El Elektromedizinische Geräte Gmbh*, IPR2019-01469, Paper No. 6 (PTAB Feb. 13, 2020) (precedential). No such demonstration was made in the Request, and there is no indication that the Examiner considered the Office's precedential opinion regarding § 325(d) in either the Determination Ordering Reexamination or the Non-Final Office Action.

Centripetal respectfully requests, therefore, that the Examiner terminate this reexamination under 35 U.S.C. § 325(d) because (1) the Request presents the same prior art and arguments previously presented to the Office in IPR2018-01559 and (2) this reexamination was improperly ordered prior to full consideration of the § 325(d) issues raised in the Request as required by the Office's policy and precedent.

[8] It does not. *See* § VII.D, *supra*.

VIII. CONCLUSION

For the foregoing reasons, each claim of the '193 Patent is not obvious over Sourcefire. Further, the Request fails to demonstrate an SNQ, and Determination Ordering Reexamination is improper under 35 U.S.C. § 325(d). Centripetal therefore requests that the Examiner issue a Notice of Intent to Issue a Reexamination Certificate, confirming the patentability of all claims of the '193 Patent, or otherwise terminate the reexamination, as appropriate.

Respectfully submitted,

Date: January 25, 2020

By /Jeffrey H. Price/

Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, New York 10036
Firm Office No: (212) 715-7502
Email: JPrice@KramerLevin.com
Customer No.: 31013

Jeffrey H. Price
Registration No. 69,141

EXHIBIT LIST

Exhibit No.	Description
Exhibit-2001	Opinion and Order, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va. Oct. 5, 2020)
Exhibit-2002	Definition of "Safe" [available at https://developer.mozilla.org/en-US/docs/Glossary/safe]
Exhibit-2003	Centripetal's Opening Brief, Appeal No. 20-1635
Exhibit-2004	Cisco's Respose Brief, Appeal No. 20-1635
Exhibit-2005	Centripetal's Reply Brief, Appeal No. 20-1635
Exhibit-2006	Cisco's Sourcefire Invalidity Chart
Exhibit-2007	Data Exfiltration: How Data Gets Out [available at https://www.computerworld.com/article/2520483/data-exfiltration--how-data-gets-out.html]
Exhibit-2008	A. Giani et al. , "Detection of Covert Channel Encoding in Network Packet Delays," Tech. Rep. TR2005-536, Department of Computer Science, Dartmouth College, Nov. 2005, http://www.ists.dartmouth.edu/library/149.pdf
Exhibit-2009	Trial Transcript of May 7, 2020, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2010	ESG White Paper – Centripetal Networks Threat Intelligence Gateway, by Tony Palmer (May 2018)
Exhibit-2011	American Banker article, "Top 10 FinTech Companies to Watch," published November 6, 2013
Exhibit-2012	Gartner – Cool Vendors in Security for Technology and Service Providers, 2017, published May 4, 2017
Exhibit-2013	Stanley Chincheck, US Naval Research Laboratory, Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day
Exhibit-2014	Trial Transcript of May 11, 2020, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)

Exhibit-2015	Cisco Security Analytics, PTX-995, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2016	Cisco Enterprise Silicon - Delivering Innovation for Advanced Networking, PTX-1303, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2017	Cisco 1000 Series Integrated Services Routers, PTX-175, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2018	Cisco ASR 1000 Overview, PTX-1313, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2019	Cisco Polaris Software System Functional Specification, PTX-1276, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2020	CiscoCognitive Threat Analytics, PTX-576, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2021	Cisco Catalyst 9000 Switches, PTX-1262, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2022	Network as a Sensor and Encrypted Traffic Analytics Integration, PTX-1280, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2023	Digital Network Architecture for Securing Enterprise Networks, PTX-563, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2024	Rapid Threat Containment in SD-Access, PTX-1356, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2025	Cisco Identity Services Engine, PTX-1326, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2029	PTX-1215, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2030	Reserved
Exhibit-2031	CleanINTERNET Components [available at https://www.centripetal.ai/products]
Exhibit-2032	Cisco Ordered To Pay $1.9B In Centripetal Patent Trial, Law360
Exhibit-2033	RuleGATE 2000 Gateway

Exhibit-2034	Reserved
Exhibit-2035	Reserved
Exhibit-2036	Email from TK Keanini, PTX-1326, Centripetal Networks, Inc., v. Cisco Sys., Inc., 2:18-cv-94 (E.D. Va.)
Exhibit-2037	Network Survivability, Recovery & Reconsitution [available at https://www.sbir.gov/sbirsearch/detail/12493]

CERTIFICATE OF SERVICE

The undersigned certifies that a complete and entire copy of Centripetal's Response to Non-Final Office Action in Control No. 90/014,476 was served via First Class Mail to the Third Party Requester at:

Patrick D. McPherson
Duane Morris LLP
505 9th Street NW, Suite 1000
Washington, D.C. 20004

Respectfully submitted,

Date: January 25, 2020

By /Jeffrey H. Price/

Kramer Levin Naftalis & Frankel LLP
1177 Avenue of the Americas
New York, New York 10036
Firm Office No: (212) 715-7502
Email: JPrice@KramerLevin.com

Jeffrey H. Price
Registration No. 69,141

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,476	03/19/2020	9686193	E4720-00206	1013

31013 7590 09/23/2020

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER
DESAI, RACHNA SINGH

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
09/23/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,476* .

PATENT UNDER REEXAMINATION *9686193* .

ART UNIT *3991* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Office Action in Ex Parte Reexamination	**Control No.** 90/014,476	**Patent Under Reexamination**	
	Examiner Minh T Nguyen	**Art Unit** 3991	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

a. ☑ Responsive to the communication(s) filed on 19 March 2020.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

b. ☐ This action is made FINAL.

c. ☑ A statement under 37 CFR 1.530 has not been received from the patent owner.

A shortened statutory period for response to this action is set to expire 2 month(s) from the mailing date of this letter. Failure to respond within the period for response will result in termination of the proceeding and issuance of an *ex parte* reexamination certificate in accordance with this action. 37 CFR 1.550(d). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).** If the period for response specified above is less than thirty (30) days, a response within the statutory minimum of thirty (30) days will be considered timely.

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☐ Notice of References Cited by Examiner, PTO-892.
2. ☐ Information Disclosure Statement, PTO/SB/08.
3. ☐ Interview Summary, PTO-474.
4. ☐ _____.

Part II SUMMARY OF ACTION

1a. ☑ Claims 1-20 are subject to reexamination.
1b. ☐ Claims _____ are not subject to reexamination.
2. ☐ Claims _____ have been canceled in the present reexamination proceeding.
3. ☐ Claims _____ are patentable and/or confirmed.
4. ☑ Claims 1-20 are rejected.
5. ☐ Claims _____ are objected to.
6. ☐ The drawings, filed on _____ are acceptable.
7. ☐ The proposed drawing correction, filed on _____ has been (7a) ☐ approved (7b) ☐ disapproved.
8. ☐ Acknowledgment is made of the priority claim under 35 U.S.C. 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the certified copies have
   1 ☐ been received.
   2 ☐ not been received.
   3 ☐ been filed in Application No. _____.
   4 ☐ been filed in reexamination Control No. _____.
   5 ☐ been received by the International Bureau in PCT application No. _____.
   * See the attached detailed Office action for a list of the certified copies not received.
9. ☐ Since the proceeding appears to be in condition for issuance of an *ex parte* reexamination certificate except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte* Quayle, 1935 C.D. 11, 453 O.G. 213.
10. ☐ Other: _____

cc: Requester (if third party requester)

EX PARTE REEXAMINATION – NON-FINAL OFFICE ACTION

Pertinent Prosecution History

Reexamination has been requested for claims 18-19 of the United States Patent Number 9,686,193 ("the '193 patent"), entitled "*Filtering Network Data Transfers*" by a third party requester ("Requester").

On May 01, 2020, the Office issued an Ex parte Reexamination Ordered Pursuant to 35 USC 257 (August 2020 Order).

The following is a non-final Office action in response to the August 2020 Order.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Status of the Claims

The '193 patent has 20 claims, among those claims 1, 8, 18 and 19 are independent. Thus, claims 1-20 are pending in this reexamination.

Prior Art

Claims 1-20 of the '193 patent are reexamined based on the following references:

Sourcefire 3D System, User Guide Version 4.10 ("Sourcefire").

Statute

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The factual inquiries for establishing a background for determining obviousness under pre-AIA 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or non-obviousness.

Claim Rejections and Comments

Claims 1-20 of the '193 patent are rejected under 35 U.S.C. § 103(a) as being obvious over Sourcefire in view of the knowledge of a POSA.

Sourcefire Overview:

Sourcefire reference is a user manual titled "Sourcefire 3D System User Guide" for the Sourcefire 3D System. The system operates via "3D Sensors", each runs the Sourcefire "Intrustion Prevention System (IPS). Sourcefire at pages 33-34, 106-107. Sourcefire describes the functionality of 3D System. Sourcefire describes a flexible approach to customizing packet-filtering rules, and the implementing of such rules. When certain rules are triggered, some packets are blocked and, when other rules are triggered, other packets are allowed to pass. *Id.* at page 761. Different rule criteria including origin/destination network, data transfer/messaging protocols *(e.g.,* HTTP, FTP, instant messaging, multimedia), and "keywords" which could include protocol methods /commands *(e.g.,* HTTP PUT, HTTP GET), encryption protocol version *(e.g.* TLS 1.0), etc. are used in different rules. *Id.* at pages 762-763.

Claim 18:

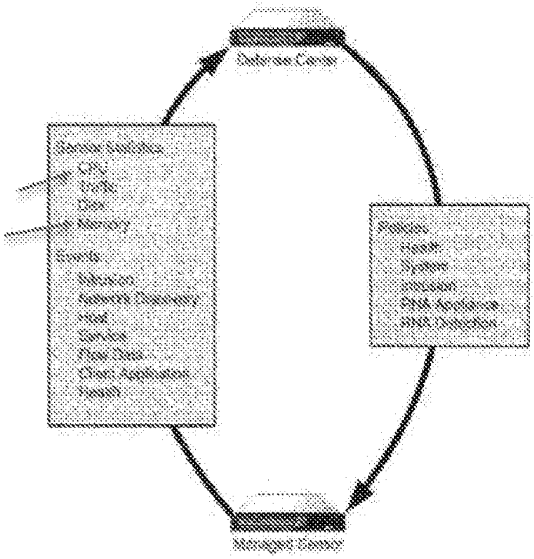
A system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:

Sourcefire describes a system that includes 3D Sensors, and that each 3D Sensor included a processor (CPU), memory, and disk storage. Sourcefire at pages 33-34, 106-107. A POSA would understand that the 3D Sensor disk memory includes instructions to control the operation of the 3D sensor.

Annotated figure at page 107, reproduced below, shows the 3D Sensor includes processor CPU, memory and disk storage. Thus, the above recited limitations are met.

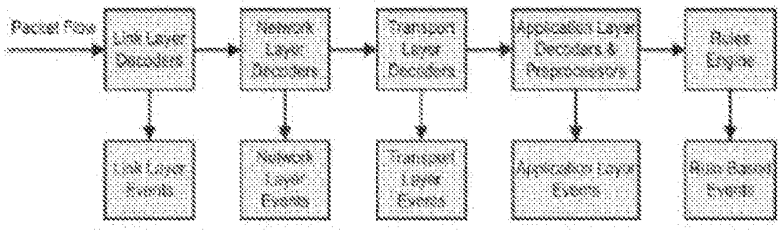


receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

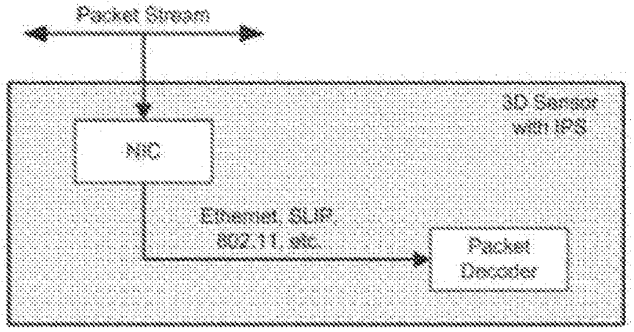
Sourcefire discloses "the packets must be captured from the network." *Id.* at page 257, emphasis added. In other words, Sourcefire discloses receiving a plurality of packets from a first network. Because each packet comprises data which include source IP address, source port, destination IP address, destination port, filtering rules …, the limitation "wherein the plurality of packets comprises a first portion of packets and a second portion of packets" is met.

Sourcefire discloses that each deployed 3D Sensor with IPS examines the receiving packets, looks for malicious activity, and reports and/or takes actions based on

detected malicious activity. The IPS performs these functions on packets using a plurality of packet-filtering rules implemented through a series of decoders, preprocessors, and a rules engine (as illustrated below). *Id.* at pages 35, 253-256.



Sourcefire further discloses that each 3D Sensor receives packets through a communication interface including "inline" interfaces in which rules dropped or allowed packets received into such decoders, preprocessors, and rules engine via such inline interfaces. Sourcefire discloses one example of how a 3D Sensor receives packets via a network interface card as shown below. *Id.* at page 257.

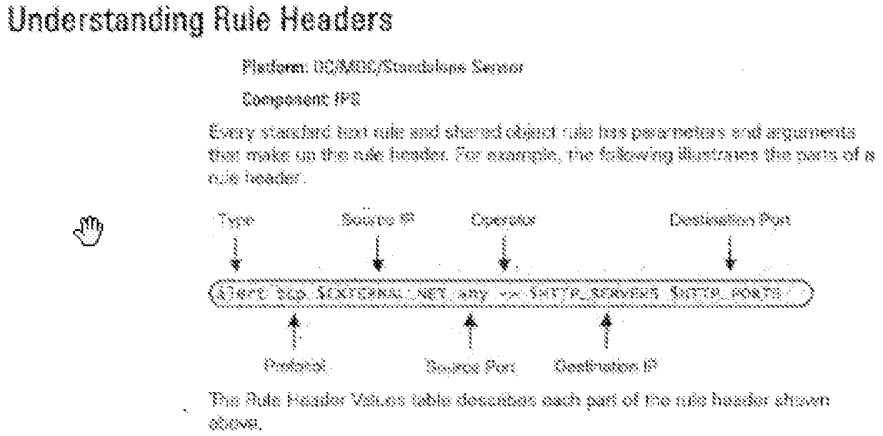


Thus, Sourcefire discloses 3D Sensors receiving a plurality of packets, some of which can be deemed to be a first portion of packets and some of which can be deemed a second portion of packets, and each Sensor is provisioned with a plurality of packet-filtering rules. Sourcefire discloses that the packets received by the 3D Sensor originate from a computing device *(e.g.,* host) located in a first network where the first network could be the network that the 3D Sensor is designed to protect *(e.g.,* HOME NET) or a network external to such network *(e.g,* EXTERNAL NET). *Id.* at pages 213-214.

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

As discussed above, Sourcefire discloses that the IPS allows a user to modify various parameters of rules to customize them as appropriate or to write their own custom intrusion rules tuned to the user's specific network environment. By writing rules and specifying the rule's event message, the system could more easily identify traffic that indicates attacks and policy evasions. *Id.* at pages.403-406.

Sourcefire further describes that all of the intrusion rules have 5-tuple criteria associated with them which include source IP addresses and source port, destination IP addresses and destination port for the received packets. *Id.* at pages 761-770.



A POSA would understand that this 5-tuple rule criteria could be used to filter packets transferring data from a first network (source) to a second network (destination), for example, from an internal protected network to an external network destination and vice versa. For example, the 5-tuple for each packet in the first portion of packets includes data that indicates the first network contains the source IP address and the second network contains the destination IP address. The well-known destination port in the 5-tuple of these packets also

often reflects the protocol *(e.g.,* HTTP (port 80), HTTPS (port 443), FTP (port 21), SMTP (port 25), XMPP (port 5222 or 5269)) being used for the data transfer if such packets are traveling over a standard port. *Id.* at pages 764-769, 54-55.

Using the rules language, a user could specify the behavior of a rule by combining keywords in the rule. Key words and their associated arguments dictate how the rules engine, and any relevant preprocessors invoke by the rule, test and evaluate packets and packet-related values by, for example, content matching, protocol-specific pattern matching, and state-specific matching. The rules engine and preprocessors allow the combination of any number of compatible keywords to create highly specific intrusion rules, and allow the user to combine any number of rules to customize a security policy tuned to the user's specific network environment. This helps decrease the chance of false positives and negatives and focus the intrusion information that a user received. *Id.* at pages 769~770.

For example, Sourcefire provides guidelines for creating rules to implement a security policy including "understand[ing] the traffic that traverses the network", "set[ting] your variables to accurately reflect your home and external networks" and including guidance that "[i]f none of the existing intrusion rules meet your needs, write new rules that inspect for intrusion attempts," *Id.* at pages.333-335. Thus, Sourcefire expressly teaches a POSA to customize/ tailor rules and rule combinations for whatever purpose is set forth in the security policy and provides the motivation for a POSA to implement the specific rules and rule combinations recited in the claim.

As described above, in addition to the destination port (and other) 5-tuple rule criteria, key words of intrusion rules could be used to filter packets as they arrive at various preprocessors and at the rules engine by searching for matched content in packets such as, for example, data associated with particular types of data transfer *(e.g.,* HTTP, FTP, SMTP, HTTPS, IM, multimedia, HTTP methods, FTP commands, TLS version). *Id.* at pages.827-828, 491-492. Sourcefire describes the type of actions that could be triggered by the rule as *pass* (and ignore), *alert* (and pass) or *drop* (block). *Id.* at pages 358-359. Thus, a POSA understood that the application of various rules could cause a first portion of packets from the first network addressed to the second network to be dropped.

For specific example regarding HTTP, Sourcefire discloses that, in addition to the 5-tuple criteria of destination port 80 (HTTP), rule keywords could be used by the HTTP Inspect preprocessor and rules engine to search for matched application-layer content in packets based on criteria including the most common HTTP methods of GET, PUT, POST and CONNECT and *pass* (allow), *alert* (and pass), or *drop* (block) packets based on results of such searches. *Id.* at pages 560, 786. A POSA would understand that identifying HTTP methods are important in existing packet-filtering firewalls with stateful inspection because application methods are used as part of rule criteria to block and pass packets, *e.g.,* a known "stateful inspection firewall allows the FTP 'GET' command but disallows the 'PUT' command" vulnerabilities with certain HTTP methods *(e.g.,* PUT, POST, DELETE) is well-known, and HTTP methods are used in IDS rules at least as early as 1997. *Id.* at pages 435-439.

Therefore, a POSA would understand that Sourcefire discloses how a user would have written a rule using the HTTP Method option of the HTTP content key word as part of the criteria to invoke the HTTP Inspect preprocessor to identify a first portion of packets using the particular PUT (or POST, DELETE, CONNECT, etc.) method type of data transfer and to block such packets with certain application payload content posing a threat from continuing towards their second network destination. Moreover, a POSA would have been motivated to write an intrusion rule to do this and have the IPS apply such a rule, for example, in the "adaptive" mode to identify and block packets associated with this particular type of data transfer *(e.g.,* HTTP PUT method) and not traveling over standard TCP port 80. *Id.* at pages.697-701.

As another specific example regarding FTP, Sourcefire discloses that, in addition to the 5-tuple criteria of destination port 21 (FTP), rule keywords could be used by the rules engine to search for matched content in packets based on criteria including FTP command (e.g., the known "PORT" FTP command), or known "anonymous" usernames, and *pass* (allow), *alert* (and pass), or *drop* (block) packets based on results of such searches. *Id.* at pages 556, 492-493. As described in Sourcefire, and as is known to a POSA, identifying this particular type of data transfer is important to address the well-known Bounce attack. *Id.* at page 556.

Therefore, a POSA would understand Sourcefire discloses how a user would have written a rule using content keywords as part of the rule criteria to identify a first portion of

packets using the particular PORT FTP command type of data transfer and to block such packets from continuing towards their second network destination. Moreover, a POSA would have been motivated to write an intrusion rule to do this and have the IPS apply such a rule, for example, in the "adaptive" mode to identify and block packets associated with this particular type of data transfer (FTP PORT command) and not traveling over standard TCP port 21. *Id.* at pages 697-701.

As a further specific example regarding HTTPS, Sourcefire discloses that, in addition to the 5-tuple criteria of destination port 443 (HTTPS), rule keywords could be used by the SSL preprocessor (when invoked by the rules engine) and either *pass* (allow), *alert* (and pass), or *drop* (block) packets based on criteria including encryption protocol version *(e.g.* TLS version). The key word ssl version could be included in such intrusion rules and used to identify and block a first portion of packets (*e.g.*, vulnerable Record Protocol packets) from continuing towards their second network destination. *Id.* at pages.827-828. A POSA would understand that certain SSL and TLS versions contained vulnerabilities *(e.g.,* TLS 1.0, SSLv2, SSLv3) and Sourcefire teaches that a *drop* rule could be written to block packets based on a ssl_version that included a known vulnerability.

Because security vulnerabilities associated with HTTPS data transfers using or proposing to use TLS 1.0, SSLv2, SSLv3 are widely known, a POSA would be motivated to write appropriate *drop* rules to identify and block Record Protocol packets that proposed using these particular less secure SSL and TLS types of data transfer from continuing toward their second network destination. Moreover, a POSA would have been motivated to write an intrusion rule to do this and have the IPS apply such a rule, for example, in the "adaptive" mode to identify and block Record Protocol packets associate with these particular less secure SSL and TLS types of data transfer and not traveling over standard port 443. *Id.* at pages 697-701.

As a further specific example regarding RTP traffic, Sourcefire discloses that multimedia 5-tuple and content keyword rule criteria could be used by the rules engine to identify matched content in a first portion of packets and block such packets from continuing towards their second network destination, for example, to enforce a security policy prohibiting employees' use of such applications. A POSA might use the default UDP port 5004 for transferring audio/video content to block some RTP traffic, or use fixed RTP header fields as content keyword targets or block

SIP/SDP packets in a control connection that indicate the use of RTP *(e.g.,* with content string 'RTP/AVP' or 'a=rtpmap'). *Id.* at pages 2040-2042.

A POSA would understand that security policies in enterprise networks restrict employees use of high bandwidth applications like streaming media while also avoiding known vulnerabilities posed by such use. Thus a POSA would understand that enforcing security policies which disallow the use of known protocols for transferring streaming multimedia (including RTP) on an internal network is simply a design choice to yield predictable results of reducing employee bandwidth usage with increased security on such network because doing so would involve nothing more than applying a known technique to a known device ready for improvement.

As discussed above, there is no technological difference between using particular type of data transfer criteria *(e.g.,* HTTP (or HTTP method), FTP (or FTP command), multimedia data *(e.g.,* RTP transfer)), over other types of rule criteria *(e.g.,* SSL/TLS version value, messaging protocol *(e.g.,* AIM, Yahoo! Messenger, XMPP)), and there are no specific technology changes needed to accommodate one data transfer protocol *(e.g.,* HTTP data transfer) over another *(e.g.,* messaging, encryption, FTP, RTP), or one data transfer method *(e.g.,* HTTP GET, FTP GET) over another *(e.g,* HTTP PUT, FTP PORT). Moreover, as also acknowledged by the '193 patent, there are no specific technology changes needed to accommodate allowing or blocking packets specifying one destination and origin from packets specifying any other possible destination and origin.

Thus, it is simply a design choice to select from a finite number of identified rule criteria that are relevant to a selected network vulnerability *(e.g.,* HTTP PUT method or FTP PORT command, and certain application payload content *(e.g.,* IM content, multimedia content)) to yield predictable results of increased network security because doing so would involve nothing more than applying a known technique to a known device ready for improvement.

Thus, Sourcefire teaches that various packet-filtering rules could be configured to prevent a particular type of data transfer from the first network to a second network, wherein the data satisfies criteria based on HTTP method, FTP command, IM content, multimedia

content *(e.g.,* RTP streams), TLS version, or any other criteria designed to prevent data transfer subject to a known vulnerability or exploit.

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

As discussed above, a first operator in this case is a "drop operator" which can be used to drop packets that meet the criteria. The following are examples regarding HTTP method PUT criteria, FTP command of PORT criteria and ssl_version criteria.

Using the HTTP method drop rule discussed above as an example, a *drop* operator could be applied to the first portion of packets that include an HTTP method of PUT.

Likewise, using the FTP command drop rule discussed above as an example, a drop operator would be applied to the first portion of packets that include an FTP command of PORT.

Likewise, using the ssl_version drop rule discussed above as an example, a drop operator would be applied to the first portion of packets having a version of TLS 1.0, SSLv2, or SSLv3.

drop each packet in the first portion of packets; and

Applying the HTTP method drop rule, FTP command drop rule, or TLS version drop rule from the examples above will result in dropping each packet in the first portion of packets.

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

As discussed above, Sourcefire discloses 3D Sensors receiving a plurality of packets, some of which can be deemed to be a first portion of packets from a first network (source) and destined for a second network (destination) where the criteria is associated with a particular

type of data transfer such as, for example, one of HTTP method (port 80 or non-standard ports), FTP command (port 21 or nonstandard ports), or ssl_version (port 443 or non-standard ports).

Likewise, Sourcefire discloses that different intrusion rules could be applied to some different portion of the plurality of packets which can be deemed to be a second portion of packets from the first network (source) and destined for a third network (destination different than second network destination).

For example, the rule applied to drop the first portion of packets could include: (i) 5-tuple criteria specifying first network source IP addresses and source port and second network FTP destination IP addresses and FTP destination port *(e.g.,* 21, second network IP addresses), and (ii) keyword criteria specifying a FTP PORT type of data transfer. In this example, the different rule applied to *allow* the second portion of packets could include (i) 5-tuple criteria specifying first network source IP addresses and third network destination IP addresses and *non*-FTP destination port (e.g., *not* port 21), and/or (ii) keyword criteria specifying application-layer data that is *not* associated with an FTP PORT type of data transfer *(e.g,,* HTTP data, multimedia *(e.g.,* RTP**)** data, Record Protocol data, IM data, SMTP data). The 5-tuple criteria in the different rule could specify, for example, ANY, or alternatively a netmask for a specifically known safe/trusted network, for destination IP addresses.

The rules engine and preprocessors allow the combination of any number of rules to customize a security policy tuned to the user's specific network environment, and Sourcefire provides guidelines on how to write rules to implement a security policy. *Id.* at pages 333-335**.** In other words, Sourcefire provides a very flexible approach for crafting rules that recognize that the same rule criteria can be utilized differently for packets to/from an internal network as compared to an external network, for traffic received from or destined for a specific port, and for whether it is desired to *pass, drop* or *alert* in response to triggering a rule.

As discussed above, there is no technological difference between combining rales that specify one particular type of data transfer criteria *(e.g.,* FTP PORT) with rules that don't specify such criteria, and other combinations that include rules that specify a different type of data transfer criteria *(e.g.,* HTTP, RTF, ssl_version), and there are no specific technology changes needed to accommodate one rale combination over another, or one packet destination and origin from another.Rather, it is simply a design choice to select from a finite number of

rules that are each relevant to a selected network vulnerability *(e.g.,* FTP Bounce attack), and combinations of such rales that allow for packets destined for one network *(e.g.,* external FTP server destination) to be treated differently than a packet destined for a different network *(e.g.,* external HTTP, RTP, IM, HTTPS, etc. server destination). In other words, Sourcefire encourages a POSA to improve IPS processing efficiency or throughput to yield predictable results tuned to improved network security of the user's particular network environment because doing so would involve nothing more than applying a known technique to a known device ready for improvement.

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

Sourcefire discloses that the 3D System with IPS can apply different *pass* (or *alert* (and pass)) rules to packets *{e.g.,* HTTP, SMTP, RTF, IM, Record Protocol packets) that are not associated with, for example, FTP packets including application-layer data specifying a FTP PORT command. In other words, a POSA would understand that, as a matter of design choice, a user could also implement intrusion rules or preprocessor rules which include a forward operator (*e.g.,pass, alert* (and pass)) configured to have the applicable preprocessor *{e.g.,* HTTP Inspect, SSL), and/or rules engine, forward *non*-FTP packets *(e.g.,* HTTP, Record Protocol, SMTP, RTP, IM packets) toward their third network destination IP address.

forward each packet in the second portion of packets toward the third network.

Because, for example, the TLS version 1.0 rule or HTTP PUT method rule is not applicable to the second portion of packets as described above, and because packet data in the second portion of packets satisfies different rule criteria of other *pass* or *alert* (and pass) intrusion rules, each packet in the second portion of packets will be forwarded toward their third network destination IP address.

Claim 19:

One or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

This claim is a computer program which is programmed to perform the corresponding system recited in claim 18. As such, it is rejected for the same reasons discussed in claim 18 above which are incorporated herein by reference.

Claim 1:

A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, each packet in first portion of packets; and

responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network:

applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forwarding, by the computing system, each packet in the second portion of packets toward the third network.

This claim is a method claim corresponding to the system claim recited in claim 18. As such, it is rejected for the same reasons discussed in claim 18 above which are incorporated herein by reference.

Claim 2:

The method of claim 1, wherein the first portion of packets comprises data indicating: a protocol type associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

As discussed above, the first portion of packets comprises data *(e.g.,* 5-tuple destination port (21), FTP PORT command) indicating a protocol type associated with the particular type of data transfer *(e.g.,* FTP) and second network destination and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g.,* 5-tuple and keyword rule criteria).

the second portion of packets comprises data indicating a protocol type not associated with the particular type of data transfer.

As discussed above, the second portion of packets comprises data *(e.g.,* 5-tuple destination port (80, 443, 25), HTTP GET method, SSL/TLS version, SMTP data, multimedia *(e.g.,* RTP) data, IM data) indicating a protocol type not associated with the particular type of data transfer *(e.g.,* HTTP, Record Protocol, SMTP, RTP, XMPP are not associated with FTP or FTP PORT).

Claim 3:

The method of claim 1, wherein:

the first portion of packets comprises data indicating a first destination port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second destination port number not associated with the particular type of data transfer.

As discussed above, the first portion of packets could comprise data indicating a first destination port number *(e.g.,* 21) associated with the particular type of data transfer *(e.g.,* FTP protocol, FTP PORT command) and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g.,* 5-tuple (e.g., port 21, FTP server IP addresses) and keyword rule criteria). Likewise, the second portion of packets comprises data indicating a second destination port number *(e.g.,* port 80, 443, 25) *not* associated with the particular type of data transfer *(e.g.,* HTTP, SSL/TLS, SMTP).

Claim 4:

The method of claim 1, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol (HTTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTP.

As discussed above, the first portion of packets could comprise data associated with HTTP *(e.g.,* port 80, HTTP PUT), and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g.,* 5-tuple *(e.g.,* port 80, HTTP server IP addresses) and HTTP Method keyword rule criteria). Likewise, the second portion of packets does not comprise data associated with HTTP *(e.g.,* port 21, FTP data).

Claim 5:

The method of claim 1, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol secure (HTTPS), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTPS.

As discussed above, a POSA would understand the first portion of packets could be Record Protocol packets comprising data associated with HTTPS *(e.g.,* port 443, SSL/TLS version), and corresponding to the criteria specified by the one or more packet filtering rules *(e.g.,* 5-tuple *(e.g.,* port 443, HTTPS server IP addresses) and SSL/TLS version keyword rule criteria). Likewise, the second portion of packets do not comprise data associated with HTTPS *(e.g.,* port 21, FTP data).

Claim 6:

The method of claim 1, wherein:

the first portion of packets comprises data associated with file transfer protocol (FTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with FTP.

As discussed above, the first portion of packets could comprise data associated with FTP *(e.g.,* port 21, FTP PORT command) and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g.,* 5-tuple (e.g., port 21, FTP server IP addresses) and FTP command content keyword rule criteria). Likewise, the second portion of packets does not comprise data associated with FTP *(e.g.,* port 80, 443, HTTP GET, SSL/TLS version.

Claim 7:

The method of claim 1, wherein:

the first portion of packets comprises data associated with real-time transport protocol (RTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with RTP.

