

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KEYSIGHT TECHNOLOGIES, INC.

Petitioner,

v.

CENTRIPETAL NETWORKS, INC.

Patent Owner.

Inter Partes Review No.: Unassigned

Patent No. 9,917,856

DECLARATION OF DR. DOUG W. JACOBSON

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. QUALIFICATIONS AND EXPERIENCE.....	2
III. MATERIALS CONSIDERED AND RELIED UPON	5
IV. LEGAL STANDARDS FOR PATENTABILITY	6
A. Obviousness.....	6
B. Claim Construction	11
V. DESCRIPTION OF THE RELEVANT FIELD AND THE RELEVANT TIMEFRAME.....	13
VI. THE PERSON OF ORDINARY SKILL IN THE RELEVANT FIELD IN THE RELEVANT TIMEFRAME.....	13
VII. TECHNICAL BACKGROUND AND STATE OF THE ART.....	15
A. Computer Network Architectures and Communication Protocols	17
B. Network Security Systems – Firewalls	19
C. Network Security Systems – Intrusion Detection Systems and Intrusion Prevention Systems.....	24
D. Network Security Systems – Detailed Concepts.....	29
VIII. OVERVIEW OF THE '856 PATENT	44
A. Patent Overview	44
B. Prosecution History	48
IX. CLAIM INTERPRETATION	49
X. GROUND 1: CLAIMS 1, 24-25 ARE RENDERED OBVIOUS BY BURUGANAHALLI.....	50

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

A.	Overview of Buruganahalli	51
B.	Challenged Claims	62
C.	Claim Chart	91
XI.	GROUND 2: CLAIMS 1, 24-25 ARE RENDERED OBVIOUS BY BURUGANAHALLI IN VIEW OF BAEHR	91
XII.	SECONDARY CONSIDERATIONS	102
XIII.	CONCLUSION.....	103

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

I, Dr. Doug W. Jacobson, hereby declare under penalty of perjury:

I. INTRODUCTION

1. My name is Dr. Doug W. Jacobson, and I have been retained by counsel for Petitioner Keysight Technologies, Inc. (“Keysight” or “Petitioner”) as an expert witness to provide assistance regarding U.S. Patent No. 9,917,856 (Ex. 1001, “the ’856 Patent”). Specifically, I have been asked to consider the validity of claims 1 and 24-25 of the ’856 Patent (the “Challenged Claims”) in view of prior art, obviousness considerations, and understanding of a person of ordinary skill in the art at the time of the invention as it relates to the ’856 Patent. I have personal knowledge of the facts and opinions set forth in this declaration and believe them to be true. If called upon to do so, I would testify competently thereto.

2. For my time working on this matter, I am being compensated at my standard hourly consulting rate. I do not have any personal or financial stake or interest in the outcome of the present proceeding, and the compensation is not dependent on the outcome of this IPR and in no way affects the substance of my statements in this Declaration. I do not have any expectation or promise of additional business with the Petitioner in exchange for the positions explained herein. My analysis here is based on my years of education, research and experience, as well as my investigation and study of relevant materials, including those cited herein.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

3. I may rely upon these materials, my knowledge and experience, and/or additional materials to rebut arguments raised by the Patent Owner. Further, I may also consider additional documents and information in forming any necessary opinions, including documents that may not yet have been provided to me.

4. My analysis of the materials in this proceeding is ongoing and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date. I reserve the right to revise, supplement, and/or amend my expert opinions stated herein based on new information and on my continuing analysis of the materials already provided.

II. QUALIFICATIONS AND EXPERIENCE

5. My qualifications can be found in my Curriculum Vitae, which includes a complete list of my publications, and is attached as **Appendix A**. Some of my background and experience that qualifies me to offer the opinions offered in this Declaration set forth as an expert in the technical issues in this case are as follows.

6. I am a University Professor in the Department of Electrical and Computer Engineering at Iowa State University and currently hold the Stanley Chair for Interdisciplinary Engineering. I joined the faculty in 1985 after receiving a PhD degree in Computer Engineering from Iowa State University in 1985. Since 1995 I have taught courses in network security and information warfare.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

7. I created the first network security course and information warfare course at Iowa State University. Both courses have taught the concepts of intrusion detection since they were created. I have authored two text books in the area of computer and network security. Both of these courses taught the concepts of intrusion detection and I have been running various forms of intrusion detection systems in my teaching and research lab since 1995.

8. I am the founding director of the Iowa State University Center for Cybersecurity Innovation and Outreach (formally known as “Information Assurance Center”), which has been recognized by the National Security Agency as a charter Center of Academic Excellence for Information Assurance Education. I am also director of the Internet-Scale Event and Attack Generation Environment (ISEAGE) project. I also serve as the executive director of the Iowa Cyber Hub, which is dedicated to creating a statewide cybersecurity ecosystem.

9. My current funded research is targeted at developing robust countermeasures for network-based security exploits and large scale attack simulation environments. A few funded projects have led to patents. I have been PI or Co-PI on over 15 million dollars of security related funding.

10. I am also the founder of Palisade Systems, Inc., an Ames-based company marketing Internet management and security devices. The core technology

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

for Palisade Systems was based on a patent I was co-inventor on.

11. I have given over 150 presentations in the area of computer security and I have testified in front of the U.S. Senate committee of the Judiciary on security issues associated with peer-to-peer networking.

12. I have advised 24 Ph.D. students since 1985, and over 50% had security related topics. I have advised over 300 master's students since 1985 and a majority of the project since 1995 have been security related.

13. A description of my qualifications and background is set forth in my curriculum vitae, which is attached as **Appendix A**. A list of publications that I have authored or co-authored is provided in **Appendix A**.

14. I have been retained as an expert witness 4 times in the past 15 years. One engagement (Recording Industry Association of America [RIAA]) was for 5 years. I have been deposed 4 times as an expert witness and have testified in court 4 times in connection with prior expert witness engagements. A listing of each case for which I have testified is provided in **Appendix A**.

15. I have been retained as an expert witness or technical consultant for the following companies: State of Iowa department of Human Services, State of Iowa Department of Administrative Services, several cities in the state of Iowa, Iowa Department of Transportation, Attorney General for the State of Iowa.

16. I hold a Secret Clearance through the United States Department of Homeland Security (“DHS”) in order to be able to help the State of Iowa recover from a large scale cyber attack.

III. MATERIALS CONSIDERED AND RELIED UPON

17. I have reviewed the ’856 patent, its prosecution history, the prior art and other documents and materials cited herein. For ease of reference, the full list of documents that I have considered is included in **Appendix B**. Each of these materials is a type of document that experts in my field would have reasonably relied upon when forming their opinions and would have had access to either through the applicable patent office and/or well-known libraries, conferences, publications, organizations and websites in the field as further discussed herein.

18. My opinions in this declaration are based on my review of these documents, as well as upon my education, training, research, knowledge, and experience.

19. I have also reviewed the Declaration of Dr. Jon Weissman in Support of Petition for *Inter Partes* Review of U.S. Patent No. 9,917,856. Ex. 1047. I understand that declaration was submitted by Palo Alto Networks in support of its Petition for *inter partes* review of the ’856 patent (IPR2022-00182). I agree with his analysis and opinions, and adopt them in this declaration. Accordingly, this

declaration largely mirrors Dr. Weissman's declaration from that IPR.

IV. LEGAL STANDARDS FOR PATENTABILITY

20. I am not a lawyer and do not provide any legal opinions, but I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding meaning and validity of patent claims. I have applied the legal standards described below, which were provided to me by counsel for Petitioner.

21. I have been informed that prior art may render a patent claim unpatentable if the prior art can be shown to have made the claim "obvious" to a person of ordinary skill in the art.

A. Obviousness

22. I have been informed that a claim may be unpatentable under (AIA) 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been obvious to a hypothetical person of ordinary skill in the art in view of a prior art reference or in view of a combination of references at the time the claimed invention was made. I have been informed that obviousness is determined from the perspective of a hypothetical person of ordinary skill in the art and that the asserted claims of the patent should be read from the point of view of such a person at the time the claimed invention was made. I have been informed that a hypothetical person of ordinary skill in the art is assumed to know and to have all relevant prior

art in the field of endeavor covered by the patent in suit.

23. I have been informed that there are two criteria for determining whether prior art is analogous and thus can be considered prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the art is not within the field of the patentee's endeavor, whether the teachings of the art are still reasonably pertinent to the particular problem with which the patentee is involved. I have also been informed that the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. I have also been informed that a prior art reference is reasonably pertinent if, even though it may be in a different field from that of the patentee's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to a patentee's attention in considering his problem.

24. I have also been informed that an analysis of whether a claimed invention would have been obvious should be considered in light of the scope and content of the prior art, the differences (if any) between the prior art and the claimed invention, and the level of ordinary skill in the pertinent art involved. I have been informed as well that a prior art reference should be viewed as a whole.

25. I have also been informed that in considering whether an invention for

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

a claimed combination would have been obvious, I may assess whether there are apparent reasons to combine known elements in the prior art in the manner claimed in view of interrelated teachings of multiple prior art references, the effects of demands known to the design community or present in the market place, and/or the background knowledge possessed by a person having ordinary skill in the art. I have been informed that other principles may be relied on in evaluating whether a claimed invention would have been obvious, and that these principles include the following:

- A combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results;
- When a device or technology is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or in a different one, so that if a person of ordinary skill can implement a predictable variation, the variation is likely obvious;
- If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill;
- An explicit or implicit teaching, suggestion, or motivation to combine

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

two prior art references to form the claimed combination may demonstrate obviousness, but proof of obviousness does not depend on or require showing a teaching, suggestion, or motivation to combine;

- Market demand, rather than scientific literature, can drive design trends and may show obviousness;
- In determining whether the subject matter of a patent claim would have been obvious, neither the particular motivation nor the avowed purpose of the named inventor controls;
- One of the ways in which a patent's subject can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims;
- Any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed;
- "Common sense" teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle;

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

- A person of ordinary skill in the art is also a person of ordinary creativity, and is not an automaton;
- A patent claim can be proved obvious by showing that the claimed combination of elements was “obvious to try,” particularly when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions such that a person of ordinary skill in the art would have had good reason to pursue the known options within his or her technical grasp; and
- One should be cautious of using hindsight in evaluating whether a claimed invention would have been obvious.

26. I have further been informed that, in making a determination as to whether or not the claimed invention would have been obvious to a person of ordinary skill, the Board may consider certain objective factors if they are present, such as: commercial success of products practicing the claimed invention; long-felt but unsolved need; teaching away; unexpected results; copying; and praise by others in the field. These factors are generally referred to as “secondary considerations” or “objective indicia” of nonobviousness. I have been informed, however, that for such objective evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a “nexus”) between the claim and the evidence, and that

this nexus must be based on what is claimed and novel in the claim rather than something in the prior art. I have also been informed that even when they are present, secondary considerations may be unable to overcome primary evidence of obviousness (*e.g.*, motivation to combine with predictable results) that is sufficiently strong.

B. Claim Construction

27. I have been informed that for purposes of this *Inter Partes* Review, the standard for claim construction is the same as the standard used in federal district court litigation: claim terms should generally be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the invention and after reading the patent and its prosecution history.

28. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill in the art of the patent at the time of the alleged invention. I have been informed that patent claims generally should be interpreted consistent with their plain and ordinary meaning as understood by a person of ordinary skill in the art in the relevant time period (*i.e.*, at the time of the purported invention, or the so called “effective filing date” of the patent application), after reviewing the patent claim language, the specification and the prosecution history (*i.e.*, the intrinsic record).

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

29. I have further been informed that a person of ordinary skill in the art must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history, the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office, and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner's rejection, by clearly and unambiguously arguing to overcome or distinguish a prior art reference, or to clearly and unambiguously disavow claim coverage.

30. In interpreting the meaning of the claim language, I understand that a person of ordinary skill in the art may also consider "extrinsic" evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of those of skill in the art at the time of the alleged invention. This can be useful for technical terms whose meaning may differ from its ordinary English meaning. I understand that

extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence, particularly if the applicant has explicitly defined a term in the intrinsic record.

V. DESCRIPTION OF THE RELEVANT FIELD AND THE RELEVANT TIMEFRAME

31. I have reviewed the '856 patent and its prosecution history in detail.

32. I understand that the '856 patent issued from U.S. Patent Application 14/757,638, filed on December 23, 2015.

33. I have been instructed by counsel to assume the relevant timeframe for my analysis in this declaration to be on or before December 23, 2015.

34. Based on my review of this material, I believe that the relevant general field for the purposes of the '856 patent is network security systems, including firewalls and other packet-filtering devices for protecting computer networks from cyber-attacks.

VI. THE PERSON OF ORDINARY SKILL IN THE RELEVANT FIELD IN THE RELEVANT TIMEFRAME

35. My opinions are based on what a person of ordinary skill in the art in the technical field of the alleged invention would have understood at the time of the alleged invention of the challenged claims. As I explained above, the relevant

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

timeframe in this Declaration is on or before December 23, 2015. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art would have interpreted those references at the time of the alleged invention of the patent using the ordinary and customary meanings of the claim terms. I understand that the person of ordinary skill in the art is a hypothetical concept referring to one who thinks along the lines of conventional wisdom at the time.

36. I was asked to provide an opinion as to the level of a person of ordinary skill in the art pertinent to the subject matter set forth in the challenged claims of the '856 patent at the time of the priority date. I have been informed that the level of one of ordinary skill in the art is evidenced by prior art references. I agree with Dr. Weissman's opinion that a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer engineering or an equivalent, as well as four years of industry experience and would have had a working knowledge of communications network, firewalls, security policies, and packets filtering. Ex. 1047, ¶29. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

37. The basis for my familiarity with the level of ordinary skill is my own

technical experience and my interaction with students and professionals in the computing field who were at this level of skill. In reaching this opinion as to the hypothetical person of ordinary skill in the art, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field. As summarized above with regards to my qualifications and experience, I was at least the level of a person of ordinary skill in the art at the time of the '856 patent.

VII. TECHNICAL BACKGROUND AND STATE OF THE ART

38. The following analysis shows that the concept of network security systems and firewalls were well known in the art prior to December of 2015. The following sections describe the historical development of the art for network security systems, including firewalls and other packet filtering devices for protecting computer networks from cyber-attacks, and the user interface systems for controlling them, leading up to the state of the art as of December 2015. The prior art references, and the discussions of what was known to a person of ordinary skill in the art, provide the factual support for the general description of the state of the art at the time of the '856 Patent. This section provides additional rationale for obviousness over Buruganahalli (Ex. 1004), obviousness over and motivation to combine the

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

teachings of Buruganahalli in view of Baehr (Ex. 1005) with the knowledge, skill, and creativity of a person of ordinary skill in the art, provides support for why a person of ordinary skill in the art would have had a reasonable expectation of success in doing so, rebuts any assertion by the Patent Owner of unpredictability in the art, and rebuts any assertion by the Patent Owner of unexpected results.

39. This overview repeats an overview that was prepared by Dr. Weissman based in part on the “State of the Art” summary provided by Dr. Stuart Staniford in his declaration in support of the petition for IPR of U.S. Pat. No. 9,413,722 (the ’722 patent) (IPR2018-01760), filed by Cisco System, Inc. The ’722 patent is directed to similar basic concepts and technology as the ’856 patent. For that reason, the state of the art relevant to the ’722 patent is necessarily also relevant to the ’856 patent. Dr. Weissman explained that any similarity between Dr. Staniford’s “State of the Art” overview and his own that I adopt herein was intentional. I reviewed Dr. Staniford and Dr. Weissman’s opinions on the state of the art and the supporting documents cited therein, and I agree with those opinions as set forth herein.

40. As of December 2015, a person of ordinary skill in the art working in the field of network security systems, including firewalls and other packet filtering devices for protecting computer networks from cyber-attacks, would have been familiar with certain common concepts and related components including, but not

limited to: computer network architectures and communication protocols, firewalls, Intrusion Detection Systems and Intrusion Prevention Systems, the layering of computer network protocols, the use of network threat indicators to prevent cyber-attacks, and filtering unencrypted and encrypted packet data based on such indicators.

A. Computer Network Architectures and Communication Protocols

41. The Internet has its roots in conceptual papers on packet switching in the 1960s. These papers led to the funding by DARPA of an experimental internetwork – the ARPANET – with the first two nodes being connected in late 1969, and then growing steadily through the 1970s as a means of doing research on computer networking. Ex. 1020 (Doomjuice). The early ARPANET used a protocol, NCP, that is no longer in use and proved not to be scalable.

42. NCP's deficiencies led to the development of two new protocols – Internet Protocol (IP) to provide best effort delivery of data packets across heterogeneous networks (Ex. 1021 (Helix)), and Transmission Control Protocol (TCP) to provide reliable delivery of streams of data across an IP internetwork (Ex. 1023 (RFC 791)). These two protocols were described in the IETF Request for Comment (RFC) documents RFC 791 and 793 respectively in 1981. Ex. 1022 (RFC 793); Ex. 1021 (Helix). The ARPANET cut over to using the new TCP/IP protocol

suite on January 1, 1983. That date can be viewed as the birth date of the modern Internet. Ex. 1007 (Leiner).

43. Logically, the Internet is a web of intermediate network nodes and communication paths interconnecting those network nodes that provide multiple data transmission routes from any given point to any other given point on the network (i.e., between any two computers.) Ex. 1008 (Jungck '06), 3:59-4:11. The disparate networks are connected where they join by special devices – IP routers – that decide which way to send each packet. A router typically creates or maintains a table of the available routes and their conditions and uses this information to determine the best route for a given packet. Ex. 1008 (Jungck '06), 3:32-46, 38:29-39:8.

44. While TCP/IP provided the basic abstract facility to move data across a global network, higher-level application protocols were required to allow data communication to be managed conveniently. Application protocol data would be transmitted in the body of packets with IP and TCP headers. The header of the IP packet contains source and destination IP addresses. The TCP header contains port numbers that act like addresses and that may provide an indication of which underlying communication protocols are associated with a packet (e.g., HTTP, FTP). Combined, this 5-tuple packet information (i.e., the IP source address, IP destination

address, source port number, destination port number, along with an identifier of the transport protocol in use (e.g., TCP)), identify all the packets exchanged during a communication session between a source computer (e.g., a client) and a destination computer (e.g., a server). Particularly important applications included email (with protocols such as SMTP, POP and IMAP), with early email systems dating back to 1972. Ex. 1007 (Leiner). Other important protocols included FTP for making files available, first defined in 1980 (Ex. 1024 (RFC 765)), and the Hypertext Transfer Protocol (HTTP) for facilitating the exchange of hypertext markup language (HTML) and World Wide Web (WWW) content, first defined in 1991 (Ex. 1025 (T. B. Lee)).

B. Network Security Systems – Firewalls

45. Throughout the mid to late 1980s, the Internet grew very rapidly as more and more researchers and developers connected departmental mainframes, minicomputers, Unix workstations, and the like to it. The Internet reflected the openness and information sharing that characterizes the research community that developed it, with few security barriers beyond the requirement to login on remote systems (which often had weak or default passwords). Ex. 1007 (Leiner).

46. This era of complete openness spawned a variety of abuses by computer hackers. A particularly spectacular and famous incident spawned the modern

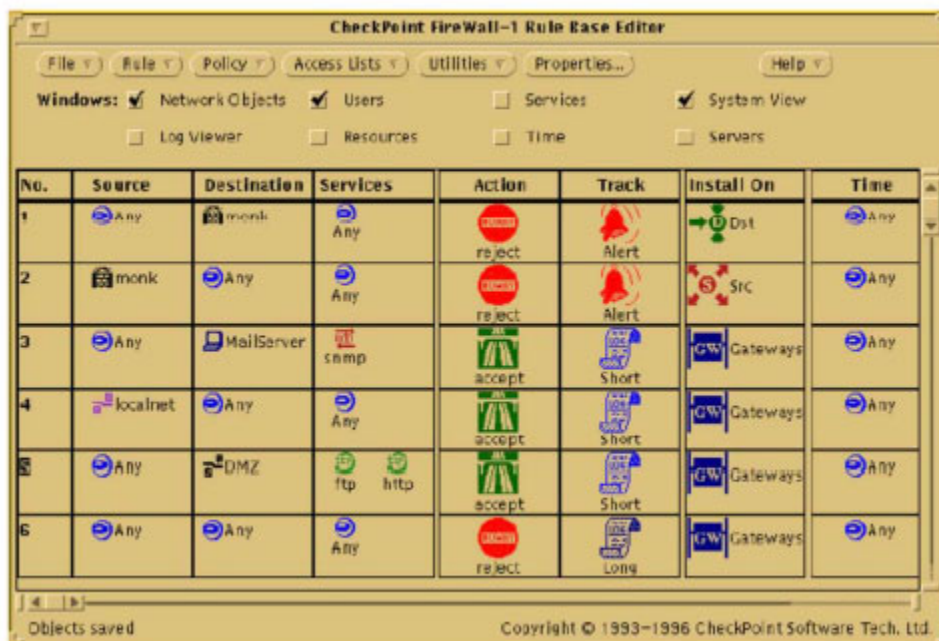
network security industry: the Internet worm of 1988. In this episode, a Cornell graduate student, Robert Morris Jr., released a worm – a self-replicating program capable of infecting other computers across the network via vulnerabilities in their operating system or applications. This worm infected about 6,000 computers across the Internet, including one of my computer systems at Iowa State University. Most of these computers were disabled, either by large numbers of copies of the worm clogging their memory, or at least by the need to disinfect and upgrade them. Many of the computers were important shared facilities with numerous users, so much of the work on the Internet was disrupted. The incident caused a great deal of analysis and soul-searching amongst the Internet community. Within a year (by 1989), both the first firewall and the first network intrusion detection system (NIDS) were under development. Ex. 1009 (Spafford), Ex. 1010 (Eichin), Ex. 1011 (Eisenberg).