As discussed above, a POSA would understand the first portion of packets could comprise data associated with RTP *(e.g.,* default UDP port for transferring audio/video content, fixed RTP header fields, control messages in a SIP connection setting up an RTP stream) and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g,,* 5-tuple *(e.g,,* RTP server IP addresses) and/or RTP content keyword rule criteria). Indeed, the '193 Patent presumes that a POSA would know how to identify packets comprising data associated with RTP, as the totality of its disclosure regarding RTP is "it may be useful for a packet filter to rapidly detect if an IP packet contains a Real-time Transport Protocol (RTP) application packet used to deliver audio or video information *(e.g.,* if a cyber-attack based on RTP has yet to be discovered, network administrators may choose to not process RTP packets through the cyber security defense systems that may be protecting their networks)." Likewise, the second portion of packets does not comprise data associated with multimedia transfer via RTP *(e.g.,* port 21, 25, FTP data, SMTP data).

Claim 8:

A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets;

responsive to a determination by the computing system that a first packet of the plurality of packets comprises data associated with eXtensible messaging and presence protocol (XMPP) and the data corresponds to criteria specified by one or more packet-

filtering rules configured to prevent a particular type of data transfer from the first network to a second network;

aplying, by the computing system and to the first packet, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, the first packet; and

responsive to a determination by the computing system that a second packet of the plurality of packets does not comprise data associated with XMPP:

applying, by the computing system, to the second packet, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the second network; and

forwarding, by the computing system, the second packet toward the second network.

This claim is a method claim corresponding to the system claim recited in claim 18 and it is rejected for the same reasons discussed in claim 18 above which are incorporated herein by reference.

While Sourcefire does not expressly identify the messaging protocol XMPP, a POSA understood that (i) XMPP (also referred to as Jabber) was the kind of well-known IM protocol that was being discussed in Sourcefire as a security concern, and (ii) the '193 Patent treats all application-layer rule criteria the same and identifies *the exact same system architecture and method* for allowing or blocking received packets using (i) data *transfer* protocols (e.g., HTTP, FTP, RTP), (ii) data *messaging* protocols *(e.g.,* XMPP) and (iii) data *encryption* protocols *(e.g,* TLS 1.0). Indeed, the '193 Patent presumes that a POSA would know how to identify packets comprising data associated with messaging protocol s such as XMPP, as the totality of its disclosure regarding XMPP is that "these methods may provide network administrators with capabilities to prevent exfiltrations that are mediated by other data transfer protocols besides HTTP and HTTPS, Examples of such protocols include ... messaging protocols such as extensible Messaging and Presence Protocol (XMPP)."

Thus, a POSA understood that the teaching of Sourcefire does not distinguish between any of the IM protocol types and thus is applicable to any IM protocols including XMPP. Further, a POSA understood the first portion of packets could comprise data indicating a default XMPP destination port number *(e.g.,* 5222, 5269) and/or other data *(e.g.,* XML stream tags, JabberID, "xmnls=", “jabber: client”) associated with XMPP and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g,* XMPP 5-tuple and keyword rule criteria).

Moreover, vulnerabilities with IM protocols generally and specifically with XMPP are known to a POSA, and thus a POSA understand that enforcing security policies which disallow employees' use of all known IM protocols, including XMPP from an internal network to a second network *(e.g.,* an external network) is simply a design choice to yield predictable results of increased security on such network because doing so would involve nothing more than applying a known technique to a known device ready for improvement.

Claim 9:

The method of claim 1, wherein:

receiving the plurality of packets comprises receiving packets comprising data associated with hypertext transfer protocol (HTTP);

As discussed above, the plurality of packets could comprise data associated with HTTP *(e.g.,* port 80, HTTP method). As also discussed above, a POSA would understand that Sourcefire discloses how a user would have written a rule using the HTTP Method option of the HTTP content keyword as part of the criteria to invoke the HTTP Inspect preprocessor to identify a first portion of packets using the particular HTTP method type of data transfer *(e.g.,* PUT, POST, CONNECT, or other known methods such as DELETE) and to block such packets with certain application payload content posing a threat from continuing towards their second network destination.

the first portion of packets comprises a first type of data associated with HTTP;

As discussed above, a POSA reading Sourcefire would understand that a first type of data associated with HTTP could be an HTTP method such as POST, PUT, DELETE or CONNECT, and thus a first portion of packets would include packets including POST, PUT, DELETE or CONNECT as the HTTP method.

the second portion of packets comprises a second type of data associated with HTTP; and

As discussed above, a POSA reading Sourcefire would understand that a second type of data associated with HTTP could be an HTTP method such as GET, and thus a second portion of packets would include packets including GET as the HTTP method.

applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises the first type of data.

As discussed above, a POSA reading Sourcefire would understand that a user could implement a specific security policy which achieved predictable benefits of protecting his or her network against a known security vulnerability by writing a rule using the HTTP Method option of the HTTP content keyword as part of the criteria to invoke the HTTP Inspect preprocessor to identify traffic using that HTTP method *(e.g.,* POST, PUT, DELETE, or CONNECT) and to *drop (i.e.,* block) such packets with certain application payload content posing a threat *(e.g.,* sensitive data or a malicious URL/URI) from continuing towards their second network destination.

Claim 10:

The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP POST method.

For the reasons described above, a POSA would be motivated to use rules as taught by Sourcefire to block a first portion of packets identifying an HTTP POST method to, for example, prevent an employee from posting sensitive data to a bulletin board or providing such data to a malicious URI on the second network.

Claim 11:

The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a

determination by the computing system that the first portion of packets comprises data corresponding to an HTTP PUT method.

For the reasons described above, a POSA would be motivated to use rules as taught by Sourcefire to block a first portion of packets identifying an HTTP PUT method to, for example, prevent an employee server from storing sensitive data under the specified URI on the second network.

Claim 12:

The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP DELETE method.

For the reasons described above, a POSA would be motivated to use rules as taught by Sourcefire to block a first portion of packets identifying an HTTP DELETE method to, for example, prevent an employee server from deleting the data identified by a malicious URI on the second network.

Claim 13:

The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP CONNECT method.

For the reasons described above, a POSA would be motivated to use rules as taught by Sourcefire to block a first portion of packets identifying an HTTP CONNECT method to, for example, prevent an employee from tunneling sensitive data to a malicious second network proxy.

Claim 14:

The method of claim 9, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second

network is performed responsive to a determination by the computing system that the second portion of packets comprises the second type of data.

For the reasons described above, a POSA would be motivated to use rules as taught by Sourcefire to forward a second portion of packets associated with an HTTP GET method to, for example, permit employees to surf the web via a third network web server.

Claim 15:

The method of claim 9, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to an HTTP GET method.

This claim is rejected for the same reason discussed in claim 14.

Claim 16:

The method of claim 1, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

As discussed above, a POSA would be motivated to use rules using the ssl_version keyword as taught by Sourcefire to block Record Protocol packets that propose using a less secure TLS version value *(e.g.*, TLS 1.0) from continuing towards their second network destination IP address to achieve predictable benefits of increased network security.

Claim 17:

The method of claim 1, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

As discussed above, a POSA would be motivated to use rules using the ssl_version keyword as taught by Sourcefire to forward Record Protocol packets that propose using a more secure TLS version value *(e.g,* TLS 1.1, TLS 1.2) toward their third network destination IP address to achieve predictable benefits of increased throughput and network security.

Claim 20:

The method of claim 1, wherein:

the first portion of packets comprises data indicating: a first source port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second source port number not associated with the particular type of data transfer.

Similar to the reasons discussed regarding claims 1 and 3, the first portion of packets could comprise data *(e.g.,* 5-tuple source port (80)) indicating HTTP and that a web server on a first network *(e.g.,* external network) seeks a response from a client on a second network *(e.g.,* internal network) associated with a particular type of data transfer *(e.g.,* HTTP PUT) and corresponding to the criteria specified by the one or more packet-filtering rules *(e.g.,* 5-tuple and keyword rule criteria). Likewise, the second portion of packets could comprise data indicating a second source port number (*e.g,* port 25) *not* associated with the particular type of data transfer *(e.g,* SMTP) and a third network destination IP address.

Service of Papers

After the filing of a request for reexamination by a third party requester, any document filed by either the patent owner or the third party requester must be served on the other party (or parties where two or more third party requester proceedings are merged) in the reexamination proceeding in the manner provided in 37 CFR 1.248. See 37 CFR 1.550(f).

Extensions of Time

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination

proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

Amendment in Reexamination Proceedings

Patent owner is reminded that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR 1.52(a) and (b), and must contain any fees required by 37 CFR 1.20(c). See MPEP § 2250(IV) for examples to assist in the preparation of proper proposed amendments in reexamination proceedings.

Submissions

In order to ensure full consideration of any amendments, affidavits or declarations or other documents as evidence of patentability, such documents must be submitted in response to the first Office action on the merits (which does not result in a close of prosecution). Submissions after the second Office action on the merits, which is intended to be a final action, will be governed by the requirements of 37 CFR 1.116, after final rejection and by 37 CFR 41.33 after appeal, which will be strictly enforced.

Notification of Concurrent Proceedings

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the '193 patent throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

Communication with the USPTO

All correspondence relating to this inter partes reexamination proceeding should be directed:

By Mail to: Mail Stop Supplemental Examination
Attn: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office

P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to: (571) 273-9900
Central Reexamination Unit

By hand: Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at https://efs.uspto.gov/efile/myportal/efs-registered. EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Notice Re Patent Owner's Correspondence Address

Effective May 16, 2007, 37 CFR 1.33(c) has been revised to provide that:

The patent owner's correspondence address for all communications in an ex parte reexamination or an inter partes reexamination is designated as the correspondence address of the patent.

Revisions and Technical Corrections Affecting Requirements for Ex Parte and Inter Partes Reexamination, 72 FR 18892 (April 16, 2007)(Final Rule)

The correspondence address for any pending reexamination proceeding not having the same correspondence address as that of the patent is, by way of this revision to 37 CFR 1.33(c), automatically changed to that of the patent file as of the effective date.
This change is effective for any reexamination proceeding which is pending before the Office as of May 16, 2007, including the present reexamination proceeding, and to any reexamination proceeding which is filed after that date.

Parties are to take this change into account when filing papers, and direct communications accordingly.

In the event the patent owner's correspondence address listed in the papers (record) for the present proceeding is different from the correspondence address of the patent, it is strongly encouraged that the patent owner affirmatively file a Notification of Change of Correspondence Address in the reexamination proceeding and/or the patent (depending on which address patent owner desires), to conform the address of the proceeding with that of the patent and to clarify the record as to which address should be used for correspondence.

Telephone Numbers for reexamination inquiries:

Reexamination Practice	(571) 272-7703
Central Reexam Unit (CRU)	(571) 272-7705
Reexamination Facsimile Transmission No.	(571) 273-9900

Any inquiry concerning this communication or earlier communication from the Examiner, or as to the status of the proceeding, should be directed to the Central Reexamination Unit at telephone number (571) 272-7705.

/Minh Nguyen/
Primary Examiner
571-272-1748
CRU, AU 3991

Conferees:
/Tuan H. Nguyen/
Primary Examiner
CRU, AU 3991

/TIMOTHY M SPEER/
Supervisory Patent Examiner, Art Unit 3991

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,476	03/19/2020	9686193	E4720-00206	1013

31013 7590 05/01/2020

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER
NGUYEN, MINH T

ART UNIT	PAPER NUMBER
3991	

MAIL DATE	DELIVERY MODE
05/01/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,476* .

PATENT UNDER REEXAMINATION *9686193* .

ART UNIT *3991* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Order Granting Request For Ex Parte Reexamination	Control No. 90/014,476	Patent Under Reexamination 9686193	
	Examiner Minh T Nguyen	Art Unit 3991	AIA (FITF) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The request for *ex parte* reexamination filed 03/19/2020 has been considered and a determination has been made. An identification of the claims, the references relied upon, and the rationale supporting the determination are attached.

Attachments: a)☐ PTO-892, b)☑ PTO/SB/08, c)☐ Other: ____

1. ☑ The request for *ex parte* reexamination is GRANTED.

RESPONSE TIMES ARE SET AS FOLLOWS:

For Patent Owner's Statement (Optional): TWO MONTHS from the mailing date of this communication (37 CFR 1.530 (b)). **EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.550(c).**

For Requester's Reply (optional): TWO MONTHS from the **date of service** of any timely filed Patent Owner's Statement (37 CFR 1.535). **NO EXTENSION OF THIS TIME PERIOD IS PERMITTED.** If Patent Owner does not file a timely statement under 37 CFR 1.530(b), then no reply by requester is permitted.

cc:Requester (if third party requester)

DECISION GRANTING *EX PARTE* REEXAMINATION

Reexamination has been requested for claims 18-19 of the United States Patent Number 9,686,193, entitled "*Filtering Network Data Transfers*" by a third party requester ("Requester").

A substantial new question of patentability affecting claims 18-19 of the United States Patent Number 9,686,193 ("the '193 patent") is raised by the request for *ex parte* reexamination.

As of this date, no record in the file indicating that patent owner (PO) waives his right to file a PO's statement under 35 USC 304 in the event reexamination is ordered for the '193 patent.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Submitted Prior Art in the Request

The substantial new question of patentability consideration is based on the following references:

Sourcefire 3D System, User Guide Version 4.10 ("Sourcefire").

Prosecution History

The '193 patent was issued on June 20, 2017 from an application serial No. 14/625,486 (the '486 application), filed on Feb 18, 2015. The '486 application is a continuation of application No. 13/795,822, filed on March 12, 2013, now Patent No. 9,124,552.

The '486 application filed with 20 claims (claims 21-40), among those, claims 21, 39 and 40 are independent claims. The prosecution history indicates that the original examiner cited references US 2011/0055916, 2010/0082811, 2010/0232445, 2013/0305311, 2004/0098511, 2010/0107240, 2009/0222877, 2002/0186683, 2004/0098511, 8,117,655, 2009/0240698 and 2013/0047,020 as reasons to reject all except claims 22, 29, 37 and 38 in a non-final Office action. In response to the Office action on June 14, 2016, the Applicant canceled claim 22,

added new claim 41 and included allowable features in claim 22 to independent claims 21, 39 and 40. The examiner allowed the case without giving any specific reason for allowance. Because the examiner objected to claim 22 in the non-final Office action filed on June 14, 2016, it is assumed that the examiner allowed independent claims 21, 39 and 40 because allowable features in claim 22 were added to independent claims 21, 39 and 40. As such, independent claims 21, 39 and 40 were allowable because the following the limitations:

> wherein receiving the plurality of packets comprises receiving a first portion of packets and a second portion of packets, wherein the first portion of packets comprises the first packet and the second packet, the method comprising:
>
> responsive to a determination by the computing system that the first portion of packets is destined for the second network, applying, by the computing system and to each packet in the first portion of packets, the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network; and
>
> responsive to a determination by the computing system that the second portion of packets is destined for a third network, applying, by the computing system, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, an operator configured to forward the packet toward the third network.

Amended independent claims 39 and 40 were renumbered as claims 18 and 19 of the '193 patent.

Requester filed a petition for IPR of the '193 patent on August 21, 2018, challenging all claims 1-20 as obvious over Sourcefire. In April 2019, the Patent Trial and Appeal Board ("the Board") denied institution on the ground that the "Petitioner has failed to establish a reasonable likehood of prevailing as to claim 1" because the Petitioner "*does not provide adequate explanation*" the term "first operator". (Case IPR2018-01559, Decision Denying Institution of *Inter Partes* Review 35 USC 314 at page 12). The Board further explained the reason for denying as *"[n]either the Petition nor the cited portions of Dr. Staniford's Declaration identifies the source of the referenced term "drop operator," and Petitioner does not direct us to any*

specific portion of Sourcefire, much less a portion that uses that term." Id. at page 10. Because independent claims 18 and 19, each has similar limitations as claim 1, these reasons for denying by the Board similarly applied to independent claims 18 and 19.

Reviewing the reasons explained by the Board, it is clear that the Board has not ruled that Sourcefire does not raise a substantial new question of patentability of claims 18 and 19 of the '193 patent, but rather the Petitioner failed to establish a reasonable likehood of prevailing because the Petitioner "*does not provide adequate explanation*" the term "first operator". As such, a substantial new question of patentability as to the claims of the '193 patent, including 18 and 19, has not been decided in an earlier concluded examination or review of the patent by the Office.

Substantial New Question

In view of the prosecution history noted above, a substantial new question of patentability would be raised if a prior art reference teaches or suggests the below limitations which were considered as a reason for allowance in the previous examination:

> wherein receiving the plurality of packets comprises receiving a first portion of packets and a second portion of packets, wherein the first portion of packets comprises the first packet and the second packet, the method comprising:
>
> responsive to a determination by the computing system that the first portion of packets is destined for the second network, applying, by the computing system and to each packet in the first portion of packets, the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network; and
>
> responsive to a determination by the computing system that the second portion of packets is destined for a third network, applying, by the computing system, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, an operator configured to forward the packet toward the third network.

Issues Raised in this Request

The Requester alleges that the cited prior art, i.e. Sourcefire, raises a substantial new question of patentability of claims 18-19 of the '193 patent because Sourcefile teaches and/or suggests the limitations which were the reasons for allowance of the '486 application noted above.

.

Analysis of the Prior Art Cited in the Request

In this Request, the Requester alleges that the consideration of Sourcefire raises a substantial new question of patentability to claims 18-19 of the '193 patent as pointed out in the Request, pages 52-81. Specifically, the Requester alleges that:

Sourcefire discloses a system that includes a 3D Sensor, and that each 3D Sensor includes a processor (CPU), a memory, and a disk storage. (Request at papes 52-53).

Sourcefire discloses 3D Sensors receiving a plurality of packets, some of which are deemed to be a first portion of packets and some of which are deemed to be a second portion of packets, and each Sensor is provisioned with a plurality of packet-filtering rules. Sourcefire discloses that the packets received by the 3D Sensor originate from a computing device (e.g., host) located in a first network where the first network could be the network that the 3D Sensor is designed to protect or a network external to such network. (Request at pages 53-55).

As pointed out in the Request at page 48, Sourcefire discloses that the intrusion rules had 5-tuple values associated with them. Intrusion rules contain two logical parts: the rule header and the rule options. Sourcefire discloses that, for a given 3D Sensor with Intrusion Protection System ("IPS"), multiple intrusion rules could be used to filter packets. These rules use the 5-tuple of the packet header to filter the packets, including both the source and destination IP addresses, which represent the source network from which the packets originated (i.e., the "first network") and the destination network to which they are directed (i.e., either the "second network" or the "third network"). The destination port in the 5-tuple also reflects the protocol (e.g., HTTP, FTP, SMTP, HTTPS) being used for data transfer. (Request at pages 48-51 and 57-58).

Using intrusion rule keywords, packets are filtered based on various application-layer data including data associated with particular types of data transfer (e.g., HTTP, FTP, SMTP, HTTPS, IM, multimedia, HTTP methods, FTP commands, TLS version) and data associated with IM applications. The type of packet-transformation functions or actions that could be triggered by the rules, when a given packet matches all of the criteria in a given rule, are: Pass (and Ignore), Alert (and Pass) or Drop (Block) such packet. (Sourcefire at pages 58-81).

For example, a rule can be applied to drop a first portion of packets could include: (1) 5-tuple criteria specifying first network source IP addresses and source port and second network destination IP addresses and HTTPS destination port (e.g., 443, second network IP addresses), and (2) a first operator specifying (i) ssl_version keyword and arguments that indicate TLS version 1.0 application-header-field-value criteria, and (ii) a rule action of "drop" (block) to packets that match the criteria. (Request at page 74).

As another example, a rule can be applied to drop a first portion of packets could include: (1) 5-tuple criteria specifying first network source IP addresses and source port and second network destination IP addresses and HTTP destination port (e.g., 80, second network IP addresses), and (2) a first operator specifying (i) HTTP Method option of the HTTP content keyword and arguments that indicate HTTP PUT method application-header-field-value criteria, and (ii) a rule action of "drop" (block) to packets that match the criteria. (Request at page 74)

In either of these examples, a different rule can be applied to allow the second portion of packets could include (1) 5-tuple criteria specifying first network source IP addresses and third network destination IP addresses and non-HTTPS destination port (e.g., not port 443) (or non-HTTP destination port (e.g., not port 80)), and (2) a second operator specifying (i) keyword and argument criteria indicating application-layer data that is not associated with a TLS version 1.0 (or HTTP PUT method data) type of data transfer (e.g., TLS version 1.1 or 1.2 data, FTP data, HTTP GET method data, etc.), and (ii) a pass or alert rule action to apply to each packet in the second portion of packets when each such packet matched this application-header-field criteria. The 5-tuple criteria in the different rule could specify, for example, ANY, or alternatively a netmask for a specifically known safe/trusted network, for destination IP addresses. (Request at page 75).

The rules engine and preprocessors allow the combination of any number of rules to customize a security policy tuned to the user's specific network environment, and Sourcefire provides guidelines on how to write rules to implement a security policy. In other words, Sourcefire provides a very flexible approach to crafting rules that recognized that the same rule criteria can be utilized differently for packets to/from an internal network as compared to an external network, for traffic received from or destined for a specific port, and, as already determined by the Board, for whether it is desired to apply a pass, drop or alert rule action as part of an operator, specified by such rule, and in response to triggering the application-header-field-value criteria also specified by such rule operator. (Request at pages 75-76).

According to the foregoing analysis, the examiner agrees that Sourcefire discloses a device comprising components and operated the same as reasons for allowance by the previous examiner as pointed out by the Requester.

There is a substantial likelihood that a reasonable examiner would consider these teachings important in deciding whether or not claims 18-19 are patentable. The prosecution history of the base application does not indicate that Sourcefire was included for consideration by the examiner in charge of the base application. Such teachings are not cumulative to any written discussion on the record of the teachings of the prior art, were not previously considered nor addressed during the prior examination and the same question of patentability was not the subject of a final holding of invalidity by the Board or the Federal Court.

Accordingly, Sourcefire raises a substantial new question of patentability as to claims 18-19 which question has not been decided in the previous examinations of the ‘193 patent.

Service of Papers

After the filing of a request for reexamination by a third party requester, any document filed by either the patent owner or the third party requester must be served on the other party (or parties where two or more third party requester proceedings are merged) in the reexamination proceeding in the manner provided in 37 CFR 1.248. See 37 CFR 1.550(f).

Extensions of Time

Extensions of time under 37 CFR 1.136(a) will not be permitted in these proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to parties in a reexamination proceeding. Additionally, 35 U.S.C. 305 requires that *ex parte* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.550(a)). Extensions of time in *ex parte* reexamination proceedings are provided for in 37 CFR 1.550(c).

Amendment in Reexamination Proceedings

Patent Owner is notified that any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFR 1.530(d)-(j), must be formally presented pursuant to 37 CFR 1.52(a) and (b), and must contain any fees required by 37 CFR 1.20(c). See MPEP § 2250(IV) for examples to assist in the preparation of proper proposed amendments in reexamination proceedings.

Submissions

In order to ensure full consideration of any amendments, affidavits or declarations or other documents as evidence of patentability, such documents must be submitted in response to the first Office action on the merits (which does not result in a close of prosecution). Submissions after the second Office action on the merits, which is intended to be a final action, will be governed by the requirements of 37 CFR 1.116, after final rejection and by 37 CFR 41.33 after appeal, which will be strictly enforced.

Notification of Concurrent Proceedings

The patent owner is reminded of the continuing responsibility under 37 CFR 1.565(a) to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving the '193 patent throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §§ 2207, 2282 and 2286.

Correspondence

All correspondence relating to this *ex partes* reexamination proceeding should be directed as follows:

By U.S. Postal Service Mail to:

Mail Stop *Ex Parte* Reexam

ATTN: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By FAX to:

571-273-9900
Central Reexamination Unit

By hand to:

Customer Service Window
Randolph Building
401 Dulany St.
Alexandria, VA 22314

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at https://efs.uspto.gov/efile/myportal/efs-registered. EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Notice Re Patent Owner's Correspondence Address

Effective May 16, 2007, 37 CFR 1.33(c) has been revised to provide that:

The patent owner's correspondence address for all communications in an *ex parte* reexamination or an *inter partes* reexamination is designated as the correspondence address of the patent.

Revisions and Technical Corrections Affecting Requirements for Ex Parte and Inter Partes Reexamination, 72 FR 18892 (April 16, 2007)(Final Rule)

The correspondence address for any pending reexamination proceeding not having the same correspondence address as that of the patent is, by way of this revision to 37 CFR 1.33(c), automatically changed to that of the patent file as of the effective date.

This change is effective for any reexamination proceeding which is pending before the Office as of May 16, 2007, including the present reexamination proceeding, and to any reexamination proceeding which is filed after that date.

Parties are to take this change into account when filing papers, and direct communications accordingly.

In the event the patent owner's correspondence address listed in the papers (record) for the present proceeding is different from the correspondence address of the patent, it is strongly encouraged that the patent owner affirmatively file a Notification of Change of Correspondence Address in the reexamination proceeding and/or the patent (depending on which address patent owner desires), to conform the address of the proceeding with that of the patent and to clarify the record as to which address should be used for correspondence.

Telephone Numbers for reexamination inquiries:

Reexamination Practice	(571) 272-7703
Central Reexam Unit (CRU)	(571) 272-7705
Reexamination Facsimile Transmission No.	(571) 273-9900

Any inquiry concerning this communication should be directed to Minh Nguyen at telephone number 571-272-1748.

/Minh Nguyen/
Primary Examiner
CRU, AU 3991

Conferees

/Tuan H. Nguyen/
Primary Examiner
CRU, AU 3991

/TIMOTHY M SPEER/
Supervisory Patent Examiner, Art Unit 3991

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
90/014,476	03/19/2020	9686193	E4720-00206	1013

31013 7590 04/13/2020

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER
NGUYEN, MINH T

ART UNIT	PAPER NUMBER
3991	

MAIL DATE	DELIVERY MODE
04/13/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

KRAMER LEVIN NAFTALIS & FRANKEL LLP
INTELLECTUAL PROPERTY DEPARTMENT
1177 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. *90/014,476* .

PATENT UNDER REEXAMINATION *9686193* .

ART UNIT *3991* .

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified *ex parte* reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the *ex parte* reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Ex Parte Reexamination Interview Summary – Pilot Program for Waiver of Patent Owner's Statement	**Control No.** 90/014,476	**Patent Under Reexamination is Requested** 9686193	
	Examiner MINH NGUYEN	**Art Unit** 3991	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

All participants (USPTO official and patent owner):

(1) SHANETTE BROWN (3) _____

(2) _____ (4) _____

Date of Telephonic Interview: 06 April 2020.

A. The USPTO official requested waiver of the patent owner's statement pursuant to the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The patent owner **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

☐ The patent owner **did not agree** to waive its right to file a patent owner's statement under 35 U.S.C. 304 at this time.

☑ USPTO personnel were unable to reach the patent owner.**

B. The Patent Owner of record telephoned the Office and indicated they would like to participate in the pilot program for waiver of patent owner's statement in *ex parte* reexamination proceedings.*

☐ The Patent owner of record telephoned the Office and **agreed** to waive its right to file a patent owner's statement under 35 U.S.C. 304 in the event reexamination is ordered for the above-identified patent.

The patent owner is not required to file a written statement of this telephone communication under 37 CFR 1.560(b) or otherwise. However, any disagreement as to this interview summary must be brought to the immediate attention of the USPTO, and no later than one month from the mailing date of this interview summary. Extensions of time are governed by 37 CFR 1.550(c).

*For more information regarding this pilot program, see *Pilot Program for Waiver of Patent Owner's Statement in Ex Parte Reexamination Proceedings, 75 Fed. Reg.* 47269 (August 5, 2010), available on the USPTO Web site at http://www.uspto.gov/patents/law/notices/2010.jsp.

**The patent owner may contact the USPTO personnel at (571) 272-7705 or at the telephone number provided below if the patent owner decides to waive the right to file a patent owner's statement under 35 U.S.C. 304.

/SHANETTE BROWN/ (571)272-6632

Signature and telephone number of the USPTO official, who contacted, was contacted by, or attempted to contact the patent owner.

cc: Requester (if third party requester)

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: Centripetal Networks, Inc.

Application No./Patent No.: 9686193 Filed/Issue Date: June 20, 2017

Titled: FILTERING NETWORK DATA TRANSFERS

Centripetal Networks, Inc., a company

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Sean Moore To: Centripetal Networks, Inc.

The document was recorded in the United States Patent and Trademark Office at Reel 034992, Frame 0949, or for which a copy thereof is attached.

2. From: Centripetal Networks, Inc. To: Douglas A. Smith

The document was recorded in the United States Patent and Trademark Office at Reel 042056, Frame 0098, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: Douglas A. Smith To: Centripetal Networks, Inc.

The document was recorded in the United States Patent and Trademark Office at
Reel 048492, Frame 0499, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Jonathan S. Caplan/	April 3, 2020
Signature	Date
Jonathan S. Caplan	38,094
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

US009686193B2

(12) **United States Patent**
Moore

(10) **Patent No.: US 9,686,193 B2**
(45) **Date of Patent: Jun. 20, 2017**

(54) **FILTERING NETWORK DATA TRANSFERS**

(71) Applicant: **Centripetal Networks, Inc.**, Herndon, VA (US)

(72) Inventor: **Sean Moore**, Hollis, NH (US)

(73) Assignee: **Centripetal Networks, Inc.**, Herndon, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/625,486**

(22) Filed: **Feb. 18, 2015**

(65) **Prior Publication Data**

US 2016/0072709 A1 Mar. 10, 2016

Related U.S. Application Data

(63) Continuation of application No. 13/795,822, filed on Mar. 12, 2013, now Pat. No. 9,124,552.

(51) **Int. Cl.**

H04L 12/741	(2013.01)
H04L 29/06	(2006.01)
H04L 29/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 45/74*** (2013.01); ***H04L 63/0254*** (2013.01); ***H04L 63/0263*** (2013.01);
(Continued)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,098,172 A 8/2000 Coss et al.
6,147,976 A 11/2000 Shand et al.
(Continued)

FOREIGN PATENT DOCUMENTS

AU 2005328336 B2 9/2011
AU 2006230171 B2 6/2012
(Continued)

OTHER PUBLICATIONS

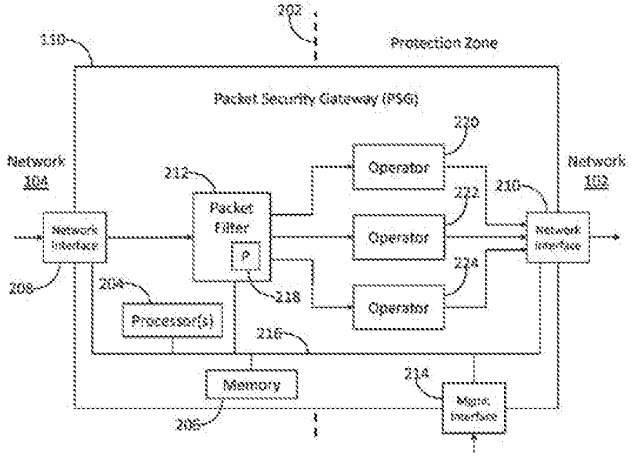
Greenwald et al., Designing an Academic Firewall: Policy, Practice, and Experience With SURF, Proceedings of SNDSS '96, IEEE, 1996, Department of Computer Science, Stanford University, Stanford, CA.
(Continued)

Primary Examiner — Anh Ngoc Nguyen
(74) *Attorney, Agent, or Firm* — Banner & Witcoff, Ltd.

(57) **ABSTRACT**

Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.