47. The development of firewalls had its roots in the late 1980s practice of using filtering rules on Internet routers. This development began primarily as a way to prevent misconfigurations on one network that generated a lot of noise packets from affecting an adjacent network. However, it then resulted in the development of security applications, with routers providing simple facilities to block packets based on their source and destination networks and TCP ports. For example, with Cisco routers in 1989: “one could deny access to all but one host on a particular network.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

The Cisco gateways also allow discrimination based on IP protocol type, and TCP or UDP (User Datagram Protocol) port numbers.” Ex. 1012 (Mogul), 3. This example illustrates that the basic functionality of blocking or admitting packets based on a rule was available prior to 1989.

48. User interfaces for firewalls developed soon after the introduction of the firewalls themselves. A particularly influential company was CheckPoint, with their FireWall-1 product. A screenshot dated 1996 of this product is below:



49. This demonstrates a view of the firewall rules, with their five tuple information (source, destination, services, etc.), and the actions the rule will take (such as rejecting or accepting the connection attempt, and alerting the user or not). Ex. 1013 (FireWall-1).

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

50. Firewall system user interfaces also came to provide dashboards with overview information about the operation of the firewall such as graphs of summary statistics and tables of top things of importance. A typical example from a SonicWALL firewall in 2009 is shown below:



51. Here is shown graphs with the number of attacks detected per hour in the recent time period, as well as the top source IPs using bandwidth over HTTP connections. Also, there is a table with current bandwidth usage across the firewall. Ex. 1014 (SonicWALL GMS), 2.

52. This system also provided functionality similar to packet logs. For example, the screenshot below shows the display of a listing of connections blocked, which a person of ordinary skill in the art would understand is stored within the system's persistent memory:

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

Log Search Results for May 1, 2007 00:00:00 to May 1, 2007 23:59:59 as of 05/01/2007 19:11:47 UTC
Message Category: Connections

Displaying records 1-500 of 25715 (Next 500) (1 2 3 4 5 6 7 8 9 10)

Time	Source/Port	Destination	Protocol	Src.Port	Dest.Port	Src.Interface	Dest.Interface	Tx.Bytes
05/01/2007 12:11:47	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:47	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:47	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:48	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:48	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:44	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:43	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:25	10.0.202.131	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:24	10.0.202.131	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:24	10.0.202.131	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:15	10.0.202.131	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:14	10.0.202.131	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:14	10.0.202.131	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:12	10.0.202.179	255.255.255.255	udp	60	0	VLAN	LAN	0
05/01/2007 12:11:09	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:09	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:09	0.0.0.0	255.255.255.255	udp	60	0	VLAN	LAN	0
05/01/2007 12:11:09	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:08	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0
05/01/2007 12:11:08	0.0.0.0	255.255.255.255	udp	60	0	VLAN	LAN	0
05/01/2007 12:11:08	10.0.56.39	224.0.0.22	igmp	34	0	VLAN	N/A	0

53. The same system was capable of providing functionality akin to packet logs or flow logs. Ex. 1015 (SonicWALL ViewPoint), 292. For example, the screenshot below (Ex. 1015 (SonicWALL ViewPoint), 253) shows a table of types of attacks the firewall is capable of detection and the counts of them occurring over a time period.



**C. Network Security Systems – Intrusion Detection Systems and
Intrusion Prevention Systems**

54. In an independent line of development from firewalls, the Internet worm and other less serious incidents of the time inspired researchers to begin exploring systems specifically designed to look for intrusions on networks by examining the data packets crossing the network. Initially, network intrusion detection was done by placing network interfaces on broadcast networks into “promiscuous” mode to inspect all the traffic, which could then be copied into a user-mode application where it could be inspected and reasoned about. The earliest such system was the Network Security Monitor (NSM) developed at University of California, Davis in 1991. Ex. 1016 (Heberlein). This evolved into the U.S. Air Force’s Automated Security Incident Measurement (ASIM) system, and a large part of the development team on that effort split off and formed a company, WheelGroup, which launched the first commercial network intrusion detection system (IDS) NetRanger in 1996.

55. NetRanger had a general facility to write rules that matched arbitrary strings in the application data inside packets, in addition to matching on IP and TCP packet header values. For example, a 1997 user guide for the NetRanger system illustrated how to log every HTTP GET request passing by in packets on the monitored network:

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

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. 1017 (NetRanger), 189.

56. NetRanger also had a GUI For example, the same user guide from 1997 provides a Figure 4.10 (Ex. 1017 (NetRanger), 127) which shows a view of an individual ‘packet log’ type display with the source and destination addresses, port numbers and so forth, and the ‘Threat-ID’ (here ‘Alarm Name’ Sweep-Echo):

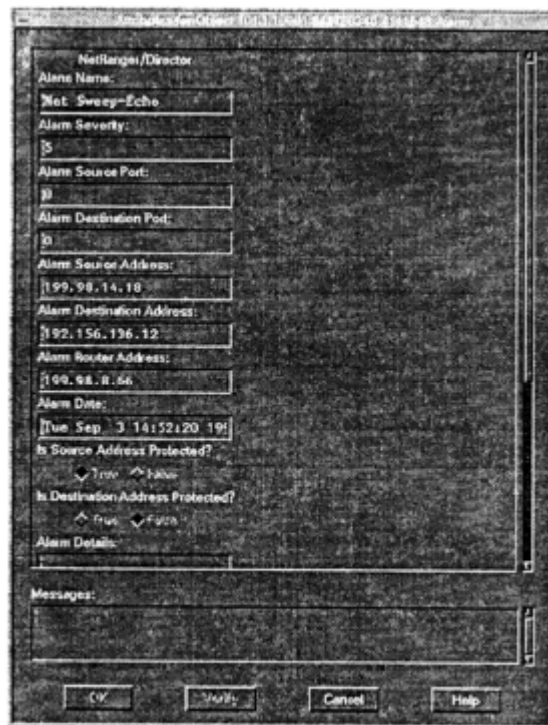


Figure 4.10: Alarm Event Attributes

57. Additionally, NetRanger had user-interface functionality for a user to block at least some traffic based on detection of a rule firing. For example, the

following (Ex. 1017 (NetRanger), 135):

Shunning IP Addresses and Class C IP Networks

The **Security→Shun** functions can be used to manually shun (block) incoming IP traffic. To shun traffic that emanates from an Alarm's Source IP Address, select the Alarm (or Alarm Set), and choose **Security→Shun→Source IP**. To shun traffic that emanates from any IP address within the Class C Network that contains an Alarm's Source IP Address, select the Alarm (or Alarm Set), and select **Security→Shun→Source Net**.

In either case, an xnmappmon window will display the output of the nrexec command that was used to shun the traffic.

This user action would reconfigure a packet filtering router to block all packets from the source IP address used in a detected attack. Ex. 1017 (NetRanger), 135.

58. The first widely adopted open source network intrusion detection system (NIDS or just IDS), Snort, was first released in 1998, and was documented in a conference paper in 1999. Ex. 1018 (Roesch). Like other NIDS before it, Snort allowed the user to write rules for detecting particular network packets based on both the 5-tuple information in the packet IP and TCP headers, as well as strings found in packet application data. For example:

```
alert tcp any any -> 10.1.1.0/24 80 (content: "/cgi-bin/phf"; msg: "PHF
probe!");
```

This rule (see Ex. 1018 (Roesch), 232, Fig. 5) shows that alerting was to be done based on TCP protocol packets from any source IP address and port, and destination IP addresses in the range 10.1.1.0/24, and with destination port 80 (characteristic of HTTP traffic). This particular content keyword (/cgi-bin/phf) matches a uniform resource locator (URL) used in a popular attack of the time, but content keywords

in general could be used to find and match any text in application data in packets transiting the network.

59. The earliest NIDS were strictly involved in detecting attacks; these systems worked off a copy of the packets and could only alert or log suspected intrusions, not directly block them. However, it was quickly realized that customers had a need to take automated action in some cases. While the first instance of this involved communication to firewalls or filtering routers, the need to block attacks quickly, as well as the need to resolve various complex ambiguities in the meaning of packet traffic that computer intruders used to get around the first NIDS, meant that the industry quickly developed systems that were “inline” in the traffic flow, and which could choose to drop or pass any given packet. These systems were known as intrusion prevention systems (IPS), with multiple companies launching such products in 2002, including Intruvert (later acquired by McAfee), Tipping Point (3Com then HP), and OneSecure (later acquired by NetScreen then Juniper).

60. These inline intrusion prevention systems were capable of applying intrusion detection rules that looked both at 5-tuple header data and application data (e.g. content) in every packet and making pass/alert/block decisions on each such packet. For example, the Zuk patent (Ex. 1019), filed in 2002, describes an IPS architecture in which packets were inspected, and the 5-tuple in the packet header

was used to lookup the correct rules in a flow table (hash table of all TCP connections or UDP pseudo-connections currently being tracked by the system). The rules described in Zuk then allowed regular expression matching of any packet content in the application layer, and packet application data content matches would result in triggering the rule and dropping the packet. Ex. 1019 (Zuk), 18:4-32, Fig. 11. Zuk described in outline terms the use of user-interface functionality for controlling the IPS:

61. “The information provided by MMIDP sensors 45a-c and MMIDP server 100 is organized in reports that provide access to a list of all the detected attacks and intrusions as well as network statistics that otherwise would be difficult to gather, such as the top IP addresses used in attacks, the top attacks, the number of alarms and incidents generated, and whether an alarm is real or false, among other statistics. In addition, network security administrators may specify which signatures from the set of signatures stored in MMIDP database 105 will be used to detect and prevent attacks, as well as create new signatures.” Ex. 1019 (Zuk), 14:14-25.

62. Similarly, the Jungck patent from 2006 is directed to a “packet interceptor/processor apparatus” that “applies one or more rules to ... intercepted packets which execute one or more functions on a dynamically specified portion of the packet and take one or more actions with the packets.” Ex. 1008 (Jungck '06),

Abstract. Actions taken on packets include “releasing the packet unmodified, deleting the packet, modifying the packet, logging/storing information about the packet or forwarding the packet to an external device for subsequent processing.”

Ex. 1008 (Jungck '06), Abstract. Further, “the rules may be dynamically modified by the external devices.” *Id.*

D. Network Security Systems – Detailed Concepts

63. As discussed further below, each element of the Challenged Claims was well-known to a person of ordinary skill in the art, and disclosed and rendered obvious by the prior art, well before the earliest possible priority date of the '856 patent—December 23, 2015. Moreover, each combination recited by the Challenged Claims would have been, at least, obvious and was at most an obvious implementation choice.

64. The Challenged Claims are directed to well-known concepts of rule-based network-threat detection whereby a packet filtering system, such as a firewall, identifies packets, correlates unencrypted packets with encrypted packets, determines whether they are associated with a network threat indicator, filters them using rules based on predetermined criteria, and routes potentially threatening packets to a proxy system. The Challenged Claims further recite generic and well-known functionalities and components for performing these well-known concepts,

including a “processor,” a “memory,” “computer-readable media,” “instructions,” “packet-filtering rules,” “network-threat indicators,” “unencrypted data,” “encrypted data,” and “a proxy system.” ’856 patent, claims 1, 24-25.

65. Each of these concepts was well-known in the art and disclosed in the prior art.

1. Applying Rules to Filter Packets in a Packet Filtering System

66. It was well-known and conventional in the art before the claimed priority date of the ’856 patent for a network security system to include a rule-based packet filtering system, e.g., a firewall or a screen, to protect a network from outside communications. A packet-filtering system, as its name indicates, filters packets to and from a system or network. It does so by applying one or more rules that specify certain criteria, e.g., based on source, destination, protocol version, etc., to identify packets that may present potential security risks to the network.

67. For example, U.S. Patent Appl. Pub. No. 2014/0283004 (Moore) (Ex. 1040) discloses a “packet security gateway” configured to receive packets and apply one or more filters to the packets. Moore, [0019]. The gateway is also configured to receive a security policy, which may include one or more rules, from a security policy management server. Moore, [0019], [0021]. The rules are then applied to filter packets. *Id.*

2. Identifying Security Risks Based on Network-Threat Indicators

68. It was further well-known and conventional in the art before the claimed priority date of the '856 patent for a network security system to identify security risks based on network-threat indicators, e.g., domain name. It was a common technique for a packet-filtering system to use indicators to identify potential network threats that may indicate security risks to a network. These indicators were known to be based on data collected through threat monitoring and to include source and destination information, such as a domain name.

69. For example, U.S. Pat. App. Pub. No. 2015/0207809 (Macaulay) (Ex. 1041) discloses that for “threat monitoring,” the operator of “a given customer network” subscribes to a service that provides “cyber threat intelligence data.” Macaulay, [0025]. Figure 4 shows the process of collecting, creating, and providing cyber threat intelligence data to a customer network where the customer network “receives customized threat report and takes actions” in step 460. Macaulay, [0099].

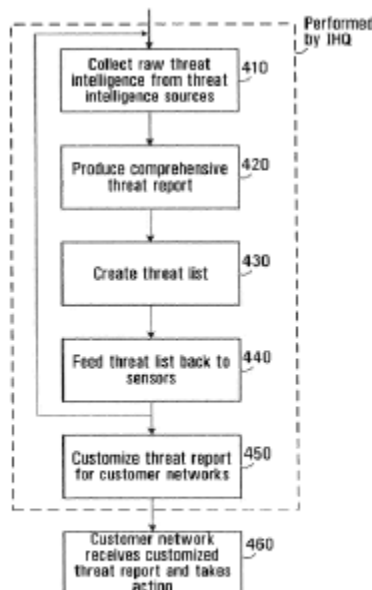


FIG. 4

The “cyber threat intelligence data” include “traffic attributes that are indicative of a threat.” Macaulay, [0024]. For example, the data may “indicate, from the perspective of a given customer network [] threats that arise from an external entity and also threats against internal assets...” Macaulay, [0024]. The threat-indicators include “domain names (both as source and as destination),” “autonomous system numbers (ASNs, both as source and as destination),” “URL strings,” and “protocol.” Macaulay, [0024], [0030], [0037] (“network communication... protocols... are then closely observed for relatively simple criteria, such as... protocols...”), [0045] (“basic tools for... understanding the threats... include... IP protocol...”), [0047]-[0048], [0056], [0060]-[0062], [0066], [0072]-[0073], [0075] (“it has been observed that P2P protocols are frequently used... by malware and botnets”), [0086], [0091],

[0101], [0052] (“domain name identified as a potential threat (i.e., on a threat list []”). They can be “cross-referenced with a list of ... domains and ASNs with which malware is known to communicate.” Macaulay, [0036]. Macaulay discloses that the customer network, after receiving the data comprising the threat-indicators from the subscription service, “may then apply the ... data directly to traffic entering or existing... the customer network.” Macaulay, [0025]. For example, the threat-indicators may be “incorporated into a filter” such that the data communications are monitored. Macaulay, [0047], [0052], [0056], [0061].

70. As another example, Moore discloses a filter that compares “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.” Moore, [0005]. Moore further discloses that “[e]ach 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...specify[] 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.” Moore, [0025].

3. Correlating Packets of a Session

71. It was well-known and conventional for a firewall to determine whether packets, unencrypted or encrypted, belong to a given communications session using IP addresses and/or port numbers. As I discussed above, a network may use a transport-layer protocol called Transmission Control Protocol (“TCP”). TCP provides a data delivery service that monitors transmissions using control information in a header that is encapsulated within an IP packet. The header of the IP packet contains source and destination IP addresses. The TCP header contains port numbers that act like addresses and that may provide an indication of which underlying communication protocols are associated with a packet (e.g., HTTP, FTP). Combined, the IP source address, IP destination address, source port number, destination port number, along with an identifier of the transport protocol in use (e.g., TCP), uniquely identify all the packets exchanged during a communication session between a source computer (e.g., a client) and a destination computer (e.g., a server). Kim (Ex. 1045), 660 (“Each session can be identified by 5-tuple packet information which is source IP address, destination IP address, protocol, source port and destination port.”); Zuk, 15:32-53, 16:13-26, Fig. 8; Boivie (Ex. 1044), 4:42-50; Moore, Fig. 3, [0025]. This 5-tuple, called a flow id, has been used to identify packets within a single end-to-end (original sender to ultimate destination)

communication session since the creation of the Internet. Zuk, 15:33-53, 16:13-26, Fig. 8; Boivie, 5:11-18; Moore, [0039]. Secure protocols such as SSL and TLS run on top of the IP and TCP layers, and are used to encrypt application layer data. Wang (Ex. 1034), 3:47-50. The IP addresses, port numbers, and other TCP session data associated with a packet are typically unencrypted and may be inspected without decrypting the packet. Moore, [0036].

4. Inspecting Handshake Messages Prior To Establishing Encrypted Sessions.

72. It was further well-known and conventional in the art before the claimed priority date of the '856 patent for a network security system to inspect unencrypted handshake messages prior to establishing encrypted sessions. It was a common technique to evaluate the security risk of establishing an encrypted session by inspecting the session's handshake message to determine whether it comprises any data that may correspond to a network threat indicator.

73. For example, U.S. Patent Appl. Pub. No. 2014/0089661 (Mahadik) (Ex. 1042) discloses a method for selectively filtering internet traffic. Mahadik, Abstract. Mahadik recognizes that “[f]or SSL/HTTPS based website access, the network traffic is encrypted and thus cannot be monitored with the same tools used in unencrypted scenario.” Mahadik, [0029]. Mahadik proposes a method to detect the encrypted traffic by examining its handshake. *Id.* Specifically, Mahadik discloses,

“[t]his preferably occurs when a site is being accessed over HTTPS using a SSL certificate of a server during a handshake. A domain is preferably detected during the handshake through a server name attribute or through some alternative parameter. The web proxy server may subsequently determine if the domain is restricted, permitted, or partially restricted. If the domain is restricted, the access may be blocked entirely. If the domain is permitted, the web proxy preferably hands client requests to the server and the server responses back to the client without making any modification to the tunneled SSL traffic.” *Id.*

74. Moore discloses that an enterprise may “enforce one or more network security policies...to restrict network communications between networks 104 and 106 (e.g., ... encrypted web sessions, and the like).” Moore, [0031]. Further, rules are applied to determine whether a session can be conducted: “rule 1 302 may allow... hosts attached to network 104 to conduct Secure Shell (SSH) sessions...; rule 2 304 may allow any e-mail servers...to conduct SMTP sessions (e.g., e-mail transfer sessions) with any e-mail servers...; 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)...; and rule 5 310 may allow web browsers attached to network 104 to conduct HTTPS sessions (e.g., secure web sessions)...but may...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).” Moore, [0031].

5. Routing Packets Between Functions of A Security Device

75. It was further well-known and conventional in the art before the claimed priority date of the '856 patent for a network security system to route packets between interfaces of functional components of a security device such as a firewall. This technique was widely implemented using a software routing function.