20 Claims, 4 Drawing Sheets



(52) U.S. Cl.
CPC *H04L 63/1466* (2013.01); *H04L 67/02* (2013.01); *H04L 69/22* (2013.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,226,372	B1	5/2001	Beebe et al.	
6,317,837	B1	11/2001	Kenworthy	
6,484,261	B1	11/2002	Wiegel	
6,611,875	B1	8/2003	Chopra et al.	
6,662,235	B1	12/2003	Callis et al.	
7,089,581	B1	8/2006	Nagy et al.	
7,107,613	B1	9/2006	Chen et al.	
7,215,637	B1	5/2007	Ferguson et al.	
7,227,842	B1	6/2007	Ji et al.	
7,237,267	B2	6/2007	Rayes et al.	
7,263,099	B1	8/2007	Woo et al.	
7,299,353	B2	11/2007	Le Pennec et al.	
7,331,061	B1	2/2008	Ramsey et al.	
7,478,429	B2	1/2009	Lyon	
7,539,186	B2	5/2009	Aerrabotu et al.	
7,610,621	B2	10/2009	Turley et al.	
7,684,400	B2	3/2010	Govindarajan et al.	
7,710,885	B2	5/2010	Ilnicki et al.	
7,721,084	B2	5/2010	Salminen et al.	
7,818,794	B2	10/2010	Wittman	
7,954,143	B2	5/2011	Aaron	
8,004,994	B1	8/2011	Darisi et al.	
3,042,167	A1	10/2011	Fulp et al.	
8,037,517	B2	10/2011	Fulp et al.	
8,117,655	B2 *	2/2012	Spielman	H04L 12/2602 726/12
8,176,561	B1	5/2012	Hurst et al.	
8,308,994	B2	11/2012	Kenworthy	
8,495,725	B2	7/2013	Ahn	
8,726,379	B1	5/2014	Stiansen et al.	
8,806,638	B1	8/2014	Mani	
8,856,926	B2	10/2014	Narayanaswamy et al.	
8,935,785	B2	1/2015	Pandrangi	
9,094,445	B2	7/2015	Moore et al.	
9,134,552	B2	9/2015	Moore	
9,137,205	B2	9/2015	Rogers et al.	
9,154,446	B2	10/2015	Gemelli et al.	
9,160,713	B2	10/2015	Moore	
2001/0039579	A1	11/2001	Trcka et al.	
2001/0039624	A1	11/2001	Kellum	
2002/0016858	A1	2/2002	Sawada et al.	
2002/0038339	A1	3/2002	Xu	
2002/0049899	A1	4/2002	Kenworthy	
2002/0164962	A1	11/2002	Mankins et al.	
2002/0165949	A1	11/2002	Na et al.	
2002/0186683	A1 *	12/2002	Buck	H04L 63/029 370/352
2002/0198981	A1	12/2002	Corl et al.	
2003/0035370	A1	2/2003	Brustoloni	
2003/0097596	A1	5/2003	Syvanne	
2003/0105976	A1	6/2003	Copeland	
2003/0120822	A1	6/2003	Nurmela et al.	
2003/0123456	A1	7/2003	Denz et al.	
2003/0142681	A1	7/2003	Chen et al.	
2003/0145225	A1	7/2003	Bunton, III et al.	
2003/0154297	A1	8/2003	Suzuki et al.	
2003/0154399	A1	8/2003	Zuk et al.	
2003/0188192	A1	10/2003	Tang et al.	
2003/0212900	A1	11/2003	Liu et al.	
2004/0010712	A1	1/2004	Hui et al.	
2004/0073655	A1	4/2004	Kan et al.	
2004/0088542	A1	5/2004	Daude et al.	
2004/0093513	A1	5/2004	Cantrell et al.	
2004/0098511	A1 *	5/2004	Lin	H04L 49/329 709/249
2004/0151155	A1	8/2004	Jouppi	
2004/0177139	A1	9/2004	Schuba et al.	
2004/0193943	A1	9/2004	Angelino et al.	
2004/0199629	A1	10/2004	Bomer et al.	
2004/0205360	A1	10/2004	Norton et al.	
2004/0250124	A1	12/2004	Chesla et al.	
2005/0010765	A1	1/2005	Swander et al.	
2005/0024189	A1	2/2005	Weber	
2005/0114704	A1	5/2005	Swander	
2005/0117576	A1	6/2005	McDysan et al.	
2005/0125697	A1	6/2005	Tahara	
2005/0138204	A1	6/2005	Iyer et al.	
2005/0138353	A1	6/2005	Spies et al.	
2005/0141537	A1	6/2005	Kumar et al.	
2005/0183140	A1	8/2005	Goddard	
2005/0229246	A1	10/2005	Rajagopal et al.	
2005/0251570	A1	11/2005	Heasman et al.	
2005/0286522	A1	12/2005	Paddon et al.	
2006/0048142	A1	3/2006	Roese et al.	
2006/0053491	A1	3/2006	Khuti et al.	
2006/0070122	A1	3/2006	Bellovin	
2006/0104202	A1	5/2006	Reiner	
2006/0114899	A1	6/2006	Toumura et al.	
2006/0136987	A1	6/2006	Okuda	
2006/0137009	A1	6/2006	Chesla	
2006/0146879	A1	7/2006	Anthias et al.	
2006/0195896	A1	8/2006	Fulp et al.	
2006/0212572	A1	9/2006	Afek et al.	
2006/0248580	A1	11/2006	Fulp et al.	
2006/0262798	A1	11/2006	Joshi et al.	
2007/0083924	A1	4/2007	Lu	
2007/0211644	A1	9/2007	Ottamalika et al.	
2007/0240208	A1	10/2007	Yu et al.	
2008/0005795	A1	1/2008	Acharya et al.	
2008/0043739	A1	2/2008	Suh et al.	
2008/0072307	A1	3/2008	Maes	
2008/0077705	A1	3/2008	Li et al.	
2008/0163333	A1	7/2008	Kasralikar	
2008/0229415	A1	9/2008	Kapoor et al.	
2008/0235755	A1	9/2008	Blaisdell et al.	
2008/0279196	A1	11/2008	Friskney et al.	
2008/0301765	A1	12/2008	Nicol et al.	
2009/0138938	A1	5/2009	Harrison et al.	
2009/0172800	A1	7/2009	Wool	
2009/0222877	A1 *	9/2009	Diehl	H04L 63/1416 726/1
2009/0240698	A1 *	9/2009	Shukla	G06F 17/30286
2009/0328219	A1	12/2009	Narayanaswamy	
2010/0011433	A1	1/2010	Harrison et al.	
2010/0011434	A1	1/2010	Kay	
2010/0082811	A1 *	4/2010	Van Der Merwe	G06F 17/30867 709/225
2010/0095367	A1	4/2010	Narayanaswamy	
2010/0107240	A1 *	4/2010	Thaler	H04L 63/20 726/15
2010/0132027	A1	5/2010	Ou	
2010/0199346	A1	8/2010	Ling et al.	
2010/0211678	A1	8/2010	McDysan et al.	
2010/0232445	A1 *	9/2010	Bellovin	H04L 45/02 370/410
2010/0242098	A1	9/2010	Kenworthy	
2010/0268799	A1	10/2010	Maestas	
2010/0296441	A1	11/2010	Barkan	
2010/0303240	A1	12/2010	Beachem et al.	
2011/0055916	A1 *	3/2011	Ahn	H04L 63/0227 726/13
2011/0055923	A1	3/2011	Thomas	
2011/0088092	A1	4/2011	Nguyen et al.	
2011/0141906	A1	6/2011	Jayawardena et al.	
2011/0185055	A1	7/2011	Nappier et al.	
2011/0270956	A1	11/2011	McDysan et al.	
2012/0023576	A1	1/2012	Sorensen et al.	
2012/0106354	A1	5/2012	Pleshek et al.	
2012/0113987	A1	5/2012	Riddoch et al.	
2012/0240135	A1	9/2012	Risbood et al.	
2012/0264443	A1	10/2012	Ng et al.	
2012/0314617	A1	12/2012	Erichsen et al.	
2012/0331543	A1	12/2012	Bostrom et al.	
2013/0047020	A1 *	2/2013	Hershko	H04L 67/02 713/323
2013/0059527	A1	3/2013	Hasesaka et al.	
2013/0061294	A1	3/2013	Kenworthy	
2013/0117852	A1	5/2013	Stute	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2013/0254766	A1	9/2013	Zuo et al.	
2013/0305311	A1*	11/2013	Puttaswamy Naga	H04L 63/0263 726/1
2014/0075510	A1	3/2014	Sonoda et al.	
2014/0115654	A1	4/2014	Rogers et al.	
2014/0201123	A1	7/2014	Ahn et al.	
2014/0215574	A1	7/2014	Erb et al.	
2014/0281030	A1	9/2014	Cui et al.	
2014/0283004	A1	9/2014	Moore	
2014/0283030	A1	9/2014	Moore et al.	
2014/0366132	A1	12/2014	Stiansen et al.	
2015/0237012	A1	8/2015	Moore	
2015/0304354	A1	10/2015	Rogers et al.	
2015/0334125	A1	11/2015	Bartos et al.	

FOREIGN PATENT DOCUMENTS

CA	2600236	A1	10/2006
EP	1086761	A2	6/2000
EP	1313290	A1	5/2003
EP	1484884	A2	12/2004
EP	1677484	A2	7/2006
EP	2385676	A1	11/2011
EP	2498442	A1	9/2012
EP	1864226	B1	5/2013
KR	20010079361	A	8/2001
WO	2005046145	A1	5/2005
WO	2006093557	A2	9/2006
WO	2006105093	A2	10/2006
WO	2007109541	A2	9/2007
WO	2011038420	A2	3/2011
WO	2012146265	A1	11/2012

OTHER PUBLICATIONS

Reumann et al., Adaptive Packet Filters, IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI.

Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, IEEE, 2004, NTT Information Sharing Platform Laboratories.

Kindervag et al., Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Nov. 5, 2010, Forrester Research, Inc., Cambridge MA.

Moore, SBIR Case Study: Centripetal Networks, How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company, Cyber Security Division, 2012 Principal Investigators' Meeting, Oct. 10, 2012, Centripetal Networks, Inc.

Designing a Zero Trust Network With Next-Generation Firewalls, Palo Alto Networks: Technology Brief, viewed Oct. 21, 2012, Palo Alto Networks, Santa Clara, CA.

Control Plane Policing Implementation Best Practices, Mar. 13, 2013, Cisco Systems.

International Search Report and Written Opinion for International App. No. PCT/US2013/057502, dated Nov. 7, 2013.

International Search Report and Written Opinion for International App. No. PCT/US2013/072566, dated Mar. 24, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2014/023286, dated Jun. 24, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2014/027723, dated Jun. 26, 2014.

International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated Sep. 16, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated May 7, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated Sep. 24, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated Sep. 24, 2015.

Communication Relating to the Results of the Partial International Search for International App. No. PCT/US2015/024691, dated Jul. 10, 2015.

International Preliminary Report on Patentability for International App. No. PCT/US2013/072566, dated Jul. 23, 2015.

Statement RE: Related Application, dated Jul. 24, 2015.

Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, Jan. 2005, Second IEEE Consumer Communications and Networking Conference, pp. 599-601.

John Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc., Nov. 5, 2010, pp. 1-26.

Palo Alto Networks; "Designing a Zero Trust Network With Next-Generation Firewalls"; pp. 1-10, last viewed on Oct. 21, 2012.

Jan. 11, 2016---(US) Non Final Rejection---U.S. Appl. No. 14/698,560.

Apr. 27, 2011---(WO) International Search Report and Written Opinion---App PCT/US2010/054520.

Mar. 4, 2011---(US) Notice of Allowance---U.S. Appl. No. 11/316,331.

Mar. 3, 2011---(EP) Communication Pursuant to Rules 70(2) and 70a(2)---App 06758213.0.

Feb. 14, 2011---(EP) Search Report---App 06758213.0.

Fulp, Errin. "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pp. 1-5 (Copyright 2010).

Sep. 30, 2010---(US) Office Action---U.S. Appl. No. 11/390,976.

Sep. 10, 2010---(AU) Office Action---App 2006230171.

Aug. 20, 2010---(AU) Office Action---App 2005328336.

Jun. 23, 2010---(US) Final Rejection---U.S. Appl. No. 11/316,331.

Apr. 29, 2010---(US) Interview Summary---U.S. Appl. No. 11/390,976.

Mar. 26, 2010---(US) Final Rejection---U.S. Appl. No. 11/390,976.

Sep. 14, 2009 (US) Office Action---U.S. Appl. No. 11/316,331.

Jun. 24, 2009---(US) Office Action---U.S. Appl. No. 11/390,976.

Jul. 3, 2008---(WO) Written Opinion of the International Searching Authority---App PCT/US06/11291.

Aug. 31, 2007---(EP) Communication Pursuant to Rules 109 and 110---App 05857614.1.

Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pp. 1-11 (2007).

Sep. 11, 2006---(WO) Written Opinion of the International Searching Authority---App PCT/US05/47008.

Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pp. 1-6 (2006).

Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005).

E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, Jan. 2004.

E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004.

E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004.

E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded Sep. 2003.

E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003.

V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003.

M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS, Oct. 2002.

Lee et al., "Development Framework for Firewall Processors," IEEE, pp. 352-355 (2002).

L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, Jun. 2001.

(56) **References Cited**

OTHER PUBLICATIONS

D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001.
E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001.
S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001.
G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001.
P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001.
D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): Feb. 2000.
A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000.
X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000.
A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000.
O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.
J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1209, Jun. 1999.
C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999.
R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999.
S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999.
J. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998.
V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998.
M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997.
S.M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994.
W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1), 15, 1994.
G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991.
M. Al-Suwaiyel et al., "Algorithms for Trie Compaction", ACM Transactions on Database Systems, 9(2): 243-263, Jun. 1984.
D. Comer, "Analysis of a Heuristic for Full Trie Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sep. 1981.
R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979.
E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion nTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978.
J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978.
R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976.
W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956.
Bellion, "High Performance Packet Classification", http://www.hipac.org (Publication Date Unknown).
Oct. 18, 2011---(EP) Communication Pursuant to Article 94(3)---App 08 758 213.0.
Jan. 9, 2011---(US) Notice of Allowance---U.S. Appl. No. 11/390,976.
Jan. 26, 2012---(EP) Extended Search Report---App 05857614.1.
Jan. 9, 2012---(AU) Notice of Acceptance---App 2006230171.
Nov. 11, 2011---(AU) Second Office Action---App 2006230171.
Jan. 17, 2013---(CA) Office Action---App 2,600,236.
Jan. 16, 2013---(CA) Office Action---App 2,594,020.
Nov. 20, 2012---(EP) Communication under rule 71(3)---App 06 758 213.0.
Apr. 18, 2013---(EP) Decision to Grant a European Patent---App 06758212.0.
Aug. 25, 2011---(US) Non Final Rejection---U.S. Appl. No. 12/871,806.
Feb. 6, 2012---(US) Final Rejection---U.S. Appl. No. 12/871,806.
Aug. 7, 2012---(US) Non Final Rejection---U.S. Appl. No. 12/871,806.
Nov. 26, 2012---(US) Final Rejection---U.S. Appl. No. 12/871,806.
Apr. 4, 2013---(US) Notice of Allowance---U.S. Appl. No. 12/871,806.
Jan. 14, 2015---(EP) Extended Search Report---App 08819667.6.
May 26, 2014---(CA) Office Action---App 2010297968.
May 25, 2015---(AU) Notice of Acceptance---App 2010297968.
May 14, 2015---(US) Non Final Rejection---U.S. Appl. No. 13/940,240.
Nov. 27, 2015---(US) Final Rejection---U.S. Appl. No. 13/940,240.
Jul. 10, 2015---(WO) Communication Relating to the Results of the Partial International Search for International App---PCT/US2015/026691.
Jul. 23, 2015---(WO) International Preliminary Report on Patentability---App PCT/US2013/072566.
Jan. 28, 2016---(WO) International Search Report and Written Opinion---App PCT/US2015/062691.
Dec. 22, 2015---(US) Final Office Action---U.S. Appl. No. 14/714,207.
Feb. 26, 2016---(US) Non Final Office Action---U.S. Appl. No. 14/753,992.
Apr. 15, 2016---(US) Notice of Allowance---U.S. Appl. No. 14/855,374.
Nov. 2, 2015---(AU) Office Action---App 2013372879.
Apr. 26, 2016---(US) Office Action---U.S. Appl. No. 14/745,207.
May 6, 2016---(US) Office Action---U.S. Appl. No. 14/714,207.
May 13, 2016---(US) Office Action---U.S. Appl. No. 13/940,240.
Feb. 25, 2016---(AU) Office Action---App 2014268055.
Feb. 24, 2016---(AU) Office Action---App 2014228257.
Jun. 9, 2016---(WO) International Search Report---PCT/US2016/026339.
Jun. 16, 2016---(CA) Office Action---App 2,888,935.
Jul. 11, 2016---(EP) Office Action---App 14720824.3.
Jul. 22, 2016---(US) Office Action---U.S. Appl. No. 14/921,718.
Jul. 29, 2016---(AU) Office Action---App 2013335255.
Oct. 5, 2016---(US) Notice of Allowance---U.S. Appl. No. 14/698,560.
Sep. 13, 2016---(CA) Office Action---App 2,902,206.
Sep. 14, 2016---(CA) Office Action---App 2,891,737.
Sep. 26, 2016---(CA) Office Action---App 2,902,158.
Oct. 26, 2016---(US) Office Action---U.S. Appl. No. 13/940,240.
Nov. 21, 2016---(US) Office Action---U.S. Appl. No. 14/745,207.
Dec. 5, 2016---(US) Notice of Allowance---U.S. Appl. No. 14/714,207.
Feb. 15, 2017---(US) Notice of Allowance---U.S. Appl. No. 14/921,718.
Apr. 12, 2017---(US) Office Action---U.S. Appl. No. 14/757,638.

* cited by examiner

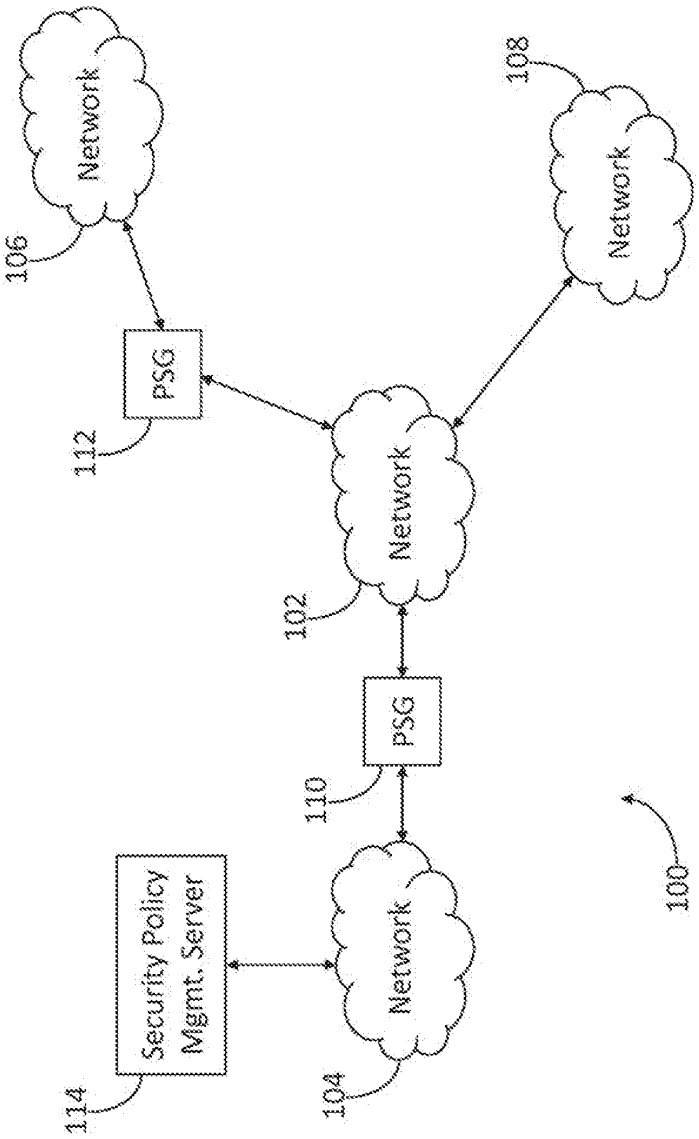

Network
106
PSG
112
Network
102
Network
108
PSG
110
Security Policy
Mgmt. Server
114
Network
104
100

FIG. 1

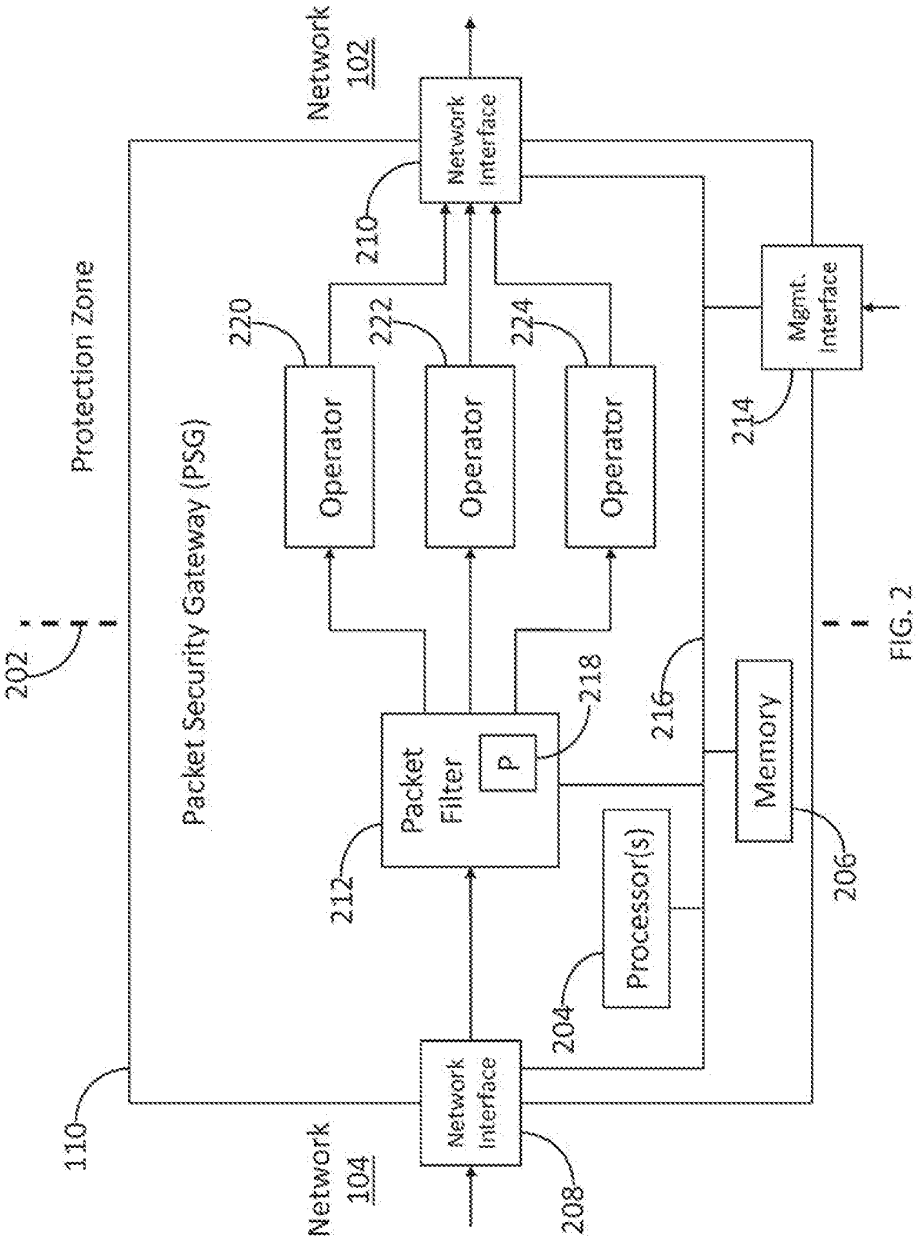
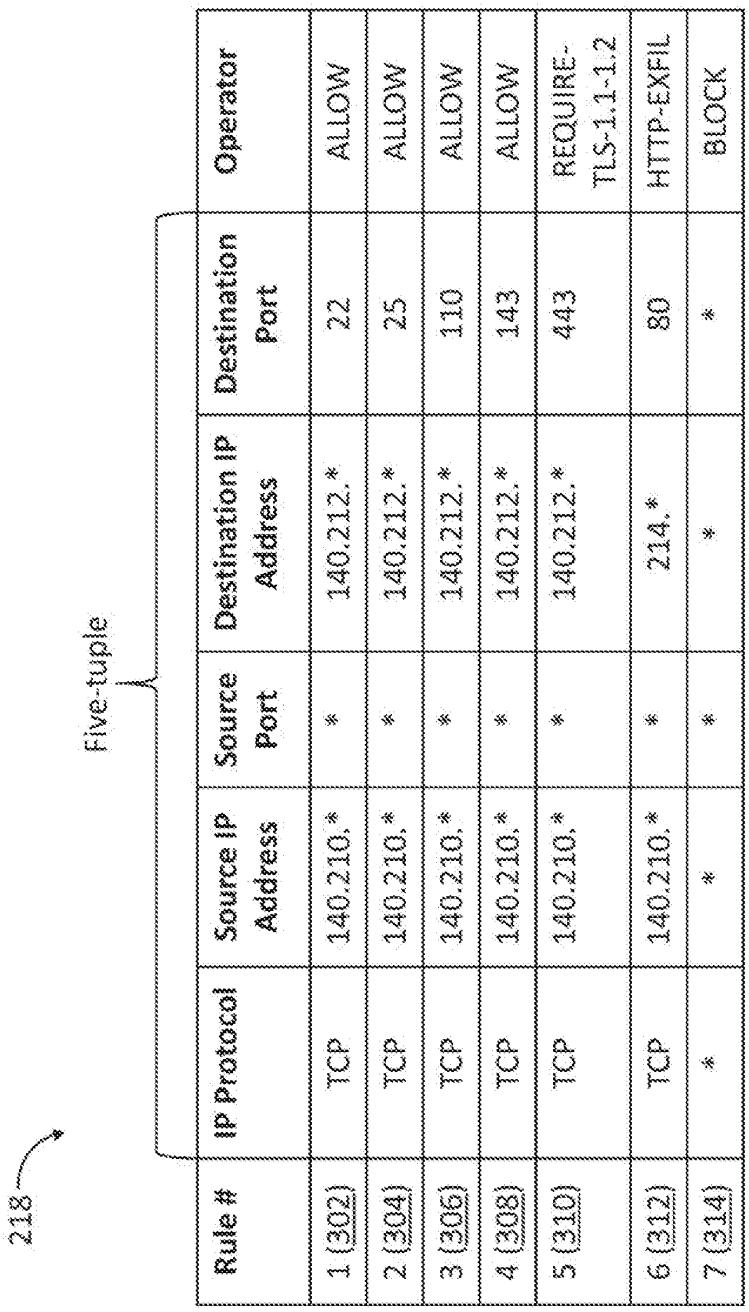

Network 102
Network Interface
210
220
222
224
Operator
Operator
Operator
Mgmt. Interface
214
Protection Zone
202
Packet Security Gateway (PSG)
Packet Filter
P
218
216
Memory
212
206
Processor(s)
204
110
Network 104
Network Interface
208

FIG. 2



Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

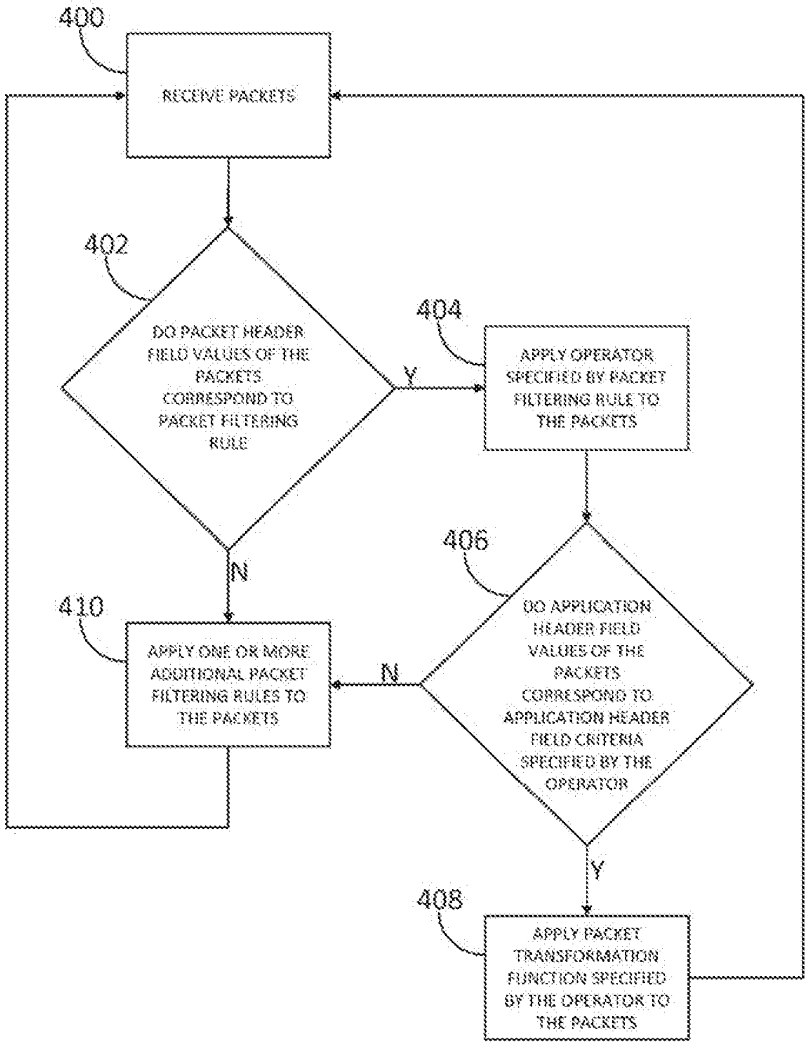

400
RECEIVE PACKETS
402
DO PACKET HEADER FIELD VALUES OF THE PACKETS CORRESPOND TO PACKET FILTERING RULE
Y
404
APPLY OPERATOR SPECIFIED BY PACKET FILTERING RULE TO THE PACKETS
N
406
DO APPLICATION HEADER FIELD VALUES OF THE PACKETS CORRESPOND TO APPLICATION HEADER FIELD CRITERIA SPECIFIED BY THE OPERATOR
N
410
APPLY ONE OR MORE ADDITIONAL PACKET FILTERING RULES TO THE PACKETS
Y
408
APPLY PACKET TRANSFORMATION FUNCTION SPECIFIED BY THE OPERATOR TO THE PACKETS

FIG. 4

FILTERING NETWORK DATA TRANSFERS

CROSS-REFERENCE TO RELATED APPLICATION

This application is a continuation of and claims priority to U.S. patent application Ser. No. 13/795,822, filed Mar. 12, 2013, and entitled "FILTERING NETWORK DATA TRANSFERS," the disclosure of which is incorporated by reference herein in its entirety and made part hereof.

BACKGROUND

The TCP/IP network protocols (e.g., the Transmission Control Protocol (TCP) and the Internet Protocol (IP)) were designed to build large, resilient, reliable, and robust networks. Such protocols, however, were not originally designed with security in mind. Subsequent developments have extended such protocols to provide for secure communication between peers (e.g., Internet Protocol Security (IPsec)), but the networks themselves remain vulnerable to attack (e.g., Distributed Denial-of-Service (DDoS) attacks, phishing attacks, and the like).

A category of cyber attack known as exfiltrations (e.g., stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent. A first cause is that many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web, that often appear to an observer (e.g., a conventional cyber defense system) as normal network behavior. A second cause is that typical network trust models, such as those used by network firewalls, interpret exfiltrations as trusted operations. A third cause is that human users often knowingly or unknowingly engage in network activities that are vulnerable to attack. A fourth cause is the general inability of conventional cyber defense systems to scale sufficiently to counter a cyber threat, for example, with respect to traffic volumes, network link speeds, network performance (e.g., latency and packet loss requirements), network usage policy enforcement, etc. Accordingly, many cyber attacks (e.g., DDoS attacks and exfiltrations) leverage Internet-scale characteristics to achieve their goals. Moreover, beyond those enumerated here, there are other causes for the failure of conventional, state-of-the-art cyber defense systems to prevent cyber attacks, such as exfiltrations.