76. For example, J. Wack et al., *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology (“NIST”) (Ex. 1036) describes the characteristics of an application-proxy gateway firewall. NIST discloses, “[a]pplication-proxy gateway firewalls do not require a Layer 3 (Network Layer) route between inside and outside interfaces of the firewall; the firewall software performs the routing. In the event the application-proxy gateway software ceases to function, the firewall system is unable to pass network packets through the firewall system. All network packets that traverse the firewall must do so under software (application-proxy) control.” NIST, 12. The application-proxy gateway

firewalls use a software application running on a firewall that is “capable of filtering a protocol and routing it [*sic*] between the interfaces of the device.” NIST 52. NIST further discloses using a firewall rule set, which is a table of instruction, “for determining how packets should be routed between its interfaces.” NIST 51.

6. Sending Suspicious Packets to a Proxy System

77. It was further well-known and conventional in the art before the claimed priority date of the '856 patent for a network security system to send packets that may present a risk to a proxy system for further processing. This technique was widely implemented to isolate a network from direct access or attacks from an outsider and uses a proxy system in its place to handle packets that may present a network threat. Proxies also provide more efficient use and handling of limited network resources. Ebrahimi (Ex. 1035), 1:25-28

78. There are two types of proxies that are generally known to handle network traffic between a client and a server: a forward proxy and a transparent proxy. Ebrahimi, 1:37-1:45. For example U.S. Patent No. 7,793,342 (“Ebrahimi”) describes the characteristics of a forward proxy and a transparent proxy:

A forward proxy is known to and configured by each of the clients, before the clients can take advantage of the forward proxies capabilities. In contrast, a transparent proxy is neither known to nor configured by the clients; rather, the

transparent proxy intercepts outgoing client requests to access origin servers/sites and transparently processes the requests on behalf of the clients. Therefore, transparent proxies can be more secure than forward proxies, since the clients do not know about the transparent proxies. Furthermore, transparent proxies can be more easily integrated into a network than forward proxies, since no client configuration is required.

Ebrahimi, 1:45-1:56.

79. A transparent proxy system, as its name suggests, is “transparent” to two endpoints (*e.g.*, a client and a server) in a communication. U.S. Patent No. 8,504,822 (“Wang”) discloses a transparent proxy between a server and clients in a computer network, as shown in Figure 1. Wang, 2:32-58.

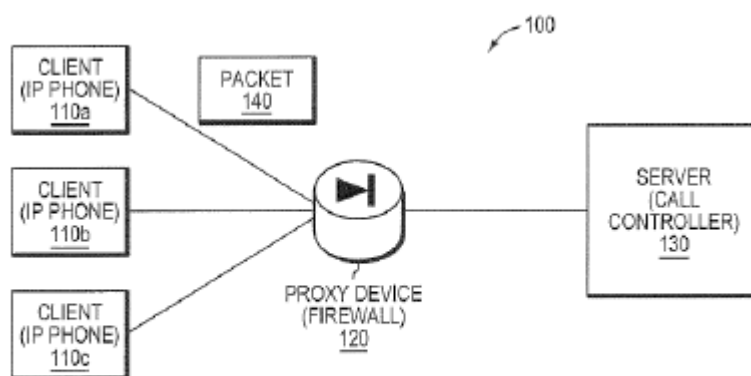


FIG. 1

Wang explains:

because the proxy device 120 is a transparent intermediary to the client-server

security session, the proxy device is able to decrypt the received traffic/packets (*e.g.*, using the session key negotiated for the client-proxy or proxy-server session, as appropriate) from each sending end device, and may re-encrypt the traffic prior to forwarding it on using the respective session key with the receiving end device.

Wang, 8:12-19. Wang explains that “neither the client nor the server is required to be provisioned to specifically communicate with the proxy device, and instead may simply attempt to directly connect to the peer (server or client, respectively) over an apparent client-server security session.” Wang, 7:53-57. Furthermore, “[w]ith the established client-proxy and proxy server security sessions acting transparently as a client-server security session, the proxy device may be allowed to inspect the traffic between the client and the server [], such as by decrypting and re-encrypting the traffic accordingly.” Wang, 8:67-9:4.

80. A proxy system may be implemented internally to, or implemented externally from, a packet filtering device such as a firewall or a screening system. For example, NIST discloses that a proxy is “a software application running on a firewall or on a dedicated proxy server...” NIST 52. “Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic but they do not contain firewall capability” and they are “typically deployed behind

traditional firewall platforms for this reason.” NIST, 14. Furthermore, a main firewall “might accept inbound traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server.” NIST, 14. NIST further discloses that “[d]edicated proxy servers perform “filtering or logging operations on the traffic and then forward it to internal systems.” NIST, 14. They are typically used to “decrease the work load on the firewall and to perform more specialized filtering and logging that otherwise might be difficult to perform on the firewall itself.” NIST 14.

81. As discussed, diverting traffic to a proxy is beneficial to protect against potential attacks. For example, U.S. Patent Application Publication No. 2007/0271605 (Le Penne) (Ex. 1033) discloses routing packets to a proxy for security reasons. It illustrates the functional blocks of a firewall device in Figure 3:

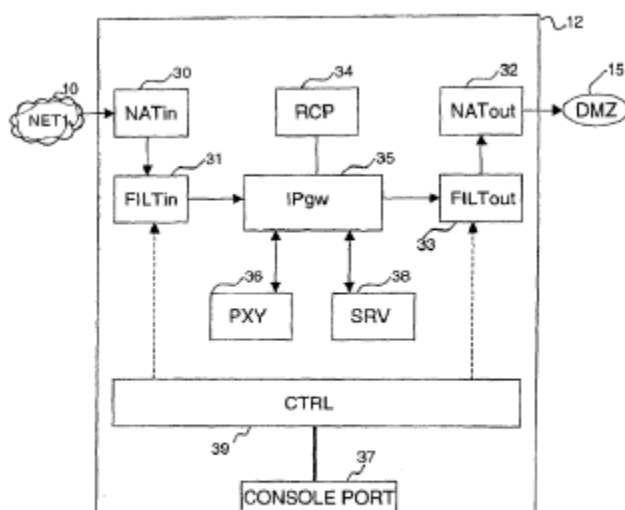
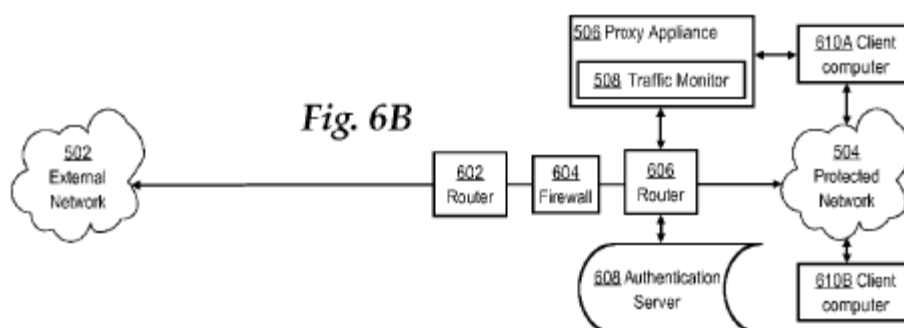


FIG. 3

The firewall filters incoming packets using “FILTin 31” and then forwards the packets to “IPgw 35” that is a forward engine. The forward engine uses a “routing control point RCP” that makes routing decisions based on certain rules. Based on these rules, the packets may be sent to “an integrated function, such as an application PXY 36” or a server SRV 38 for further processing. Le Pennec, [0022]; *see also id.*, [0006]-[0008], [0023]-[0044].

82. As another example, U.S. Patent No. 7,849,502 (Bloch) (Ex. 1043) discloses that a proxy “provides protection against spyware and web-based malware, including managing network traffic into and out of an internal network to block or redirect the traffic to avoid malware, such as spyware...” Bloch, 3:35-41. Bloch illustrates an example of using a proxy appliance to protect a network. Figure 6B illustrates that traffic that has been filtered by a firewall is routed to a proxy appliance for further processing. Bloch, 6:52-67.



“Referring to FIG. 6B, external network 502 is coupled to proxy appliance 506 through an edge router 602 and firewall 604 that protect the protected network 504.

A second router 606, which may be located anywhere within network 504, is coupled to the proxy appliance 506 and authentication server 608. The second router 606 may comprise a WCCP router or a Layer 4 switch. Client computers 610A, 610B may be coupled to protected network 504 and one or more of the client computers may connect to the proxy appliance 506 in forward mode.” Bloch, 8:29-39.

83. As yet another example, as disclosed above, Mahadik discloses “[r]edirecting the client to a web proxy server based on the user identification requirements.” Mahadik, Fig. 8.

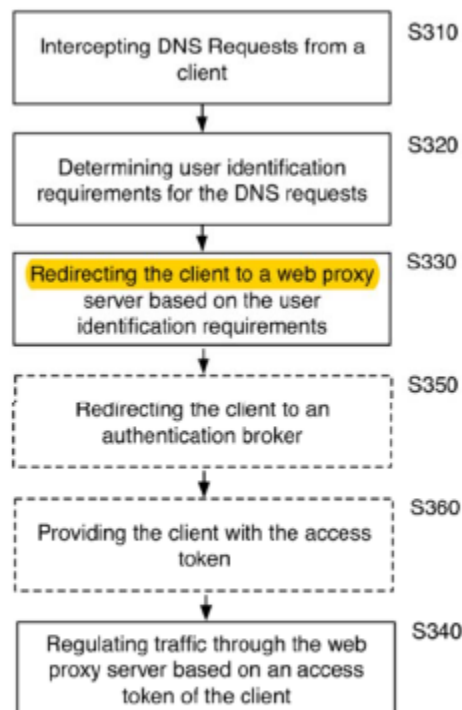


FIGURE 8

Mahadik discloses that the proxy “functions to provide a form of traffic monitoring for resources not fully trusted.” Mahadik, [0017]. It is further configured to process

the traffic such that suitable actions would be taken. *Id.*

VIII. OVERVIEW OF THE '856 PATENT

A. Patent Overview

84. The title of the '856 patent is “Rule-Based Network-Threat Detection for Encrypted Communications.” '856, *Title*. It is directed to a “packet-filtering system configured to filter packets in accordance with packet-filtering rules may receive data indicating network-threat indicators and may configure the packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. A portion of the unencrypted data may correspond to one or more of the network-threat indicators, and the packet-filtering rules may be configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.” '856, *Abstract*, 1:32-45. Figure 7 illustrates this method for rule-based network threat detection:

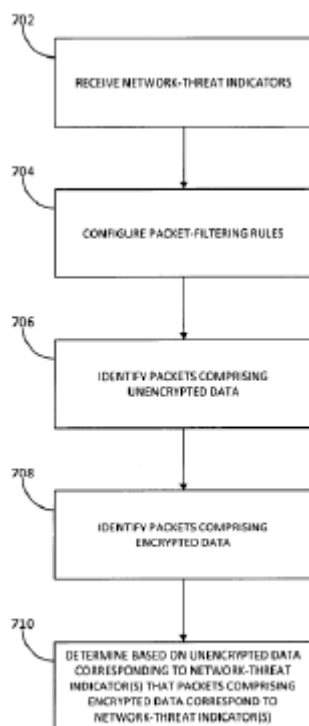


FIG. 7

'856, 23:63-65. Referring to step 702 of Fig. 7, the packet-filtering system “may receive data indicating network-threat indicators,” such as “network addresses, domain names, uniform resource identifiers (URIs), and the like.” '856, 1:11-15. 3:67-4:3. This data received by the system are rules from “rule providers 138 based on network-threat indicators provided by threat-intelligence providers 140.” '856, 23:66-24:4, 4:3-7. In step 704, the packet-filtering system configures rules to identify packets corresponding to the network-threat indicators. '856, 24:4-7, 4:3-7, 4:18-21.

85. Again referring to Figure 7, “[i]n step 706, the packet-filtering system may identify packets comprising unencrypted data. For example, packet-filtering

system 200 may identify packets comprising a DNS query, a reply to a DNS query, or a handshake message configured to establish an encrypted communication session.” ’856, 24:8-12, 9:19-28. Further, “[i]n step 708, the packet-filtering system may identify packets comprising encrypted data. For example, packet-filtering system 200 may identify packets encrypted in accordance with one or more parameters of sessions...” ’856, 24:14-17, 6:42-45. “In step 710, the packet-filtering system may determine based on a portion of the unencrypted data corresponding to the network-threat indicators that the packets comprising encrypted data correspond to the network-threat indicators. For example, packet-filtering system 200 may determine that a domain name included in the DNS query, the reply to the DNS query, or the handshake message corresponds to the network-threat indicators, and packet-filtering system 200 may determine that one or more of the packets encrypted in accordance with the parameters of sessions 306, 308, 408, 410, 504, or 606 correlate to one or more packets comprising the DNS query, the reply to the DNS query, or the one or more handshake messages.” ’856, 24:18-30, 9:29-33. The filtered packets are routed to a proxy system based on a determination that the packets comprise data corresponding to one or more of the network-threat indicators. ’856, 6:45-59. The proxy system may decrypt encrypted data, which then may be filtered using the unencrypted data in the packets, e.g., URI, data indicating a

protocol version, request, or command, before the packets are re-encrypted. '856,
10:56-11:40.

86. Representative Claim 1 of the '856 patent recites:

A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on

a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

B. Prosecution History

87. The '856 patent was matured from a U.S. Patent Application No. 14/757,638, which was filed on December 23, 2015.

88. During prosecution and on April 12, 2017, Examiner issued a non-final rejection on the pending claims under §101 and §112, and further under §103 as obvious in view of Spies (U.S. Patent Publication 2005/0138353), Sorensen (U.S. Patent Publication 2012/0023576), and in further view of Bomer (U.S. Patent Publication 2004/0199629). EX1002, 1064-1083. In response and on October 11, 2017, Applicant amended the claims and argued that Spies does not teach the determining step of claim 1. EX1002, 1365. Applicant argued that Spies teaches filtering unencrypted data and processing decrypted data, and does not teach “any determination regarding any encrypted data based on any unencrypted data corresponding to one or more network-threat indicators.” *Id.* In addition, Applicant argued that Spies fails to teach network-threat indicators comprise a domain name as recited in the claims because, according to Applicant, Spies teaches a domain name but that domain name is not identified as a network threat. *Id.* Lastly, Applicant argued that neither Sorenson nor Bomer remedy the defects of Spies. EX1002, 1351-

1367.

89. Examiner allowed the claims in a Notice of Allowance issued on December 20, 2017, indicating that the amended claims were sufficient to overcome the prior art of record. EX1002, 1374-1390. On January 23, 2018, Applicant requested additional amendments to the claims prior to issuance. EX1002, 1413-1422. Further on February 5, 2018, the amendment was entered. EX1002, 145-1450. The '856 issued on 03/13/2018. EX1002, 1453.

IX. CLAIM INTERPRETATION

90. I have been informed that only terms necessary to resolve the controversy need to be construed. For the purposes of the present declaration, I have applied the legal principles outlined above in Section IV.B and propose construction for one claim term, as indicated below.

91. I understand that the following term is being construed in this proceeding:

a. “network-threat indicators”

92. Independent claims 1, 24 and 25 of the '856 patent recite “receiv[e]/ing. . .] data indicating a plurality of network-threat indicators.” '856, cls. 1, 24-25. I understand the term “network-threat indicator” has been interpreted to mean “indicators that represent the identity of a resource associated with a network threat.”

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

I have reviewed the patent specification and prosecution history. I agree with this interpretation.

93. The '856 patent specification provides that “[n]etwork-threat services provide information associated with network threats, for example, reports that include listings of network-threat indicators (e.g., network addresses, domain names, uniform resource identifiers (URIs), and the like).” ’856, 1:11-15. Each of those example indicators in parentheses represents the identity of a resource. Similarly, the '856 patent specification provides that “[t]he threat-intelligence reports may include one or more network-threat indicators, for example, domain names (e.g., fully qualified domain names (FQDNs)), URIs, network addresses, or the like.” ’856, 3:65-4:4.

94. I understand that this construction was adopted for this same term in IPRs filed against other of patent owner’s patents in which this same claim term appears.

**X. GROUND 1: CLAIMS 1, 24-25 ARE RENDERED OBVIOUS BY
BURUGANAHALLI**

95. The '856 patent has three independent claims. Claim 1 is a method claim; Claim 24 is a system claim; and Claim 25 is a non-transitory computer-readable medium claim. Other than the differences based on the types of claims, the recited limitations in the three claims are largely identical and substantively similar.

Claim 1 is representative of Claims 24 and 25 and is analyzed below.

A. Overview of Buruganahalli

96. Buruganahalli (Ex. 1004) is generally directed to firewall technologies. Buruganahalli explains that “[a] firewall generally protects networks from unauthorized access while permitting authorized communications to pass through the firewall.” Buruganahalli, 1:20-22. Buruganahalli discloses that there are many ways to implement a firewall, for example as a device, a set of devices or software executed on a device that provides a firewall function for network access; and there are also a number of ways to implement Buruganahalli’s disclosed techniques, including as a process, apparatus, a computer program and/or a processor. Buruganahalli, 1:21-31, 2:14-32, 2:48-60. Furthermore, Buruganahalli’s firewall may be implemented in a security device that includes many functions, such as a proxy function (which is a type of security function) and a routing function. *Id.*, 1:36-38, 3:5-15. Buruganahalli further discloses that the “routing functions can be based on source information (*e.g.*, IP address and port), destination information (*e.g.*, IP address and port), and protocol information.” *Id.*

97. Buruganahalli discloses “a firewall can filter inbound traffic by applying a set of rules or policies to prevent unwanted outside traffic from reaching protected devices.” Buruganahalli, 2:61-66, 1:32-36. These rules specify certain

matching criteria or heuristics, such as domain (*e.g.*, destination domain). Buruganahalli, 14:60-67, 4:23-30, 5:35-43. As an example, a security policy may be a “whitelist/blacklist policy” where a destination domains may be listed on a “blacklist” such that destination domains extracted from packets would be compared against the domains listed on the blacklist. Buruganahalli, 7:39-67, 10:66-11:2. The firewall then filters packets of a session between a client and a remote server associated with the domain name. Buruganahalli, 7:39-51, 7:60-67. Also, there are several ways to identify a domain, such as using a URL or an IP address. Buruganahalli, 3:5-24, 5:6-23, 7:39-8:44, 9:25-28, 10:21-28, 13:52-14:1, 15:37-45.

98. Figure 3A illustrates a firewall that filters packets in communications between a client and a remote server. More specifically, it illustrates an SSL/TLS session passing through a firewall between the client and the remote server. Buruganahalli, 4:31-40.

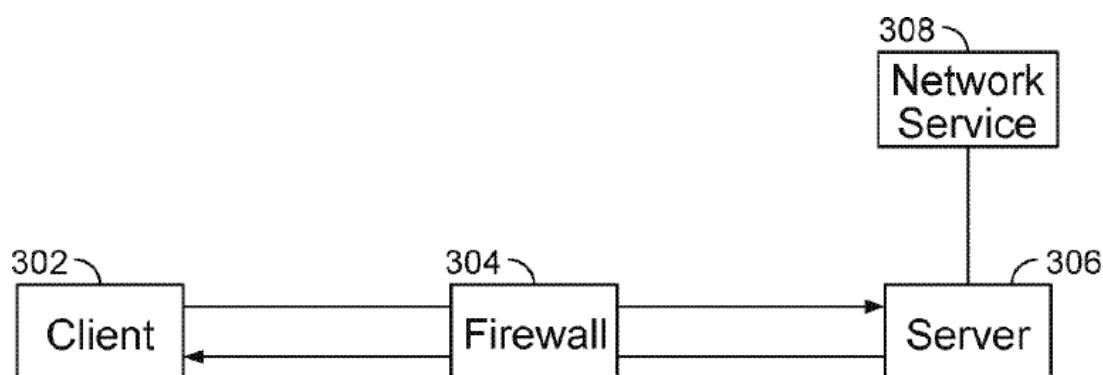


FIG. 3A

In the SSL/TLS session, “a typical firewall can initially just inspect the handshake traffic (*e.g.*, the initial negotiation to setup a secure communication channel/tunnel between a client and a remote server), as all the application data is encrypted.” Buruganahalli, 10:54-61, 11:7-42. In Buruganahalli’s system, the firewall extracts information, such as a destination domain, in unencrypted packets from the handshake message. Buruganahalli, 5:24-51, 7:24-25, 11:7-13. It then applies rules to the extracted information, such as determining whether it corresponds to the domains listed on a blacklist. Buruganahalli, 5:24-36, 7:42-67, 11:7-19, 11:30-54. The firewall then filters the unencrypted packets from the handshake message and may take additional actions (*e.g.*, decryption) that apply to the encrypted packets in the secure session based on the determination whether they correspond to the blacklist. *Id.*, *Abstract*, 4:16-22, 4:31-44, 6:12-39, 6:62-7:9. The firewall may intercept a client’s initial request for an encrypted session. *Id.*, 15:4-21, Fig. 7. One example of an initial request is a TLS “hello message sent from the client to the remote server.” *Id.* The firewall then extracts a domain name from the unencrypted request. *Id.* Based on the information in the initial request, the firewall applies rules by which the packets of the session between the client and the remote server are filtered. *Id.*

99. Buruganahalli discloses that the firewall uses a decrypt engine to decrypt encrypted traffic in a secure session associated with the handshake message. Buruganahalli, 7:42-51, 7:60-67, 8:45-54, 9:61-10:9. Figure 3B depicts establishing an SSL session between a client and a server and the corresponding description explains the decryption of encrypted packets in accordance with this process. Buruganahalli, 9:61-10:9, 12:4-18. In response to intercepting and detecting a request to establish a secure session, Figure 3B shows that the firewall splits the SSL session between the client and the remote server into two half sessions as “Session A” and “Session B”. Buruganahalli, 12:12-18.

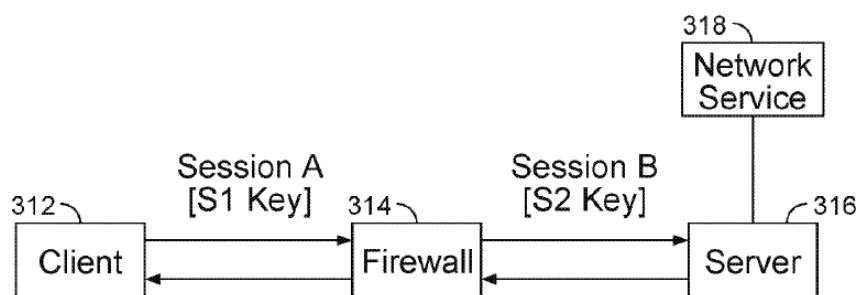


FIG. 3B

Specifically, Buruganahalli discloses, “[i]n Session A, the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316. Session A traffic is encrypted using the session key S1 associated with the firewall device. In Session B, the firewall 314 acts as the client 312 such that it is transparent to the remote server 316

that it is not communicating directly with the client 312. Session B traffic is encrypted using the session key S2 associated with the firewall device (e.g., the firewall device can store the fingerprint from the remote server in association with that remote server IP address).” Buruganahalli, 12:14-28. Accordingly, the firewall uses “S1 key” to decrypt data communicated from the client to the firewall, and uses “S2 key” to decrypt data communicated from the server to the firewall. Buruganahalli, 12:29-32, 12:52-55. In this manner, the firewall processes the packets “transparent” to the client and the server (that are the end points of the communication) such that neither the client or server would detect the presence of the firewall that applies that trusted man-in-the-middle techniques for decryption.

100. Buruganahalli uses a “self-signed certificate” in applying “trusted man-in-the-middle” techniques. Buruganahalli, 9:61-67. This means that the firewall replaces the public key in the original server certificate with its own key, and then generates a new certificate signed with its own public key, *i.e.*, “S1 key,” to replace the server certificate. Buruganahalli, 5:6-23, 5:52-61, 8:25-32, 9:61-67, 12:18-36. Buruganahalli further discloses that “[t]hese decryption techniques can be used in addition to and/or in combination with the various techniques described herein for destination domain extraction,” which includes the example provided in Figure 3A above. *Id.*, 11:59-12:3.

101. In Buruganahalli's system, a firewall intercepts and inspects packets sent from and to a client. Buruganahalli, 12:4-55. In accordance with one or more rules implementing a blacklist, the firewall identifies a request as part of a session-initiating handshake from the client to establish a secure session with a destination domain. Buruganahalli, 12:4-55, 7:39-67. As described in connection with Figure 3B, the firewall filters the unencrypted packets establishing the session, as well as the subsequent encrypted packets of the secure session in accordance with the one or more rules. Buruganahalli, 12:4-55. The firewall determines that the encrypted packets are part of the session established by the client request using unencrypted information, such as IP addresses in the packets. *Id.* at 9:25-28. It was well-known and conventional to use IP addresses and other unencrypted header data to determine if packets belong to a session. For example, Buruganahalli explains to use "IP address... for a monitored traffic flow (*e.g.*, a session) based on packet analysis." Buruganahalli, 9:25-28. IP addresses generally reside in the unencrypted portion of a packet and can be analyzed without first decrypting the packet. Therefore it would be routine to use IP addresses to determine if a packet is associated with a session.

102. Returning to Figure 3B, the firewall passes the client's secure session request to the server. Buruganahalli, 12:4-55. The server responds, and the firewall intercepts the response, determines that it is a response to the request, and then

decodes and filters it. *Id.* The firewall extracts a key from the server's response and substitutes it with its own key. *Id.* The firewall passes the response, along with the substituted key, to the client. *Id.* The key substitution effectively splits the original session into two half sessions: Session A and Session B. In Session A, the client encrypts packets using the substituted key (S1 key), and the firewall filters and then decrypts the encrypted packets from the client (having identified those packets as being part of the secure session) using that key. *Id.* And in Session B, the firewall re-encrypts the same information using the server's key (S2 key), and sends the encrypted packets to the server. *Id.* at 12:4-55. Similarly, when information is sent from the server back to the client, a reverse process of filtering and decryption/re-encryption takes place. *Id.*

103. Buruganahalli describes this process of session decryption and encryption using an intermediary interface as "transparent" to the client and server (which are end points of the communications). This description essentially describes the functions of a proxy, and more specifically, a "transparent" proxy, which was well-known in the art. For example, Wang, discloses, "because the proxy device 120 is a transparent intermediary to the client-server security session, the proxy device is able to decrypt the received traffic/packets (*e.g.*, using the session key negotiated for the client-proxy or proxy-server session, as appropriate) from each sending end

device, and may re-encrypt the traffic prior to forwarding it on using the respective session key with the receiving end device.” Wang, 8:12-19. As another example, Ebrahimi discloses that “a transparent proxy is neither known to nor configured by the clients; rather, the transparent proxy intercepts outgoing client requests to access origin servers/sites and transparently processes the requests on behalf of the clients.” Ebrahimi, 1:48-52. *See also*, NIST, 14. It was also well-known that proxies would operate in a manner that is invisible to an outsider, just as described as “transparent” in connection with Figure 3B of Buruganahalli. *See, e.g.*, Baehr, 4:50-63, 8:36-47, 8:65-9:7. Accordingly, although the description of Fig. 3B in Buruganahalli does not explicitly refer to implementing its decryption and encryption functionality as a proxy, a person of ordinary skill would have recognized the intermediary nature of that functionality (*i.e.*, implemented in a firewall that is in line between the client and the server), and that functionality’s transparent operation relative to communicating endpoints, as a proxy. This is in further view of Buruganahalli’s disclosure stating that “security devices were known to include both firewall and proxy functions.” Buruganahalli, 3:5-8. The prior art also recognizes that a software application running on a firewall is “a proxy agent.” NIST, 52.

104. Buruganahalli may not explicitly disclose “routing” filtered packets (*i.e.* encrypted packets of a secure session directed to a blacklisted domain after

having been filtered as being part of the secure session established by the initial client request) to a proxy system, but a person of ordinary skill would have understood that the filtered encrypted packets are “routed” to Buruganahalli’s decrypt engine. As I have mentioned above, a person of ordinary skill would have understood that a decrypt engine would be implemented as performing the functions of a proxy. This is because the function of a decrypt engine is decryption and Buruganahalli discloses the packets corresponding to a blacklist would be decrypted. Buruganahalli, 7:39-51, 9:61-67. Buruganahalli also explains that a proxy is a well-known component of a security device. Buruganahalli, 3:5-15. A person of ordinary skill would have understood that transmitting packets between interfaces of functional components of a security device such as a firewall, using a software routing function, was also well-known. For example, NIST discloses that “[a]pplication-proxy gateway firewalls do not require a Layer 3 (Network Layer) route between inside and outside interfaces of the firewall; the firewall software performs the routing.” NIST, 12. NIST also discloses, “[a] firewall ruleset is a table of instructions that the firewall uses for determining how packets should be routed between its interfaces”; and “[a] proxy agent is a software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it [*sic*] between the interfaces of the device.” NIST, 51-52.

105. Alternatively, a person of ordinary skill would have at least found it obvious to route the filtered encrypted packets in Buruganahalli to a proxy because proxies were known and routine components of firewalls and other network security devices. This is explicitly disclosed in Buruganahalli: “[s]ecurity devices... can include various security functions (*e.g.*, firewall, ... proxy...)... routing functions can be based on source information... destination information...” Buruganahalli, 3:5-15. Proxies were also known to be used for SSL/TLS decryption. *See, e.g.*, Wang, 8:6-27, 3:44-57, 4:21-28, 9:30-35. And as I have explained in Section VII.D.6, it was also known to route filtered packets to a proxy implemented internally to, or implemented externally from, the packet filtering device. The two configurations were disclosed extensively in prior art. *See, e.g.*, NIST, 12-14; Baehr, 2:25-30, 5:2-8, 8:12-18, Figs. 6-7; Wang, Fig. 1, 2:32-58; Le Pennec, Fig. 3, [0021]-[0023].

106. A person of ordinary skill would have been further motivated to route filtered packets to a proxy system in implementing the split session disclosed by Buruganahalli for security purposes. It was well known in the art is to isolate potentially dangerous traffic using a proxy, which is isolated from a network, to perform inspection, filtering, logging and/or virus detection. For example, NIST describes dedicated proxy servers as providing filtering, logging and virus detection.

NIST, 14. The advantage of a proxy is that it performs these important security functions without the need to alter the network, as was known in the art. Baehr, 2:38-42, 8:13-17, 8:37-47; Wang, 7:53-57, 8:12-21, 8:67-9:4 (no special client/server provisioning required, and decryption and inspection is isolated to the proxy device).

107. Furthermore, a person of ordinary skill would be motivated to perform the session splitting operation by routing filtered packets to a proxy system for performance reasons. The use of dedicated proxy servers improves the overall performance of a system by handing off decryption and encryption that are known to be computationally intensive processing tasks. For example, NIST discloses that dedicated proxy servers were used to decrease the work load of a firewall. NIST, 14. Indeed, Buruganahalli recognizes the need for “workload balancing of network related resources.” Buruganahalli, 3:5-15. Buruganahalli further discloses using “special purpose hardware” to implement firewalls “as dedicated appliances” that would “generally provide higher performance levels for application inspection than software executed on general purpose hardware.” Buruganahalli, 4:7-15. Buruganahalli also discloses implementing firewalls as a set of devices such that the proxy would be implemented as its own device. 1:22-25. Accordingly, a person of ordinary skill would have been motivated to use dedicated proxy servers for session splitting to reduce load on a firewall and improve performance.

B. Challenged Claims

1. Preamble¹

(a) [1.pre] A method comprising:

(b) [24.pre] A packet-filtering system comprising:

(c) [25.pre] One or more non-transitory computer- readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:²

108. Regardless of whether the preamble is limiting, Buruganahalli discloses a method.

109. Buruganahalli discloses “a firewall... [that] protects networks from unauthorized access while permitting authorized communications to pass through the firewall.” Buruganahalli, 1:20-22.

110. Buruganahalli further discloses “policy based filtering on... communication flows (e.g., sessions) prior to the set-up of the encrypted data communication,” such as “to monitor the initial unencrypted/clear text data communications exchanged as part of an initial handshake to setup a secure

¹ To the extent they are limiting, the preambles of all Challenged Claims are nonetheless met by the art of record.

² Please see limitation [1.a] for additional mapping.

connection for a new session between a client and a remote server...” to determine if the establishment of the new session should be allowed for transmitting encrypted packets. Buruganahalli, 4:34-40.

111. Buruganahalli’s techniques may be implemented in many ways. For example, Buruganahalli discloses that “a firewall is typically a device, such as a computer... [and] can also be... executed as software on computer servers, gateways, network/routing devices (e.g., network routers), or data appliances...” 1:22-30. The firewall “can be implemented...as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a process or...[which] may be referred to as techniques.” Buruganahalli, 2:14-22. Buruganahalli further discloses that the firewall is “a device, a set of devices, or software executed on a device that provides a firewall function for network access.” Buruganahalli, 2:50-52.

2. Limitation a

- (a) [1.a] receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat;**
- (b) [24.a] at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to: receive data**

- indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;**
- (c) **[25.a] receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;**

112. **Buruganahalli discloses receiving, by a packet-filtering system (e.g., “packet-filtering firewall,” “a security device”) comprising a hardware processor (e.g., a processor) and a memory (e.g., a memory) and configured to filter packets in accordance with a plurality of packet-filtering rules (e.g., “set of rules... referred to as policies,” “firewall policies/rules”), data indicating a plurality of network-threat indicators (e.g., “blacklist,” data that identify “threats” or “vulnerabilities”), wherein at least one of the plurality of network-threat indicators comprises a domain name (e.g., “domain name,” “destination domain”) identified as a network threat.**

113. Buruganahalli discloses that the techniques of its firewall or security device “can be implemented in numerous ways...embodied on...a processor configured to execute instructions stored on and/or provided by a memory coupled to the processor.” Buruganahalli, 2:14-31, 2:55-60, 3:16-24, 4:23-30.

114. Buruganahalli discloses, “firewalls....deny or permit network transmission based on a set of rules. These sets of rules are often referred to as

policies (e.g., network policies or network security policies).” Buruganahalli, 2:61-64. Furthermore, a firewall “can filter inbound traffic by applying a set of rules or policies to prevent unwanted outside traffic from reaching protected devices”; and it “can also filter outbound traffic by applying a set of rules or policies...” Buruganahalli, 2:64-3:4. These “policies are received and stored in the management plane [of the security device],” as shown in Figure 6. Buruganahalli, 14:59-60.

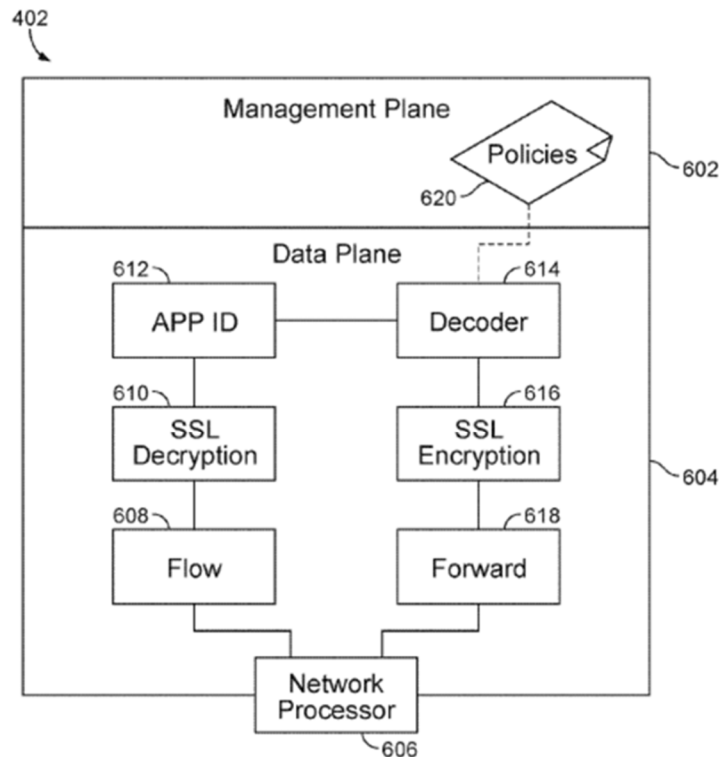


FIG. 6

Buruganahalli, Fig 6.

115. Buruganahalli further discloses that “policies can include one or more rules, which can be specified using domain and/or host/server names, and rules can

apply one or more signatures or other matching criteria or heuristics...”

Buruganahalli, 14:61-64. A firewall may “apply[] a policy (e.g., a security policy) based on the destination domain to filter traffic at a security device.” Buruganahalli, 7:27-29, 8:1-44, 10:66-11:2. For example, Buruganahalli discloses “blocking the session traffic using the security device is performed if a violation of a first firewall policy is determined, in which the first firewall policy includes a policy for verifying that the destination domain name extracted from a server name indication (SNI) matches...” Buruganahalli, 15:38-42, 5:37-42 (disclosing that the “domain name can be extracted by parsing the client hello message to extract the host name...which can then be used to apply firewall policies or take responsive actions based on this information without having to wait for data to be decrypted...”). Buruganahalli emphasizes that “it is generally desirable for a security device...to extract information about the destination domain for any given new flow (e.g., new session) as early as possible...information about the destination domain can be critical as well as relevant for security processing based on which policies and a set of actions that can be applied to the flow.” Buruganahalli, 4:23-30.

116. Buruganahalli discloses that “the security policy can include...a whitelist/blacklist policy” and “the destination domain [can be] included in [a] blacklist...” Buruganahalli, 7:42-43, 7:49-50. Buruganahalli further discloses that

“the security device 402 can extract destination domain information... that can facilitate identification of new, zero-day threats, new vulnerabilities, prevent false positives, and/or provide a feedback loop for any of such activities or trends aggregated and correlated.” Buruganahalli, 13:44-51. Taken together, Buruganahalli discloses packet-filtering rules (*e.g.*, policies or rules) that are based on whether certain data (*e.g.*, a destination domain) is identified as a network threat (*e.g.*, by matching the data on a blacklist).

3. Limitation b

- (a) [1.b] identifying packets comprising unencrypted data;**
- (b) [24.b] identify packets comprising unencrypted data;**
- (c) [25.b] identify packets comprising unencrypted data;**

117. **Buruganahalli discloses identifying (*e.g.*, “identifies”) packets comprising unencrypted data (*e.g.*, “unencrypted/clear text data communications exchanged as part of an initial handshake,” “handshake traffic,” “handshake exchange,” “hello message”).**

118. Buruganahalli discloses a security device having a “Flow 608” that “identifies packets as being part of a new session and creates a new session flow. Subsequent packets will be identified as belonging to the session based on a flow lookup.” Buruganahalli, 14:25-28. Buruganahalli further discloses that “an initial

TLS handshake exchange of that flow can be parsed to extract a hostname to facilitate destination domain extraction for secure protocols...” Buruganahalli, 14:28-31. Buruganahalli further discloses “monitor[ing] the initial unencrypted/clear text data communications exchanged as part of an initial handshake to setup a secure connection for a new session between a client and a remote server...” Buruganahalli, 4:37-40. Therefore, the system is able to “intercept[] a request to establish an encrypted session from the client to the remote server...” and “extract the hostname from the client hello message in order to apply various policies based on the destination domain.” Buruganahalli, 8:26-28, 11:49-51; *see also id.*, 11:59-12:64, 15:22-26.

119. Buruganahalli discloses that a “firewall can...inspect the handshake traffic (e.g., the initial negotiation to setup a secure communication channel/tunnel between a client and a remote server)...” Buruganahalli, 10:55-60. This is discussed in connection with Figure 3A.

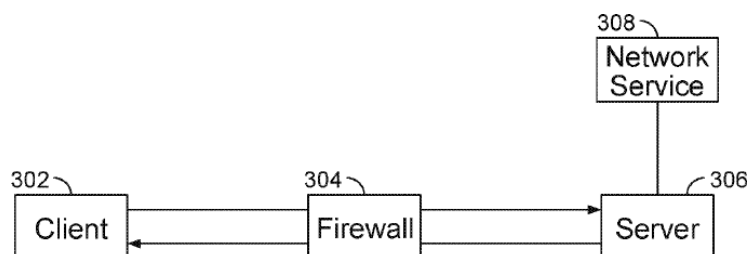


FIG. 3A

Buruganahalli also discloses “parsing the handshake traffic (e.g., parsing a client

hello message to extract a hostname that identifies the destination domain...)).

Buruganahalli, 11:9-11; *see also id.*, 12:32-36.

120. Buruganahalli discloses that the “handshake exchange (e.g., handshake/negotiation)” contains and transmits unencrypted packet data including “the client hello message is an unencrypted communication.” Buruganahalli, 7:24-25, 11:31-41. This allows early extraction of relevant information by “appl[ying] sooner based on this early extraction of the hostname...such that the rest of the stream can be forwarded without any decryption resulting in....enhanc[ed] performance (e.g., of the security device, such as a firewall).” Buruganahalli, 5:47-51. Therefore, to set up a new session, the system identifies unencrypted packet data within the initial handshake.