SUMMARY

The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is neither intended to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts in a simplified form as a prelude to the detailed description below.

Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.

In some embodiments, a network packet filter may be located at a boundary between a secured network and an unsecured network (e.g., the Internet). The filter may observe packets traversing the network link between the secured network and the unsecured network. The filter may be capable of comparing certain packet header information (e.g., source and destination IP address(s), source and destination port(s), and protocol type(s)) with one or more packet filtering rules, which may define a network usage policy or network security policy. One or more of the rules may be associated with an operator that may be applied to a packet that matches one or more criteria specified by the rule.

Such packet filters may implement at least two operators: an identity operator, which may allow the packet to continue towards its destination, and a null operator which may prevent, or block, the packet from continuing towards its destination. In some embodiments, the network packet filter may implement one or more additional operators having the capability to determine if a packet contains an application-level header that specifies a particular method associated with a data transfer protocol; and, if so, whether to apply an identity operator or null operator to the packet. To distinguish a network packet filter that implements said additional operators from network packet filters that do not, a network packet filter that implements such additional operators will be referred to hereinafter as a packet security gateway (PSG).

For example, such an operator may be able to perform one or more of the following functions: (1) determine if an IP packet traversing a boundary contains an HTTP packet (e.g., an application-level HTTP packet) that specifies one or more specific HTTP methods (e.g., GET, PUT, POST, etc.), and (2) allow the packet (e.g., if a GET method is specified), or block the packet (e.g., if a PUT or POST method is specified). One or more administrators of the secured network may associate such an operator with one or more rules in a network security policy in order to enforce, via the PSG, a Web usage policy that may, for example, allow users to surf (e.g., GET) to one or more web sites attached to the Internet, but may prevent such user(s) from one or more of writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more web sites. For example, administrator(s) may utilize such functionality to prevent one or more exfiltrations (e.g., file transfers containing sensitive information, posting of login credentials (usernames and passwords), etc.) to network nodes (e.g., web sites) that they may not trust.

Other details and features will be described in the sections that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements.

FIG. **1** illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented.

FIG. **2** illustrates an exemplary packet security gateway.

FIG. **3** illustrates an exemplary dynamic security policy with operators that filter on data transfer protocol, or application-layer protocol, header information.

FIG. **4** illustrates an exemplary method for protecting a secured network by enforcing one or more network usage policies or network security policies.

DETAILED DESCRIPTION

In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the present disclosure.

Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless, physical or logical. In this respect, the specification is not intended to be limiting.

FIG. **1** illustrates an exemplary network environment **100** in which one or more aspects of the disclosure may be implemented. Referring to FIG. **1**, network **102** may function as an interconnect between networks **104**, **106**, and **108**. For example, network **102** may be the public Internet, or some other large TCP/IP network functioning as an interconnect between one or more Local Area Networks (LANs) or Wide-Area Networks (WANs), (e.g., the Non-classified Internet Protocol (IP) Router Network (NIPRNet), operated by the United States Defense Information Systems Agency (DISA)). Networks **104**, **106**, and **108** may be LANs or WANs operated by or otherwise associated with various organizations (e.g., one or more commercial enterprises, companies, universities, military commands, government agencies, or cyber criminal organizations).

For example, a geographically distributed commercial enterprise X may own and operate networks **104** and **106**, and use network **102** (e.g., the Internet) to interconnect networks **104** and **106**, and to access other networks (e.g., other networks not owned or operated by enterprise X) attached to network **102**. One or more computing devices (e.g., workstations, servers, etc.) of enterprise X may be attached to network **104** or **106**. Network **108** may be owned and operated by a cyber criminal organization Z, which may attempt to steal information (e.g., sensitive data) from enterprise X, for example, via network **102**. Members of organization Z may attach one or more computing devices (e.g., workstations or servers) to network **108**, and may use these workstation(s) or server(s) to attack or collect data from one or more networks affiliated with enterprise X (e.g., network **104** or **106**).

As used herein, a packet security gateway (PSG) may include one or more computing devices configured to receive packets, and apply one or more filters or operators, including an identity (e.g., allow) or null (e.g., block) operator, to the packets. In some embodiments, a packet security gateway may be configured to apply one or more additional operators as described herein. As used herein, a security policy management server may include one or more computing devices configured to communicate a dynamic security policy to a packet security gateway. In some embodiments, a security policy management server may be configured to perform one or more additional functions as described herein. As used herein, a dynamic security policy may include one or more rules, messages, instructions, files, data structures, or the like specifying criteria corresponding to one or more packets and may identify one or more operators to be applied to packets corresponding to the specified criteria. In some embodiments, a dynamic security policy may specify one or more additional parameters as described herein.

Network environment **100** may include one or more packet security gateways and one or more security policy management servers. For example, network environment **100** may include packet security gateways **110** and **112**, and security policy management server **114**. One or more security policy management servers may be associated with a protected network. For example, networks **104** and **106** may each be distinct LANs associated with a common enterprise X, and may each form part of a protected or secured network associated with security policy management server **114**. Enterprise X may desire to prevent cyber attacks (e.g., exfiltrations) from one or more of its networks (e.g., network **104** or **106**). Accordingly, it may locate one or more packet security gateways at each boundary between its networks and one or more public interconnect networks (e.g., network **102**), which may be utilized by a cyber criminal, such as organization Z, to attempt to remotely access its networks (e.g., network **104** or **106**), and which may, for example, potentially be used to attempt to transfer data from one or more of its networks (e.g., network **104** or **106**) to one or more networks affiliated with organization Z (e.g., network **108**). For example, packet security gateway **110** may protect network **104** from one or more cyber attacks (e.g., exfiltrations) mediated by network **102** (e.g., the Internet), and packet security gateway **112** may protect network **106** from one or more cyber attacks (e.g., exfiltrations) mediated by network **102**.

As will be described in greater detail below, each of one or more packet security gateways associated with a security policy management server may be configured to receive a dynamic security policy from a security policy management server, receive packets associated with a network protected by the packet security gateway, and perform one or more operations specified by the dynamic security policy on the packets. For example, each of packet security gateways **110** and **112** may be configured to receive a dynamic security policy from security policy management server **114**. Each of packet security gateways **110** and **112** may also be configured to receive packets associated with networks **104**, **106**, or **108**. Each of packet security gateways **110** and **112** may further be configured to apply one or more rules or operators specified by the dynamic security policy received from security policy management server **114** to packets associated with networks **104**, **106**, or **108**.

FIG. **2** illustrates an exemplary packet security gateway according to one or more aspects of the disclosure. Referring to FIG. **2**, as indicated above, packet security gateway **110** may be located at network boundary **202** between networks **104** and **102**. Packet security gateway **110** may include one or more processors **204**, memory **206**, network interfaces **208** and **210**, packet filter **212**, and management interface **214**. Processor(s) **204**, memory **206**, network interfaces **208** and **210**, packet filter **212**, and management interface **214** may be interconnected via data bus **216**. Network interface **208** may connect packet security gateway **110** to network **104**. Similarly, network interface **210** may connect packet security gateway **110** to network **102**. Memory **206** may

include one or more program modules that when executed by processor(s) **204**, may configure packet security gateway **110** to perform one or more of various functions described herein.

Packet security gateway **110** may be configured to receive a dynamic security policy from security policy management server **114**. For example, packet security gateway **110** may receive dynamic security policy **218** from security policy management server **114** via management interface **214** (e.g., via out-of-band signaling) or network interface **208** (e.g., via in-band signaling). Packet security gateway **110** may include one or more packet filters or packet discriminators, or logic for implementing one or more packet filters or packet discriminators. For example, packet security gateway **110** may include packet filter **212**, which may be configured to examine information associated with packets received by packet security gateway **110** and forward such packets to one or more of operators **220**, **222**, or **224** based on the examined information. For example, packet filter **212** may examine information associated with packets received by packet security gateway **110** (e.g., packets received from network **104** via network interface **208**) and forward the packets to one or more of operators **220**, **222**, or **224** based on the examined information.

As will be described in greater detail below, dynamic security policy **218** may include one or more rules and the configuration of packet filter **212** may be based on one or more of the rules included in dynamic security policy **218**. For example, dynamic security policy **218** may include one or more rules specifying that packets having specified information should be forwarded to operator **220**, that packets having different specified information should be forwarded to operator **222**, and that all other packets should be forwarded to operator **224**. Operators **220**, **222**, and **224** may be configured to perform one or more functions on packets they receive from packet filter **212**. For example, one or more of operators **220**, **222**, or **224** may be configured to forward packets received from packet filter **212** into network **102**, forward packets received from packet filter **212** to an IPsec stack (not illustrated) having an IPsec security association corresponding to the packets, or drop packets received from packet filter **212**. In some embodiments, one or more of operators **220**, **222**, or **224** may be configured to drop packets by sending the packets to a local "infinite sink" (e.g., the /dev/null device file in a UNIX/LINUX system).

FIG. **3** illustrates an exemplary dynamic security policy in accordance with one or more embodiments. Referring to FIG. **3**, dynamic security policy **218** may include rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, 6 **312**, and 7 **314**. Each of these rules may specify criteria and one or more operators that may be applied to packets associated with (e.g., matching) the specified criteria. The specified criteria may take the form of a five-tuple, which may, for example, comprise one or more values selected from, packet header information, specifying a protocol type of the data section of an IP packet (e.g., TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or one or more other protocols), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

For example, rule 1 **302** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **22** (e.g., associated with the Secure Shell (SSH) protocol) should have an ALLOW operator (e.g., an identity operator) applied to them. Similarly, rule 2 **304** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **25** (e.g., associated with the Simple Mail Transfer Protocol (SMTP)) should have an ALLOW operator applied to them.

Rule 3 **306** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **110** (e.g., associated with Post Office Protocol version 3 (POP3)) should have an ALLOW operator applied to them.

Rule 4 **308** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **143** (e.g., associated with the Internet Message Access Protocol (IMAP)) should have an ALLOW operator applied to them.

Rule 5 **310** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port **443** (e.g., associated with the port for the Hypertext Transfer Protocol Secure (HTTPS) protocol) should have a specified Transport Layer Security (TLS) protocol (e.g., REQUIRE-TLS 1.1-1.2) operator (as described in greater detail below) applied to them.

Rule 7 **314** may be a "wildcard" rule and may apply a BLOCK operator (e.g., a null operator which "drops" any packets it is applied to) to any packets that do not match the criteria of any of Rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, or 6 **312** (e.g., when rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, 6 **312**, and 7 **314** are applied to packets in a linear fashion).

As described above with respect to FIG. **1**, networks **104** and **106** may be owned or operated by enterprise X. Enterprise X may have allocated IPv4 addresses 140.210.0.0/16 to network **104**, and IPv4 addresses 140.212.0.0/16 to network **106**. Enterprise X may have loaded PSG **110** with dynamic security policy **218**, and may utilize PSG **110** to enforce one or more network security policies embodied in one or more rules of dynamic security policy **218** to restrict network communications between networks **104** and **106** (e.g., to secure system logins, e-mail, encrypted web sessions, and the like). For example, based on standard usage of ports, rule 1 **302** may allow any hosts attached to network **104** to conduct Secure Shell (SSH) sessions (e.g., system logins) with any hosts attached to network **106**; rule 2 **304** may allow any e-mail servers attached to network **104** to conduct SMTP sessions (e.g., e-mail transfer sessions) with any e-mail servers attached to network **106**; rule 3 **306** and rule 4 **308**, may respectively allow e-mail clients attached to network **104** to conduct POP3 and IMAP sessions (e.g., e-mail download sessions into a webmail browser application) with any e-mail servers attached to network **106**; and rule 5 **310** may allow web browsers attached to network **104** to conduct HTTPS sessions (e.g., secure web sessions) with any web servers attached to network **106**, but may, as described in greater detail below, utilize the REQUIRE-TLS-1.1-1.2 operator to ensure that only HTTPS secure web sessions using version 1.1 or 1.2 of the Transport Layer Security (TLS) protocol to secure such HTTPS sessions are allowed (e.g., because the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions).

Rule 6 **312** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210., having any source port, destined for an IP address that begins with 200.214, and destined for port **80** (e.g., associated with the HTTP protocol) should have an HTTP-EXFIL operator applied to them. As described in greater detail below, an HTTP-EXFIL operator may allow HTTP packets containing a GET method, but may block HTTP packets containing other HTTP methods (e.g., PUT, POST, CONNECT, etc.). Such an operator may thus allow a web browser to "surf the web" (e.g., download web pages hosted by web servers), but may prevent the web browser from writing files to a web server (e.g., using the PUT method), posting forms (e.g., forms that might contain login credentials, such as usernames or passwords) to a web server (e.g., using the POST method), or otherwise communicating with a web server (e.g., using any HTTP method except GET). Because attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data, operators such as HTTP-EXFIL may be used to stop such exfiltrations.

Returning to the example described above, organization Z may own or operate network **108**, and may have allocated network IP addresses 214.0.0.0/8 to network **108**. Enterprise X may not have a business relationship with organization Z, and may therefore not consider network **108** to be trusted. While enterprise X could simply block all communications to networks that are owned or operated by organizations it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet. Enterprise X's employees, therefore, could not freely surf the Web, which may restrict the employees' ability to conduct business on behalf of enterprise X. By enforcing sets of rules similar to rule 6 **312** that may apply operators like or similar to HTTP-EXFIL, enterprise X may enable its employees to freely surf the web and conduct company business, but may prevent one or more cyber attacks (e.g., HTTP-mediated exfiltrations).

One function of operators like HTTP-EXFIL and REQUIRE-TLS-1.1-1.2 may be to inspect fields in the headers of application packets contained in IP packets, determine field values, and depending on the field values, decide to allow, block, or otherwise apply a packet transformation function (e.g., encapsulate the packet into a tunnel, alter one or more header field values, etc.) to the packets. The logic for this function may be executed by one or more of operators **220**, **222**, or **224**. The logic may be developed in a high-level programming language such as C. An example of such programmatic logic, written in pseudocode, for the HTTP-EXFIL operator, is as follows:

```
Operator HTTP-EXFIL(ip-packet):
    Inspect app-pld(ip-packet) match GET return ALLOW;
    Inspect app-pld(ip-packet) match POST return BLOCK;
    Inspect app-pld(ip-packet) match PUT return BLOCK;
    Inspect app-pld(ip-packet) match DELETE return BLOCK;
    Inspect app-pld(ip-packet) match CONNECT return BLOCK;
    Return BLOCK;
End Operator HTTP-EXFIL;
```

Referring to the above-example, Operator HTTP-EXFIL may accept as input an IP packet that matches a rule, such as rule 6 **312** of dynamic security policy **218**. If the application packet contained in the IP packet is an HTTP packet, the value of the HTTP method field in the HTTP packet header may be compared to the values that encode the GET, POST, PUT, DELETE, and CONNECT methods. If a match is found, then the HTTP-EXFIL operator may return either ALLOW or BLOCK, depending on the method value. If no match is found, then the HTTP-EXFIL operator may return BLOCK.

An example of programmatic logic, written in pseudocode, for a REQUIRE-TLS-1.1-1.2 operator is provided below. The REQUIRE-TLS-1.1-1.2 operator may be associated with filter rules for HTTPS sessions, such as rule 5 **310** of dynamic security policy **218**. HTTPS may be used to encrypt HTTP sessions. HTTPS is not a protocol per se, but rather the result of layering the HTTP protocol on top of the TLS protocol. For an HTTPS session composed of IP packets, the application packets contained in the IP packets may be TLS Record Protocol packets. The header fields of TLS Record Protocol packets may not be encrypted. One of the header fields may contain a value indicating the TLS version.

Exemplary programmatic logic for a REQUIRE-TLS-1.1-1.2 operator, written in pseudocode, is as follows:

```
Operator REQUIRE-TLS-1.1-1.2(ip-packet):
    Inspect app-pld(ip-packet) match 1.0 return BLOCK;
    Inspect app-pld(ip-packet) match 1.1 return ALLOW;
    Inspect app-pld(ip-packet) match 1.2 return ALLOW;
    Return BLOCK;
End Operator REQUIRE-TLS-1.1-1.2;
```

Referring to the above-example, Operator REQUIRE-TLS-1.1-1.2 may accept as input an IP packet that matches a rule, such as rule 5 **310** of dynamic security policy **218**. If the application packet contained in the IP packet is a TLS Record Protocol packet, the value of the version field in the TLS Record Protocol packet header may be compared to the values that encode version numbers 1.0, 1.1, and 1.2. If a match is found, then the REQUIRE-TLS-1.1-1.2 operator may return either ALLOW or BLOCK, depending on the version number value. If no match is found, then the REQUIRE-TLS-1.1-1.2 operator may return BLOCK.

The filtering process described herein may be viewed as having two (2) stages: A first stage in which the "5-tuple" of IP packet header field values and transport protocol (e.g., TCP, UDP, etc.) packet header field values may be filtered; and, a second stage in which application packet header field values may be filtered (e.g., by applying operator logic similar to that described above). Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication (e.g., file read, file write, encrypted communication, etc.) between the resources. Such a method may, however, be used in other conceptual models.

The methods described above may be modified to achieve different functionality and may be extended to other data transfer protocols or to other application-layer protocols. These methods may provide network administrators with capabilities to enforce network usage policies and network security policies that have capabilities and functionalities beyond those described above. For example, these methods may provide network administrators with capabilities to prevent exfiltrations that are mediated by other data transfer protocols besides HTTP and HTTPS. Examples of such protocols include File Transfer Protocol (FTP) and messaging protocols such as eXtensible Messaging and Presence Protocol (XMPP). Moreover, new network applications may emerge in the future which may use new data transfer protocols or application-layer protocols to which the present

methods may be applied. These methods may also be used for purposes other than network policy enforcement and exfiltration prevention. For example, it may be useful for a packet filter to rapidly detect if an IP packet contains a Real-time Transport Protocol (RTP) application packet used to deliver audio or video information (e.g., if a cyber attack based on RTP has yet to be discovered, network administrators may choose to not process RTP packets through the cyber security defense systems that may be protecting their networks).

FIG. **4** illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments of the present disclosure. The steps may be performed at one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways **110** and **112** may be associated with security policy management server **114**, and the steps may be performed at packet security gateway **110** or **112**. At step **400**, packets may be received. For example, packet security gateway **110** may receive packets from network **104** via network interface **208** that are destined for network **106**. At step **402**, a determination may be made as to whether a portion of the received packets have packet header field values corresponding to a packet filtering rule. For example, a determination may be made as to whether a portion of the packets received from network **104** have packet header field values (e.g., one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to rule 5 **310**. At step **404**, responsive to determining that one or more of the portion of received packets have packet header field values corresponding to the packet filtering rule, an operator specified by the packet filtering rule may be applied to the portion of the received packets. For example, the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** may be applied to the portion of the received packets.

At step **406**, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator. For example, a determination may be made as to whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., application header field values corresponding to TLS version 1.1 or 1.2). At step **408**, responsive to determining that one or more of the portion of received packets have application header field values corresponding to one or more application header field criteria specified by the operator, a packet transformation function specified by the operator may be applied to the one or more of the portion of the received packets. For example, an ALLOW packet transformation function specified by the REQUIRE TLS-1.1-1.2 operator may be applied to the one or more of the portion of the received packets having application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., each of the one or more of the portion of the received packets may be allowed to continue toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (e.g., one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

Returning to step **406**, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator. For example, a determination may be made as to whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., application header field values corresponding to TLS version 1.1 or 1.2). Responsive to determining that one or more of the portion of received packets have application header field values that do not correspond to one or more application header field criteria specified by the operator, one or more additional packet filtering rules may be applied to the one or more of the portion of the received packets. For example, rule 7 **314** may be applied to the one or more of the portion of the received packets having application header field values that do not correspond to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (e.g., each of the one or more of the portion of the received packets may be blocked from continuing toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (e.g., one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

Returning to step **402**, a determination may be made as to whether a portion of the received packets have packet header field values corresponding to a packet-filtering rule. For example, a determination may be made as to whether a portion of the packets received from network **104** have packet header field values (e.g., one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to rule 5 **310**. Responsive to determining that the portion of received packets have packet header field values that do not correspond to the packet filtering rule, one or more additional packet filtering rules may be applied to the one or more of the portion of the received packets. For example, rule 7 **314** may be applied to the portion of received packets that do not have packet header field values that correspond to rule 5 **310** (e.g., each of the portion of the received packets may be blocked from continuing toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (e.g., one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more processors in a computer or other data processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired in various embodiments. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field programmable gate arrays (FPGA), and the like. Particular data structures may be used to more effectively implement one or more aspects of the disclosure,

and such data structures are contemplated to be within the scope of computer executable instructions and computer-usable data described herein.

Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

As described herein, the various methods and acts may be operative across one or more computing devices and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (e.g., a server, a client computer, etc.).

Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional.

What is claimed is:

1. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, each packet in first portion of packets; and

responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria wherein the data indicates that the second portion of packets is destined for a third network:

applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forwarding, by the computing system, each packet in the second portion of packets toward the third network.

2. The method of claim 1, wherein

the first portion of packets comprises data indicating: a protocol type associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules, and

the second portion of packets comprises data indicating a protocol type not associated with the particular type of data transfer.

3. The method of claim 1, wherein:

the first portion of packets comprises data indicating a first destination port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second destination port number not associated with the particular type of data transfer.

4. The method of claim 1, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol (HTTP), and corresponding to the criteria specified by the one or more packet-filtering rules, and

the second portion of packets does not comprise data associated with HTTP.

5. The method of claim 1, wherein:

the first portion of packets comprises data associated with hypertext transfer protocol secure (HTTPS), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with HTTPS.

6. The method of claim 1, wherein:

the first portion of packets comprises data associated with file transfer protocol (FTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with FTP.

7. The method of claim 1, wherein:

the first portion of packets comprises data associated with real-time transport protocol (RTP), and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets does not comprise data associated with RTP.

8. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets;

responsive to a determination by the computing system that a first packet of the plurality of packets comprises data associated with eXtensible messaging and presence protocol (XMPP) and the data corresponds to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network:

applying, by the computing system and to the first packet, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, the first packet; and

responsive to a determination by the computing system that a second packet of the plurality of packets does not comprise data associated with XMPP:

applying, by the computing system, to the second packet, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the second network; and

forwarding, by the computing system, the second packet toward the second network.

9. The method of claim 1, wherein:

receiving the plurality of packets comprises receiving packets comprising data associated with hypertext transfer protocol (HTTP);

the first portion of packets comprises a first type of data associated with HTTP;

the second portion of packets comprises a second type of data associated with HTTP; and

applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises the first type of data.

10. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP POST method.

11. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP PUT method.

12. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP DELETE method.

13. The method of claim 9, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to an HTTP CONNECT method.

14. The method of claim 9, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises the second type of data.

15. The method of claim 9, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to an HTTP GET method.

16. The method of claim 1, wherein applying the first operator configured to drop packets associated with the particular type of data transfer is performed responsive to a determination by the computing system that the first portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

17. The method of claim 1, wherein applying the first operator configured to forward packets not associated with the particular type of data transfer toward the second network is performed responsive to a determination by the computing system that the second portion of packets comprises data corresponding to a particular transport layer security (TLS) version value.

18. A system comprising:

at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

19. One or more non-transitory computer-readable media comprising instructions that when executed by one or more computing devices cause the one or more computing devices to:

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

drop each packet in the first portion of packets; and

responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and

forward each packet in the second portion of packets toward the third network.

20. The method of claim 1, wherein:

the first portion of packets comprises data indicating: a first source port number associated with the particular type of data transfer, and corresponding to the criteria specified by the one or more packet-filtering rules; and

the second portion of packets comprises data indicating a second source port number not associated with the particular type of data transfer.

* * * * *

Electronic Acknowledgement Receipt	
EFS ID:	38909698
Application Number:	90014476
International Application Number:	
Confirmation Number:	1013
Title of Invention:	FILTERING NETWORK DATA TRANSFERS
First Named Inventor/Applicant Name:	Sean Moore
Customer Number:	39290
Filer:	Patrick Dennis McPherson/Josh Staples
Filer Authorized By:	Patrick Dennis McPherson
Attorney Docket Number:	E4720-00206
Receipt Date:	19-MAR-2020
Filing Date:	
Time Stamp:	10:48:59
Application Type:	Reexam (Third Party)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$12000
RAM confirmation Number	E20203IA49409070
Deposit Account	041679
Authorized User	Josh Staples
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Receipt of Orig. Ex Parte Request by Third Party	193ReexamRequest.pdf	941021 4025f0433987e86850bafd25350fe2b5b85df305	no	97
Warnings:					
Information:					
2	Transmittal Letter	2TransmittalForm.pdf	248769 0254966cc8ba6e9385009178cb6b1e3d0a00a64e	no	3
Warnings:					
Information:					
3	Power of Attorney	3PowerofAttorney.pdf	97278 fe64cb330450da5335439ca3e14690a2a2f4b7b4	no	3
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	4IDS.pdf	1094750 71499926f9fa412c02e278a5876662a6150e5479	no	9
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Copy of patent for which reexamination is requested	EX-1001.pdf	3442592 790bf9fcaa09dcbab20a1af1c67d250ce05d10f2	no	16
Warnings:					
Information:					
6	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1002v1.pdf	9337288 be97a6ed92e1c4148506acddfaa379b4f370e0b7	no	165
Warnings:					

Information:					
7	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1002v2.pdf	11303287 f6f04f131adb3b2f312b80b93e58018e74535508	no	172
Warnings:					
Information:					
8	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1003.pdf	1904526 31d228320a7cb3108c512b386451d659785e9319	no	131
Warnings:					
Information:					
9	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v1of9v1.pdf	6977029 600a9bf5768f9f8d158bcc22adb771401ecaf834	no	100
Warnings:					
Information:					
10	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v1of9v2.pdf	14195554 9ba4b956500918c28d1e8b6c81633f07a58fe7a2	no	100
Warnings:					
Information:					
11	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v2of9v1.pdf	20448798 3a065d4ab7bb5247e0f65df9ea0a9172e7c2a6a0	no	70
Warnings:					
Information:					
12	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v2of9v2.pdf	19136360 0a0f3158363481b5f6ca27d7c0099962b7f813a8	no	70
Warnings:					
Information:					
13	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v2of9v3.pdf	6902290 3460bfe27d3b2a53f955927c63484f9cc18e0e11	no	60
Warnings:					
Information:					

14	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v3ofv9.pdf	6277916 060243d9ae1321ba58d0c7a19559c272715da04a	no	200
Warnings:					
Information:					
15	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v4of9.pdf	6231578 b6158ea2eca052db0e888c5e106f02dfc41c9eb5	no	200
Warnings:					
Information:					
16	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v5of9.pdf	6440406 a251667882633912 5f24616891cefae456cd84c6	no	400
Warnings:					
Information:					
17	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v6of9v1.pdf	22509974 5761b26c11ef90c37aa65cf2e68c776565e9d1a5	no	70
Warnings:					
Information:					
18	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v6of9v2.pdf	20939096 044d8878bbb180732fa8cedf470fb8b799a379ea	no	70
Warnings:					
Information:					
19	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v6of9v3.pdf	17220117 546a9a1ecf77810b3f65454de56596292632ec26	no	60
Warnings:					
Information:					
20	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v7of9.pdf	5416255 e473eeead6e28f7d5f11844a08fa3cd37bbafbe4	no	400
Warnings:					
Information:					

21	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v8of9.pdf	7747561 5a2a8d9ad8335e439c76e07c7fea9b754ace3434	no	200
Warnings:					
Information:					
22	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1004v9of9.pdf	3390383 a2f44bd96b64bb93e75a81d09a154c8f26d4ea98	no	123
Warnings:					
Information:					
23	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1005.pdf	810257 4278132fc3a4ba58d5fa15ba2915b84f0b49946c	no	12
Warnings:					
Information:					
24	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1006.pdf	12724459 f1eaddf9e4e5289ecde654b64669fd5f753eecc1	no	47
Warnings:					
Information:					
25	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1008.pdf	7380927 f96ffbc114e198f484c46def609927bcc4da5f7e	no	33
Warnings:					
Information:					
26	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1009.pdf	729458 1c01adf2cac76daa257e2309dd8c094f46f34c10	no	11
Warnings:					
Information:					
27	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1010.pdf	830783 ce4321d88f60803aca322db705d3500a9fa6327f	no	4
Warnings:					
Information:					

28	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1011.pdf	714902 57d1154440d66b9f7cd755b34b675c9eb9cd8eb9	no	4
Warnings:					
Information:					
29	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1013.pdf	240631 06a4f11a02198568365ac61ddab359ba38d4adec	no	1
Warnings:					
Information:					
30	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1014.pdf	302213 169ef7ecc4f2d506b56009b8a15edc107e9a250f	no	10
Warnings:					
Information:					
31	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1015.pdf	330443 4c92049fdab8ead2f50bf65716e03e0077d5fb73	no	82
Warnings:					
Information:					
32	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1016.pdf	299724 52b64311fc8a70e7b248f70cefaae71369b3c8bf	no	5
Warnings:					
Information:					
33	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1017.pdf	697515 6d0cc24f973e95dfbe445d1005d96f7156b7ce99	no	3
Warnings:					
Information:					
34	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1018.pdf	848874 d6bb03a5ecc95199932c892577774d12e3862fbe	no	4
Warnings:					
Information:					

35	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1020.pdf	637079 b3c3d64338bab18aa3e47f9ff8fbd1fda7a74c73	no	19
Warnings:					
Information:					
36	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1021.pdf	981006 15f5436d7f034cfc87f56f13489d5e7f0a02cd42	no	36
Warnings:					
Information:					
37	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1022.pdf	324881 7399572c70f640ae85ab1f6ddbb74c178306bafa	no	64
Warnings:					
Information:					
38	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1023.pdf	340431 7eaaa61951ce44dc269bf1818a06630f440bb320	no	41
Warnings:					
Information:					
39	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1024.pdf	3711803 76c2328754c9e946b5f32059befa733d7422d41f	no	10
Warnings:					
Information:					
40	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1025.pdf	1317370 ca3f9532c06f6686c617d8d83580743959e421d8	no	4
Warnings:					
Information:					
41	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1026.pdf	133725 11ec0fdf867cf08c8cbd4a4aa2531c399a30100e	no	34
Warnings:					
Information:					

42	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1027.pdf	2318111 884a89839fec1b9f18d4861fef39d6970f61a954	no	37
Warnings:					
Information:					
43	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1028v1.pdf	20339087 47e69774acf33d69da0930272a44a1f6bbf5700b	no	60
Warnings:					
Information:					
44	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1028v2.pdf	18715855 c743e2d2ab0532fe162c5acd552eeef3f118e8c9	no	60
Warnings:					
Information:					
45	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1028v3.pdf	21621954 e3ec817b583da5addfc0873f85ceb867418fa49c	no	60
Warnings:					
Information:					
46	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1028v4.pdf	18668259 dbebe0f9dc4e2e8ca7eb138352888cec1d0350d4	no	60
Warnings:					
Information:					
47	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1028v5.pdf	18352601 c25d0c65eed127d0496039e60821911dcab02758	no	60
Warnings:					
Information:					
48	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1028v6.pdf	9993519 73811c1ee6ef3e37d4292674fd8d198066af87d4	no	35
Warnings:					
Information:					

49	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1029.pdf	298555 dc8dcd6757622938d255e0a84b2f66c66a8d10a3	no	11
Warnings:					
Information:					
50	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1030.pdf	744601 817155311d792255e605ecf76332acd06d5bfd41	no	6
Warnings:					
Information:					
51	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1031.pdf	957497 b5c1760b8a93cce09231f6e9022c3d89cd413a82	no	25
Warnings:					
Information:					
52	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1032.pdf	303095 9b0cd99be4d1f9e4154411a7aa0914446b56388d	no	42
Warnings:					
Information:					
53	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1033.pdf	722982 b52cde8a0e48d377ed59f35f51b994095ce076ae	no	2
Warnings:					
Information:					
54	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1034.pdf	772714 7f0d864b8a8496525eae98d4a77f9e56344b74b1	no	3
Warnings:					
Information:					
55	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1035.pdf	293462 497cb453658dac3bed41a5f33fe79451f308a79c	no	52
Warnings:					
Information:					

56	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1036.pdf	765306 3c977838eef62a02f476c71553d95245f7ecb7b6	no	2
Warnings:					
Information:					
57	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1037.pdf	373216 e3726ce1e33aa0e656ce04a51ca4fd1c6f7c14b8	no	34
Warnings:					
Information:					
58	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1038.pdf	794156 604c3f1b917cb9b4170af77bbd86eadd0834adbe	no	6
Warnings:					
Information:					
59	Reexam - Affidavit/Decl/Exhibit Filed by 3rd Party	EX-1039.pdf	657195 0d0b06af60d80eceedd3627045820dfaf3a696fa	no	28
Warnings:					
Information:					
60	Fee Worksheet (SB06)	fee-info.pdf	29867 14c5e5995d739be0d31790721da364303c4bda55	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	342281341		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/57 (01-18)
Approved for use through 11/30/2021. OMB 0651-0064
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Also referred to as FORM PTO-1465)

REQUEST FOR *EX PARTE* REEXAMINATION TRANSMITTAL FORM

Address to:
Mail Stop *Ex Parte* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attorney Docket No.: E4720-00206

Date: March 19, 2020

1. ■ This is a request for *ex parte* reexamination pursuant to 37 CFR 1.510 of patent number 9,686,193 issued June 20, 2017. The request is made by:
   ☐ patent owner. ■ third party requester.

2. ■ The name and address of the person requesting reexamination is:
   Cisco Systems, Inc.
   170 West Tasman Drive
   San Jose, CA 95134-1706

3. Requester ☐ asserts small entity status (37 CFR 1.27) or ☐ certifies micro entity status (37 CFR 1.29). Only a patent owner requester can certify micro entity status. Form PTO/SB/15A or B must be attached to certify micro entity status.

4. This request is accompanied by payment of the reexamination fee as set forth in:
   ■ 37 CFR 1.20(c)(2); **or**
   ☐ 37 CFR 1.20(c)(1). **In checking this box for payment of the fee set forth in 37 CFR 1.20(c)(1), requester asserts that this request has forty (40) or fewer pages and complies with all other requirements of 37 CFR 1.20(c)(1).**

   Payment of the reexamination fee is made by the method set forth below.
   a. ☐ A check in the amount of $_____ is enclosed to cover the reexamination fee;
   b. ☐ The Director is hereby authorized to charge the reexamination fee to Deposit Account No. _____;
   c. ☐ Payment by credit card. Form PTO-2038 is attached; **or**
   d. ■ Payment made via EFS-Web.

   ■ In addition, the Director is hereby authorized to charge any fee deficiencies to Deposit Account No. 04-1679.

5. ■ Any refund should be made by ☐ check or ■ credit to Deposit Account No. 04-1679. 37 CFR 1.26(c). If payment is made by credit card, refund must be to credit card account.

6. ■ A copy of the patent to be reexamined having a double column format on one side of a separate paper is enclosed. 37 CFR 1.510(b)(4).

7. ☐ CD-ROM or CD-R in duplicate, Computer Program (Appendix) or large table
   ☐ Landscape Table on CD

This collection of information is required by 37 CFR 1.510. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) a request for reexamination. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 18 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop *Ex Parte* Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

8. ☐ Nucleotide and/or Amino Acid Sequence Submission
If applicable, items a. – c. are required.
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM (2 copies) or CD-R (2 copies) **or**
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies.

9. ■ A copy of any disclaimer, certificate of correction or reexamination certificate issued in the patent is included.

10. ■ Reexamination of claim(s) 18 and 19 is requested.

11. ☐ A copy of every patent or printed publication relied upon is submitted herewith including a listing thereof on Form PTO/SB/08, PTO-1449, or equivalent.

12. ☐ An English language translation of all necessary and pertinent non-English language patents and/or printed publications is attached.

13. ■ The attached detailed request includes at least the following items:
   a. A statement identifying each substantial new question of patentability based on prior patents and printed publications. 37 CFR 1.510(b)(1).
   b. An identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited art to every claim for which reexamination is requested. 37 CFR1.510(b)(2).

14. ☐ A proposed amendment is included (only where the patent owner is the requester). 37 CFR 1.510(e).

15. ■ It is certified that the statutory estoppel provisions of 35 U.S.C. 315(e)(1) or 35 U.S.C. 325(e)(1) do not prohibit requester from filing this *ex parte* reexamination request. 37 CFR 1.510(b)(6).

16. Service
   a. ■ It is certified that a copy of this request (if filed by other than the patent owner) has been served in its entirety on the patent owner as provided in 37 CFR 1.33(c).

   The name and address of the party served are:

   Banner & Witcoff, LTD, USPTO Customer No. 22907, 1100 13th Street, N.W., Suite 1200, Washington D.C. 20005

   Kramer Levin Naftalis & Frankel LLP, 990 March Road, Menlo Park, CA 94025

   Date of Service: March 19, 2020

   OR

   b. ☐ A duplicate copy is enclosed since service on patent owner was not possible. An explanation of the efforts made to serve patent owner **is attached**. See MPEP 2220.

17. Correspondence Address: Direct all communication about the reexamination to:

☒ The address associated with Customer Number: 39290

OR

☐ Firm or Individual Name _____
(at the address identified below)

Address

City	State	Zip

Country

Telephone	Email

18. ☒ The patent is currently the subject of the following concurrent proceeding(s):

a. ☐ Copending reissue Application No. _____

b. ☐ Copending reexamination Control No. _____

c. ☐ Copending Interference No. _____

d. ☒ Copending litigation styled:
Centripetal Networks, Inc. v. Cisco Systems, Inc.,
No. 2-18-cv-00094 (E.D. Va. filed Feb. 13, 2018)

WARNING : Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

/Patrick D. McPherson/ — Authorized Signature

March 19, 2020 — Date

Patrick D. McPherson — Typed/Printed Name

46,255 — Registration No.

☐ For Patent Owner Requester ☒ For Third Party Requester

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of:		)
		)
Patent No.:	9,686,193	)
		)
Issued:	June 20, 2017	)
		)
For:	FILTERING NETWORK DATA TRANSFERS	)

DETAILED REQUEST FOR *EX PARTE* REEXAMINATION

Mail Stop *Ex Parte* Reexam
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir or Madam:

Pursuant to 37 CFR § 1.510, Cisco Systems, Inc. ("Cisco"), the real party-in-interest and a third party requester, respectfully requests *ex parte* reexamination of Claims 18-19 of U.S. Patent No. 9,686,193 (the "193 Patent"). A Request for *Ex Parte* Reexamination Transmittal Form (PTO/SB/57) is attached hereto.

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. RELATED PROCEEDINGS 9

A. Related Litigation (*EX-1070, EX-1071*) 9

B. Related PTAB Proceedings 10

1. IPR2018-01559 (*EX-1003*, *EX-1005*, *EX EX-1065 – EX-1069*) 10

2. IPR2018-01436 (*EX-1053 – EX-1058*, *EX-1073*) 12

3. IPR2018-01437 (*EX-1059 – EX-1064*, *EX-1074*) 14

III. THE 193 PATENT 15

A. The Specification 15

B. The Prosecution History 23

C. The Challenged Claims 25

D. Claim Construction 27

1. "Operator" 27

IV. CERTIFICATION REGARDING STATUTORY ESTOPPEL 27

V. CENTRIPETAL IS ESTOPPED FROM ARGUING THE PATENTABILITY OF THE CHALLENGED CLAIMS 28

VI. IDENTIFICATION OF SUBSTANTIAL NEW QUESTION OF PATENTABILITY 35

VII. IDENTIFICATION OF CHALLENGES 36

A. Challenged Claims 36

B. Statutory Grounds for Challenges 36

VIII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE 37

A. Challenge 1: Claims 18 and 19 37

1. State of the Art 37

2. Sourcefire 45

3. Detailed Application of Sourcefire and the Knowledge of a POSA to the Challenged Claims 52

IX. TESTIMONIAL EVIDENCE 82

X. CONCLUSION 82

I. INTRODUCTION

Pursuant to 37 C.F.R. § 1.510, Cisco submits this Request for *Ex Parte* Reexamination (the "Request") seeking reexamination of Claims 18 and 19 of the 193 Patent (the "Challenged Claims"). The 193 Patent is assigned to Centripetal Networks, Inc. (hereinafter, "Centripetal" or "Patent Owner")

The Challenged Claims are unpatentable for the same reasons and based on the same prior art that the Patent Trial and Appeal Board ("Board") determined that all claims were unpatentable in U.S. Patent No. U.S. 9,124,552 (the "Parent 552 Patent") – the parent patent to the 193 Patent, and which has a word-for-word identical disclosure[1] and identical drawings as the 193 Patent.

Specifically, in a final written decision, the Board determined in the Parent 552 Patent that all of the claims, including independent Claim 8 ("Unpatentable Claim 8"), were unpatentable as obvious over Sourcefire 3D System User Guide Version 4.10 ("Sourcefire") (*EX-1004*) in view of the knowledge, skill and creativity of a person of ordinary skill in the art ("POSA"). IPR2018-01436, Paper 40 (P.T.A.B. Jan. 23, 2020) (*EX-1058*). The unpatentable claims of the Parent 552 Patent were directed to a system, method, and computer-readable media for

[1] The 193 Patent is a continuation of the 552 Patent. Thus, the only difference between the disclosure of the Parent 552 Patent and the 193 Patent is the 193 Patent's section "Cross-Reference to Related Applications" which claims priority to, and incorporates by reference, the Parent 552 Patent. 193 Patent at 1:6-10.

executing a packet-filtering rule to received packets and either blocking or allowing packets based on the criteria set forth in the rule.

Specifically, Unpatentable Claim 8 is directed to:

(1) receive packets;

(2) apply a packet-filtering rule specifying packet header criteria (corresponding to 5-tuple packet data) and application-header-field value criteria (corresponding to TLS-version value packet data); and

(3) block the packet if it satisfies the rule criteria.

The rule criteria used to block packets in Unpatentable Claim 8 matches data in both the 5-tuple (*e.g.* IP address, port, protocol) and the application header (TLS version value) of a packet, the latter—TLS version value—being a particular type of data transfer for HTTPS packets. Challenged Claim 18 substantially overlaps with Unpatentable Claim 8 in that it recites a first packet filtering rule[2] that blocks packets based on both 5-tuple data and particular type of data transfer data in such packets. Challenged Claim 18 includes further limitations of a second packet filtering rule[3] that forwards packets based on different 5-tuple data, and a type of

---

[2] For simplicity, Cisco refers to the recited "one or more packet-filtering rules" in Challenged Claims 18 and 19 as the first packet-filtering rule.

[3] Although Claim 18 does not explicitly recite a "second packet-filtering rule", *i.e.*, a different rule than the first packet-filtering rule, the claim requires (1) a determination that 5-tuple data in packets "does *not* correspond to *the* criteria," *i.e.* the criteria in the first packet filtering rule, (2) applying a "second operator" to

data transfer different from the particular type of data transfer, of the first packet filtering rule. The Board found that this further limitation was disclosed in Sourcefire when the Board addressed the dependent limitations of the Parent 552 Patent.

The relationship between Challenged Claim 18 and Unpatentable Claim 8 is illustrated in the table below with yellow highlighting identifying claim limitations that are (1) common to both Challenged Claim 18 and Unpatentable Claim 8 and (2) that were determined by the Board to be disclosed in Sourcefire. In other words, the manner in which Challenged Claim 18 reads on Unpatentable Claim 8 (and on the limitations that were determined by the Board to be disclosed in the identical prior art – Sourcefire – relied on in this request for *ex parte* re-examination) is illustrated below in the yellow highlighting.

Challenged Claim 18	**Unpatentable Claim 8 (held to be unpatentable by the Board)**
18. A system comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:	8. An apparatus, comprising: at least one processor; and a memory storing instructions that when executed by the at least one processor cause the apparatus to:

each such packet "*without* applying *the*" first packet-filtering rule, and (3) that the "second operator" be "configured to forward packets *not* associated with *the* particular type of data transfer," *i.e.*, the particular type of data transfer specified by the first packet-filtering rule.

receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;	receive a plurality of hypertext transfer protocol secure (HTTPS) packets;
responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network: apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and	responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values corresponding to a packet-filtering rule, apply an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations; and responsive to a determination by the at least one processor that one or more packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values

	corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations,
drop each packet in the first portion of packets; and	apply at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination.
responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network: apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and forward each packet in the second portion of packets toward the third network.	[These limitations in Challenged Claim 18 that are not expressly recited in Unpatentable Claim 8 were found by the Board to be disclosed in Sourcefire, the prior art cited in this Request, during the Board's analysis of the dependent claims of the 552 Patent, as described below.]

In reviewing the Parent 552 Patent, the Board held that "Sourcefire discloses an 'operator'" as part of a packet-filtering rule "that specifies (1) the keyword and argument that indicates 'application-header-field-value criteria,' e.g., TLS version 1.0, and (2) a 'packet transformation function', e.g., blocking packets that match the criteria." *EX-1058* at 49-50. The Board also held that "Sourcefire teaches (1) the use of different ssl_version keyword arguments or criteria and (2) that for each of these keywords and arguments 'a corresponding action of *pass* (allow), *alert* (and pass), or *drop* (block) can be specified.'" *Id.* at 50-51. As illustrated in the table above, a portion of Challenged Claim 18 reads on Unpatentable Claim 8 because the "packets associated with the particular type of data transfer" in Challenged Claim 18 read on "packets having one or more application-header-field values corresponding to one or more TLS-version values" in Unpatentable Claim 8, and further, the packet filtering rules in both claims include an operator configured to block packets that meet the recited criteria related to the particular type of data transfer.

The limitations in Challenged Claim 18 that are not expressly recited in Unpatentable Claim 8 were found by the Board to be disclosed in Sourcefire, the prior art cited in this Request. First, Challenged Claim 18 recites that the first portion of packets is destined for a second network and the second portion of packets is destined for the third network. The Board in reviewing the Parent 552

Patent held that Sourcefire taught a user how "to write its own custom intrusion rules tuned to the user's specific network environment" including "destination IP addresses." *EX-1058* at 34. Moreover, the Board in reviewing the Parent 552 Patent held that "Sourcefire discloses applying an operator in two-stage packet filtering" and, among other evidence, pointed to Sourcefire's disclosure at pp. 766-768 ("You can restrict packet inspection to the packets originating from [specific IP addresses/specific ports] or those destined to [a specific IP address/specific ports]." *Id.* at 52-53.

Second, Challenged Claim 18 recites that the "first operator configured to drop packets associated with the particular type of data transfer" is not specified in the same packet-filtering rule as the "second operator configured to forward packets not associated with the particular type of data transfer." *See* n. 3 above. In other words, in Challenged Claim 18, the "second operator" may be part of a different packet-filtering rule than the packet-filtering rule specifying the "first operator."

The Board, in reviewing the Parent 552 Patent and discussing the dependent claims, held that Sourcefire teaches using two packet filtering rules where one rule blocks packets based on TLS version, and another rule forwards packets "without applying the TLS-version packet-filtering rules":

> if a first portion of packets match certain rule header criteria (e.g., specific addresses/specific ports), they will be evaluated

> against a first 'subset' of rules (e.g., including the TLS-version packet filtering rules) – some of these packets may pass and some may be blocked. Pet., 56-58. If a second portion of packets does not match this rule header criteria for the first 'subset' of rules (e.g., different addresses/different ports), they will not be evaluated against the remainder of the rule criteria (e.g., rule keywords and arguments) for the first 'subset' of rules. *Id.* And, if this second portion of packets matches certain rule header criteria of a second 'subset' of rules, they will instead be evaluated against the remainder of the rule criteria for the second 'subset' of rules (i.e., without applying the TLS-version packet-filtering rules). Reply 21–22.

EX-1058 at 53.

As illustrated in the above table, some limitations recited in Challenged Claim 18 are broader than Unpatentable Claim 8 because where Claim 18 recites "packets" and "a particular type of data transfer", Claim 8 recites specific types of packets, e.g., "HTTPS packets" and specifically recites that the "particular type of data transfer" is a protocol using a "TLS version." Thus, the Board's finding that all claims of the Parent 552 Patent are unpatentable means that Challenged Claim 18, which recites a combination of the elements that the Board found is disclosed in Sourcefire, is unpatentable over the same prior art.

Challenged Claim 19 of the 193 Patent is a computer-readable media ("CRM") claim reciting limitations corresponding to the same substantive elements recited in system Challenged Claim 18. For the same reasons as discussed above with respect to Challenged Claim 18, every limitation recited in Challenged Claim

19 has been determined by the Board to be disclosed in the prior art cited in this Request.

Additionally, as an independent ground of unpatentability, Centripetal is estopped from arguing that the Challenged Claims of the 193 Patent are patentable pursuant to 37 C.F.R. § 42.73 precluding a patent owner from taking action inconsistent with an adverse judgment, including obtaining in any patent, a claim that is not patentably distinct from finally refused or canceled claims. Because the Board issued an adverse judgment determining all claims of the Parent 552 Patent to be unpatentable, Centripetal is estopped from arguing that the Challenged Claims of the 193 Patent are patentable.

The Request below mirrors the analysis conducted by the Board in determining that the claims of the Parent 552 Patent are unpatentable and meets the statutory requirements for showing a substantial new question of patentability for the Challenged Claims.

II. RELATED PROCEEDINGS

A. Related Litigation (*EX-1070, EX-1071*)

The 193 Patent is the subject of patent litigation entitled *Centripetal Networks, Inc. v. Cisco Systems, Inc.*, No. 2-18-cv-00094, United States District Court for the Eastern District of Virginia. Trial is scheduled to begin in this litigation on May 6, 2020.

B. Related PTAB Proceedings

1. IPR2018-01559 (*EX-1003*, *EX-1005*, *EX EX-1065– EX-1069*)

Cisco filed a petition for IPR of the 193 Patent on August 21, 2018, challenging all claims as obvious over Sourcefire. In April 2019, the Board denied institution. In response to arguments Centripetal raised in its Patent Owner's Preliminary Response, the Board held that the term "operator" used in Claims 18 and 19 was a "term of art" that required Cisco to provide a claim construction for such term in its IPR Petition, beyond just "plain and ordinary meaning," in order for the Board to determine whether "first operator" and "second operator" were shown to be disclosed in Sourcefire. *EX-1058* at 5-6, 12.

Specifically, the Board stated "[p]resumptively, the first operator refers to something other than the recited packet-filtering rule(s) because a different term is used, including within the same claim limitation—e.g., claims 18 and 19 recite that the "first operator" is "specified by the one or more packet-filtering rules." *EX-1058* at 11. The Board further held that "[t]he Specification of the '193 Patent also indicates that the recited operators may be distinct from the recited packet-filtering rules. For example, the Specification indicates that some packet-filtering rules are associated with an operator, but others are not . . . . The Specification describes that rules are used by a network packet filter to determine whether a packet meets certain criteria, while some operators themselves have the capability to analyze

packets for certain information." *Id.* The Board held that because the Petition for IPR of the 193 Patent did not provide the Board with a construction of the term "operator", and only identified Sourcefire's description of operators like "drop" or "pass" that are associated with packet filtering rules, and applied to packets when data in such packets matches other rule criteria associated with those same packet-filtering rules, the Board was unable to resolve the issues raised by the IPR Petition. *Id.* at 5-6, 9-12. The Board entered a decision on April 2, 2019, denying institution of *inter partes* review on the basis that the petitioner should have provided a specific construction of the term "operator" rather than relying on the plain and ordinary meaning of the term. *Id.*

As discussed below, based on a complete trial record in the IPR proceeding for the Parent 552 Patent, including the construction of the term "operator" per the common specification of the 552 and 193 Patents, the Board held that the meaning of the term "operator", per this common specification, would include (1) simply a rule action (packet-transformation function) such as "pass" or "drop" disclosed in Sourcefire, as well as (2) a combination of (i) application-layer rule criteria, such as a rule keyword and associated arguments disclosed in Sourcefire, and (ii) a rule action (packet-transformation function), such as "pass" or "drop" disclosed in Sourcefire. *EX-1058* at 15-17, 34-35, 48-56.

2. IPR2018-01436 (*EX-1053 – EX-1058, EX-1073*)

The Parent 552 Patent was the subject of a Petition for IPR by Cisco (the "552 Petition"). IPR2018-01436, Paper 1 (*EX-1053*). The proceedings of IPR2018-01436 (the "552 IPR") are part of the prosecution history of the Parent 552 Patent. *See Aylus Networks, Inc. v. Apple Inc.*, No. 2016-1599, slip op. at 10-11 (Fed. Cir. May 11, 2017).

In a final written decision issued January 23, 2020, the Board made several factual determinations that are relevant to this Request.

a. Sourcefire Is a Printed Publication

During the 552 IPR, Patent Owner disputed that Sourcefire was publicly accessible and therefore qualified as a printed publication that would be prior art to the Parent 552 Patent.

In weighing the evidence, the Board conclusively found that Cisco proved by a preponderance of the evidence that Sourcefire was distributed commercially through sales of the Sourcefire 3D system to customers with no obligations of confidentiality and with expectations that the information could be shared for non-commercial use. *EX-1058* at 23-31. The Board therefore concluded that Sourcefire qualifies as a prior art printed publication under § 102(b). *Id*

b. Claim Construction of the Term "Operator"

During the IPR proceeding of the Parent 552 Patent, Centripetal told the Board that the term "operator" is described in the Specification of the 552 Patent, which is identical to the specification of the 193 Patent (*see* n. 1), and has "two meanings: (1) a packet transformation function, without specifying application-header-field-value criteria; and, (2) a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria." Cisco agreed that the two constructions asserted by Centripetal are the plain and ordinary meanings of the term "operator" as used in the specification.

The Board expressly noted the parties' agreement as to the over-arching construction of the term "operator" in the specification of the Parent 552 Patent. *EX-1058* at 16.

c. Surefire Renders Obvious All Claims of the Parent 552 Patent

Cisco asserted that all claims of the Parent 552 Patent were rendered obvious by Sourcefire in view of the knowledge of a POSA. After considering arguments from Cisco and Centripetal, the Board determined that Cisco had shown by a preponderance of the evidence that Sourcefire in view of the knowledge of a POSA teaches or suggests each limitation of each challenged claim. The Board further noted that "[Cisco]'s showing that the claims are taught or suggested by Sourcefire

in view of the knowledge of a person or ordinary skill was ***very strong***." *Id.*, p. 66 (emphasis added). Accordingly, the Board determined that all claims of the Parent 552 Patent are unpatentable. *Id.*, 71.

d. Centripetal's Evidence of Secondary Considerations Is Insufficient to Establish Patentability

Centripetal presented evidence of four objective indicia of nonobviousness: (1) long-felt but unresolved need, and failure of others, (2) industry praise, (3) skepticism of experts, and (4) commercial success. The Board reviewed Centripetal's evidence and concluded that for each of the four objective indicia of nonobviousness, Centripetal failed to demonstrate a nexus between the evidence and the claimed invention. Without such a nexus, the Board found Centripetal's evidence of secondary considerations to be insufficient to establish patentability of the challenged claims of the Parent 552 Patent.[4]

3. IPR2018-01437 (*EX-1059– EX-1064, EX-1074*)

Cisco filed a petition for IPR of U.S. Patent No. 9,160,713[5] (the "713 Patent", a sister patent of the 193 Patent) on July 20, 2018, challenging all claims

---

[4] *See also* p. 66 ("[W]e find that Patent Owner has not established the requisite nexus between the challenged claims and *any* of the asserted secondary considerations." (emphasis in original).

[5] Like the 193 Patent, the 713 Patent is a continuation of the 552 Patent. Thus, and like the 193 Patent, the only difference between the disclosure of the Parent 552 Patent and the 713 Patent is the 713 Patent's section "Cross-Reference to Related

of the 713 Patent. On the same day that the final written decision was issued in the 552 IPR, a separate panel at the Board issued a final written decision in the 713 IPR. Consistent with the 552 IPR, the panel in the 713 IPR determined: (1) that Sourcefire constituted a printed publication, (2) that Centripetal failed to establish a nexus between the challenged claims and any asserted secondary consideration, and (3) that all claims of the 713 Patent were unpatentable as obvious over Sourcefire in view of the knowledge of a POSA.

III. THE 193 PATENT

The 193 Patent issued on June 20, 2017 from Application No. 14/625,486 filed on February 18, 2015, as a continuation of Application No. 13/795,822 filed on March 12, 2013, now U.S. Patent No. 9,124,552 – the Parent 552 Patent.

A. The Specification

As discussed above, the specification of the 193 Patent has the word-for-word identical disclosure and identical drawings as the Parent 552 Patent and the 713 Patent. The 193 Patent is directed to systems and methods for filtering data packets leaving a network to ensure that the packets are not improperly transferring sensitive data from the network, a category of cyber-attacks known as exfiltrations. For example, exfiltrations are often facilitated by using popular network data

---

Applications" which claims priority to, and incorporates by reference, the Parent 552 Patent. 713 Patent at 1:6-11.

transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the Web. Such attacks may appear to a casual observer as normal network behavior; older network trust models (*e.g.*, those used by firewalls that do not interpret application-layer data like HTTP) may interpret exfiltrations as trusted operations. *EX-1001* 1:24-47; *EX-1003* ¶33.

The 193 Patent describes a two-stage filtering process for addressing such attacks implemented at a Packet Security Gateway (PSG) examining packets that are exiting a trusted network towards an external network. *EX-1001* 8:39-52, 2:20-35 ("To distinguish a network packet filter that implements said additional operators from network packet filters that do not, a network packet filter that implements such additional operators will be referred to hereinafter as a packet security gateway (PSG)."), 2:36-54, 7:38-8:37, FIG. 3 (Rules 5 and 6); *EX-1003* ¶34.

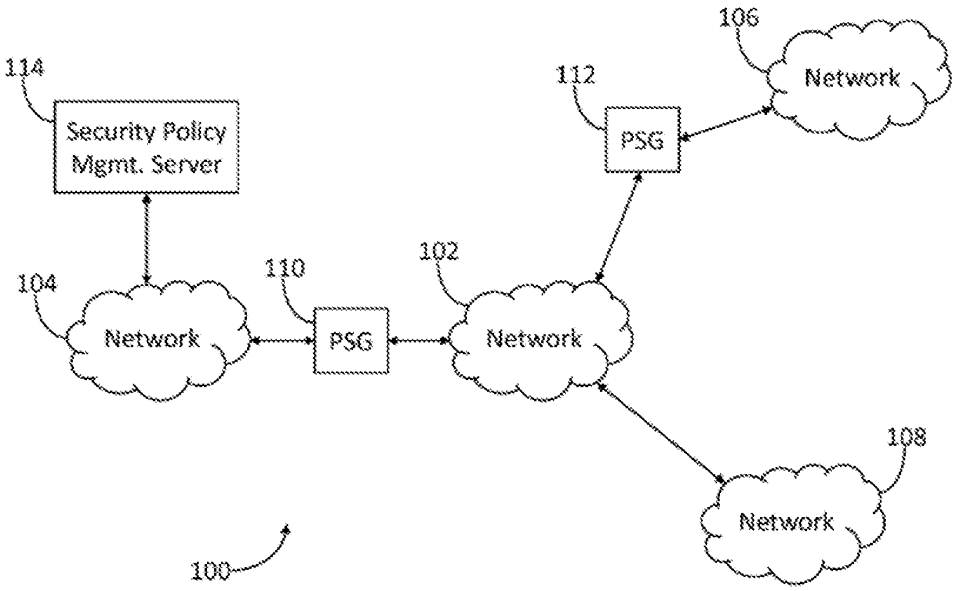


FIG. 1

FIG. 1 of the 193 Patent (above) illustrates a network environment 100 of various networks protected by PSGs 110, 112. Networks 104, 106, and 108 may be private networks such as Local Area Networks (LANs) or Wide-Area Networks (WANs) operated by various organizations. Network 102 represents the public Internet functioning as an interconnect between networks 104, 106 and 108. *EX-1001* 3:27-41. Networks 104 and 106 are protected by PSGs 110, 112, which in turn are administered by security policy management server 114. A PSG (110 or 112) receives packets and applies one or more filters to allow or block transmission of the received packets according to rules specified in the security policy management server 114. *EX-1001* 3:58-4:23; 5:25-45; *EX-1003* ¶35.

As illustrated in FIG. 1, networks 104 and 106 may each form part of a single organization's protected network associated with security policy management server 114. For example, PSG 110 may protect network 104 from one or more cyber-attacks mediated by network 102 (*e.g.*, the Internet), and PSG 112 may protect network 106 from one or more cyber-attacks mediated by network 102. *EX-1001* 4:23-37; *EX-1003* ¶36.

In operation, each PSG performs a two-stage filtering process for received packets. In a first stage, the "5-tuple" of packet header fields (*e.g.*, source/destination Internet Protocol (IP) addresses, transport protocol, and source/destination ports, as defined in either the Transmission Control Protocol (TCP), or User Datagram Protocol (UDP)) are filtered. In a second stage, application packet-header-field values are filtered. Conceptually, the first stage may determine if the network security policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication (*e.g.*, read/write, encrypted communication) between the resources. *EX-1001* 8:39-51, FIG. 4, 9:19-61, 7:41-45; *EX-1003* ¶¶37-42.

In one embodiment, the 193 Patent describes that an operator, specified by a rule, specifies one or more application-header-field-value criteria and a packet transformation function, for example, to (i) determine if an IP packet traversing a

boundary contains an HTTP packet having application layer data specifying one or more specific methods (*e.g.*, GET, PUT, POST), and (ii) allow the packet *(e.g.*, if GET is specified), or block the packet (*e.g.*, if PUT or POST is specified). *EX-1001* 2:36-43; FIG. 3 (below) (rule 6); *EX-1003* ¶43.

FIG. 3 of the 193 Patent illustrates the rules and operators that may be specified by the security policy for the specific example of packets sent from network 104 and received at PSG 110.



Five-tuple

Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

FIG. 3 illustrates seven example rules, each of which may specify criteria and one or more operators that may be applied to packets matching the specified criteria.

In Stage I, the specified rule criteria are based on the 5-tuple in the packet header for a received packet. *EX-1001* 5:46-60, 8:39-43, 8:45-47; *EX-1003* ¶¶44-45. For two-stage packet-filtering rules (*e.g.* Rules 5, 6), in Stage II, the specified rule criteria is also based on application-layer data in the application packet for a received packet, where such additional rule criteria is specified in an additional operator (*e.g.*, "Require TLS-1.1-1.2", "HTTP-EXFIL"). *EX-1001* 6:22-30, 6:60-67, 7:1-10, 7:32-8:38, 8:43-45, 8:48-51.

For example, rule 1 specifies that IP packets containing one or more TCP packets, originating from a source IP address beginning with 140.210 (network 104), having any source port, destined for an IP address beginning with 140.212 (network 106), and destined for port 22 (*e.g.*, associated with SSH protocol) has an ALLOW operator which simply applies an ALLOW packet-transformation function to packets matching the rule criteria (*i.e.* PSG should transmit the packets). Similarly, rules 2, 3 and 4 instruct the PSG to ALLOW similar packets destined for port 25 (*e.g.*, associated with SMTP), port 110 (*e.g.*, associated with POP3), and port 143 (*e.g.*, associated with IMAP), respectively. *EX-1001* 5:61-6:21; *EX-1003* ¶46.

However, Rule 5 instructs the PSG that packets with similar packet header information except destined for port 443 (*e.g.*, associated with Hypertext Transfer Protocol Secure (HTTPS)) should have a Require-TLS-1.1-1.2 operator

(specifying application layer criteria (TLS version value criteria) and one or more packet-transformation functions) applied to them in a second stage. *EX-1001* 6:22-30, 8:4-38; *EX-1003* ¶47. The Require-TLS-1.1-1.2 operator allows HTTPS packets specifying a Transport Layer Security (TLS) version value of 1.1 or 1.2, but blocks HTTPS packets specifying a TLS version value of 1.0. Rule 5 allows browsers in network 104 to conduct HTTPS sessions with any web servers in network 106, but requires the field value in the application data headers of packets (TLS Record headers) to specify version 1.1 or 1.2 of the TLS protocol "because the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions." *EX-1001* 6:57-67, 7:38-45, 8:4-38; *EX-1003* ¶47.