4. Limitation c

(a) [1.c] identifying packets comprising encrypted data;

(b) [24.c] identify packets comprising encrypted data;

(c) [25.c] identify packets comprising encrypted data;

121. **Buruganahalli discloses identifying (e.g., “identifies”) packets comprising encrypted data (e.g., “encrypted data communication”).**

122. Buruganahalli discloses a security device having a “Flow 608” that “identifies packets as being part of a new session and creates a new session flow.

Subsequent packets will be identified as belonging to the session based on a flow lookup.” Buruganahalli, 14:25-28. Buruganahalli further discloses that “[v]arious techniques...can be used to determine whether a new session...violates a policy... if a new flow is determined to violate a policy...the flow can be blocked...” Buruganahalli, 5:62-6:1. The new session using a secure protocol is an encrypted data communication; furthermore, the encrypted data communication would be evaluated based on handshake traffic configured to set up the session. Buruganahalli, 5:62-6:22, 4:31-44, 5:43-52, 12:33-48. For example, Buruganahalli discloses “monitor[ing] the initial unencrypted/clear text data communications exchanged as part of an initial handshake... prior to the establishment of the secure communication channel/tunnel after which... would be encrypted.” Buruganahalli, 4:37-44. A person of ordinary skill would have recognized that the encrypted data communication comprises data packets. Buruganahalli, 3:16-24, 3:40-50, 8:25-27. Specifically, Buruganahalli discloses “various techniques for destination domain extraction for secure protocols (e.g., by *facilitating deep packet inspection of the session traffic, which can include...encrypted data communications* associated with the session using a secure protocol, such as SSL/TLS).” Buruganahalli, 8:55-60. This is accomplished by “monitored traffic flow...based on packet analysis...” (Buruganahalli, 9:27-28) and “monitor[ing] encrypted data communications

associated with the session.” Buruganahalli, 6:15-16, 8:11-44 (referring to a “session” as “encrypted data communications.”). Therefore, Buruganahalli teaches identifying data packets comprising encrypted data during set up of a new session, and during the session.

5. Limitation d

- (a) [1.d] determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;**
- (b) [24.d] determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network- threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;**
- (c) [25.d] determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network- threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;**

123. Buruganahalli discloses determining, by the packet-filtering system and based on a portion of the unencrypted data (e.g., “unencrypted/clear text data communications exchanged as part of an initial handshake,” “handshake traffic,” “handshake exchange,” “hello message”) corresponding to one or more network-threat indicators of the plurality of network-threat indicators (e.g., destination domain on a blacklist), packets comprising encrypted data (e.g.,

“encrypted data communication”) **that corresponds to the one or more network-threat indicators** (e.g., destination domain on a blacklist).

124. Buruganahalli discloses that “a firewall can intercept and monitor data communications from a client and a remote server in order to extract the hostname data from the SNI field...which is sent as an unencrypted data communication from the client...at the start of the handshaking process for setting up a secure TLS communication channel/session...” Buruganahalli, 5:27-34. Buruganahalli further discloses “various techniques...for destination domain extraction for secure protocols...by parsing the handshake traffic (e.g., parsing a client hello message to extract a hostname that identifies the destination domain being requested by the client to the remote server)” Buruganahalli, 11:7-12. Buruganahalli discloses “a TLS handshake exchange (e.g., handshake/negotiation) between a client (C) and a remote server (s) using the SNI approach:

Step 1. C: (TLS Handshake) Hello, I support XYZ Encryption, and I am trying to connect to 'website.example.com'.
Step 2. S: (TLS Handshake) Hi there, here is my Public Certificate, and let's use this encryption algorithm.
Step 3. C: (TLS Handshake) Agreed.
Step 4. C: (Encrypted) HTTP Request.
Step 5. S: (Encrypted) HTTP Reply.

... the firewall can intercept and decode (e.g., parse) this TLS handshake exchange to extract the hostname from the client hello message in order to apply various policies based on destination domain.” Buruganahalli, 11:31-51.

125. Buruganahalli discloses applying a security policy to compare extracted information from a handshake traffic with information on a blacklist to determine whether the handshake traffic and the encrypted data communication it seeks to set up present any security threats. For example, Buruganahalli discloses “applying a security policy based on the destination domain to filter traffic at the security device, in which the security policy includes a... blacklist policy, and... if the destination domain is included in a blacklist...” Buruganahalli, 7:61-67. Therefore, the firewall inspects the handshake exchange to verify the presence of network-threat indicators by comparing against the blacklist. Buruganahalli further discloses that “the firewall 304 can apply one or more firewall policies/rules... (e.g., a policy that includes requirements or rules related to destination domains that may be used for secure protocol communications)” Buruganahalli, 11:13-17.

126. Buruganahalli correlates packets associated with a session using certain identifying information. For example, Buruganahalli discloses using “[a]n IP address and port engine [] determines [that] an IP address and port number for a monitored traffic flow (e.g., a session) based on packet analysis.” Buruganahalli, 9:26-28. It was well-known and conventional that IP addresses for source and destination associated with a packet, or other TCP session data, would be located in an unencrypted portion of a packet (e.g., a clear header) that can be inspected without

decrypting the packet so that the packet can be routed using the IP addresses. Buruganahalli further discloses having “storage stores tables that include host names/identifiers (e.g., destination domains) and associated IP addresses and possibly other information...for implementing policies using destination domain extraction for secure protocols.” Buruganahalli, 13:63-14:1.

127. Based on these disclosures, Buruganahalli teaches correlating encrypted packets in a session with the hello message in TLS handshake traffic that initiates the session. A person of ordinary skill would have understood that this correlation is accomplishing using at least address information (e.g., IP address) associated with the destination domain in the hello message. Accordingly, a person of ordinary skill would have understood that determining encrypted packets comprising data corresponding to one or more network-threat indicators (e.g., a blacklisted destination domain) based on data included in the hello message (e.g., destination domain and associated IP address) configured to establish the encrypted session, because both the encrypted session and the hello message would be associated with the same destination IP address of the remote server.

128. Indeed, Buruganahalli’s use of a handshake message in performing the determining step is similar to those in the specification of the ’856 patent. The ’856 patent discusses to “determine that the packets comprise data corresponding to the

network-threat indicators based on data included in the one or more handshake messages configured to establish session” and to “determine that one or more of the packets encrypted... correlate to one or more packets comprising ... the one or more handshake messages.” ’856, 9:30-33, 24:18-30.

6. Limitation e

- (a) **[1.e] filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:**
- (b) **[24.e] filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:**
- (c) **[25.e] filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network- threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:**

129. **Buruganahalli teaches filtering, by the packet-filtering system and**

based on data indicating a request (*e.g.*, “a request to create a secure connection”) **specified by the plurality of packet-filtering rules.**

130. Please see my discussion above in [1.a]. Buruganahalli discloses that “[a] firewall can filter inbound traffic by applying a set of rules or policies.” Buruganahalli, 1:32-35, 2:61-66. Buruganahalli further discloses that “a network service activity that is in violation of one or more firewall policies/rules implemented by the firewall device [] (*e.g.*, a policy that includes requirements or rules related to destination domains...)”). Buruganahalli, 10:63-11:2.

131. Please see my discussion above in [1.d]. Buruganahalli discloses parsing a client’s SSL/TLS request, such as packets in a hello message or as part of a handshake traffic, to establish a secure connection with a remote server to determine whether the destination domain extracted from the request corresponds to information on a blacklist. For example, Buruganahalli discloses “destination domain extraction for secure protocols includes... initiating a setup for a secure protocol-based connection... destination domain is extracted from the server name indication (SNI) of a client hello message” and this destination domain extraction approaches further includes “applying a policy (*e.g.*, a security policy).” Buruganahalli, 7:12-28, 5:42-52. Buruganahalli also discloses “applying a security policy based on the destination domain to filter traffic at the security device, in which

the security policy includes a whitelist/blacklist policy, and [determines] if the destination domain is included in a blacklist of the whitelist/blacklist policy.” Buruganahalli, 7:63-67; *see also*, 7:39-51. Buruganahalli further discloses “extracting a destination domain from the *request* to create the secure connection” and “applying a policy (e.g., a security policy) based on the destination domain to filter traffic using a security device.” 15:8-21, 8:25-44. Taken together, a person of ordinary skill would have understood that Buruganahalli teaches filtering packets based on a SSL/TLS request specified by security rules or policy.

132. Buruganahalli discloses filtering, by the packet-filtering system and based on a uniform resource identifier (URI) (e.g., a uniform resource locator (URL)) specified by the plurality of packet-filtering rules.

133. Please see my discussion above in [1.a]. Buruganahalli discloses that “[a] firewall can filter inbound traffic by applying a set of rules or policies.” Buruganahalli, 1:32-35, 2:61-66, 10:63-11:2.

134. Buruganahalli discloses “applying a security policy based on the destination domain to filter traffic at the security device,” such as “a uniform resource locator (URL)/category filtering policy.” Buruganahalli, 7:39-7:51, 10:24-25. Buruganahalli also discloses “blocking the session traffic using the security device is performed if a violation...is determined, in which...the destination domain

name extracted from a server name indication (SNI) matches the domain associated with a uniform resource locator (URL) for a session associated with the network communications between the client and the remote server.” Buruganahalli, 15:38-45. A person of ordinary skill would have recognized, as it was well-known and conventional in the art, that URLs are examples of uniform resource identifiers. For example, U.S. Patent 8,813,228 (“Magee”) (Ex. 1037) discloses that “[t]he module will also gather a taxonomy of the uniform resource identifiers (URIs) (e.g., URLs...) associated with the target host.” Magee, 12:26-27. Accordingly, Buruganahalli teaches filtering based on a URI (e.g., URL) specified by a rule. Buruganahalli further discloses the ability to “perform application layer filtering...” (Buruganahalli, 3:25-26) and “real-time content scanning...” (Buruganahalli, 4:2) through “state-based firewall...[to] monitor traffic flows...” (Buruganahalli, 9:18) as well as utilizing “application identification, user identification, and/or other information to match signatures (e.g., file-based, protocol-based, and/or other types/forms of signatures) for detecting malware or suspicious behavior.” Buruganahalli, 10:15-20, 9:29. In view of these disclosures, a person of ordinary skill would have further understood that a firewall filters packets by scanning content for the URL in the application layer where a URL would be found.

135. Corresponding limitation [e] of Challenged Claim 25 has an additional

limitation reciting “filter[ing], by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules *indicating one or more of the plurality of network-threat indicators.*” Please see my discussion above in [1.a]. Buruganahalli teaches packet-filtering rules that indicate network-threat indicators. As an example, Buruganahalli discloses that firewalls “deny or permit network transmission based on a set of rules” and “filter inbound traffic by applying a set of rules or policies to prevent unwanted outside traffic from reaching protected devices” and thus these rules are implemented for security purposes to protect the network. Buruganahalli, 2:61-66, 1:32-36. Buruganahalli further discloses the policies or rules include requirements related to destination domains, which are listed on a blacklist if they are deemed to present a security risk to the system. Buruganahalli, 10:66-11:2, 7:27-29, 7:42-67, 8:1-44, 13:43-52. A person of ordinary skill would have understood that destination domains that are included on a blacklist are network-threat indicators as they present a potential security risk.

136. **Buruganahalli also teaches filtering, by the packet-filtering system and based on data indicating a protocol version (e.g., “protocol information,” version of TLS protocol with “server name indication (SNI)” extension) specified by the plurality of packet-filtering rules.**

137. Buruganahalli discloses that firewalls “inspect the individual packets themselves and apply rules based on the inspected packets[’]...source and destination address information, ***protocol information***, and a and port number...” Buruganahalli, 3:16-24. Buruganahalli further discloses “monitored network traffic can include... traffic using ***other types of known or unknown protocols***...” Buruganahalli, 9:18-19. A person of ordinary skill would have understood that protocol information would include a version number that identifies the specific version of the protocol because it was widely known that certain SSL and TLS versions have significant security vulnerabilities and risk assessment would be properly conducted only if the protocol version is known. For example, such security vulnerabilities were described in a Request for Comments for “Prohibiting Secure Sockets Layer (SSL) Version 2.0” (Turner) (Ex. 1031), which lists various deficiencies in SSL version 2.0: “Message authentication uses MD5. Most security-aware users have already moved away from any use of MD5”; “Handshake messages are not protected...”; “Message integrity and message encryption use the same key...”; and “Sessions can be easily terminated...” Turner, 2. Similarly, a “SSL/TLS and PKI History” article (Ristic) (Ex. 1032) also identifies security issues with various versions of SSL and TLS, e.g., “SSL v2 is shot down because of serious security issues...” Ristic, 1. Accordingly, a person of ordinary skill would have been

motivated and found it obvious to filter packets based on SSL/TLS versions specified by packet-filtering rules.

138. Buruganahalli further discloses “monitoring network communications...and extracting a destination domain from the request to create the secure connection. ...the secure protocol is a secure sockets layer (SSL) protocol or transport layer security (TLS) protocol and the destination domain is extracted from the server name indication (SNI) of a client hello message...” Buruganahalli, 7:13-23, *Abstract*, 4:45-5:4, 15:4-21. A person of ordinary skill would have understood that this refers to a version of the TLS protocol using the SNI extension.

7. Limitation f

- (a) [1.f] packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network- threat indicators; and**
- (b) [24.f] packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network- threat indicators; and**
- (c) [25.f] packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network- threat indicators; and**

139. **Buruganahalli discloses filtering packets comprising the portion of the unencrypted data** (*e.g.*, “unencrypted/clear text data communications exchanged as part of an initial handshake,” “handshake traffic,” “handshake exchange,” “hello message”) **that corresponds to one or more network-threat**

indicators of the plurality of network-threat indicators (e.g., destination domain on a blacklist).

140. Please see my discussion above in [1.b], [1.d] to [1.e]. Buruganahalli discloses that it is “desirable for a security device...to extract information about the destination domain for any given new flow... as early as possible.” Buruganahalli, 4:23-26. Buruganahalli further discloses that it is also “desirable and efficient to...facilitate policy-based filtering on such data communication flows (e.g., sessions) prior to the set-up of the encrypted data communication for such flows (e.g., to monitor the initial unencrypted/clear text data communications exchanged as part of an initial handshake to setup a secure connection for a new session between a client and a remote server, which is prior to the establishment of the secure communication channel/tunnel after which any data communications intercepted between the client and the remote server would be encrypted).” Buruganahalli, 4:34-44. Buruganahalli discuss as an example that “intercepting a request to establish an encrypted session from the client to the remote server...” Buruganahalli, 8:26-28, 15:24-25. Furthermore, Buruganahalli discloses “filter[ing] traffic at the security device... if the destination domain is included in a blacklist...” based on inspecting the handshake traffic,” which is known to be the unencrypted portion of the encrypted secure tunnel session traffic. Buruganahalli, 7:41-66, 10:54-11:19.

Accordingly, Buruganahalli teaches filtering packets comprising unencrypted data in the handshake traffic that correspond to a blacklisted destination domain.

8. Limitation g

- (a) **[1.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and**
- (b) **[24.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and**
- (c) **[25.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and**

141. Buruganahalli teaches filtering the determined packets comprising the encrypted data (e.g., “encrypted data communication”) that corresponds to the one or more network-threat indicators (e.g., destination domain on a blacklist).

142. Please see my discussion above in [1.c] to [1.e]. Buruganahalli discloses filtering “encrypted data communications” based on a security policy or rule as discussed above. Buruganahalli, 4:20-22. The encrypted data communications are filtered after it is determined that information extracted from the handshake traffic matches with those on a blacklist, and thus corresponds to a network-threat indicator. Buruganahalli, 6:12-39 (encrypted data communications associated with a secure session monitored for filtering based on a firewall policy);

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

see also id., Abstract (applying a policy based on the destination domain to filter traffic), 4:31-44 (policy-based filtering on a session with encrypted data communications), 6:62-7:9 (applying policy to a resumed session), 7:12-29 (applying a policy based on the destination domain to filter traffic), 7:39-51 (same), 7:60-67 (same), 15:4-21 (same). To the extent it is argued that Buruganahalli does not explicitly disclose filtering encrypted data using network-threat indicators, a person of ordinary skill would have understood that packets transmitted as part of a secure session are filtered after determining whether the handshake message that initiates the session corresponds to a network threat indicator, such as a blacklisted destination domain. This is in view of the disclosure that the handshake message and the encrypted data of the session are correlated to the same session using network address information. A person of ordinary skill would have understood that both correspond to the same network-threat indicator because any security risks presented by the handshake message would also apply to the encrypted session based on the correlation. A person of ordinary skill, would at a minimum, would have been motivated and found it obvious to filter the encrypted data of a secure session that was initiated by a handshake message with data corresponding to a network- threat indicator in order to monitor transmission, into or out of a protected network, of data that potentially presents a security risk.

9. Limitation h

- (a) **[1.h] routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.**
- (b) **[24.h] route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.**
- (c) **[25.h] route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.**

143. **Buruganahalli teaches routing, by the packet-filtering system, filtered packets to a proxy system** (*e.g.*, a “decrypt engine... applying trusted man-in-the middle techniques,” a “proxy” that is one of the “security functions”) **based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators** (*e.g.*, destination domain on a blacklist).

144. Buruganahalli discloses that “if the destination domain is included in the blacklist” (*i.e.*, if the filtered packets correspond to a network-threat indicator), then the encrypted data communications between the client and the server are “decrypted.” Buruganahalli, 7:39-51, 7:60-67. A person of ordinary skill would have understood that the filtered encrypted data are decrypted by the decrypt engine of the firewall. As shown in Figure 1, Buruganahalli discloses that firewall 100 has a

decrypt engine 110 that decrypts monitored traffic. Buruganahalli, 9:61-67.

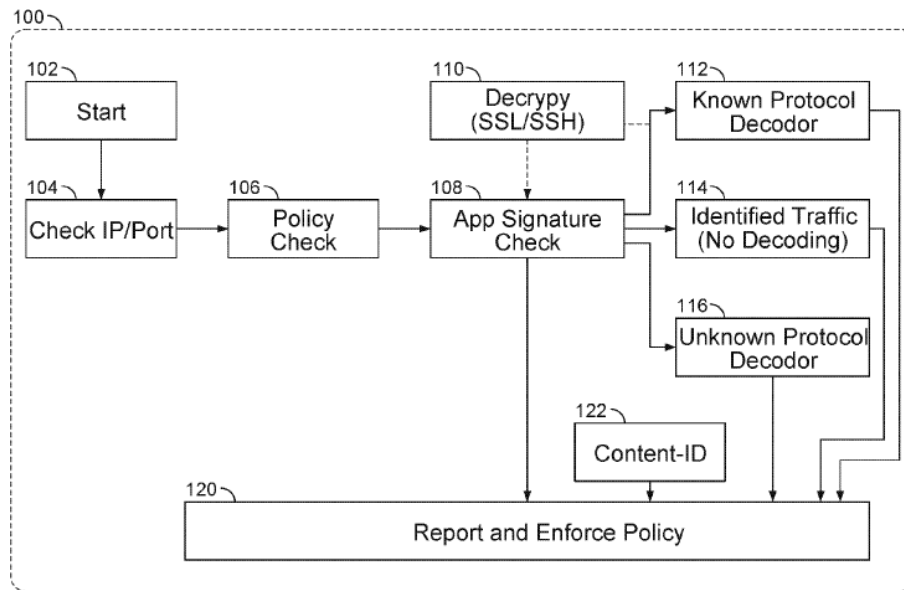


FIG. 1

145. Buruganahalli describes the process of decrypting the encrypted data in more details. Figure 3B of Buruganahalli illustrates a process of establishing an SSL session. Buruganahalli, 12:4-18.

Here, a SSL session request from a client to a server is detected and intercepted by a firewall. Buruganahalli, 12:12-14. The session is split in half with Session A between the client and the firewall and Session B between the firewall and the server.

146. When the client makes an SSL session request, Buruganahalli discloses that, “the SSL session request is intercepted and detected by the firewall.” The firewall handles the request as follows: “In Session A, the firewall 314 acts as the

remote server 316 such that it is transparent to the client 312 that it is not communicating directly with the remote server 316. Session A traffic is encrypted using the session key S1 associated with the firewall device. In Session B, the firewall 314 acts as the client 312 such that it is transparent to the remote server 316 that it is not communicating directly with the client 312. Session B traffic is encrypted using the session key S2 associated with the firewall device...” Buruganahalli, 12:14-28. Buruganahalli describes the packets of a secure session are processed in a manner transparent to the end points (*i.e.*, the client and the server) of the communications such that they would not detect the presence of the firewall applying the “trusted man-in-the-middle technique.” Buruganahalli, 12:14-15.