Rule 6 instructs the PSG that packets with similar packet header information except destined for port 80 (*e.g.*, associated with HTTP) should have an HTTP-EXFIL operator (specifying application layer criteria (HTTP method criteria) and one or more packet-transformation functions) applied to them in a second stage. An HTTP-EXFIL operator allows HTTP packets specifying a GET method, but blocks HTTP packets specifying other HTTP methods (*e.g.*, PUT, POST, CONNECT). Rule 6 allows a browser to "surf the web" (*e.g.*, download web pages using HTTP GET), but prevents the browser from writing files to a server (using HTTP PUT), posting forms to a server (using POST), or otherwise

communicating with a server (using any HTTP method except GET). The 193 Patent describes that, "[b]ecause attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data, operators such as HTTP-EXFIL of rule 6 may be used to stop such exfiltrations." *EX-1001* 7:1-20, 7:21-8:3; *EX-1003* ¶48.

Rule 7 is a "wildcard" rule and applies a BLOCK operator which simply applies a BLOCK packet-transformation function to any packets that do not match the criteria of any of Rules 1-6. *EX-1001* 6:31-36; *EX-1003* ¶49.

The claims of the 193 Patent are directed to a method, system and computer program for implementing particular combinations of packet-filtering rules at the PSG. Independent Claim 1 is directed to the method; Claim 18 is a corresponding system claim performing the steps of Claim 1; and Claim 19 is a corresponding computer program programmed to perform the steps of Claim 1. Independent Claim 8 is a method claim similar to Claim 1 except that the packet-filtering rules are applied to packets destined to the same network, while in the other independent claims the packet-filtering rules are applied to packets destined to two different networks. *EX-1003* ¶52.

Challenged Claims 18 and 19 each recite that the "first operator configured to drop packets associated with the particular type of data transfer" is not specified in the same packet-filtering rule as the "second operator configured to forward packets not associated with the particular type of data transfer." *See* n. 3. In other

words, in the Challenged Claims 18 and 19 of the 193 Patent, the "second operator" may be part of a different packet-filtering rule than the packet-filtering rule specifying the "first operator." Thus, independent Claims 18 and 19, while verbose, may be interpreted as being directed to providing two rules, one for "dropping" (*i.e.*, blocking) packets and one for "forwarding" (*i.e.*, allowing) packets. The first rule (recited in the first "responsive" and first "apply" elements of Claims 18 and 19) is crafted to "drop" packets associated with a particular type of data transfer (*e.g.*, packets specifying an HTTP PUT method or a TLS version 1.0 value) that are going from a first network (*e.g.*, internal network) to a second network (*e.g.*, external network). The second rule (recited in the second "responsive" and second "apply" elements of Claims 18 and 19) is crafted to "forward" packets that are going from the first network to a different network (the "third network") where those packets are *not* associated with the particular type of data transfer that was blocked by the first rule (*e.g.*, packets specifying an HTTP GET method or a TLS version 1.1 or 1.2 value). *EX-1003* ¶53.

B. The Prosecution History

Prior to examination, the independent claims were directed to applying two rules, one for "dropping" (*i.e.*, blocking) packets and one for "forwarding" (*i.e.*, allowing) packets, to packets being transferred from a first network to the same second network. *EX-1002,* 47-54; *see also* n. 3. In the first Office Action, the

examiner rejected the independent claims over prior art, but indicated the allowability of dependent claims that recited (1) that the second rule operated on packets that were destined to a different "third network", and (2) a "dropping" rule directed to XMPP. *EX-1002*, 157-181; *EX-1003* ¶58; *see also* n. 3.

Applicant then amended the independent claims to include the limitations recited in the allowed dependent claims, and in response, a notice of allowance issued. *EX-1002* 271-283, 292-294; *EX-1003* ¶59.

Regarding independent claims 18 and 19, the USPTO examiner found patentability in the particular combination of, as discussed above, (1) a rule specifying "dropping" packets transiting from a first network to a second network and that are associated with a particular type of data transfer (*e.g.*, HTTP PUT method, TLS version 1.0 value), and (2) another rule specifying "allowing" packets transiting from the first network to a third network and that are *not* associated with the particular type of data transfer (*e.g.*, HTTP GET method, TLS version 1.1 or 1.2 value). However, the 193 Patent does not make any distinction that the use of either rules' criteria, or particular combinations of rules specifying such criteria, is more technologically challenging than, for example, use of other application-layer rule criteria (*e.g.*, RTP criteria, FTP criteria), or other combinations of different rules. *EX-1001* 6:58-9:10; *EX-1003* ¶60; *see also* n. 3.

Rather, the 193 Patent treats all application-layer rule criteria the same, and all combinations of rules the same, and identifies *the exact same system architecture and method* for allowing or blocking received packets using rule criteria, and combinations of rule criteria, specifying each of the different application-layer data types (*e.g.*, HTTP method, TLS version value, RTP, FTP, etc.), any possible destination, and any possible origin. *Id.*; *EX-1003* ¶61.

C. The Challenged Claims

This Request seeks reexamination of Claims 18 and 19 of the 193 Patent. Each of the claims is an independent claim with Claim 18 being directed to a system for implementing particular combinations of packet-filtering rules at a PSG, and Claim 19 being directed to a corresponding computer program programmed to perform the implementations of Claim 18. The claims are shown in the table below with corresponding elements labeled accordingly:

Claim 18	Claim 19
[P] A system comprising:	**[P]** One or more non-transitory computer-readable media comprising
[A] at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:	**[A]** instructions that when executed by one or more computing devices cause the one or more computing devices to:
[B] receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets	**[B]** receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets

comprises a first portion of packets and a second portion of packets;	comprises a first portion of packets and a second portion of packets;
[C] responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:	**[C]** responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:
[D] apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and	**[D]** apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and
[E] drop each packet in the first portion of packets; and	**[E]** drop each packet in the first portion of packets; and
[F] responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:	**[F]** responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:
[G] apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a	**[G]** apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a

second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and	second operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and
[H] forward each packet in the second portion of packets toward the third network.	**[H]** forward each packet in the second portion of packets toward the third network.

D. Claim Construction

1. "Operator"

As described above, the Board in the Parent 552 Patent IPR proceedings held that the term "operator" described in the specification[6] had two meanings: (1) a packet transformation function, without specifying application-header-field-value criteria; and, (2) a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria. *EX-1058* at 16.

IV. CERTIFICATION REGARDING STATUTORY ESTOPPEL

Petitioner hereby certifies per 37 C.F.R. § 1.510(b)(6) that the statutory estoppel provisions of 35 U.S.C. §§ 315(e)(1) and 325(e)(1) do not prohibit Petitioner from filing this ex parte reexamination request. The provisions of § 315(e)(1) apply to "final written decisions" under 35 U.S.C. § 318(a) resulting

[6] As discussed above, the specification of the 193 Patent has the word-for-word identical disclosure and identical drawings as the Parent 552 Patent.

from instituted *inter partes* review proceedings. As such, no estoppel arises from the decisions denying institution in IPR2018-01559. The provisions of 35 U.S.C. § 325(e)(1) apply after a final written decision under 35 U.S.C. § 328(a) in post-grant proceedings. Petitioner has not been a party to, and is aware of no, instituted post-grant review proceedings of the 193 Patent.

V. CENTRIPETAL IS ESTOPPED FROM ARGUING THE PATENTABILITY OF THE CHALLENGED CLAIMS

A patent owner is precluded from taking action inconsistent with an adverse judgment, including obtaining in any patent, a claim that is not patentably distinct from finally refused or canceled claims. 37 C.F.R. § 42.73. In IPR2018-01436, the Board issued an adverse judgment determining all claims of the Parent 552 Patent, including Unpatentable Claim 8 discussed above, to be unpatentable. *EX-1058*. As illustrated in the table below, and the discussion that follows it, Challenged Claims 18 and 19 are not patentably distinct from Unpatentable Claims 8 of the Parent 552 Patent, respectively, with yellow highlighting identifying claim limitations that are common:

Challenged Claim 18	**Unpatentable Claim 8 (held to be unpatentable by the Board)**
18. A system comprising: at least one processor; and	8. An apparatus, comprising: at least one processor; and

a memory storing instructions that when executed by the at least one processor cause the system to:	a memory storing instructions that when executed by the at least one processor cause the apparatus to:
receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;	receive a plurality of hypertext transfer protocol secure (HTTPS) packets;
responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network: apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and	responsive to a determination by the at least one processor that at least a portion of the plurality of HTTPS packets have packet-header-field values [data] corresponding to a packet-filtering rule, apply an operator specified by the packet-filtering rule to the at least a portion of the plurality of HTTPS packets, wherein the operator specifies one or more application-header-field-value criteria identifying one or more transport layer security (TLS)-version values for which packets should be blocked from continuing toward their respective destinations; and responsive to a determination by the at least one processor that one or more

drop each packet in the first portion of packets; and	packets, of the at least a portion of the plurality of HTTPS packets, have one or more application-header-field values corresponding to one or more TLS-version values of the one or more TLS-version values for which packets should be blocked from continuing toward their respective destinations, apply at least one packet-transformation function specified by the operator to the one or more packets to block each packet of the one or more packets from continuing toward its respective destination.
responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network: apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and	[These limitations in Challenged Claim 18 that are not expressly recited in Unpatentable Claim 8 were found by the Board to be disclosed in Sourcefire, the prior art cited in this Request, during the Board's analysis of the dependent claims of the 552 Patent, as described below.]

forward each packet in the second portion of packets toward the third network.	

With respect to the highlighted limitations, in reviewing the 552 Parent Patent, the Board held that "Sourcefire discloses an 'operator'", as part of a packet-filtering rule, "that specifies (1) the keyword and argument that indicates 'application-header-field-value criteria,' e.g., TLS version 1.0, and (2) a 'packet transformation function, e.g., blocking packets that match the criteria." *EX-1058* at 49-50. The Board also held that "Sourcefire teaches (1) the use of different ssl_version keyword arguments or criteria and (2) that for each of these keywords and arguments 'a corresponding action of *pass* (allow), *alert* (and pass), or *drop* (block) can be specified.'" *Id.* at 50-51. As illustrated in the table above, a portion of Challenged Claim 18 reads on Unpatentable Claim 8 because the "packets associated with the particular type of data transfer" in Challenged Claim 18 read on "packets having one or more application-header-field values corresponding to one or more TLS-version values" and the packet filtering rules in both claims block packets that meet the recited criteria related to type of data transfer.

The limitations in Challenged Claim 18 that are not expressly recited in Unpatentable Claim 8 were found by the Board to be disclosed in Sourcefire, the identical prior art cited in this Request. First, Challenged Claim 18 recites that the

first portion of packets is destined for a second network and the second portion of packets is destined for the third network. The Board in reviewing the Parent 552 Patent held that Sourcefire taught a user how "to write its own custom intrusion rules tuned to the user's specific network environment" including "destination IP addresses." *EX-1058* at 34. Moreover, the Board in reviewing the Parent 552 Patent held that "Sourcefire discloses applying an operator in two-stage packet filtering" and, among other evidence, pointed to Sourcefire's disclosure at pp. 766-768 ("You can restrict packet inspection to the packets originating from [specific IP addresses/specific ports] or those destined to [a specific IP address/specific ports]."). *Id.* at 52-53.

Second, Challenged Claim 18 recites that the "first operator configured to drop packets associated with the particular type of data transfer" is not specified in the same packet-filtering rule as the "second operator configured to forward packets not associated with the particular type of data transfer." *See* n. 3 above. In other words, in Claim 18, the "second operator" may be part of a different packet-filtering rule than the packet-filtering rule specifying the "first operator." *Id.*

The Board, in reviewing the Parent 552 Patent and discussing the dependent claims, held that Sourcefire teaches using two packet filtering rules where one rule blocks packets based on TLS version, and another rule that forwards packets "without applying the TLS-version packet-filtering rules":

> if a first portion of packets match certain rule header criteria (e.g., specific addresses/specific ports), they will be evaluated against a first "subset" of rules (e.g., including the TLS-version packet filtering rules) – some of these packets may pass and some may be blocked. Pet., 56-58. If a second portion of packets does not match this rule header criteria for the first "subset" of rules (e.g., different addresses/different ports), they will not be evaluated against the remainder of the rule criteria (e.g., rule keywords and arguments) for the first "subset" of rules. Id. And, if this second portion of packets matches certain rule header criteria of a second "subset" of rules, they will instead be evaluated against the remainder of the rule criteria for the second "subset" of rules (i.e., without applying the TLS-version packet-filtering rules). Reply 21–22.

EX-1058 at 53[7].

As illustrated in the above table, some limitations recited in Challenged Claim 18 are broader than Unpatentable Claim 8 because where Claim 18 recites "packets" and "a particular type of data transfer", Claim 8 recites specific types of packets, e.g., "HTTPS packets" and specifically recites that the "particular type of data transfer" is a protocol using a "TLS version." Thus, the Board's finding that all claims of the Parent 552 Patent are unpatentable, also means that Challenged

[7] In the 713 Patent IPR, the Board held that "Petitioner explains that Sourcefire discloses rules other than TLS version rules—including '5-tuple' rules based on protocol type, and source or destination IP addresses or ports—which teaches that a second portion of packets (as well as the first portion) can be filtered to be forwarded or dropped (based on such other rules) without applying the TLS version rule applied to the first portion of packets, as recited in claims 2–4 . . . We agree with Petitioner's analysis and find that the cited evidence supports its contentions by a preponderance of the evidence that Sourcefire teaches all of the limitations of claims 2–7." IPR2018-01437, Paper 40 at 22 (*EX-1064*).

Claim 18, which recites a combination of the elements that the Board found is disclosed in Sourcefire, is unpatentable over the same prior art.

Challenged Claim 19 of the 193 Patent is a computer-readable media ("CRM") claim reciting limitations corresponding to the same substantive elements recited in system Claim 18, and thus is unpatentable for the same reasons discussed above with respect to Challenged Claim 18.

Additionally, the findings by the Board that all claims of the Parent 552 Patent are unpatentable raises a substantial new question (SNQ) of patentability for Claims 18 and 19 of the 193 Patent, respectively. Pursuant to 37 C.F.R. § 42.73, Centripetal is estopped from arguing the patentability of the Challenged Claims, and therefore, the Request should be granted.

Moreover, once the Request is granted, Centripetal is further estopped from obtaining a claim during the reexamination by amendment that is not patentably distinct from Claims 1-21 of the Parent 552 Patent, and Claims 1-20 of the 713 Patent. In other words, Centripetal bears the burden of proving that any amended claims are patentably distinct from the claims of the related 552 and 713 Patents that were found unpatentable by the Board.

VI. IDENTIFICATION OF SUBSTANTIAL NEW QUESTION OF PATENTABILITY

The newly cited prior art raises the following SNQ:

> Claims 18 and 19 are unpatentable under pre-AIA 35 U.S.C. § 103 over Sourcefire in view of the knowledge of a POSA and based on the construction of "operator" from the specification of the 193 Patent.

As set forth above, the Board has determined that:

1. the Sourcefire reference constitutes a printed publication and is prior art to the Challenged Claims under 35 U.S.C. § 102;

2. the construction of "operator" per the common specification of the 193 Patent and Parent 552 Patent has "two meanings: (1) a packet transformation function, without specifying application-header-field-value criteria; and, (2) a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria."

3. that all claims in the Parent 552 Patent are unpatentable as obvious over Sourcefire in view of the knowledge of a POSA; and

4. that Centripetal's evidence of secondary considerations is insufficient to establish nonobviousness.

As also demonstrated above, the Challenged Claims are not patentably distinct from the claims in the Parent 552 Patent determined to be unpatentable

over Sourcefire in view of the knowledge of a POSA. As such, the ground of unpatentability as obvious over Sourcefire in view of the knowledge of a POSA raises a substantial new ground of patentability as to the Challenged Claims.[8]

VII. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

Claims 18 and 19 are challenged in this Request.

B. Statutory Grounds for Challenges

The Challenge is set forth in detail below and summarized as follows:

Ground	Claims	Basis	Reference
1	18, 19	§ 103	Sourcefire in view of knowledge, skill and creativity ("Knowledge") of a POSA

Ground 1: Claims 18 and 19 of the 193 Patent are invalid as being obvious over Sourcefire in view of the Knowledge of a POSA. *EX-1003* ¶148.

The Sourcefire reference (*EX-1004*) is a user manual titled "Sourcefire 3D System User Guide" Version 4.10 ("Sourcefire"). As determined by the Board in

[8] IPR2018-01559 did not reach a final written decision. A substantial new question may be established based on a question raised in a ground presented in an AIA petition prior to the issuance of a final written decision. *See* MPEP 2242(I) ("If the prior art patents and printed publications raise a substantial question of patentability of at least one claim of the patent, then a substantial new question of patentability as to the claim is present, unless the same question of patentability has already been: . . . (B) decided in an earlier **concluded** examination or review of the patent by the Office.") (emphasis added).

the 552 IPR, Sourcefire was publicly accessible at least as early as April 2011 and qualifies as prior art under §102(b) as it was enclosed on documentation disks (CD-ROM/DVD) included with each Sourcefire 3D System appliance subsequently sold (*e.g.*, 3D Sensor, Defense Center) by Sourcefire, Inc. (EX-1005), including to at least 586 unique customers including large commercial entities (EX-1075, ¶9), was advertised (EX-1034, EX-1076, EX-1077), was publicly accessible for download by persons who had received a login and password from Sourcefire, Inc. to its support website (*EX-1005*), and was disseminated with restriction (*EX-1004* at 2). *EX-1058* at 23-31. It was not cited or applied by the examiner during the 193 Patent prosecution.

VIII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Challenge 1: Claims 18 and 19

1. State of the Art

The following describes the state of the art for network security systems as of March 2013. *EX-1003* ¶¶64-113.

The Internet is logically a web of intermediate network nodes and communication paths interconnecting such nodes that provides multiple data transmission routes from any given point to any other given point on the network (*i.e.*, between any two computers.) *EX-1006* 3:32-46, 3:59-4:11, 38:29-39:8; *EX-1003* ¶¶66-68.

While TCP/IP allowed data to move across a global network, higher-level application protocols were required to allow data communication to be managed conveniently. *EX-1022*[9]; *EX-1021*; *EX-1020*; *EX-1003* ¶69. Application protocol data was transmitted in packet bodies with IP and TCP headers. Particularly important applications included email (*e.g.*, SMTP, POP, IMAP), dating back to 1972 (*EX-1020*), File Transfer Protocol (FTP) to 1980 (*EX-1035*), HTTP to 1991 (*EX-1036*). *EX-1003* ¶69. Protocols were also developed for voice/video services (VoIP) in the 1990s (*e.g.*, Session Initiation Protocol (SIP) (*EX-1051*) for call setup/tear-down, Session Description Protocol (SDP) (*EX-1052*) to specify call media format, and Real-Time Protocol (RTP) (*EX-1041*; *EX-1050*) to carry call audio/video streams. *EX-1003* ¶70. Telnet then SSH, were also well-known, as were various instant messaging (IM) protocols (*e.g.*, AOL Instant Messenger (AIM), Yahoo! Messenger, Jabber (using XMPP protocol (*EX-1044*; *EX-1045*))). *EX-1030*; *EX-1003* ¶69.

Throughout the mid to late 1980s, the Internet grew rapidly and had few security barriers beyond requirements to login on remote systems (often having weak/default passwords). *EX-1020*; *EX-1003* ¶71. This era spawned abuses by

[9] The Declaration of Christopher Butler (EX-1072) demonstrates that various exhibits cited in this request are prior art to the 193 Patent. The location within EX-1072 at which each of these various, prior art exhibits found is provided in the table immediately following the Exhibit List at the end of this report.

hackers, leading to development of the first firewall and first network intrusion detection system (NIDS). *EX-1023*, *EX-1024*, *EX-1025*; *EX-1003* ¶72.

It was well-known to include firewall functionality in a router to review packets for security purposes. Indeed, routers provided simple facilities to block packets based on their source/destination networks and TCP ports. For example, in 1989, Cisco routers "could deny access to all but one host on a particular network" and "allow[ed] discrimination based on IP protocol type, and TCP or UDP port numbers." *EX-1026* p. 3; *EX-1003* ¶¶73-74.

Cost and security weaknesses in early packet filters led to the development of "stateful" inspection firewalls which parsed the application data inside passing packets, and investigated whether they might be significant to application traffic routing. *EX-1031; EX-1003* ¶¶75-77. For example, the Zuk patent, filed in 2002, stated:

> A packet filtering firewall with stateful inspection also has the ability to examine a packet in order to allow certain types of commands within an application while disallowing others. For example, a stateful inspection firewall can allow the FTP "get" command while disallowing the "put" command. *EX-1008* 4:31-41.

Thus, well before 2013, a POSA knew that some firewalls discriminated whether to pass or block packets based on examining not only the 5-tuple (*e.g.*,

ports and IP addresses), but also application-layer data in the packet data bodies. *EX-1003* ¶78.

The first commercial NIDS (or IDS), NetRanger, launched in 1996, had a general facility to write rules that matched arbitrary strings in the application data inside packets, in addition to matching IP and TCP packet header values. *EX-1003* ¶¶79-80. For example, a 1997 user guide illustrated:

> The following example shows how to log every HTTP GET on a network. The context info provided with the string will show what URL was used in the GET.

Web	SIGID	Port	Direction	Occurrences	String Match
RecordOfStringName	8001	80	1	1	"GET[ ]+"

EX-1028 p. 189; *EX-1003* ¶80. Thus, from the very beginning of the IDS industry, it was known to look at application header data, and HTTP methods in particular, when examining packets transiting a network. *EX-1003* ¶81. Vulnerabilities with various HTTP methods were also known; indeed, the 1999 HTTP RFC categorized GET and HEAD methods as "safe" and "other methods, such as POST, PUT, and DELETE, in a special way, so that the user is made aware of the fact that a possibly unsafe action is being requested." *EX-1046* pp. 44, 46-50, 130-134; *EX-1003* ¶82.

A widely adopted open source IDS, Snort, was released in 1998 and, like prior IDS, allowed a user to write rules for detecting particular packets based on both the 5-tuple in the IP and TCP headers, as well as packet application data. For

example, the below rule alerted the user based on TCP packets from any source IP address and port, destination IP addresses in the range 10.1.1.0/24, and with destination port 80 (characteristic of HTTP):

```
alert tcp any any -> 10.1.1.0/24 80 (content: "/cgi-bin/phf"; msg: "PHF
probe!";)
```

EX-1029, p. 232, FIG. 5; *EX-1003* ¶83. The particular content keyword (/cgi-bin/phf) matched a uniform resource locator (URL) used in a popular attack, but content keywords generally could be used to match any text in application data in transiting packets. *EX-1029*, p. 232, FIG. 5; *EX-1003* ¶¶83-84.

The needs to block attacks, and resolve various complex ambiguities that intruders used to avoid the first NIDS, resulted in the development of systems "inline" in the traffic flow that could drop or pass any given packet. *EX-1003* ¶¶85-86. These inline intrusion prevention systems (IPS) applied intrusion detection rules that looked both at the 5-tuple and application data in every packet and made pass/alert/block decisions on each such packet. For example, the Zuk patent described an IPS which used the 5-tuple to lookup rules in a flow table; the rules then allowed content matching in the application layer, and matches resulted in triggering the rule and dropping the packet. *EX-1008* col. 18, FIG. 11; *EX-1003* ¶87.

As another example, the below Snort rule alerted the user based on TCP packets from any external network source IP address and port 5050 (characteristic

of Yahoo! Messenger traffic) to any internal network destination IP address and any destination port:

```
alert tcp $EXTERNAL_NET 5050 -> $HOME_NET any (msg:"CHAT Yahoo IM successful logon";
flow:from_server,established; content:"YMSG"; depth:4; nocase; content:"|00 01|";
depth:2; offset:10; classtype:policy-violation; sid:2450; rev:3;)
```

EX-1042 p. 2; *EX-1003* ¶88. The particular content keyword (YMSG) matched content indicative of an internal host's successful attempt to login to this popular IM service. *Id.* The rule identified that such action would violate corporate policy and the corresponding signature document for the rule further detailed:

> Instant Messenger programs may not be appropriate in certain network environments . . . A user must successfully logon to an Yahoo Instant Messenger server before participating in any exchanges . . . Many of these activities are not appropriate in a corporate environment . . . Once logged in, a Yahoo IM user may unwittingly accept a malicious file that may contain a worm, virus, Trojan, or backdoor to name a few. Ease of Attack: Easy . . . Corrective Action: Disallow the use of IM clients on the protected network and enforce or implement an organization wide policy on the use of IM clients.

EX-1043 pp. 1-2; *EX-1003* ¶88. Vulnerabilities with various IM protocols, including Jabber (using XMPP), were known to a POSA; thus a POSA understood that enforcing security policies which disallowed the use of IM protocols on a protected network was a straightforward way to protect such network from such

vulnerabilities. *Id.*; *EX-1044* pp. 41-44; *EX-1045* p.5 8; *EX-1047*; *EX-1003* ¶¶88, 91-100.

As another example, the below Snort rule alerted the user based on TCP packets from any external network source IP address and port 80 to any internal network destination IP address monitored by Snort and any destination port:

```
alert tcp $EXTERNAL_NET 80 -> $HOME_NET any (msg:"MULTIMEDIA Windows Media
download"; flow:from_server,established; content:"Content-Type|3A|"; nocase;
pcre:"/^Content-Type\x3a\s*(?=[av])(video\/x\-ms\-(w[vm]x|asf)|a(udio\/x\-ms\-w(m[av
]|ax)|pplication\/x\-ms\-wm[zd]))/smi"; classtype:policy-violation; sid:1437;
rev:6;)
```

EX-1048 p. 1; *EX-1003* ¶89. The particular content keyword matched content indicative of an internal host's use of the popular Windows Media application. *Id.* The rule identified that such action would violate corporate policy and the corresponding signature document for the rule further detailed:

> This event is generated when network traffic indicating the use of a multimedia application is detected . . . This may be a violation of corporate policy since these applications can be used to bypass security measures designed to restrict the flow of corporate information to destinations external to the corporation . . . Use of these programs may constitute a violation of company policy. Clients may also contain vulnerabilities that can give an attacker an attack vector for delivering Trojan horse programs and viruses . . . A user can download files from a source external to the protected network that may contain malicious code hidden in the file giving an attacker

the opportunity to gain access to a host inside the protected network.

Ease of Attack: Simple.

EX-1049 pp.1-2; *EX-1003* ¶89. Vulnerabilities with various multimedia transfer protocols including RTP were known to a POSA; thus a POSA understood that enforcing security policies which disallowed the use of such protocols on a protected network was a straightforward way to protect such network from such vulnerabilities. *Id.*; *EX-1041* p.51; *EX-1050* p.27; *EX-1003* ¶¶89, 91-100.

Early versions of HTTP transmitted data unencrypted, leaving them vulnerable to eavesdropping. The Secure Sockets Layer (SSL) protocol was developed in 1995 to address this vulnerability. *EX-1038* p.1; *EX-1003* ¶101. As security issues were identified, new versions were released (SSLv2 → v3 in 1996), and IETF began standardizing them, releasing SSL's successor TLS 1.0 protocol as a minor improvement on SSLv3 in 1999. To address well-known security vulnerabilities in SSLv2, SSLv3, and TLS 1.0, the IETF released TLS 1.1 in 2006, and then TLS 1.2 in 2008. *EX-1013*; *EX-1014*; *EX-1015* pp.4-5, 20, 74; *EX-1016*; *EX-1003* ¶101.

The SSL/TLS protocols were well understood and standardized prior to March 2013. *EX-1003* ¶103. The Record Protocol[10] includes (i) fragmenting the

[10] Unless otherwise specified, Petitioner refers to "SSL/TLS Record Protocol packets," "SSL/TLS Record headers," and "SSL/TLS Records" herein simply as "Record Protocol packets," "Record headers," and "Records."

higher-layer subprotocol data into blocks, (ii) if applicable (for Finished *handshake* message data, and *application data* message data) encrypting each block, and (iii) prepending a Record header. *EX-1015* pp.13, 16-19, 24-32, 48, 50; *EX-1038* p. 3, *EX-1003* ¶¶103-104. For SSL/TLS versions higher than SSLv2[11], the Record header added to *every* Record (*i.e.* the block formed using the Record protocol) includes a SSL/TLS version field in bytes 1-2. *EX-1015* pp.16-17; *EX-1003* ¶¶104-105

2. Sourcefire

Sourcefire is a user manual for the Sourcefire 3D System. The 3D System could identify changing assets and vulnerabilities on the network, determine the types of attacks against the network and their impact, and defend the network in real time. *EX-1004* p.32; *EX-1003* ¶122.

Sourcefire describes packet-filtering devices (3D Sensors) of the 3D System that a user (*e.g.*, network security administrator) deployed and configured in a network to passively or "inline" monitor network traffic. Each 3D Sensor deployed in a network was capable of running any combination of three major software components: (1) Intrusion Protection System (IPS), (2) Real-time Network Awareness (RNA), and (3) Real-time User Awareness (RUA). The IPS

[11] In SSLv2, the SSL version could only be obtained by examining unencrypted records of handshake packets and not the Record header. *EX-1018*; *EX-1003* ¶105.

provided "best-in-class intrusion detection and prevention by harnessing the power of the industry-standard Snort® rules-based detection engine. Backed by the acclaimed Sourcefire Vulnerability Research Team™ (VRT), Sourcefire delivers its customers unrivaled protection against known and unknown threats." *EX-1004* pp.33-34; *EX-1003* ¶123.

The 3D Sensor running the IPS monitored the network for attacks that might affect the availability, integrity, or confidentiality of hosts on the network. Each deployed 3D Sensor with IPS examined packets traversing a network, looked for malicious activity, and reported and/or took actions based on detected malicious activity. *EX-1004* pp.35, 254-256; *EX-1003* ¶124. The IPS performed these functions on packets using a series of decoders, preprocessors, and a rules engine (as illustrated in §VIII.A.3), each of which implemented rules to look for the broad range of exploits that attackers had developed. *Id.*

The layer-specific decoders converted the headers and payloads of packets captured from the network by the 3D Sensor into a format that could easily be used by the preprocessors and rules engine. The decoders also detected a variety of possibly suspicious error or anomaly conditions in the packet headers and alerted or blocked packets based on abstract "decoder rules" that indexed these different error checks. The preprocessors normalized packets at the application layer, detected anomalies (such checks were indexed as preprocessor rules), and could be

invoked by the rules engine based on certain "keywords" of intrusion rules. The rules engine implemented intrusion rules to determine whether the headers and/or payloads of received packets triggered one or more of such rules. *EX-1004* pp.256-259, 513, 2084, 2089; *EX-1003* ¶¶125, 128. The 3D Sensor with IPS could be deployed in an "inline" detection mode to drop or replace packets that the various rules implemented thereon detected as being harmful. *EX-1004* pp.262-265, 276-277, 761, 2093; *EX-1003* ¶126.

The rules supplied with a 3D Sensor with IPS were developed by the Sourcefire VRT. These rules (implemented by the code of the decoders and preprocessors, or in the rules engine) were selectable by a user to detect the most likely attacks to occur on such user's network. IPS allowed a user to modify various parameters of the rules to customize them as desired for a network and to write their own custom intrusion rules tuned to the user's specific network environment and the types of anomalies and malicious activities that such environment is likely to encounter. *EX-1004* pp.256-260, 428-430, 761-770. Sourcefire explains that the most successful rules targeted traffic that attempted to exploit known vulnerabilities rather than specific known exploits. By writing rules and specifying the rule's event message, the 3D System could more easily identify traffic that indicated attacks and policy evasions. *EX-1004* pp.403-406, 435-439, 485, 762-766.

The intrusion rules had 5-tuple values associated with them. *EX-1004* pp.256-259, 761-762. Intrusion rules[12] contained two logical parts: the rule header and the rule options. The rule header part contained:

- the 5-tuple:
    - protocol;
    - source and destination IP addresses and netmasks;
    - source and destination ports;
- rule's action or type (*e.g.* alert and allow, drop, ignore and allow); and
- direction indicators showing the flow of traffic from source to destination.

The rule options part contained:

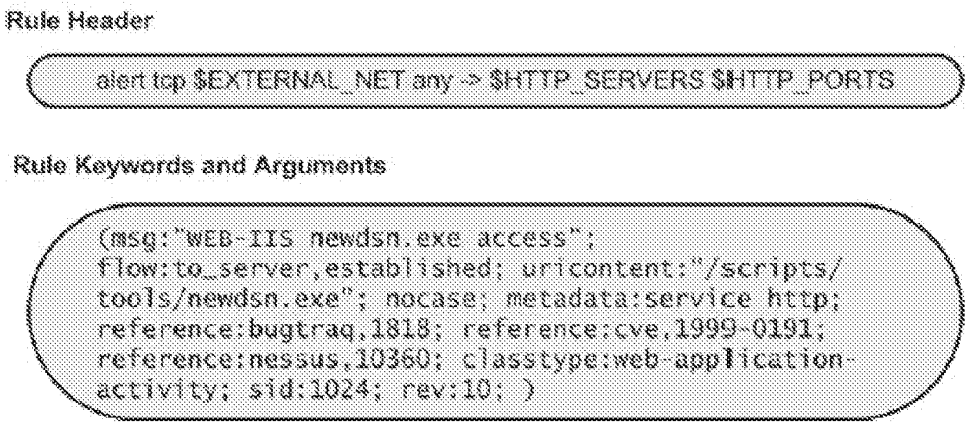
- event messages;
- keywords and their parameters and arguments;
- patterns that a packet's payload must match to trigger the rule; and
- specifications of which parts of the packet the rules engine should inspect;

EX-1004 pp.761-770; *EX-1003* ¶¶132-133.

An example intrusion rule in Sourcefire illustrates these different parts of a rule:

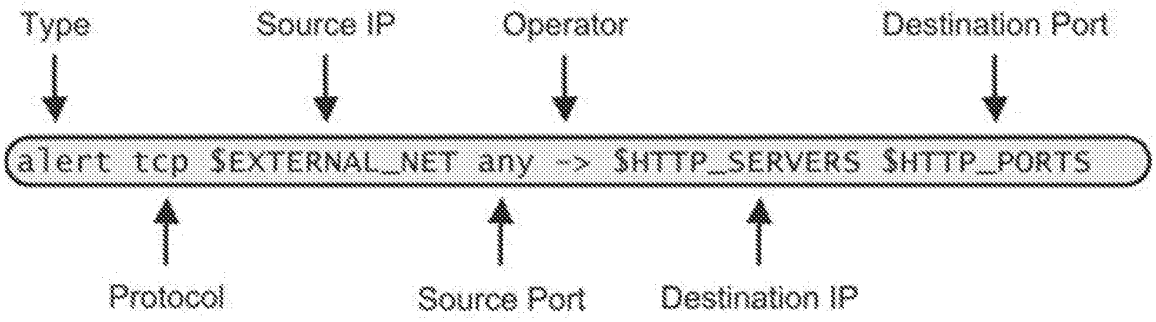
---

[12] Petitioner uses "intrusion rules" herein to refer to "standard text" rules as opposed to "shared object" rules which included customizable "rule header" parts but not customizable "rule options" parts. *EX-1004* pp.405-406, 761-771; *EX-1003* ¶131.



EX-1004 pp.762-763; *EX-1003* ¶134.

Sourcefire explains that every intrusion rule had parameters and arguments that made up the rule header (including the 5-tuple). For example, the following figure and table illustrate the parts of a rule header in the example intrusion rule and how they could be used by IPS:



Rule Header Values

Rule Header Component	Example Value	This Value...
Action	alert	Generates an intrusion event when triggered.
Protocol	tcp	Tests TCP traffic only.
Source IP Address	$EXTERNAL_NET	Tests traffic coming from any host that is not on your internal network.
Source Ports	any	Tests traffic coming from any port on the originating host.
Operator	->	Tests external traffic (destined for the web servers on your network).
Destination IP Address	$HTTP_SERVERS	Tests traffic to be delivered to any host specified as a web server on your internal network.
Destination Ports	$HTTP_PORTS	Tests traffic delivered to an HTTP port on your internal network.

EX-1004 pp. 762-764; *EX-1003* ¶¶135-136.

A user could specify rule behavior by combining keywords in the non-rule header part of a rule. Keywords and their associated "arguments" dictated how the rules engine, and any relevant preprocessors, tested and evaluated packets and packet-related values. Intrusion rule keywords allowed performance of inspection functions, such as content matching, protocol-specific pattern matching, and state-specific matching. To customize a security policy tuned to the user's specific network environment, the rules engine and preprocessors allowed the combination of any number of: (i) compatible keywords to create highly specific intrusion rules and (ii) rules. This helped decrease the chance of false positives and negatives and focused the intrusion-based information that a user received. *EX-1004* pp.769-770, 333-335; *EX-1003* ¶137.

Like the 193 Patent claims, Sourcefire discloses that, for a given 3D Sensor with IPS, multiple intrusion rules could be used to filter packets. These rules used the 5-tuple of the packet header to filter the packets, including both the source and destination IP addresses, which represent the source network from which the packets originated (*i.e.*, the "first network" of claim 1) and the destination network to which they are directed (*i.e.*, either the "second network" or the "third network" of claim 1). The destination port[13] in the 5-tuple also reflected the protocol (*e.g.*, HTTP, FTP, SMTP, HTTPS) being used for the data transfer. *EX-1004* pp.256-259, 764-769; *EX-1003* ¶138.

Based on intrusion rule keywords, packets were filtered based on various application-layer data including data associated with particular types of data transfer (*e.g.*, HTTP, FTP, SMTP, HTTPS, IM, multimedia, HTTP methods, FTP commands, TLS version) and data associated with IM applications. *EX-1004* pp.334, 373, 428-429, 435-439, 491, 538-542, 546-560, 597-601, 697-701, 765, 785-786, 827-828, 874, 2032-2043, 2092. The type of packet-transformation functions or actions that could be triggered by the rules, when a given packet matched all of the criteria in a given rule, were *pass* (and ignore), *alert* (and pass)

[13] A POSA understood that the destination port in client → server communication packets is the source port in server → client communication packets. *EX-1003* ¶138.

or *drop* (block) such packet. *EX-1004* pp.762, 764-769, 358-359; *EX-1003* ¶¶140-146, 160.

Thus, Sourcefire described a very flexible approach to customizing Sourcefire-provided intrusion rules, and writing new intrusion rules (including using Sourcefire-provided keywords), which enabled users to implement many different types of intrusion rules in their particular intrusion policy in their particular IPS on received packets that, when certain rules triggered, some packets were allowed to pass (with or without an alert), and, when other rules triggered, other packets were blocked.

3. Detailed Application of Sourcefire and the Knowledge of a POSA to the Challenged Claims

a. <u>Sourcefire and the Knowledge of a POSA disclose the Preamble and Element [A]</u>

i. **18[P]** A system comprising:

ii. **18[A]** at least one processor; and a memory storing instructions that when executed by the at least one processor cause the system to:

iii. **19[P]** One or more non-transitory computer-readable media comprising

iv. **19[A]** instructions that when executed by one or more computing devices cause the one or more computing devices to:

Sourcefire describes a system that includes a 3D Sensor, and that each 3D Sensor included a processor (CPU), memory, and disk storage. *EX-1004* pp.33-34,

106-107. A POSA understood that the 3D Sensor disk memory is non-transitory computer-readable media that included instructions to control the operation of the 3D Sensor. *Id.* The Board similarly found in IPR2018-01436 that the substantively identical limitation in the Parent 552 Patent was disclosed by Sourcefire.[14] *EX-1058* at 36-37.

b. <u>Sourcefire and the Knowledge of a POSA disclose Element [B]</u>

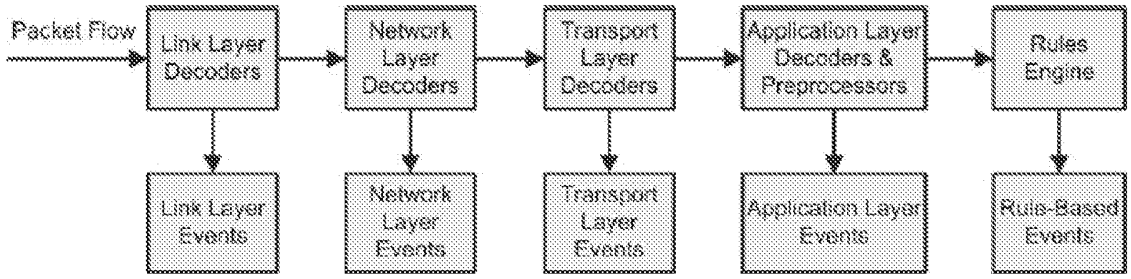
i. **18[B]** receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

ii. **19[B]** receive, from a computing device located in a first network, a plurality of packets wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

Sourcefire describes that 3D Sensors with IPS monitored a network for attacks that might affect the availability, integrity, or confidentiality of hosts located in a network that it was designed to protect. Each deployed 3D Sensor with IPS examined the traversing packets, looked for malicious activity, and reported and/or took actions based on detected malicious activity. The IPS

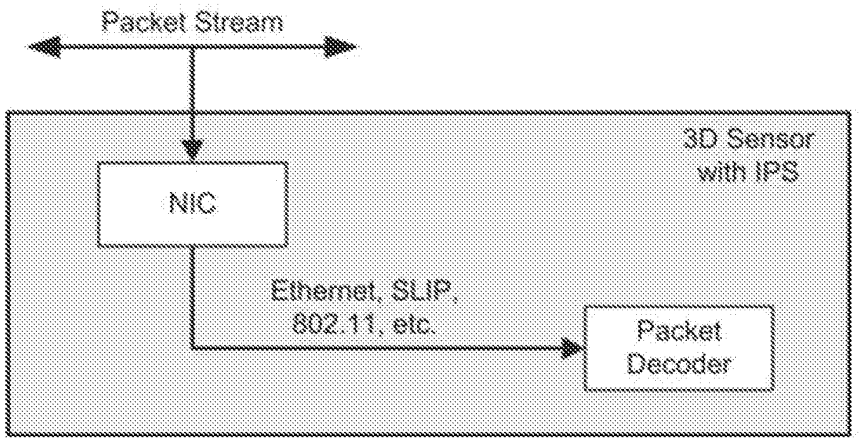
[14] The Board held that independent Claims 1, 8, and 15 of the 552 Patent have substantially similar limitations, and therefore the Board focused its analysis on Claim 1, but it applied equally to Claims 8 and 15. *EX-1058* at 36-37.

performed these functions on packets using a plurality of packet-filtering rules implemented through a series of decoders, preprocessors, and a rules engine (as illustrated below), each of which implemented rules to look for the broad range of exploits that attackers had developed:



EX-1004 pp.35, 253-256; *EX-1003* ¶150.

Sourcefire discloses that each 3D Sensor received packets through a communication interface including "inline" interfaces in which rules dropped or allowed packets received into such decoders, preprocessors, and rules engine via such inline interfaces. Sourcefire discloses one example of how a 3D Sensor received packets via a network interface card as shown below:



EX-1004 pp.222-223, 234-235, 253-254, 257, 262-264, 435-439; *EX-1003* ¶151.

Thus, Sourcefire discloses 3D Sensors receiving a plurality of packets, some of which can be deemed to be a first portion of packets and some of which can be deemed a second portion of packets, and each Sensor is provisioned with a plurality of packet-filtering rules. Sourcefire discloses that the packets received by the 3D Sensor originate from a computing device (*e.g.*, host) located in a first network where the first network could be the network that the 3D Sensor is designed to protect (*e.g.*, HOME_NET) or a network external to such network (*e.g.*, EXTERNAL_NET). *EX-1004* pp.213-214, 225-227, 234-235, 260, 277-278, 333-335, 373-379; *EX-1003* ¶152.

The Board similarly found in IPR2018-01436 that the substantively identical limitation in the Parent 552 Patent was disclosed by Sourcefire. *EX-1058* at 37-38.

c. **Sourcefire and the Knowledge of a POSA disclose Element [C]**

i. **18[C]** responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

ii. **19[C]** responsive to a determination that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

As discussed above, Sourcefire discloses that IPS allowed a user to modify various parameters of rules to customize them as appropriate or desired for a network and/or to write their own custom intrusion rules tuned to the user's specific network environment and the types of anomalies and malicious activities that such network environment is likely to encounter. Sourcefire explains that the most successful rules targeted traffic that may attempt to exploit known vulnerabilities rather than specific known exploits. By writing rules and specifying the rule's event message, the system could more easily identify traffic that

indicated attacks and policy evasions. *EX-1004* pp.403-406, 435-439, 485, 762-770; *EX-1003* ¶155.

Sourcefire describes that all of the intrusion rules had 5-tuple criteria associated with them which included the source IP addresses and source port and the destination IP addresses[15] and destination port for the received packets. *EX-1004* pp. 256-259, 761-770; *EX-1003* ¶156. A POSA understood that this 5-tuple rule criteria could be used to filter packets transferring data from a first network (source) to a second network (destination), for example, from an internal protected network to an external network destination and vice versa. *EX-1003* ¶156. For example, the 5-tuple for each packet in the first portion of packets would include data that indicated the first network contained the source IP address and the second network contained the destination IP address. *EX-1004* pp.358, 488-490, 761-770; *EX-1003* ¶156. The well-known destination port in the 5-tuple of these packets also often reflected the protocol (*e.g.*, HTTP (port 80), HTTPS (port 443), FTP (port 21), SMTP (port 25), XMPP (port 5222 or 5269)) being used for the data transfer if such packets were traveling over a standard port. *EX-1004* pp.256-259, 764-769, 54-55; *EX-1044*, pp.43-44; *EX-1050* pp.24-25; *EX-1003* ¶157.

[15] The IP address 5-tuple rule criteria could be a range of IP addresses or a specific IP address. *EX-1004* pp.762-763, 767, 769, 702-704, 59-60; *EX-1003* ¶156.

As discussed above, by using the rules language, a user could specify the behavior of a rule by combining keywords in the rule. Keywords and their associated arguments dictated how the rules engine, and any relevant preprocessors invoked by the rule, tested and evaluated packets and packet-related values by, for example, content matching, protocol-specific pattern matching, and state-specific matching. The rules engine and preprocessors allowed the combination of any number of compatible keywords to create highly specific intrusion rules, and allowed the user to combine any number of rules to customize a security policy tuned to the user's specific network environment. This helped decrease the chance of false positives and negatives and focused the intrusion information that a user received. *EX-1004* pp.769-770; *EX-1003* ¶158.

For example, Sourcefire provided guidelines for creating rules to implement a security policy including "understand[ing] the traffic that traverses the network", "set[ting] your variables to accurately reflect your home and external networks" and including guidance that "[i]f none of the existing intrusion rules meet your needs, write new rules that inspect for intrusion attempts." *EX-1004* pp.333-335; *EX-1003* ¶159. Thus, Sourcefire expressly taught a POSA to customize/tailor rules and rule combinations for whatever purpose is set forth in the security policy and provides the motivation for a POSA to implement the specific rules and rule combinations recited in the Challenged Claims. *EX-1003* ¶159.

As described above, in addition to the destination port and destination network (and other) 5-tuple rule criteria, keywords of intrusion rules could be applied to filter packets as they arrived at various preprocessors and at the rules engine by searching for matched content in packets such as, for example, data associated with particular types of data transfer (*e.g.*, HTTP, FTP, SMTP, HTTPS, IM, multimedia, HTTP methods, FTP commands, TLS version). *EX-1004* pp.827-828, 491, 597-601, 435-439, 785-786, 334, 373, 428-429, 874, 2032-2043, 2092; *EX-1003* ¶¶141-146, 160. Sourcefire describes the type of packet-transformation functions actions that could be triggered by the rules, when a given packet matched all of the criteria in a given rule, as *pass* (and ignore), *alert* (and pass) or *drop* (block) such packet. *EX-1004* pp.762, 764-769, 358-359; *EX-1003* ¶160. Thus, a POSA understood that the application of various rules could cause a first portion of packets from the first network addressed to the second network to be dropped. *EX-1003* ¶160.

For example, Sourcefire discloses how a user would write an intrusion rule that, in addition to the 5-tuple criteria of destination port 80 (HTTP) and second network destination, applied rule keywords by the HTTP Inspect preprocessor and rules engine to search for matched application-layer content in packets based on criteria including the most common HTTP methods of GET, PUT, POST and CONNECT and *pass* (allow), *alert* (and pass), or *drop* (block) packets based on

results of such searches. *EX-1004* pp.560, 568, 786, 700; *EX-1003* ¶¶143, 161. A POSA understood that identifying HTTP methods was important in existing packet-filtering firewalls with stateful inspection because application methods were used as part of rule criteria to block and pass packets, *e.g.*, a known "stateful inspection firewall allowed the FTP 'GET' command but disallowed the 'PUT' command" (EX-1008 4:31-41), vulnerabilities with certain HTTP methods (*e.g.*, PUT, POST, DELETE) were well-known, and HTTP methods were used in IDS rules at least as early as 1997. *EX-1028* p.189; *EX-1004* pp.785-786, 807, 435-439, 491; §VIII.A.1; *EX-1003* ¶161. The HTTP standard specification itself identified that certain HTTP methods (*e.g.*, HTTP POST, PUT, DELETE) were riskier than other HTTP methods (*e.g.*, HTTP GET). *See, e.g.,* CS-1046 pp. 44 ("[HTTP GET] method[] ought to be considered 'safe'" compared to "other methods, such as POST, PUT and DELETE."), 46-49, 130-134.

Therefore, a POSA understood Sourcefire disclosed how a user would have written an intrusion rule that applied the HTTP Method option of the HTTP content keyword as part of the criteria to invoke the HTTP Inspect preprocessor to identify a first portion of packets using the particular PUT (or POST, DELETE, CONNECT, etc.) method type of data transfer and to block such packets with certain application payload content posing a threat from continuing towards their

second network destination. *EX-1003* ¶¶143, 162; §VIII.A.1; *EX-1004* pp.697-701.

A POSA understood Sourcefire disclosed how a user would have implemented a specific security policy which achieved predictable benefits of protecting his or her network against a known security vulnerability by writing an intrusion rule that applied the HTTP Method option of the HTTP content keyword as part of the rule's criteria to invoke the HTTP inspect preprocessor to identify traffic using that HTTP method (*e.g.*, POST, PUT, DELETE, or CONNECT) and to *drop* (*i.e.*, block) such packets with certain application payload content posing a threat (*e.g.*, sensitive data or a malicious Uniform Resource Identifier (URI)) from continuing towards their second network destination. *EX-1004* pp. 785-786, 807, 435-439, 491. Moreover, for example, a POSA would be motivated to use rules as taught by Sourcefire to block a first portion of packets identifying an HTTP POST method to, for example, prevent an employee from posting sensitive data to a bulletin board or providing such data to a malicious URI on the second network. *Id.*; *EX-1046* pp. 44, 47. Furthermore, for example, a POSA would be motivated to use rules as taught by Sourcefire to block a first portion of packets identifying an HTTP CONNECT method to, for example, prevent an employee from tunneling sensitive data to a malicious second network proxy. *Id.*; *EX-1046* pp. 44, 49.

As another example, Sourcefire discloses that, in addition to the 5-tuple criteria of destination port 21 (FTP) and second network destination, rule keywords would be applied by the rules engine to search for matched content in packets based on criteria including FTP command (*e.g.*, the known "PORT" FTP command), or known "anonymous" usernames, and *pass* (allow), *alert* (and pass), or *drop* (block) packets based on results of such searches. *EX-1004* pp.556, 765, 538-542, 546-560, 700, 492; 776-783, 861-864; § VIII.A.1; *EX-1003* ¶¶144, 163. As described in Sourcefire, and as was known to a POSA, identifying this particular type of data transfer was important to address the well-known Bounce attack. *EX-1004* p.556; § VIII.A.1; *EX-1040* pp.2-3; *EX-1003* ¶163. Therefore, a POSA understood Sourcefire disclosed how a user would have written a rule applying content keywords as part of the rule criteria to identify a first portion of packets using the particular PORT FTP command type of data transfer and to block such packets from continuing towards their second network destination. *EX-1003* ¶164; *EX-1004* pp.697-701.

As a further example, Sourcefire discloses that, in addition to the 5-tuple criteria of destination port 443 (HTTPS) and second network destination, rule keywords would be applied by the SSL preprocessor (when invoked by the rules engine) and either *pass* (allow), *alert* (and pass), or *drop* (block) packets based on criteria including encryption protocol version (*e.g.* TLS version). A POSA

understood Sourcefire disclosed how a user would include the keyword ssl_version in such intrusion rules and be applied to identify and block a first portion of packets (*e.g.*, vulnerable Record Protocol packets) from continuing towards their second network destination. *EX-1004* pp.827-828, 491, 597-601, 435-439; *EX-1003* ¶¶141-142, 165. A POSA understood that certain SSL and TLS versions contained vulnerabilities (*e.g.*, TLS 1.0, SSLv2, SSLv3) and Sourcefire teaches that a *drop* rule could be written to block packets based on a ssl_version that included a known vulnerability. *EX-1037*; *EX-1038*; *EX-1039* p.4; *EX-1013*; *EX-1014*; *EX-1015*; *EX-1003* ¶165.

Because security vulnerabilities associated with HTTPS data transfers using or proposing to use TLS 1.0, SSLv2, SSLv3 were widely known, a POSA would be motivated to write appropriate *drop* rules to identify and block Record Protocol packets that proposed using (or did use) these particular less secure SSL and TLS types of data transfer from continuing toward their second network destination. *EX-1003* ¶166; *EX-1004* pp.697-701.

As a further example, a POSA reading Sourcefire understood that Sourcefire taught a user how to include multimedia 5-tuple and content keyword rule criteria in intrusion rules and applied by the rules engine to identify matched content in a first portion of packets and block such packets from continuing towards their second network destination, for example, to enforce a security policy prohibiting

employees' use of such applications. A POSA might use the default UDP port 5004 for transferring audio/video content to block some RTP traffic, or use fixed RTP header fields as content keyword targets or block SIP/SDP packets in a control connection that indicated the use of RTP (*e.g.*, with content string 'RTP/AVP' or 'a=rtpmap'). *EX-1004* pp.266, 333-335, 429-430, 1453, 1470-1471, 2030, 2034, 2037, 2039, 2040-2042, 2092; *EX-1050* pp.24-25; *EX-1050* pp.77-79, *CS 1052* p.7; § VIII.A.1; EX-*1003* ¶¶146, 167.

A POSA understood that such security policies in enterprise networks restricted employees' use of high bandwidth applications like streaming media while also avoiding known vulnerabilities posed by such use. *Id.*; § VIII.A.1; *EX-1003* ¶168. Thus a POSA understood that enforcing security policies which disallowed the use of known protocols for transferring streaming multimedia (including RTP) on an internal network was simply a design choice to yield predictable results of reducing employee bandwidth usage with increased security on such network because doing so would involve nothing more than applying a known technique to a known device ready for improvement. *EX-1003* ¶168.

As discussed above, and as acknowledged by the 193 Patent, there is no technological difference between applying one particular type of data transfer criteria over another (*e.g.*, HTTP (or HTTP method), FTP (or FTP command), multimedia data (*e.g.*, RTP transfer), SSL/TLS version value, messaging protocol

(*e.g.*, AIM, Yahoo! Messenger, XMPP)), and there are no specific technology changes needed to accommodate one data transfer protocol (*e.g.*, HTTP data transfer) over another (*e.g.*, messaging, encryption, FTP, RTP), or one data transfer method (*e.g.*, HTTP GET, FTP GET, TLS 1.2) over another (*e.g.*, HTTP PUT, FTP PORT, TLS 1.0). §III.B; *EX-1003* ¶169. Moreover, as also acknowledged by the 193 Patent, there are no specific technology changes needed to accommodate allowing or blocking packets specifying one destination and origin from packets specifying any other possible destination and origin. §III.B; *EX-1003* ¶170.

Thus, it is simply a design choice to select from a finite number of identified rule criteria that are relevant to a selected network vulnerability (*e.g.*, HTTP PUT method, FTP PORT command, TLS version 1.0 and certain application payload content (*e.g.*, IM content, multimedia content)) to yield predictable results of increased network security because doing so would involve nothing more than applying a known technique to a known device ready for improvement. *EX-1003* ¶170.

Thus, Sourcefire teaches a user how to configure various packet-filtering rules with 5-tuple rule criteria and rule keywords and arguments to prevent a particular type of data transfer from the first network to a second network, wherein the data in such packets satisfies criteria based on HTTP method, FTP command, IM content, multimedia content (*e.g.*, RTP streams), TLS version, or any other

criteria designed to prevent data transfer subject to a known vulnerability or exploit. *EX-1004* pp.333-335, 435-439, 491-492, 538-542, 546-560, 597-601, 697-701, 765, 785-786, 807, 827-828; *EX-1003* ¶171.

d. <u>Sourcefire and the Knowledge of a POSA disclose Element [D]</u>

i. **18[D]** apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

ii. **19[D]** apply, to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

As discussed above (and held by the Board in the 552 IPR), Sourcefire discloses whether to apply a first-operator in a two-stage packet filtering operation. IPR2018-01436, Paper 40, at 52-53. As set forth above, "[t]he rules engine implemented intrusion rules to determine whether the packet headers . . . of received packets triggered one or more of such rules," and "Sourcefire describes filtering packets based on packet header information including the 5-tuple, just like the Stage I evaluation described in the '552 Patent" as "[e]very intrusion rule is qualified by the 5-tuple." IPR2018-01436, Paper 40, at 52 *citing EX-1004*, 256-259, 761-770. As detailed in these cited excerpts in Sourcefire, the intrusion rules,

which included user-customizable rule header and rule options criteria, were organized into groups or "subsets" based on commonalities in the respective rule header criteria (*e.g.*, 5-tuple, direction indicator (specifying which direction a packet must be traveling (*e.g.*, from the protected network and toward an external network) for the rule to inspect the packet), etc.):

> When you apply an intrusion policy to the detection engines, and before any packets are processed, the rule optimizer reads in all the activated rules and then classifies them in subsets based on criteria such as transport layer, application protocol, direction to or from the protected network, and so on. As packets arrive at the rules engine, it selects the appropriate rule subsets to apply to each packet.

EX-1004, 259; 761-770 (showing customizable rule header criteria); IPR2018-01436, Paper 40, at 52.

As also discussed above, and in the cited Sourcefire excerpts, as packets arrive at the rules engine, it first checked whether packet-header-field values in the packets matched this rule header criteria and, only if so, did it "test" whether the remainder of the rule criteria (*e.g.*, rule keywords and arguments) matched to trigger the Rule Action:

> As packets arrive at the rules engine, it selects the appropriate rule subsets to apply to each packet.

EX-1004, 259.

> Rule headers include the source and destination [IP addresses/ports] of traffic that the rule inspects. You can restrict packet inspection to the packets originating from [specific IP

> addresses/specific ports] or those destined to [a specific IP address/specific ports]. This reduces the amount of packet inspection the system must perform. This also reduces false positives by making the rule more specific and removing the possibility of the rule triggering against packets whose source and destination [IP addresses/ports] do not indicate suspicious behavior.

EX-1004, 766-768; *see also id.*, 761 (discussing alert, pass, drop rule actions), 764 ("tests traffic" in example rule header values table), 765-766 (specifying rule actions), 358-359 ("A *drop rule* is an intrusion rule . . . whose rule state is set to Drop and Generate Events."); IPR2018-01436, Paper 40, at 52.

Based on these and other disclosures in Sourcefire, the Board in the 552 IPR held that "Sourcefire discloses determining whether to apply an operator in a two-stage packet filtering operation:

> if a first portion of packets match certain rule header criteria (*e.g.*, specific addresses/specific ports), they will be evaluated against a first "subset" of rules (e.g., including the TLS-version packet-filtering rules) – some of these packets may pass and some may be blocked. Pet., 56-58. If a second portion of packets does not match this rule header criteria for the first "subset" of rules (*e.g.*, different addresses/different ports), they will not be evaluated against the remainder of the rule criteria (*e.g.*, rule keywords and arguments) for the first "subset" of rules. *Id.* And, if this second portion of packets matches certain rule header criteria of a second "subset" of rules, they will instead be evaluated against the remainder of the rule criteria for the second "subset" of rules (i.e., without applying the TLS-version packet-filtering rules)."

IPR2018-01436, Paper 40, at 53; *see also id.* at 48-52, 64-65.

As also discussed above, the Board held that the construction of "operator" per the common specification of the 193 Patent and Parent 552 Patent has "two meanings: (1) a packet transformation function, without specifying application-header-field-value criteria; and, (2) a function specified by a packet-filtering rule that specifies one or more application-header-field criteria and a packet transformation to apply to the packet for each of the application-header-field criteria." Thus, as discussed above (*see* 18[C] and 19[C]) and already found by the Board, Sourcefire disclosed how a user would write a two-stage intrusion rule that specified a first operator configured to drop packets associated with a TLS version 1.0 type of data transfer and where such first operator would be applied responsive to a determination that the intrusion rule's first stage criteria was met (5-tuple criteria specifying, at least in part, packet header data indicating a second network destination). *EX-1058* at 48-54.

Using the ssl_version drop rule discussed above as an example (*see* 18[C], 19[C]), the Board determined that Sourcefire disclosed a "first operator", as part of an intrusion rule, that specified (i) the ssl_version keyword and arguments that indicates application-header-field criteria (*e.g.*, TLS version 1.0) to identify the first portion of packets using that TLS version, and (ii) a *drop* (*i.e.*, block) rule action to apply to each packet in the first portion of packets when each such packet matched this application-header-field criteria.

Likewise, using the HTTP method drop rule discussed above as an example (*see* 18[C], 19[C]), Sourcefire disclosed a "first operator", as part of an intrusion rule, that specified (i) the HTTP Method option of the HTTP content keyword that indicates application-header-field criteria to invoke the HTTP inspect preprocessor to identify the first portion of packets using that HTTP method (*e.g.*, HTTP PUT), and (ii) a *drop* (*i.e.*, block) rule action to apply to each packet in the first portion of packets when each such packet matched this application-header-field criteria. *EX-1004* pp. 785-786, 807, 435-439, 491.

Indeed, in the 552 IPR, the Board specifically determined that:

> Regarding claim 3, Petitioner contends that Sourcefire discloses that rules could be written, which included the most common HTTP methods of GET, PUT, POST, and CONNECT as one or more of the rule criteria. Pet. 47 (citing Ex. 1004, 568, 786; Ex. 1003 ¶ 172). Petitioner also contends that Sourcefire discloses that such rules can be implemented by the HTTP inspect preprocessor and by the rules engine and provides a specific keyword option just to access the HTTP method. *Id.* at 48 (citing Ex. 1004, 785–786, 807, 435–439, 491; Ex. 1003 ¶¶ 173, 124). We find Petitioner's arguments and evidence to be persuasive.
>
> Regarding claim 4, Petitioner contends that a POSA understood that Sourcefire disclosed how a user would have written a rule using the HTTP Method option of the HTTP content keyword as part of the application-layer rule criteria to invoke the HTTP inspect preprocessor to identify a packet using the "PUT" HTTP method and to block such a packet with certain application payload content posing a threat from continuing towards its destination." *Id.* at 51–52 (citing Ex. 1004, 560, 568, 786; Ex. 1003 ¶ 184). We find Petitioner's arguments and evidence to be persuasive.

EX-1058 at 63-64.