147. Buruganahalli describes the decryption engine of the firewall as applying “trusted man-in-the the-middle techniques using a self-signed certificate.” Buruganahalli, 9:61-67. As I have mentioned in the overview section of Buruganahalli above, Buruganahalli uses a “self-signed certificate” in applying “trusted man-in-the-middle” techniques. Buruganahalli, 9:61-67. A person of ordinary skill would have understood that the firewall replaces the public key in the original server certificate with its own key, and then generates a new certificate signed with its own public key (“S1 key”) to replace the server certificate. Buruganahalli, 5:6-23, 5:52-61, 8:25-32, 9:61-67, 12:18-36.

148. Buruganahalli further discloses that “[t]hese decryption techniques can be used in addition to and/or in combination with the various techniques described herein for destination domain extraction,” which includes the example provided in Figure 3A above. *Id.*, 11:59-12:3. Accordingly, a person of ordinary skill would have understood that these techniques described in connection with Figure 3A and Figure 3B are taught to be combined in implementing Buruganahalli’s security system.

149. Also, as I discussed in the overview section of Buruganahalli above, a person of ordinary skill would have understood Buruganahalli to describe a firewall containing functionality that acts as a proxy based on its disclosure in connection with Figure 3B where a function of the firewall stands in line of communications between a client and a server in a “transparent” manner. This understanding is consistent with the description of a proxy in the ’856 specification, which describes “proxy devices” as “the man in the middle.” *See* ’856, 10:62-63. This understanding, as I have discussed in the overview section of Buruganahalli above, is further consistent with the prior art’s description of a proxy device. *See, e.g.,* Wang, 8:12-19; NIST, 14; Baehr, 4:50-63, 8:36-47, 8:65-9:7.

150. Buruganahalli also discloses “[s]ecurity devices (e.g., security appliances, security gateways, security services, and/or other security devices) can include various security functions (e.g., firewall, anti-malware, and intrusion

prevention/detection, proxy, and/or other security functions), networking functions (e.g., routing, Quality of Service (QoS), workload balancing of network related resources, and/or other networking functions), and/or other functions. For example, routing functions can be based on source information (e.g., IP address and port), destination information (e.g., IP address and port), and protocol information.” Buruganahalli, 3:5-15; *id.*, 1:36-38. In view of these disclosures, a person of ordinary skill would have understood, or at minimum would have been motivated and found it obvious, to route filtered packets to the decrypt engine of the firewall that is used as part of the proxy function, as discussed above. In this manner, the filtered encrypted packets would be decrypted using a substituted key (*i.e.*, S1 key) and inspected by the firewall; and this process would take place “[a]fter the session set-up handshaking is completed.” Buruganahalli, 12:29-32, 15:22-44. A person of ordinary skill would have further understood that routing may be implemented as a software process that may be internal within a firewall. For example, as I discussed in the overview section of Buruganahalli above, NIST discloses that “[a]pplication-proxy gateway firewalls do not require a Layer 3 (Network Layer) route between inside and outside interfaces of the firewall.” NIST, 12. Accordingly, a person of ordinary skill would have understood, or would have been motivated and found it obvious, to route filtered encrypted packets to a proxy system, *i.e.*, the decrypt

engine of the firewall used as part of the proxy function, which applies the “trusted man-in-the-middle” techniques as taught in Buruganahalli.

151. To the extent one argues that Buruganahalli’s disclosure of session splitting described along with Figure 3B does not explicitly teach routing filtered packets to a proxy system, at minimum a person of ordinary skill would have been motivated and found it obvious to perform session splitting by routing filtered packets to a proxy system using software or the routing function as taught in Buruganahalli. This would be done for security purposes such that potentially dangerous packets would be routed to a proxy system for separate handling. Furthermore, implementing a proxy system with other functions of a firewall in this manner (same device or separate devices) was already well-known and conventional in the art, as I have discussed in Section VII.D.6. *See, e.g.*, NIST, 12-14; Baehr, 2:25-30, 5:2-8, 8:12-18, Figs. 6-7; Wang, Fig. 1, 2:32-58; Le Pennec, Fig. 3, [0021]-[0023].

152. Indeed, it would be advantageous to divert potentially dangerous traffic for separate inspection (*e.g.*, actions such as filtering and logging) by a proxy system such that the security functions performed by the proxy system are isolated from the rest of the interconnecting network. *Id.* A person of ordinary skill would have recognized that it was well known and conventional to isolate a network from direct

access by an outsider by using a proxy system to intercept communications to and from the network. *See, e.g.*, Baehr, Abstract, 8:37-40. Furthermore, Buruganahalli recognizes to implement a firewall as a set of devices such that a proxy function would be implemented on its own device separate from other firewall functions. Buruganahalli, 1:22-25; 2:50-52. Such implementation would be advantageous because it would offload intensive processes, such as decryption and encryption, to a proxy system that would be dedicated to perform these tasks, in order to reduce the overall workload of a firewall. *See* NIST, 14. Moreover, isolating a proxy system from firewall functions would further Buruganahalli's security purpose to protect a system against malware or other security attacks. Buruganahalli, 3:5-8, 7:39-51, 7:60-67, 8:20-24, 10:15-20, 13:43-52. For example, as I have discussed in connection with the overview section of Buruganahalli above, such purpose is achieved by routing potentially dangerous packets to a proxy function acting as a trusted man-in-the-middle to decrypt the encrypted data. *Id.*

C. Claim Chart

153. Furthermore, I have reviewed and endorse the claim charts of the accompanying Petition showing that each element of claims 1, 24-25 are rendered obvious by Buruganahalli.

XI. GROUND 2: CLAIMS 1, 24-25 ARE RENDERED OBVIOUS BY BURUGANAHALLI IN VIEW OF BAEHR

154. As explained in connection with Ground 1, the Challenged Claims 1 and 24-25 are rendered obvious by Buruganahalli. To the extent it is argued that routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators (*e.g.*, claim limitations [1.h], [24.h], and [25.h]) is not explicitly taught by Buruganahalli, that limitation is rendered obvious by Buruganahalli in view of Baehr (Ex. 1005), which explicitly discloses a packet-filtering system that sends packets aside to a proxy network.

155. Buruganahalli teaches firewall techniques based on securities policies to filter packets in communications exchanged between a client and a remote server. Buruganahalli, 4:31-40. This includes intercepting an initial clear handshake message to set up an encrypted session between the client and the server. *Id.* Buruganahalli also teaches that if data from the handshake message corresponds to information on a blacklist, *e.g.*, such as via a comparison of destination domains, then the packets from the encrypted session would be decrypted. Buruganahalli, 7:39-51, 7:60-67, 12:29-32. The firewall has a decrypt engine to perform the decryption by applying “trusted man-in-the-middle techniques.” Buruganahalli, 9:7-8, 9:61-67. In applying these techniques, “the firewall 314 acts as the remote server 316 such that it is transparent to the client 312 that it is not communicating directly

with the remote server 316,” and vice versa. Buruganahalli, 12:13-33.

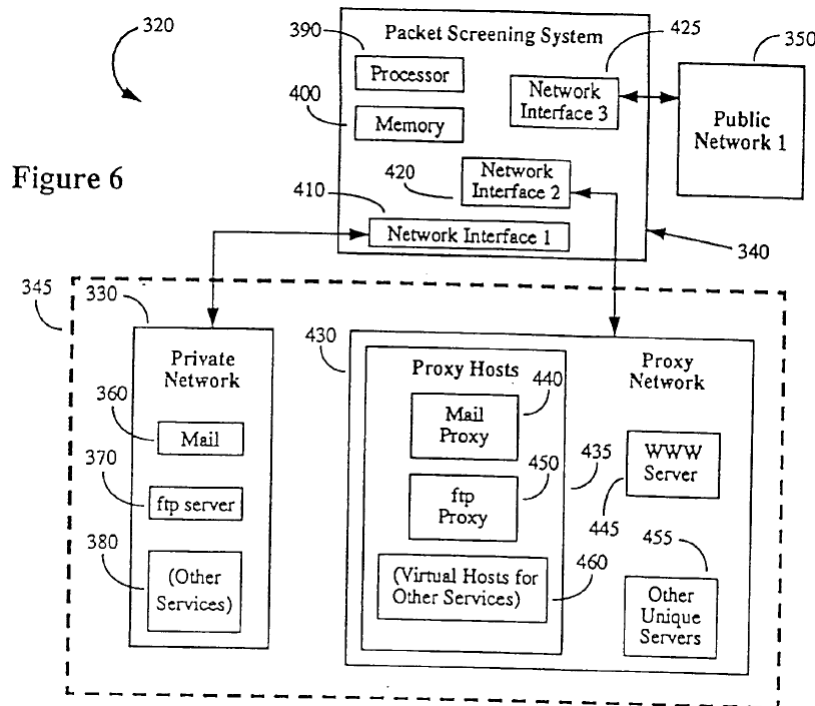
156. Buruganahalli further discloses “[s]ecurity devices... can include various security functions (*e.g.*, firewall, proxy...)... and/or other functions. For example, routing functions can be based on source information (*e.g.*, IP address and port), destination information (*e.g.*, IP address and port), and protocol information.” Buruganahalli, 3:5-15. As I have explained above, a person of ordinary skill would have recognized that the disclosures in connection with Figure 3B of Buruganahalli describes functions for a proxy system that stands between a client and server and acts on behalf of a server to process a client’s request. This understanding is further apparent by Buruganahalli’s disclosure to pass packets between software functions of a firewall and route filtered packets to the proxy function. Buruganahalli, 3:16-24.

157. Buruganahalli discloses the need for “workload balancing of network related resources.” Buruganahalli, 3:5-15. Buruganahalli also states that “special purpose hardware for next generation firewalls implemented, for example, as dedicated appliances, generally provide higher performance levels for application inspection than software executed on general purpose hardware...” Buruganahalli, 4:7-15. Buruganahalli further discloses that “[a] firewall is typically a device or a set of devices.” Buruganahalli, 1:22-25. To reduce the workload of a firewall, a person

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

of ordinary skill would have known, as was conventional, that the firewall would pass filtered traffic to a dedicated proxy server, rather than performing the functions of a proxy internally within a firewall. NIST, 14 (“a main firewall might accept inbound traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server.”). Therefore, a person of ordinary skill would have been motivated and found it obvious to incorporate the teachings of Baehr, which discloses sending filtered packets to a proxy system outside of a packet screening system acting as a firewall, in implementing Buruganahalli’s security system.

158. Baehr discloses “[a] system for screening data packets transmitted between a network to be protected, such as a private network, and another network, such as a public network” and the system has a “screen” that acts as a firewall and filters packets. Baehr, Abstract, 2:10-12. Such system is illustrated in Figure 6 of Baehr. Baehr, 2:66-67.



Baehr discloses that, “[a] screen is positioned on the network connection between, for example, a public network and a private network that is to be protected from targeting for attack.” Baehr, 2:10-17. Baehr discloses that the screen “includes a packet filtering subsystem or module, which inspects each incoming packet and sends it to an engine, which determines, based upon the packet inspector and other information, what actions should be taken on the packet.” Baehr, 2:18-23. Baehr further discloses “[t]he screen 340 includes instructions stored in memory 400 governing its control of actions to be taken on the incoming (and outgoing) data packets.” Baehr, 6:37-39. Specifically, the screen “includes instructions stored in memory... [and] include a predetermined set of criteria based upon the... contents

of the data packets (source and destination addresses...)” that allow the screen to determine whether a packet comes from or goes to a network location that may indicate a security problem. Baehr, 6:37-7:7.

159. To protect its private network, Baehr discloses routing filtered packets to a proxy network, rather than to the private network. Baehr discloses a host sending a packet to a public network that is intercepted at the interface of a screen 340. Baehr, 10:2-5, 9:63-67. The screen 340 uses a set of predetermined “screening criteria” for filtering packets. Baehr, 6:37-7:10. The screen 340 then takes actions on the packets, based on the screening, in order to prevent attacks on the system. Baehr, 7:8-25. Baehr discloses that “an important action for security purposes is that of sending packets aside to the proxy network...” Baehr, 8:12-18. This is done so for “security purposes” even if the packets’ intended destination is the private network. Baehr, 2:25-30, 10:43-49. The proxy network would then execute “appropriate operations.” Baehr, 2:25-30. Furthermore, “[a] proxy network may [] include proxy hosts representing actual hosts, and/or proxy hosts with unique servers, in any combination...” Baehr, 4:26-63.

160. Baehr provides reasons to explain why routing filtered packets to a proxy network, rather than sending them to a private network, would be advantageous. Baehr explains that “[t]he proxy network is isolated from the private

network, so it cannot be used as a jumping off point for intruders.” Baehr, *Abstract*. Therefore, it has the advantage of “preventing outsiders from ever actually entering the private network.” Baehr, 8:37-40. This is in contrast to allowing a user to access the network directly, because “once a user has been allowed access or a connection to a private network, it is much more difficult to restrict his/her actions than if no access at all is allowed.” Baehr, 8:37-40. Furthermore, “the private network 330 and the proxy network 430 together form a single logical or apparent network 345, i.e. a single apparent domain from the point of view of outsiders, such as users on the public network 350, so that when a user attempts to access a service or host of the private network, the request may be shunted aside to the proxy network to either a mirroring proxy host or a unique proxy host, without any indication being given to the user that this has occurred.” Baehr, 4:50-63, 8:36-47, 8:65-9:7. This approach allows the proxy network to communicate seamlessly with the outsiders as if the outsiders are communicating directly with the private network. *Id.*

161. In terms of implementations, Baehr discloses that the proxy network may be a separate computer system—this is shown in Figure 6; alternatively, the proxy network does not have to be physically separate from the screen, but rather a separate logical entity—this is shown in Figure 7. Baehr, 4:26-31, 5:2-8. Regardless of whether there is a physical separation between the screen and the proxy network,

the proxy is implemented as a dedicated function separate from the screen that filters packets. Baehr further discloses that the proxy network may be implemented “entirely in program instructions stored in the memory” of the packet screening system, “or as additional processor(s) and memory(-ies) controlled by program instructions stored in one or more of the memories.” Baehr, 4:64-5:2.

162. A person of ordinary skill would have been motivated and found it obvious to implement Buruganahalli’s system in view of the teachings of Baehr to route the filtered packets to a proxy system separate from or included in a firewall such that Buruganahalli’s techniques (that in essence describe a transparent proxy function) would have been implemented in a proxy system separate from and external to a firewall. A person of ordinary skill would have been motivated and found it obvious to implement the techniques describing a proxy in a dedicated function for the advantages of preserving computing resources, achieving load balancing, and maximizing performance, as recognized in Buruganahalli. *See, e.g.*, Buruganahalli, 3:16-24, 4:7-15. For example, having a dedicated function separate from other functions allows the proxy function to manage its own resources efficiently without having to share resources with another function; and this approach also increases the overall system performance by allowing each function to focus on performing its own specialized tasks. These advantages were well known

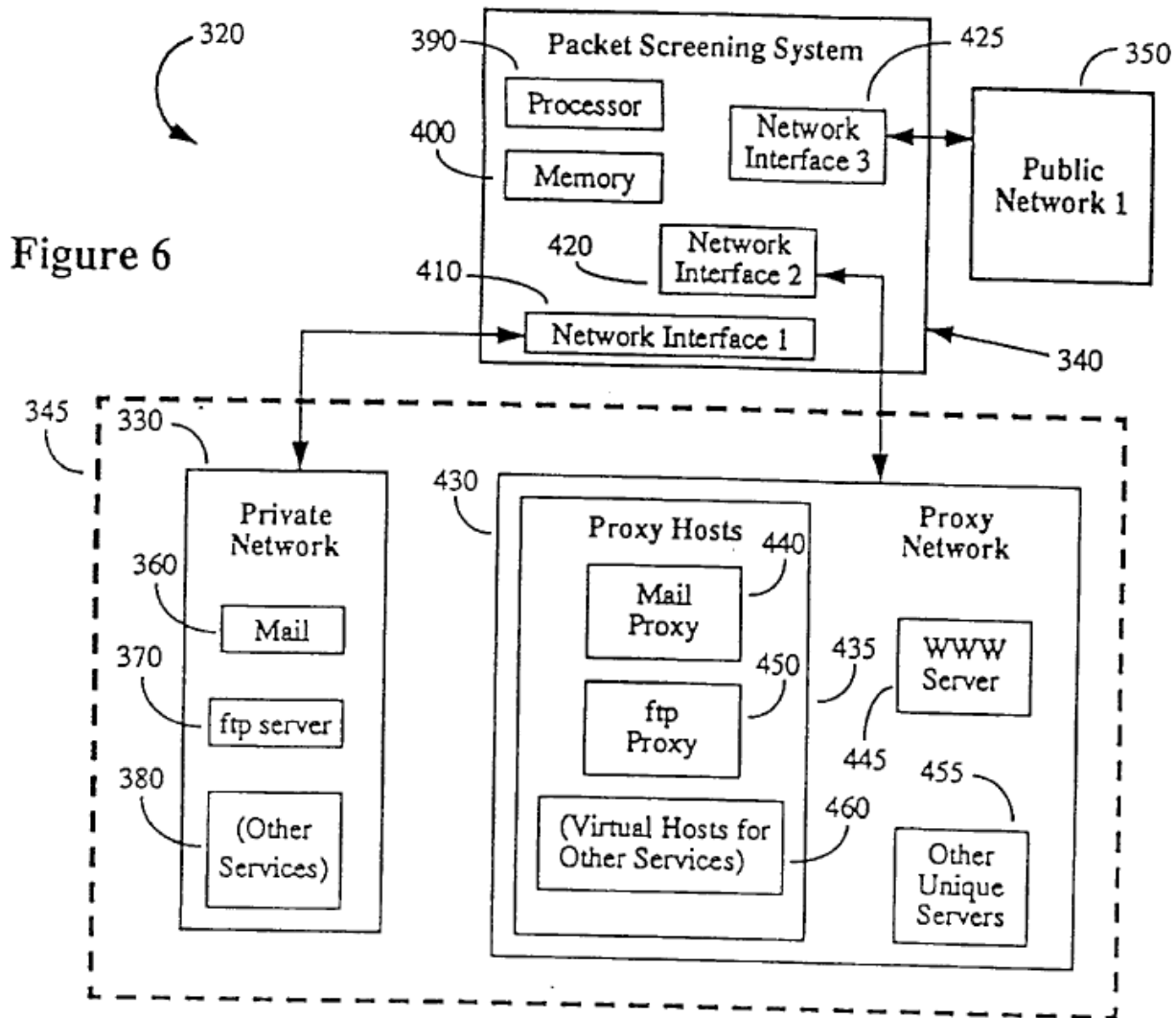
in the prior art. For example, NIST discloses that “dedicated proxy servers are used to decrease the work load on the firewall...” and “can be used to secure less time-sensitive services...” NIST, 14. Baehr also teaches other advantages of its implementation to isolate a private network from an outsider in order to strengthen security. For example, an isolated proxy network “cannot be used as a jumping off point for intruders” because it prevents outsiders from actually accessing the private network. Baehr, *Abstract*, 8:36-47.

163. When a proxy system is implemented as separate from a screen/firewall, the proxy system and the protected private network do not communicate directly with one another; rather, each would communicate separately with the screen/firewall via a separate interface and provide the opportunity for the screen/firewall to inspect any packets sent to or from the proxy. Therefore, having a separate proxy external to a firewall helps isolate the proxy from the private network by positioning the screen/firewall between the two networks. This configuration is also beneficial to limit any potential security vulnerability to only one component of a larger system. For example, even if the proxy system was compromised, the screen/firewall would remain unaffected.

164. It would be routine, straightforward and advantageous to modify Buruganahalli’s system to incorporate Baehr’s teachings of routing to a proxy

external to a firewall. A person of ordinary skill would have known that such a combination (yielding the claimed limitations) would predictably work and provide the expected functionality. Both functionalities described in Buruganahalli and Baehr are transparent to an outsider. For example, Buruganahalli discloses the firewall acts as a remote server such that it is “transparent” to the client. Buruganahalli, 12:17-21. Similarly, the description of Baehr’s proxy system matches with that of a transparent proxy where the proxy is invisible to an outsider and meets the outsider’s request at the same time. Baehr, *Abstract*, 4:50-63 (describing the proxy and network forming “a single apparent domain from the point of view of outsiders... without any indicator being given to the user” that the proxy network is involved in processing the user’s request), 8:36-47 (“invisibly preventing him/her from ever actually accessing the private network”), 8:65-9:7 (“no IP address for the proxy host exists, and none is appended to any packets”). A person of ordinary skill would have expected the modified system to predictably work. For example, in accordance with Buruganahalli’s teachings, when a firewall receives an encrypted packet in a session associated with a suspect domain, the firewall would route the packet to an interface, such as “Network Interface 2” shown in Figure 6 of

Baehr, for processing by a proxy network that is situated external to the firewall.



165. Buruganahalli and Baehr are in the same field of endeavor—data communications and security in a computer network—and are analogous art to the '856 patent. Both Buruganahalli and Baehr are directed to a packet-filtering system to prevent unauthorized access to a network by applying a set of rules for security purposes. For example, Buruganahalli is directed to a firewall to prevent

unauthorized access to a network by applying a set of rules. Buruganahalli, 1:20-39, 2:48-3:24. Baehr is directed to a system for packet filtering of data packets at a computer network interface for protection against attacks. Baehr, Title, Abstract, 2:10-17.

XII. SECONDARY CONSIDERATIONS

166. I understand that Patent Owner raised evidence of alleged secondary considerations regarding the '856 patent in a litigation involving Cisco and in the prior litigation with Keysight. I understand that the underlying evidence is not publicly available and I have not been provided such evidence. I provided an expert report relating to non-infringement in the prior Keysight litigation and do not recall having seen evidence of secondary considerations. To the extent I may have had access to any purported evidence of secondary considerations from the prior Keysight litigation, I do not recall it and I no longer have access to it.

167. At this time, after review of the documents and materials cited herein, such as the prosecution history of the '856 patent, I have found no evidence of secondary considerations or objective factors of non-obviousness relevant to the Challenged Claims, and it is my opinion that Challenged Claims of the '856 patent are obvious over the prior art. To the extent Patent Owner alleges secondary considerations in this proceeding, it is my opinion that they would not outweigh the

strong evidence of obviousness of the '856 patent claims, as set forth herein. I have been informed that if the Patent Owner presents in this proceeding evidence of objective factors that it argues support a finding of non-obviousness, I may be asked to review such evidence and to formulate an opinion and reserve the right to address any such evidence and/or arguments that Patent Owner may raise in this regard.

XIII. CONCLUSION

168. In summary, I have concluded that each of the Challenged Claims is unpatentable as obvious under 35 U.S.C. § 103 in light of the prior art references as discussed above and the knowledge of one of ordinary skill in the art, as described in this declaration.

169. Specifically, in my opinion, for at least the above reasons: Buruganahalli alone or in view of Baehr renders obvious claims 1, 24-25.

170. Furthermore, as discussed in Sections II-III above, I have used my background and experience in forming my opinions that the Challenged Claims are unpatentable as obvious over the prior art.

171. Even if it were argued that any further disclosure is required for a limitation in the Challenged Claims that I have identified above as having been disclosed by the cited references, a person of ordinary skill in the art would have found that limitation obvious to include based on the same disclosure and analysis I

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

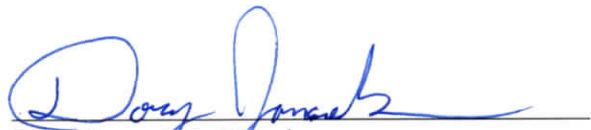
have identified above.

172. I currently hold the opinions expressed in this declaration. But my analysis may continue, and I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me. In signing this declaration, I understand that the declaration will be filed as evidence in a review proceeding before the Patent Trial and Appeal Board of the U.S. Patent and Trademark Office. I acknowledge that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

173. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code and that such willful false statements may jeopardize the results of these proceedings.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

Executed on June 23, 2022 in Ames, Iowa



Dr. Doug W. Jacobson

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

Appendix A

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

IOWA STATE UNIVERSITY
Electrical and Computer Engineering Department

Revised 6/21/2022

I. PERSONAL DATA

Name: Douglas W. Jacobson
Address: 2215 Coover Hall, 515-294-8307
Email: dougj@iastate.edu
Orig. Date of Employment: July 1, 1985
Citizenship: U.S.A.

II. EDUCATION

Ph.D. CprE Iowa State University 1985
M.S. EE Iowa State University 1982
B.S. CprE Iowa State University 1980

III. ACADEMIC EXPERIENCE

1/1/22 – 12/31/22	Stanley Chair in Interdisciplinary Engineering
8/19 - present	Executive Director, Iowa Cyber Hub, Iowa State University
7/08 - present	University Professor Electrical and Computer Engineering, Iowa State University
5/07 – present	Professor Electrical and Computer Engineering, Iowa State University
7/06 – 2011	Director of Undergraduate Education, Electrical and Computer Engineering Department
9/05 – 7/11	Director NSF I/U CRC Center for Information Protection
9/03 – 2018	Computer Forensics Analyst, ISU Police Department
9/01 – present	Director of Graduate Education, Cybersecurity graduate program
11/00-present	Director, ISU Center for Cybersecurity Innovation and Outreach
5/98 – 8/06	Computer Engineering Learning Community Coordinator
7/99 - 2011	Coordinator Active Learning Complex
7/98 - 6/02	Miller Faculty Fellow
7/89 - 5/2007	Associate Professor Electrical and Computer Engineering, Iowa State University
1986 - 6/89	Assistant Professor Electrical and Computer Engineering, Iowa State University
1985 - 1986	Temporary Instructor Electrical and Computer Engineering, Iowa State University

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

IV. INDUSTRIAL AND NON-ACADEMIC EXPERIENCE

I hold a Secret Clearance through DHS to help the State of Iowa recover from a large-scale cyber attack.

1996 - 2010	Founder and Chief Technical Officer Palisade Systems
1983 – 1996	Founded D & D Digital Systems
1982 - 1985	Senior Design Engineer- ISU Computation Center

V. HONORS AND AWARDS

2021	College of Engineering Engineering Extension and Outreach Award
2018	SC Media Professional Award Finalist
2016	Finalist R&D 100 award for ISERink
2013	Distinguished member ACM
2012	2012 IEEE EAB Major Educational Innovation Award
2011	2011 Security & Award (top 7 security professionals)
2011	Fellow IEEE
2010	2010 Cyber 7 Award (top 7 cyber security professionals in government)
2008	Mervin S. Coover Distinguished Service Award
2007	Educator of the Year, Technology Association of Iowa
2006	Distinguished Service Award, Iowa Academy of Science
2005	InfraGard Meeting the Challenge Award
2004	Board of Regents Faculty Excellence Award
2004	Faculty Escort College Engineering summer commencement
2004	ISU Inventor
2003	R&D 100 Award
2003	Warren Boast Undergraduate Teaching award
2003	Certificate of Appreciation, Department of Public Safety
2002	Engineering Student Body, e-Week professor of the semester
2002	Finalist, EY Entrepreneur of the year
2002	Louis Thompson Distinguished Undergraduate Teaching Award
2001	R&D 100 Award
2001	Iowa diVinci Award
2000	Special Recognition Award, College of Engineering LEAD program
1999	ISU Inventor
1999	Wakonse Fellow
1999	Warren Boast Undergraduate Teaching award
1999	Engineering Student Council Outstanding Engineering Professorship in Computer Engineering
1998	College of Engineering Superior Engineering Teacher Award
1998	Engineering Student Council Outstanding Engineering Professorship in Computer Engineering
1996	College of Engineering Superior Engineering Extension Award

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

1995 Eta Kappa Nu
1985 Iowa State University Research Excellence Award
1983 Phi Kappa Phi

VI. ACADEMIC AREAS OF SPECIALIZATION

Teaching

CprE 131 Computer security literacy (13, 14, 15)
CprE 181X Introduction to Computer Engineering I (98F)
CprE 182X Introduction to Computer Engineering II (99S)
CprE 183 Introduction to Computer Engineering and Problem Solving I (99F, 00F, 01F)
CprE 184 Introduction to Computer Engineering and Problem Solving II (00S, 01S, 02S)
CprE 185 Introduction to Computer Engineering and Problem Solving (02F, 03F, 04F, 05F)
CprE 211 Digital Systems Design (95F,96S,96F,97S, 97SS, 97F, 98S, 98F)
CprE 281 Intro to Digital Systems Design (93F,94S,94F,95S)
CprE 284X UNIX and C Fundamentals (89F)
CprE 287 Digital Laboratory I (91F)
CprE 389 Introduction to Design of Computer Based Systems (88F)
CprE 487X PC Bas Intfac Inst (89F)
CprE 489 Data Communications and Computer Networks (87F,90F,91F,93F,94F,96F)
CprE 580 Advanced Computer Networks (88-00)
CprE 530 Advanced Computer Networks (01F, 01S, Every fall 2002 through 2019)
CprE 587X Local Area Network (88F)
CprE 532 Information Warfare (Every spring 1996S through 2020)
CprE 534X Ethics in computer Security (99S)
CprE 592 Seminar (94S,94F)
CprE 632 IA Capstone (09-20)
CprE 631X Security Operations Practicum
CprE 634 Research in IA
CprE 685 Advanced Topics in Local Area Networks (87F,88S,90S,90F)
CprE 699 Research (87F-current)

Course Supervision (Current courses)

CprE 530 Advanced Computer Networks
CprE 532 Information Warfare
CprE 632 IA Capstone
CprE 631X Security Operations Practicum
CprE 634 Research in IA
CprE 131 Computer security literacy

Course Development

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

CprE 181X	Introduction to Computer Engineering I
CprE 182X	Introduction to Computer Engineering II
CprE 183X	Introduction to Computer Engineering and problem solving I
CprE 184X	Introduction to Computer Engineering and problem solving II
CprE 185	Introduction to Computer Engineering and Problem Solving
CprE 211	Digital Systems Design
CprE 281	Digital Systems Design
CprE 284X	Fundamentals of UNIX and C (with J. A. Davis)
CprE 287	Digital Laboratory I
CprE 389	Introduction to Design of Computer Based System (Lab Development)
CprE 685	Advanced Topics in Local Area Networks
CprE 580	Advanced Computer Networks
CprE 532	Information Warfare
CprE 534X	Ethics in computer security (with J. A. Davis)
CprE 587X	Local Area Networks
CprE 632	IA Capstone

VII. GRANTS AND CONTRACTS

Submitted

1. **Jacobson, D.W.**, Julie Rursch. “ISU SFS program”, NSF, \$3,000,000

Funded

1. **Jacobson, D.W.**, Julie Rursch, DoD CySP program, 8/15/21-8/14/22, \$68,917
2. **Jacobson, D.W.** Gilman U.S. Future Leaders Topical Seminar, Department of State, \$17,390
3. **Jacobson, D.W.**, Et.al. “Regional Coalition for Critical Infrastructure Protection, Education, and Practice (ReCIPE),” NSA, 10/1/21-12/31/23, \$2,000,000
4. Qiao, Amariuca, Guan, **Jacobson**, “II-EN: IoT Event Emulation Environment (IoTE³) based on Cyber-Physical Integration”, NSF, 7/1/2017 – 6/30/2019, \$498,077
5. Jacobson, Rursch, “Teaching Security”, NSA, 7/1/2017-6/30/2018, \$280,645
6. M. Govindarasu, **D. Jacobson**, and V. Ajjarapu, "Attack Surface Reduction Tools", DOE, \$1.16M (anticipated total \$2.98M, ISU share: ~\$1.2M), Oct. 1, 2016 - Sept. 30, 2019.
7. Zambreno, et al. “S-STEM WI-ECSEL Scholarship Program (Women in Electrical, Computer, and Software Engineering as Leaders)”, NSF, 7/1/2016-6/30/2021, \$4,054,476
8. **Jacobson, D.W.**, “IT-Adventures”, Technology Association of Iowa”, 9/4/2015-6/15/2016, \$85,000
9. Manimaran, Ajjarapu, **Jacobson, D.W.**, “Risk Modeling and Cyber Defense Exercise for Critical Infrastructure Security (CyDECS)”, NSF, 7/1/2015-06/30/17, \$299,942
10. Manimaran, Ajjarapu, **Jacobson, D.W.**, “CPS: Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments”, NSF, 1/1/2015-12/31/17, \$998,900

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

11. **Jacobson, D.W.**, “IT-Adventures”, Technology Association of Iowa”, 9/4/2014-6/15/2015, \$85,000
12. **Jacobson, D.W.**, Rursch, Daniels, Manimaran “EDU: CPS-CDC - A framework for Cyber-Physical Systems based Cyber Defense Competition”, NSF, 7/1/2013-6/30/2015, \$300,000
13. **Jacobson, D.W.**, Licklider, B., Bergman, C., Wong, J., “SFS Fellowships for information assurance students”, 8/15/14 – 8/14/18, NSF, \$2,377,279
14. **Jacobson, D.W.**, Rursch, J. “IT-Adventures”, Technology Association of Iowa”, 5/1/2013-12/31/2013, \$45,000
15. **Jacobson, D.W.**, Rursch, J. “Information Systems Security Laboratory (ISSL)”, ISU Provost Strategic Initiative”, 8/1/2012-7/30/2014, \$175,000
16. **Jacobson, D.W.**, Rursch, J. “IT-Adventures”, Technology Association of Iowa”, 2/1/2013-12/31/2013, \$45,000
17. **Jacobson, D.W.**, Rursch, J. “IT-Adventures”, Technology Association of Iowa”, 2/1/2012-12/31/2012, \$45,000
18. **Jacobson, D.W.** “IT-Adventures”, Iowa Department of Economic Development, 2/1/2011-12/31/2011, \$50,000
19. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 12/31/10-12/31/15, \$400,000
20. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 12/31/10-12/31/15, \$200,000
21. **Jacobson, D.**, “Iowa community college information assurance and computer security training”, NSF, 9/1/2010-8/30/2012, \$245,303
22. **Jacobson, D.W.**, “NSF I/U CRC Collaborative Research: Security and Software Engineering Research Center (SSERC)”, NSF, 2/10/2010-1/31/2015, \$275,000
23. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 12/31/09-12/31/12, \$650,000
24. **Jacobson, D.W.**, Licklider, B., Bergman, C., Wong, J., “SFS Fellowships for information assurance students”, 5/1/09-4/30/13, NSF, \$1,956,883
25. **Jacobson, D.W.** “IT-Adventures”, Iowa Department of Economic Development, 3/1/2010-12/31/2010, \$50,000
26. **Jacobson, D.W.** “IT-Adventures”, Iowa Math and Science Education”, 5/30/2009-5/1/2010, \$60,000
27. **Jacobson, D.W.** “IT-Adventures”, Iowa Department of Economic Development, 3/1/2009-12/31/2010, \$50,000
28. **Jacobson, D.W.** “IT-Adventures”, Iowa Math and Science Education”, 3/1/2009-5/1/2009, \$43,200
29. Daniels, T., **Jacobson, D.W.** “Scalable Virtual Machine Laboratory Systems”, NSF, 9/1/08-8/31/10, \$180,000
30. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 12/31/07-12/31/10, \$611,000
31. **Jacobson, D.W.** “IT-Adventures”, Iowa Department of Economic Development, 3/1/2008-12/31/2009, \$50,000
32. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 8/1/06-7/31/09, \$148,048

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

33. **Jacobson, D.W.** “High School Cyber Defense Competition”, Iowa Department of Economic Development, 3/1/2007-12/31/2008, \$15,000
34. **Jacobson, D.W.**, Licklider, Daniels, “Scholarship Program”, 8/1/2006-1/31/2008, DoD, \$112,600
35. **Jacobson, D.W.**, Daniels, T. “Programmable security devices”, Boeing, 11/1/2005-6/1/2006, \$15,000
36. **Jacobson, D.W.**, “NSF I/U CRC Center for Information Protection”, NSF, 8/1/2005-7/31/2009, \$230,000
37. **Jacobson, D.W.**, “NSF I/U CRC Center for Information Protection”, 7 companies, 8/1/2005-12/31/2007, \$300,000
38. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 7/1/05-12/31/07, \$496,750
39. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 7/1/05-12/31/07, \$197,329
40. **Jacobson, D.W.**, Licklider, B., Bergman, C., Wong, J., “SFS Fellowships for information assurance students”, 7/1/05-6/30/09, NSF, \$888,008
41. **Jacobson, D.W.**, “Computer Engineering Learning communities”, ISU Provost 2005, \$10,000
42. **Jacobson, D.W.**, “Active Directory Penetration Test”, State of Iowa Department of Administrative Services, 5/24/04-5/23/05, \$6,000
43. **Jacobson, D.W.** “ISEAGE: Internet-Scale Event and Attack Generation Environment ”, Department of Justice, 10/1/04-10/31/05, \$496,750
44. **Jacobson, D.W.**, Davis, J.A., Schmidt, S., Bergman, C., Wong, J., “Information assurance educational support program”, 2003-2004 NSF, \$75,000 Supplemental funding
45. **Jacobson, D.W.**, “Computer Engineering Learning communities”, ISU Provost 2004, \$7,500
46. Guan, Yong, **Jacobson, D.W.**, Davis, J.A. “Cyberspace Forensics: Research, Course Development, and Laboratory Development (Capacity Building Track)”, NSF, \$200,000, 7/1/03-6/30/05
47. **Jacobson, D.W.**, “Cyber Protection Laboratory”, John Deere Foundation, \$30,000
48. **Jacobson, D.W.**, “Computer Engineering Learning communities”, ISU Provost 2003, \$15,000
49. **Jacobson, D.W.**, Davis, J.A., “NSF I/U CRC Cyber protection center: Planning Grant”, NSF, \$10,000
50. **Jacobson, D.W.**, “Computer Engineering Learning communities”, ISU Provost 2002, \$15,000
51. **Jacobson, D.W.**, Davis, J.A., Schmidt, S., Bergman, C., Wong, J., “Information assurance educational support program”, 2001-2003 NSF, \$200,000
52. Davis, J.A., **Jacobson, D.W.**, Miller, C., Bergman, C., Wong, J., “SFS Fellowships for information assurance students”, 2001-2006 NSF, \$2,637,027
53. **Jacobson, D.W.**, “Computer Engineering Learning communities”, ISU Provost 2001, \$22,000
54. Ryan, S., Egbelu, P., Gemmill, D., Min, J., Qamhiyah, A., **Jacobson, D.**, "An enabling system for market driven product design and recycling", 1999, NSF, \$180,002.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

55. **Jacobson, D.W.**, Davis, J.A., Lawson, K., Covert, G., Miller Fellowship "A web-based Information Assurance Awareness Delivery System", July 2000 - June 2001, \$17,500
56. Daniel Berleant (Primary) and Steve Russell, Carolina Cruz-Neira, Julie Dickerson, **Doug Jacobson**, John Lamont, Arun Somani, and Charles Wright, Miller Fellowship, "Using Software Engineering Concepts to Enhance Learning: A Novel Approach", July 2000 - June 2001
57. Barbara Licklider (Primary) and J. Davis, G. Nonnecke, M.J. Oakland, W. Slagle, S. Mickelson, A. Rohach, S. Ravenscroft, M. Wiedenhoeft, B. Keller, T. Boylston, and **D. Jacobson**, Miller Fellowship, " Impacting Students LEA/RNing Through a Faculty Mentoring Program" July 2000 - June 2001
58. **Jacobson, D.W.**, ISU Provost "Support for Project Success", Aug 2000 - May 2001, \$32,000
59. Davis, J.A., **Jacobson, D.W.**, Russell, S, Bergman, C., Wong, J. "Integrated Security Curricula Modules", Total 467,000, NSF, \$325,000, ISU match \$162,000 8/1/99-7/31/02
60. **Jacobson, D.W.**, Davis, J.A., Russell, S, Bergman, C., Wong, J. "NSA Certification of ISSL as a Center of Excellence in Information Assurance Education"
61. **Jacobson, D.W.**, ISU Provost "Peer Mentors for Learning Communities", Aug 1999 - May 2000, \$7,500
62. **Jacobson, D.W.**, Miller Fellowship "Project SUCCESS", July 1999 - June 2000, \$24,000
63. **Jacobson, D.W.**, ISU Provost "Project Success", May 1999 - June 1999, \$8,000
64. **Jacobson, D.W.**, ISU Provost "Peer Mentors for Learning Communities", January 1999 - May 1999, \$1,000
65. Davis, J.A., **Jacobson D.W.** NSA Information Security University Research Program, "Detection of and countermeasures for network denial of service attacks", 8/15/98 - 8/14/01, \$195,226
66. **Jacobson, D.W.**, ISU Provost "Peer Mentors for Learning Communities", September 1998 - December 1998, \$2,000
67. **Jacobson, D.W.**, Miller Fellowship "A Student Centered Approach to Computer Engineering Through Learning Communities", July 1998 - June 1999, \$25,000
68. Evans, M, **Jacobson, D. W.**, Wright, C.W., Maney, A., Vary, J, "International Women in Science and Engineering", ISU Promag, January 1998 - December 1998, \$20,000
69. **Jacobson, D. W.** and Davis, J. A., "Network watchdog," CATD, January 1998 - December 1998 \$49,000.
70. **Jacobson, D. W.** and Davis, J. A., "CISE Research Instrumentation," 1996, NSF, \$49,500.
71. **Jacobson, D. W.** and Davis, J. A., "Network Security," CATD, June 1995 - June 1996, \$60,000.
72. **Jacobson, D. W.** and Davis, J. A., "A Multilevel Security Access Mechanism for Distributed Tasks," NSA, June 1994 - June 1996, \$200,000.
73. **Jacobson, D. W.**, "Network Security Bridge," Department of Commerce, July 1992-June 1995, \$91,800.
74. Director of Computer Systems Affiliate program. \$29,000 in 1990
 - a. \$17,000 in 1993
 - b. \$17,000 in 1992
 - c. \$17,000 in 1991
 - d. \$29,000 in 1990