And, in the 713 IPR, the Board specifically determined that:

> Petitioner explains that Sourcefire discloses rules other than TLS version rules—including '5-tuple' rules based on protocol type, and source or destination IP addresses or ports—which teaches that a second portion of packets (as well as the first portion) can be filtered to be forwarded or dropped (based on such other rules) without applying the TLS version rule applied to the first portion of packets, as recited in claims 2–4. *Id.* at 46–50 (citing Ex. 1003 ¶¶ 154, 157, 160–161, 163, 165, 168, 171). The Petition also explains how Sourcefire discloses an 'HTTP inspect preprocessor' that can detect HTTP methods such as GET, PUT, POST, and CONNECT, which teaches determining that a packet comprises data corresponding to such HTTP methods, as recited in claims 5 and 6. *Id.* at 50–55 (citing Ex. 1003 ¶¶ 174–180, 183) . . . We agree with Petitioner's analysis and find that the cited evidence supports its contentions by a preponderance of the evidence that Sourcefire teaches all of the limitations of claims 2–7.

EX-1064 at 22.

Thus, as discussed above (*see* 18[C] and 19[C]), the Board determined that Sourcefire disclosed how a user would write a two-stage intrusion rule that specified a first operator configured to drop packets associated with an HTTP PUT type of data transfer and where such first operator would be applied responsive to a determination that the intrusion rule's first stage criteria was met (5-tuple criteria specifying, at least in part, packet header data indicating a second network destination).

Likewise, using the FTP command drop rule discussed above as an example (*see* 18[C], 19[C]), Sourcefire disclosed a "first operator", as part of an intrusion rule, that specified (i) a content keyword that indicates application-header-field criteria to identify the first portion of packets using the particular FTP PORT command type of data transfer, and a *drop* (*i.e.*, block) rule action to apply to each packet in the first portion of packets when each such packet matched this application-header-field criteria. *EX-1004* pp.556, 765, 538-542, 546-560, 700, 492; 776-783, 861-864. Thus, as discussed above (*see* 18[C] and 19[C]), Sourcefire disclosed how a user would write a two-stage intrusion rule that specified a first operator configured to drop packets associated with an FTP PORT type of data transfer and where such first operator would be applied responsive to a determination that the intrusion rule's first stage criteria was met (5-tuple criteria specifying, at least in part, packet header data indicating a second network destination).

e. <u>Sourcefire and the Knowledge of a POSA disclose Element [E]</u>

i. **18[E]** drop each packet in the first portion of packets; and

ii. **19[E]** drop each packet in the first portion of packets; and

Applying the HTTP method drop rule, FTP command drop rule, or TLS version drop rule from the examples above will result in dropping each packet in the first portion of packets. *See* 18[C]-18[D], 19[C]-19[D]. *EX-1003* ¶179.

The Board treated the substantively identical limitations in the Parent 552 Patent corresponding to limitations [C], [D] and [E] of Claims 18/19 together and found that these limitations were disclosed by Sourcefire. *EX-1058* at 38-54.

f. <u>Sourcefire and the Knowledge of a POSA disclose Element [F]</u>

i. **18[F]** responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

ii. **19[F]** responsive to a determination that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

As discussed above, Sourcefire discloses 3D Sensors receiving a plurality of packets, some of which can be deemed to be a first portion of packets from a first network (source) and destined for a second network (destination) where the criteria are associated with a particular type of data transfer such as, for example, one of

HTTP PUT method (port 80), FTP PORT command (port 21), or TLS version 1.0 (port 443). *EX-1003* ¶182.

Likewise, Sourcefire discloses that different intrusion rules could be applied to some different portion of the plurality of packets which can be deemed to be a second portion of packets from the first network (source) and destined for a third network (destination different than second network destination). *EX-1003* ¶183.

For example, the rule applied to drop the first portion of packets could include: (1) 5-tuple criteria specifying first network source IP addresses and source port and second network destination IP addresses and HTTPS destination port (*e.g.*, 443, second network IP addresses), and (2) a first operator specifying (i) ssl_version keyword and arguments that indicate TLS version 1.0 application-header-field-value criteria, and (ii) a rule action of "drop" (block) to packets that match the criteria. *See* Claim 18[D], 19[D]; IPR2018-01436, Paper 40, at 48-54. Additionally, for example, the rule applied to drop the first portion of packets could include: (1) 5-tuple criteria specifying first network source IP addresses and source port and second network destination IP addresses and HTTP destination port (*e.g.*, 80, second network IP addresses), and (2) a first operator specifying (i) HTTP Method option of the HTTP content keyword and arguments that indicate HTTP PUT method application-header-field-value criteria, and (ii) a rule action of "drop" (block) to packets that match the criteria.

In either of these examples, the different rule applied to *allow* the second portion of packets could include (1) 5-tuple criteria specifying first network source IP addresses and third network destination IP addresses and *non*-HTTPS destination port (*e.g.*, *not* port 443) (or *non*-HTTP destination port (*e.g.*, *not* port 80)), and (2) a second operator specifying (i) keyword and argument criteria indicating application-layer data that is *not* associated with a TLS version 1.0 (or HTTP PUT method data) type of data transfer (*e.g.*, TLS version 1.1 or 1.2 data, FTP data, HTTP GET method data, etc.), and (ii) a *pass* or *alert* rule action to apply to each packet in the second portion of packets when each such packet matched this application-header-field criteria. *See* Claim 18[C]-18[D], 19[C]-19[D]; IPR2018-01436, Paper 40, at 52-53, IPR2018-01437, Paper 40, at 22. The 5-tuple criteria in the different rule could specify, for example, ANY, or alternatively a netmask for a specifically known safe/trusted network, for destination IP addresses. *Id.*

The rules engine and preprocessors allowed the combination of any number of rules to customize a security policy tuned to the user's specific network environment, and Sourcefire provided guidelines on how to write rules to implement a security policy. *EX-1004* pp.333-335, 761-778; *EX-1003* ¶185. In other words, Sourcefire provided a very flexible approach to crafting rules that recognized that the same rule criteria can be utilized differently for packets to/from

an internal network as compared to an external network, for traffic received from or destined for a specific port, and, as already determined by the Board, for whether it is desired to apply a *pass*, *drop* or *alert* rule action as part of an operator, specified by such rule, and in response to triggering the application-header-field-value criteria also specified by such rule operator. *Id.*

As discussed above, and as acknowledged by the 193 Patent, there is no technological difference between combining rules that specify one particular type of data transfer criteria (*e.g.*, TLS version 1.0, HTTP PUT) as part of the rule's operator, with rules that don't specify such criteria, and other combinations that include rules that specify a different type of data transfer criteria (*e.g.*, HTTP GET, RTP, FTP, SMTP, TLS version 1.1 or 1.2) as part of the different rule's operator, and there are no specific technology changes needed to accommodate one rule combination over another, or one packet destination and origin from another. *See EX-1003* ¶186. Rather, it is simply a design choice to select from a finite number of rules that are each relevant to a selected network vulnerability (*e.g.*, TLS 1.0 vulnerabilities, HTTP PUT method vulnerabilities), and combinations of such rules that allow for packets destined for one network (*e.g.*, external second network server destination) to be treated differently than a packet destined for a different network (*e.g.*, external third network server destination). *See EX-1003* ¶186. In other words, Sourcefire encourages a POSA to improve IPS processing efficiency

or throughput to yield predictable results tuned to improved network security of the user's particular network environment because doing so would involve nothing more than applying a known technique to a known device ready for improvement. *EX-1003* ¶186.

g. <u>Sourcefire and the Knowledge of a POSA disclose Element [G]</u>

i. **18[G]** apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

ii. **19[G]** apply, to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator, configured to forward packets not associated with the particular type of data transfer toward the third network; and

Sourcefire discloses that the 3D System with IPS can apply different intrusion rules with different operators (than the first operators in 18[D], 19[D] above) that identify packets (*e.g.*, SMTP, RTP, IM, packets) that are not associated with, for example, HTTPS packets including application-layer data specifying a TLS version of 1.0 (or packets including application-layer data specifying an

HTTP PUT method) and apply a *pass* (or *alert* (and pass)) rule action to packets matching such criteria. *See EX-1003* ¶189.

In other words, a POSA would understand that Sourcefire disclosed, as a matter of design choice, how a user would also implement intrusion rules which include a second operator, as part of such rule, that specified, for example, (i) the ssl_version keyword and arguments that indicates application-header-field criteria (*e.g.*, TLS version 1.1 or 1.2) to identify the second portion of packets using that TLS version, and (ii) a *pass* (or *alert* and pass) rule action to apply to each packet in the second portion of packets destined toward their third network destination IP address when each such packet matched this application-header-field criteria. Additionally, for example, a POSA would understand that Sourcefire disclosed, as a matter of design choice, how a user would also implement intrusion rules which include a second operator, as part of such rule, that specified, for example, (i) the HTTP GET Method option of the HTTP content keyword and arguments that indicates application-header-field criteria (*e.g.*, HTTP GET) to identify the second portion of packets using that HTTP GET method, and (ii) a *pass* (or *alert* and pass) rule action to apply to each packet in the second portion of packets destined toward their third network destination IP address when each such packet matched this application-header-field criteria. Furthermore, for example, a POSA would understand that Sourcefire disclosed, as a matter of design choice, how a user

would also implement intrusion rules which include a second operator, as part of such rule, that specified, for example, content keywords and arguments that indicate application-header-field criteria to identify the second portion of packets using a different type of data transfer (*e.g.*, FTP, SMTP, RTP, etc.), and (ii) a *pass* (or *alert* and pass) rule action to apply to each packet in the second portion of packets destined toward their third network destination IP address when each such packet matched this application-header-field criteria. .

h. <u>Sourcefire and the Knowledge of a POSA disclose Element [H]</u>

i. **18[H]** forward each packet in the second portion of packets toward the third network.

ii. **19[H]** forward each packet in the second portion of packets toward the third network.

Because, for example, the TLS version 1.0 rule or HTTP PUT method rule is not applicable to the second portion of packets as described above, and because packet data in the second portion of packets satisfies different rule criteria of other *pass* or *alert* (and pass) intrusion rules, each packet in the second portion of packets will be forwarded toward their third network destination IP address. *EX-1003* ¶192.

The Board treated the substantively identical limitations in the Parent 552 Patent corresponding to limitations [F], [G] and [H] of Claims 18/19 together and

found that these limitations were disclosed by Sourcefire.[16] *EX-1058* at 63-66. First, Challenged Claims 18 and 19 recite that the first portion of packets is destined for a second network and the second portion of packets is destined for the third network. The Board in reviewing the Parent 552 Patent held that Sourcefire taught a user how "to write its own custom intrusion rules tuned to the user's specific network environment" including "destination IP addresses." *EX-1058* at 34. Moreover, the Board in reviewing the Parent 552 Patent held that "Sourcefire discloses applying an operator in two-stage packet filtering" and, among other evidence, pointed to Sourcefire's disclosure at pp. 766-768 ("You can restrict packet inspection to the packets originating from [specific IP addresses/specific ports] or those destined to [a specific IP address/specific ports]."). *Id.* at 52-53.

Second, Challenged Claims 18 and 19 recite that the "first operator configured to drop packets associated with the particular type of data transfer" is not specified in the same packet-filtering rule as the "second operator configured to forward packets not associated with the particular type of data transfer." *See also* n.3 above. In other words, in Challenged Claims 18 and 19, the "second operator"

[16] The Board held that Claims 9 and 16 of the 552 Patent have substantially similar limitations as Claim 2 of the 552 Patent, and therefore the Board focused its analysis on Claim 2, but it applied equally to Claims 9 and 16. *EX-1058* at 66.

may be part of a different packet-filtering rule than the packet-filtering rule specifying the "first operator." *Id.*

The Board in reviewing the Parent 552 Patent and discussing the dependent claims held that Sourcefire teaches using two packet filtering rules where one rule blocks packets based on TLS version, and another rule that forwards packets "without applying the TLS-version packet-filtering rules":

> if a first portion of packets match certain rule header criteria (e.g., specific addresses/specific ports), they will be evaluated against a first "subset" of rules (e.g., including the TLS-version packet filtering rules) – some of these packets may pass and some may be blocked. Pet., 56-58. If a second portion of packets does not match this rule header criteria for the first "subset" of rules (e.g., different addresses/different ports), they will not be evaluated against the remainder of the rule criteria (e.g., rule keywords and arguments) for the first "subset" of rules. Id. And, if this second portion of packets matches certain rule header criteria of a second "subset" of rules, they will instead be evaluated against the remainder of the rule criteria for the second "subset" of rules (i.e., without applying the TLS-version packet-filtering rules). Reply 21–22.

EX-1058 at 53.

Thus, every limitation recited in Challenged Claims 18 and 19 of the 193 Patent has been determined by the Board to be disclosed in the prior art cited in this Request.

IX. TESTIMONIAL EVIDENCE

The showing in this Request that the Challenged Claims are unpatentable over Sourcefire in view of the knowledge of a POSA is fully supported by the Declaration of Dr. Stuart Staniford submitted to the Board in IPR2018-01559. A copy of that declaration is provided herewith as Exhibit 1003.

Additionally, the Board relied on the testimony of Dr. Staniford in rendering its decisions IPR2018-01436 and IPR2018-01437 determining that all claims of the Parent 552 Patent and the 713 Patent respectively are unpatentable. Copies of the declarations from those proceedings are provided herewith as Exhibits 1073 and 1074.

X. CONCLUSION

For the reasons set forth above, Cisco has established substantial new questions of patentability regarding Challenged Claims 18 and 19 of the 193 Patent. Furthermore, the prior art relied upon in this Request establishes that Claims 18 and 19 of the 193 Patent are unpatentable for the reasons discussed above. In addition, because all claims of the Parent 552 Patent have been found by the Board to be unpatentable, and Claims 18 and 19 of the 193 Patent are not patentably distinct from the claims of the Parent 552 Patent, the Patent Owner is estopped from arguing that Claims 18 and 19 are patentable pursuant to 37 C.F.R. § 42.73.

All the requirements for *ex parte* reexamination have been met. Accordingly, it is respectfully requested that the PTO order such reexamination and find that claims 18 and 19 of the 193 Patent are unpatentable.

Respectfully submitted,

DUANE MORRIS LLP

BY: /Patrick D. McPherson/
Patrick D. McPherson
USPTO Reg. No. 46,255
Duane Morris LLP
505 9th Street NW, Suite 1000
Washington, D.C. 20004

Dated: March 19, 2020

Exhibit List

Exhibit #	*Description*
1001	U.S. Patent No. 9,686,193 (the "193 Patent")
1002	Select portions of prosecution history of the 193 Patent ("File History")
1003	Declaration of Petitioner's Expert Dr. Stuart Staniford in Support of Petition for *Inter Partes* Review of U.S. Patent No. 9,686,193, IPR2018-01559 (August 15, 2018) ("Staniford")
1004	Sourcefire 3D System User Guide Version 4.10 ("Sourcefire")
1005	Declaration of John Leone, IPR2018-01559 (July 20, 2018)
1006	U.S. Pat. No. 7,032,031 ("Jungck")
1008	U.S. Pat. No. 8,370,936 ("Zuk")
1009	U.S. Pat. No. 7,900,042 ("Hall")
1010	SSL Inspection – Sourcefire Cybersecurity, archived at Internet Archive Wayback Machine on December 20, 2010 at https://web.archive.org/web/20101220151851/http://www.sourcefire.com/security-technologies/cyber-security-products/3d-system/ssl-encryption-decryption ("SSL Appliances Webpage").
1011	Sourcefire SSL Appliances data sheet, archived at Internet Archive Wayback Machine on March 16, 2012 at https://web.archive.org/web/20120316165725/http://www.ndm.net:80/sourcefirestore/downloads/Sourcefire%20SSL%20Appliance%20Fact%20Sheet%20%28English%29.pdf ("SSL Appliances Data Sheet").
1013	Bard, G.V., "Cryptology ePrint Archive: Report 2006/136: A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL," archived at Internet Archive Wayback Machine on May 3, 2006 at https://web.archive.org/web/20060503043443/http://eprint.iacr.org:80/2006/136.

Exhibit #	*Description*
1014	Bard, G.V., "A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL," archived at Internet Archive Wayback Machine on May 3, 2006 at https://web.archive.org/web/20060503043634/http://eprint.iacr.org:80/2006/136.pdf.
1015	T. Dierks & E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1," *IETF RFC 4346*, April 2006, archived at Internet Archive Wayback Machine on June 26, 2006 at https://web.archive.org/web/20060626134135if_/http://www.ietf.org:80/rfc/rfc4346.txt.
1016	S. Turner & C. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0," *IETF RFC 6176*, March 2011, archived at Internet Archive Wayback Machine on March 18, 2011 at https://web.archive.org/web/20110318184421/https://tools.ietf.org/html/rfc6176.
1017	NDM Company ("Sourcefire Authorized Distributor") Product Data Sheets Webpage, archived at Internet Archive Wayback Machine on October 28, 2011 at https://web.archive.org/web/20111028104123/http://www.ndm.net:80/sourcefirestore/Product-Data-Sheets/product-data-sheets ("NDM Webpage").
1018	A. Shostack, "An Overview of SSL (version 2)," May 1995, available from https://adam.shostack.org/ssl.html (accessed July 11, 2018), archived at Internet Archive Wayback Machine on May 25, 1997 at https://web.archive.org/web/19970525224610/http://www.homeport.org/~adam/ssl.html.
1020	Barry M. Leiner *et al*., "A Brief History of the Internet," *Internet Society*, 1997, available at: https://www.internetsociety.org/internet/history-internet/brief-history-internet/.

Exhibit #	*Description*
1021	"Internet Protocol," *IETF RFC 791*, J. Postel, ed., September 1981, archived at Internet Archive Wayback Machine on February 4, 2007 at https://web.archive.org/web/20070204151303/https://tools.ietf.org/html/rfc791.
1022	"Transmission Control Protocol," *IETF RFC 793*. J. Postel, ed., September 1981, archived at Internet Archive Wayback Machine on February 2, 2007 at https://web.archive.org/web/20070202201546/https://tools.ietf.org/html/rfc793.
1023	E. H. Spafford, "The Internet Worm Program: An Analysis," *Purdue Technical Report CSD-TR-823*, 1988.
1024	Eichin, M.W. and Rochlis, J.A., "With Microscope and Tweezers: The Worm from MIT's Perspective," *Communications of the ACM*, Volume 32 Number 6, June 1989.
1025	T. Eisenberg *et al.*, "The Cornell Commission: On Morris and the Worm," *Communications of the ACM*, Volume 32 Number 6, June 1989.
1026	J. C. Mogul, "Simple and Flexible Datagram Access Controls for Unix-based Gateways," *Digital Western Research Laboratory Technical Report No. 89/4*, 1989.
1027	Heberlein, L. T.L, *et al.*, "A Network Security Monitor," *Proceedings, 1990 IEEE Computer Society Symposium on Security and Privacy*, 1990.
1028	"NetRanger Network Security Management System User Guide". v1.3.1 *Wheelgroup Corporation*, 1997.
1029	Roesch, M., "Snort: Lightweight Intrusion Detection for Networks," *Lisa* (Vol. 99, No. 1, pp. 229-238), 1999.
1030	Brandon De Hoyos, "IRC, ICQ, AIM and More: A History of Instant Messaging," *Lifewire*, Oct 2016, available from https://www.lifewire.com/im-a-brief-history-1949611.

Exhibit #	*Description*
1031	M. Chatel, "Classical vs. Transparent IP Proxies," *IETF RFC 1919*, March 1996, archived at Internet Archive Wayback Machine on June 30, 2007 at https://web.archive.org/web/20070630145311/https://tools.ietf.org/html/rfc1919.
1032	K. Ingham & S. Forrest, "A History and Survey of Network Firewalls," *University of New Mexico Computer Science Department Technical Report* archived at Internet Archive Wayback Machine on September 2, 2006 at https://web.archive.org/web/20060902171316/https://www.cs.unm.edu/~treport/tr/02-12/firewall.pdf.
1033	Sourcefire Support Website Webpage, archived at Internet Archive Wayback Machine on April 30, 2011 at https://web.archive.org/web/20110430194135/https:/support.sourcefire.com/ ("Sourcefire Support Webpage").
1034	Business Wire, "Sourcefire Expands IPS Solutions Portfolio, Adding FirePOWER to the Industry's Leading Protection," April 18, 2011, available at https://www.businesswire.com/news/home/20110418005189/en/Sourcefire-Expands-IPS-Solutions-Portfolio-Adding-FirePOWER.
1035	"File Transfer Protocol," *IETF RFC 765*, J. Postel, ed., June 1980, archived at Internet Archive Wayback Machine on February 6, 2007 at https://web.archive.org/web/20070206005843/https://tools.ietf.org/html/rfc765.
1036	T. B. Lee, "The Original HTTP as defined in 1991," World Wide Web Consortium, 1991, archived at Internet Archive Wayback Machine on June 5, 1997 at https://web.archive.org/web/19970605071155/https://www.w3.org/Protocols/HTTP/AsImplemented.html.
1037	I. Ristic, "SSL/TLS and PKI History," April 2018, available from https://www.feistyduck.com/ssl-tls-and-pki-history/.

Exhibit #	*Description*
1038	E. Rescorla, "HTTP over TLS", *IETF RFC 2818*, May 2000, archived at Internet Archive Wayback Machine on January 25, 2007 at https://web.archive.org/web/20070125003236/https://tools.ietf.org/html/rfc2818.
1039	J. Moser, "The First Few Milliseconds of an HTTPS Connection", *Moserware*, June 10, 2009, archived at Internet Archive Wayback Machine on June 13, 2009 at https://web.archive.org/web/20090613041022/http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html.
1040	M. Allman, et al., "FTP Security Considerations," *IETF RFC 2577*, May 1999, archived at Internet Archive Wayback Machine on March 18, 2007 at https://web.archive.org/web/20070318022322/https://tools.ietf.org/html/rfc2577.
1041	H. Schulzrinne, et al., "RTP: A Transport Protocol for Real-Time Applications," *IETF RFC 3550*, July 2003, archived at Internet Archive Wayback Machine on February 6, 2007 at https://web.archive.org/web/20070206011723/https://tools.ietf.org/html/rfc3550.
1042	Sourcefire, Inc., "Chat.rules" file, April 2005, downloaded from "Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release) . . . VRT Certified Rules for Snort v2.3," archived at Internet Archive Wayback Machine on January 12, 2006 at https://web.archive.org/web/20060112063540/http://www.snort.org:80/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.3.tar.gz.
1043	Sourcefire Research Team, "2450.txt" file, April 2005, downloaded from "Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release) . . . VRT Certified Rules for Snort v2.3," archived at Internet Archive Wayback Machine on January 12, 2006 at https://web.archive.org/web/20060112063540/http://www.snort.org:80/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.3.tar.gz.

Exhibit #	*Description*
1044	P. Saint Andre, Ed., "Extensible Messaging and Presence Protocol (XMPP): Core," *Network Working Group RFC 3920*, October 2004, archived at Internet Archive Wayback Machine on October 10, 2006 at https://web.archive.org/web/20061010092431/https://xmpp.org/rfcs/rfc3920.html.
1045	P. Saint Andre, Ed., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence," *Network Working Group RFC 3921*, October 2004, archived at Internet Archive Wayback Machine on October 10, 2006 at https://web.archive.org/web/20061010092547/http://xmpp.org:80/rfcs/rfc3921.html.
1046	R. Fielding, et. al., "Hypertext Transfer Protocol -- HTTP/1.1," *Network Working Group RFC 2616,* June 1999, archived at Internet Archive Wayback Machine on August 15, 2000 at https://web.archive.org/web/20000815082940/https://www.ietf.org/rfc/rfc2616.txt.
1047	"XMPPloit – A Tool to Attack XMPP Connections," August 27, 2012, archived at Internet Archive Wayback Machine on August 29, 2012 at https://web.archive.org/web/20120829042816/https:/www.darknet.org.uk/2012/08/xmpploit-a-tool-to-attack-xmpp-connections/.
1048	Sourcefire, Inc., "Multimedia.rules" file, April 2005, downloaded from "Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release) . . . VRT Certified Rules for Snort v2.3," archived at Internet Archive Wayback Machine on January 12, 2006 at https://web.archive.org/web/20060112063540/http://www.snort.org:80/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.3.tar.gz.
1049	Sourcefire Research Team, "1437.txt" file, April 2005, downloaded from "Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release) . . . VRT Certified Rules for Snort v2.3," archived at Internet Archive Wayback Machine on January 12, 2006 at https://web.archive.org/web/20060112063540/http://www.snort.org:80/pub-bin/downloads.cgi/Download/vrt_pr/snortrules-pr-2.3.tar.gz.

Exhibit #	*Description*
1050	H. Schulzrinne, et al., "RTP Profile for Audio and Video Conferences with Minimal Control," *IETF RFC 3551*, July 2003, archived at Internet Archive Wayback Machine on February 6, 2007 at https://web.archive.org/web/20070206011733/https://tools.ietf.org/html/rfc3551.
1051	J. Rosenberg, et al., "SIP: Session Initiation Protocol," *IETF RFC 3261*, June 2002, archived at Internet Archive Wayback Machine on April 28, 2006 at https://web.archive.org/web/20060428031957/https://tools.ietf.org/html/rfc3261.
1052	M. Handley, et al., "SDP: Session Description Protocol," *IETF RFC 4566*, July 2006, archived at Internet Archive Wayback Machine on January 28, 2007 at https://web.archive.org/web/20070128163222/http://tools.ietf.org:80/html/rfc4566.
1053	Petition for *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436, Paper 1 (July 20, 2018).
1054	Patent Owner's Preliminary Response to Petition for *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436, Paper 6 (October 26, 2018).
1055	Decision – Institution of *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436, Paper 7 (January 24, 2019).
1056	Patent Owner's Response in *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436, Paper 18 (July 30, 2019).
1057	Petitioner's Reply to Centripetal's Patent Owner Response in *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436, Paper 25 (October 16, 2019).
1058	Final Written Decision in *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436, Paper 40 (January 23, 2020).

Exhibit #	*Description*
1059	Petition for *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437, Paper 1 (July 20, 2018).
1060	Patent Owner's Preliminary Response to Petition for *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437, Paper 6 (October 26, 2018).
1061	Decision – Institution of *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437, Paper 7 (January 24, 2019).
1062	Patent Owner's Response in *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437, Paper 18 (July 30, 2019).
1063	Petitioner's Reply to Centripetal's Patent Owner Response in *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437, Paper 25 (October 16, 2019).
1064	Final Written Decision in *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437, Paper 40 (January 23, 2020).
1065	Petition for *Inter Partes* Review of U.S. Patent No. 9,686,193, IPR2018-01559, Paper 1 (August 21, 2018).
1066	Patent Owner's Preliminary Response to Petition for *Inter Partes* Review of U.S. Patent No. 9,686,193, IPR2018-01559, Paper 6 (January 4, 2019).
1067	Decision – Denying Institution of *Inter Partes* Review of U.S. Patent No. 9,686,193, IPR2018-01559, Paper 7 (April 2, 2019).
1068	Petitioner's Motion for Rehearing of Decision – Denying Institution of *Inter Partes* Review of U.S. Patent No. 9,686,193, IPR2018-01559, Paper 8 (May 2, 2019).
1069	Decision Denying Petitioner's Request for Rehearing of Decision – Denying Institution of *Inter Partes* Review of U.S. Patent No. 9,686,193, IPR2018-01559, Paper 9 (September 18, 2019).
1070	Amended Complaint for Patent Infringement, No. 2-18-cv-00094, Docket No. 29 (E.D. Va. March 29, 2018).

Exhibit #	*Description*
1071	Opinion & Order Memorializing and Explaining the Court's Claim Construction Ruling, No. 2-18-cv-00094, Docket No. 202 (E.D. Va. February 20, 2020).
1072	Declaration of Christopher Butler (May 8, 2019).
1073	Declaration of Dr. Stuart Staniford in Support of Petition for *Inter Partes* Review of U.S. Patent No. 9,124,552, IPR2018-01436 (July 20, 2018).
1074	Declaration of Dr. Stuart Staniford in Support of Petition for *Inter Partes* Review of U.S. Patent No. 9,160,713, IPR2018-01437 (July 20, 2018).
1075	Declaration of Jacob H. Baiugher III, IPR2018-01760 (December 4, 2019)
1076	Product Information Sheet for Sourcefire 3D IPS1000 (May 1, 2006)
1077	Sourcefire 3D advertisement, ITPRO

Location in the Declaration of Christopher Butler (EX-1072) at which the following Exhibits are Located.

Exhibit No.	Butler Dec. Page No.
1010	5-8
1011	941-945
1013	9-14
1014	946-956
1015	957-1034
1016	10-14
1017	15-17
1018	18-22
1022	23-73
1031	165-200
1032	1036-1077
1033	201-202
1035	203-273
1036	274-275
1038	276-283
1039	284-315
1040	316-324
1041	325-429
1044	430-502
1045	503-590
1046	1078-1234
1047	591-595
1050	596-640
1051	641-880
1052	881-930

CERTIFICATION OF SERVICE ON PATENT OWNER

Pursuant to 37 C.F.R. §§ 1.33(c) and 1.510(b)(5), the undersigned certifies that on the 19th of March, 2019, a complete and entire copy of this Request for *Ex Parte* Reeexamination of U.S. Patent No. 9,686,193 and all supporting exhibits were served via Federal Express, postage prepaid, to Centripetal Networks, Inc. by serving the correspondence address of record for the 193 Patent:

BANNER & WITCOFF, LTD.
USPTO Customer Number 22907
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON DC 20005-4051

and a courtesy copy, by email, upon counsel of record for the Patent Owner in the litigation before the United States District Court for the Eastern District of Virginia:

Paul J. Andre pandre@kramerlevin.com
Lisa Kobialka lkobialka@kramerlevin.com
James Hannah jhannah@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025

/Patrick D. McPherson/
Patrick D. McPherson, Reg. No. 46,255
505 9th Street, N.W., Suite 1000
Washington, D.C. 20004
P: (202) 776-5214
F: (202) 776-7801
PDMcPherson@duanemorris.com

ATTORNEY FOR REQUESTER

DM2\12423227.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of:		)
		)
Patent No.:	9,686,193	)
		)
Issued:	June 20, 2017	)
		)
For:	FILTERING NETWORK DATA TRANSFERS	)

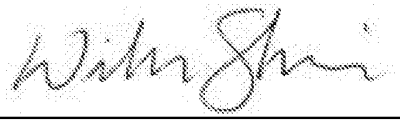
POWER OF ATTORNEY FOR *EX PARTE* PATENT REEXAMINATION

Cisco Systems, Inc. hereby appoints the following practitioners to transact all business in the United States Patent and Trademark Office associated with the above captioned ex parte reexamination request:

LEAD COUNSEL	BACK-UP COUNSEL
Patrick D. McPherson Reg. No. 46,255 PDMcPherson@duanemorris.com DUANE MORRIS LLP 505 9th St. NW, Suite 1000 Washington, D.C. 20004 P: (202) 776-5214 F: (202) 776-7801	Christopher Tyson Reg. No. 63,850 CJTyson@duanemorris.com DUANE MORRIS LLP 505 9th St. NW, Suite 1000 Washington, D.C. 20004 P: (202) 776-7851 F: (202) 776-7801
	Joseph A. Powers Reg. No. 47,006 JAPowers@duanemorris.com DUANE MORRIS LLP 30 South 17th Street Philadelphia PA 19103-4196 P: (215) 979-1842 F: (215) 689-3797
	Patrick Muldoon Reg. No. 47,343 PCMuldoon@duanemorris.com DUANE MORRIS LLP 505 9th St. NW, Suite 1000 Washington, D.C. 20004 P: (202) 776-7840 F: (202) 776-7801
	D. Joseph English Reg. No. 42,514 DJEnglish@duanemorris.com DUANE MORRIS LLP 505 9th St. NW, Suite 1000 Washington, D.C. 20004 P: (202) 776-5228 F: (202) 776-7801

The individual signing below has the authority to execute this document on behalf of Cisco Systems, Inc.

Name: William Silverio

Signature: 

Title: Senior Corporate Counsel

Telephone: (404) 317-9488

Date: March 16, 2020