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

75. **Jacobson, D. W.**, "Real-Time Programming Course," NSF, October 1993 - September 1994, \$3,000.
76. **Jacobson, D. W.**, "NEEDS Image Navigator/NEEDS Access Server," NSF, October 1993 - September 1994, \$42,000.
77. **Jacobson, D. W.**, "NEEDS database," NSF, October 1992 - September 1993, \$35,000.
78. **Jacobson, D. W.**, "Real-Time Control," Fisher Controls, September 1991 - August 1992, \$10,800.
79. **Jacobson, D. W.** and Davis, J. A., Co-Principal Investigators, "A Virtual Transport Protocol for Interconnecting Networks," US West, August 1989 - August 1991, \$97,340.
80. Davis, J. A. and **Jacobson, D. W.**, "3B2 Parallel Processing Upgrade," ISU Engineering College Research Grant, October 1990, \$3,200.
81. **Jacobson, D. W.**, "Local Area Network Protocols for Integrated Voice, Data and Video Services," U S West Advanced Technologies, August 1, 1988 - July 31, 1989, \$40,521.
82. **Jacobson, D. W.**, "Local Area Network Laboratory," Texas Instruments, January 1988 - December 1988, \$46,804.
83. **Jacobson, D. W.**, "Local Area Network Protocols for Integrated Voice, Data and Video Services," Northwestern Bell, July 1987 - July 1989, \$20,000.
84. **Jacobson, D. W.**, "Local Area Network Protocols for Integrated Voice, Data and Video Services," US West Advanced Technologies, July 1987 - July 1988, \$57,000.
85. **Jacobson, D. W.**, "Token Ring Network Laboratory," Texas Instruments, February 1987 - December 1987, \$12,490.
86. **Jacobson, D. W.**, "Network Protocol Analysis," Rockwell-Collins, July 1985 - July 1987, \$108,000.
87. **Jacobson, D. W.** and J. A. Davis, "Distributed Network Performance Monitor," AT&T Information Systems, September 1985 - December 1987, \$25,000.
88. Russell, S. F., Basart, J. P., and **Jacobson, D. W.**, "Research in Networking for HF Frequency Hopping Radio Communication Systems," RCA/Communications and Information Systems Division Grant, December 1985 - March 1986, \$25,000.

Equipment Grants

1. **Jacobson, D.W.**, Davis, J.A. "Security equipment grant" November 2003 Cisco Systems, \$99,930
2. **Jacobson, D. W.**, Equipment Grant from Intermec, November 2000, \$25,000
3. **Jacobson, D. W.**, Software Grant from NFR, December 2000, \$4500
4. **Jacobson, D. W.**, Equipment Grant from Anacot, July 1993, \$4000. (SCSI bus Analyzer)
5. **Jacobson, D. W.**, Equipment Grant from AMD, July 1990, \$36,000. (FDDI interface cards)
6. **Jacobson, D. W.**, Equipment Grant from HP, July 1991, \$75,000. (Network test equipment)
7. **Jacobson, D. W.** and Davis, J. A., Equipment Grant from AT&T, July, 1988, \$89,000.
8. **Jacobson, D. W.** and Davis, J. A., Equipment Grant from Tektronix, December 1987, \$75,280.
9. **Jacobson, D. W.** and Davis, J. A., Equipment Grant from AT&T, July, 1987, \$150,000.
10. **Jacobson, D. W.** and J. A. Davis, Equipment Grant from AT&T, September 1985, \$1,800,000.

VIII. TECHNICAL PUBLICATIONS

Refereed Journals

1. J.A. Rursch, A. Luse and **D. Jacobson**, "Using a Network Testbed and Weekly Skill Mastery Assignments to Facilitate a Real World Final Project in a Networking Course," submitted to *IEEE Transactions on Education*, December 2014.
2. A. Luse, J.A. Rursch and **D. Jacobson**, "Identifying Factors Contributing to IT Major Choice Utilizing A Social Cognitive Career Theory Perspective," *ACM Transactions on Education*, Vol 14, No 3, August 2014.
3. Andy Luse, Brian Mennecke, Anthony Townsend and **Doug Jacobson**, "Employing Interactive Maps to Increase User Utilization of Visualization Mechanisms for Network Security", *The Journal of Information System Security (JISSec)*, Vol 8, Num 3, 2014.
4. Kasthurirangan Gopalakrishnan, Manimaran Govindarasu, **Doug W. Jacobson**, Brent M. Phares, "Cyber Security for Airports". *International Journal for Traffic and Transport Engineering*, 2013, 3(4): 365 – 376.
5. Idziorek, J., Tannian, M., **Jacobson, D.W.**, "The Insecurity of Cloud Utility Models", *IEEE IT Professional*, Vol. 15, Issue 2, pages 22-27, March-April 2013.
6. Luse, Andy; Mennecke, Brian E.; Triplett, Janea; Karstens, Nate; and **Jacobson, Doug** (2011) "A Design Methodology and Implementation for Corporate Network Security Visualization: A Modular-Based Approach," *AIS Transactions on Human-Computer Interaction* (3) 2, pp. 104-132
7. Julie Rursch, Andy Luse, and **Doug Jacobson**, "IT-Adventures -- A Program to Spark IT Interest in High School Students using Inquiry-Based Learning with Robotics, Game Design, and Cyber Defense", *IEEE Transactions on Education*, Vol. 53, Issue 1, pages 71-79, 2009. (IEEE Education Society 2011 Transactions on Education best paper award 2011)
8. Gaitonde, S., **Jacobson, D. W.**, Pohm, A. V., "Bounding Delay on a Token Ring Network With Voice, Data and Facsimile Applications: A Simulation Study," *Communications of the ACM*, January 1990.
9. **Jacobson, D. W.**, et al., "A Master/Slave Monitor Measurement Technique for an Operating Ethernet Network," *IEEE Network*, Vol. 1, No. 3, July 1987.
10. Rowley, W. A., **Jacobson, D. W.**, Jones, M.D. and Clarke, S. L., "A Microcomputer Monitored Mosquito Activity System," *Annals of the Entomological Society of America*, 80(4):534-538, 1987.
11. Clarke, J. L., III, Rowley, W. A., Christiansen, S. and **Jacobson, D. W.**, "Microcomputer Based Monitoring and Data Acquisition System for a Mosquito Flight Mill," *Annals of the Entomological Society of America*, 77(2): 119-122, 1984.
12. **Jacobson, D. W.** and Steffen, D. D., "Low Cost Ski Jump Timer," *IEEE Student Papers*, pp. 302-306, 1980.

Proceeding Articles

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

1. A. Sedighi, **D. Jacobson** and T. Daniels, "T-PKI for Anonymous Attestation in TPM," 2021 IEEE 6th International Conference on Smart Cloud (SmartCloud), 2021, pp. 96-100, doi: 10.1109/SmartCloud52277.2021.00024.
2. A. Sedighi, S. D'Mello, G. Isaacs and **D. Jacobson**, "BitemporalDB: A Bitemporal Database in the Cloud for Financial Services Data," 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 68-73, doi: 10.1109/SmartCloud49737.2020.00021.
3. **Jacobson, D. W.**, & Rursch, J. A. (2020, June), Building a Cybersecurity Engineering Program? Begin by Cloning Your Computer Engineering Program Paper presented at 2020 ASEE Virtual Annual Conference Content Access, Virtual On line . 10.18260/1-2—34232
4. Frickey, E. A., & Rover, D. T., & Zambreno, J., & Khokhar, A. A., & **Jacobson, D. W.**, & Larson, L. M., & Shelley, M. (2020, June), Changing an Electrical and Computer Engineering Department Culture from the Bottom Up: Action Plans Generated from Faculty Interviews Paper presented at 2020 ASEE Virtual Annual Conference Content Access, Virtual On line . 10.18260/1-2—34273
5. Lotfi Ben Othmane, **Doug Jacobson**, Edgar Weippl, Special Issue on Security and Privacy in Smart Cyber-physical Systems, Computers & Security, Volume 87, 2019, 101611, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2019.101611>.
6. Paul Pfister, Mat Wymore, **D Jacobson**, and Daji Qiao, "Design and Implementation of a Cyber Physical Testbed for Security Training," 12th USENIX Workshop on Cyber Security Experimentation and Test (CSET), Santa Clara, CA, August 2019
7. Art Sedighi and **D. Jacobson**. "Forensic Analysis of Cloud Virtual Environments" 2019 IEEE International conference on Computational Science and Engineering, New York, NY, Aug 1-3, 2019.
8. J. -N. Tioh, M. Mina and **D. W. Jacobson**, "Cyber security training a survey of serious games in cyber security," 2017 IEEE Frontiers in Education Conference (FIE), 2017, pp. 1-5, doi: 10.1109/FIE.2017.8190712.
9. J.A. Rursch and **D. Jacobson**. "When a testbed does more than testing - The Internet-Scale Event Attack and Generation Environment (ISEAGE) - providing learning and synthesizing experiences for cyber security students," Frontiers in Education, Oklahoma City, OK, Oct. 23-26, 2013.
10. J.A. Rursch and **D. Jacobson**. "This IS child's play - Creating a playground (computer network testbed) for high school students to learn, practice and compete in cyber defense competitions," Frontiers in Education, Oklahoma City, OK, Oct. 23-26, 2013.
11. Diane T. Rover, Douglas **W. Jacobson**, Ahmed E. Kamal, Akhilesh Tyagi, "Implementation and Results of a Revised ABET Assessment Process", 2013 ASEE Conference, Atlanta, GA. June 23-26, 2013
12. J. Idziorek, J.A. Rursch, and **D. Jacobson**. "Security Across the Curriculum and Beyond," Frontiers in Education, Seattle, WA, Oct. 3-6, 2012.
13. Idziorek, J., Tannian, M., **Jacobson, D.W.**, "Attribution of Fraudulent Resource Consumption in the Cloud", In Proceedings of the 2012 IEEE 5th International Conference on Cloud Computing, pages 99-106, Honolulu, HI. 24-29 June, 2012

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

14. J.A. Rursch, **D. Jacobson** and A. Luse, "Using Content Analysis to Evaluate Student Inquiry-Based Learning: The Case of High School Students Preparing for a Cyber Defense Competition," 2012 ASEE Annual Conference, San Antonio, TX, June 10-13, 2012.
15. J.A. Rursch, **D. Jacobson** and M. Sullivan, "Information Assurance Student Group: How to Turn a Club into a Valuable Learning Experience for Students," 2012 ASEE Annual Conference, San Antonio, TX, June 10-13, 2012.
16. **D. Jacobson** and J.A. Rursch, "Beyond Certifications", Information Security, [Online], 14(9), 11-13,
http://www.bitpipe.com/data/demandEngage.action?resId=1348682836_93, [Nov. 3, 2012].
17. **D. Jacobson** and J.A. Rursch, "End the Bolt On Era", Information Security, [Online], 14(8), 11-13,
http://www.bitpipe.com/data/demandEngage.action?resId=1348682836_93, [Oct. 3, 2012].
18. **D. Jacobson** and J.A. Rursch, "Data/Computer Recovery Guidelines", CIRAS Extension Publication in response to Hurricane Sandy, funded by Department of Commerce's National Institute of Standards and Technology's Manufacturing Extension Program (MEP) [Nov. 8, 2012].
19. Rursch, J., **Jacobson, D.W.**, "The Building of Teams During an IT Competition: Success with Combining Multiple Schools into Teams to Perform Collaborative Challenges During a Two-Day Competition", In Proceedings of the 2011 ASEE Annual Conference. Vancouver, B.C. 26-29 June, 2011.
20. Rursch, J., **Jacobson, D.W.**, "A.A.S. + 2 = Iowa State University Bachelors of Engineering Technology: A Iowa Grassroots Success Story of Developing a 2+2 for "Career Track" Students.", In Proceedings of the 2011 ASEE Annual Conference. Vancouver, B.C. 26-29 June, 2011.
21. Idziorek, J., Tannian, M., **Jacobson, D.W.**, "Teaching Computer Security Literacy to Students from Non-Computing Disciplines", In Proceedings of the 2011 ASEE Annual Conference. Vancouver, B.C. 26-29 June, 2011.
22. Idziorek, J., Tannian, M. and **Jacobson, D.** "Modeling Web Usage Profiles of Cloud Services for Utility Cost Analysis." In Proceedings of the 2011 Winter Simulation Conference (WSC). Phoenix, AZ. 11-14 Dec. 2011. (Invited Paper)
23. Idziorek, J., Tannian, M. and **Jacobson, D.** "Detecting Fraudulent Use of Cloud Resources." In Proceedings of the 2011 ACM Workshop on Cloud Computing Security (CCSW) at CCS. Chicago, IL. 21 Oct. 2011. (Acceptance Rate 13/45 = 29%)
24. Evans, J., Jacobson, D.W., "A Computer Engineering Technology Body of Knowledge", *Proc. Frontiers in Education* (Washington D.C, Oct. 27-29, 2010).
25. Rursch, J., **Jacobson, D.W.**, "Using Cyber Defense Competitions to Build Bridges Between Community Colleges and Four Year Institutions: A Footbridge for Students into an IT Program", *Proc. Frontiers in Education* (San Antonio, TX, Oct. 18-21, 2009).
26. Rursch, J., Burkhardt, B., **Jacobson, D.W.**, "Training Non-IT Teachers to Advise and Facilitate Inquiry-Based Learning in IT: A Pilot Study", *Proc. Frontiers in Education* (San Antonio, TX, Oct. 18-21, 2009).

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

27. Rursch, J., **Jacobson, D.W.**, "IT-Adventures: Turning High School Students "ON" to Information Technology", *Proc. Frontiers in Education* (San Antonio, TX, Oct. 18-21, 2009).
28. Evans, N., Blakely, B., **Jacobson, D.**, "A Security Capstone Course: An Innovative Practical Approach to Distance Education", *Proc. Frontiers in Education* (San Antonio, TX, Oct. 18-21, 2009).
29. Pubali Banerjee, **Doug Jacobson**, "Optimal Configuration of Clustering Protocols for Sensor Networks", 18th IASTED International Conference on Parallel and Distributed Computing and Systems, Dallas, TX, November 13-15, 2007
30. Pubali Banerjee, **Doug Jacobson**, "Optimal configuration of a secure clustering protocol for sensor networks", 20th ISCA International Conference on Parallel and Distributed Computing Systems, September 24-26, 2007, Las Vegas, Nevada, pp. 145-150. ISBN 978-1-880843-64-2.
31. Pubali Banerjee, **Doug Jacobson**, Soumendra Lahiri "Security and performance analysis of a secure clustering protocol for sensor networks", 6th IEEE International Symposium on Network Computing and Applications, Cambridge, MA, July 12-14, 2007, pp134-144
32. **Doug Jacobson**, "Computer Security Summer Camp", InfraGard Guardian 3/30/2006
33. **Doug Jacobson**, Tom Daniels, "Information Assurance Faculty Development Workshop", Proceedings of the 2006 American Society for Engineering Education, Chicago, June 18-21 2006.
34. **Doug Jacobson**, "Computer Security Summer Camp for High School Students", Proceedings of the 2006 American Society for Engineering Education, Chicago, June 18-21 2006.
35. **Doug Jacobson**, Nate Evans, "Cyber Defense Competition", Proceedings of the 2006 American Society for Engineering Education, Chicago, June 18-21 2006.
36. **Doug Jacobson**, "Teaching Information Warfare with Lab Experiments via the Internet", 2004 FIE conference Savanna Georgia, October 20-23.
37. **Doug Jacobson**, James A. Davis "Computer Security Faculty Development Workshop", 2004 FIE conference Savanna Georgia, October 20-23
38. **Doug Jacobson**, "Development of a Graduate Certificate in Information Assurance", Proceedings of the 2004 American Society for Engineering Education, Salt Lake City, June 2004.
39. **Doug Jacobson**, "Teaching Information Warfare with a Break-in Laboratory", Proceedings of the 2004 American Society for Engineering Education, Salt Lake City, June 2004.
40. Tom Richardson, James A. Davis, and **Doug Jacobson**, "Developing a database of vulnerabilities to support the study of denial of service attacks", Second Annual CERT conference, September 27-29, 2000, Omaha, NE
41. Tom Richardson, James A. Davis, and **Doug Jacobson**, "Countermeasures for Denial of Service Attacks", First Annual CERT conference, August 29-31, 1999, Omaha, NE
42. **Jacobson, Doug**, Licklider, Barb, "Freshman year learning communities in a computer engineering program", 2000 FIE Conference October, 2000
43. **Jacobson, Doug**, **Licklider, Barb**, "Project SUCCESS", 2000 ASEE Conference June 2000
44. **Jacobson, Doug**, **Venkata, S.S.**, "An Active Learning Complex: Can Space be used to foster student interaction?" 2000 ASEE Conference June, 2000

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

45. Jacobson, Doug, **Davis James, Licklider, Barb**, "See one, do one, teach one Two faculty member's path through student-centered learning", 1998 **Frontiers in Education Conference, Nov 1998**
46. Jacobson, Doug, **Davis James, Licklider, Barb**, "Ten Myths of Cooperative Learning in Engineering Education", 1998 **Frontiers in Education Conference, Nov 1998**
47. Davis, J., **D. Jacobson**, "Capstone Laboratory Exercise for CprE 532: Computer Security II", Workshop on Education in Computer Security, Pacific Grove, CA January 19-21, 1998.
48. **D. Jacobson**, S. Bridges "Hiring a lifeguard: Keeping your kids safe while surfing the Internet", Techlaunch 2010, Sioux City, IA, September 18, 1997.
49. Davis, J., **D. Jacobson**, S. Bridges, K. Wright, "An Implementation of MLS on a Network of Workstations Using X.500/X.509", IEEE International Performance, Computing, and Communications Conference, Phoenix, AZ, February 5-7, 1997.
50. Hastings, N., J. Whitmer, J. Davis, and **D. Jacobson**, "A Case Study of Authenticated and Secure File Transfer: The Iowa Campaign Finance Reporting System (ICFRS)", IEEE International Performance, Computing, and Communications Conference, Phoenix, AZ, February 5-7, 1997.
51. Chan, S.C.; Minghua Lu; Udpa, S.S.; Udpa, L.; **Jacobson, D.W.**; , "All-optical dense WDM wide-area communication network," *Circuits and Systems, 1996., IEEE 39th Midwest symposium on* , vol.3, no., pp.1157-1160 vol.3, 18-21 Aug 1996
52. Davis, J.A., **Jacobson, D.**, "MLS Access method", INFOSEC Research and Technology Transfer Conference, Baltimore, MA, August 6-8, 1996
53. **Jacobson, D.**, Reddy, S., Kuhl, J., Hassoun, M., Jones, E. C., Jr., "A Course Exchange Using Television," **Frontiers in Education Conference**, November 1994. (Received honorable mention in the best paper competition)
54. Ahuja, R., Gaitonde, S., and **Jacobson, D. W.**, "Design of an Integrated Services Lan Architecture," **Proceedings of the International Conference on Communications**, Denver, Co., June 23-26, 1991.
55. Gercek, G., Ahuja, R. P. S., and **Jacobson, D. W.**, "LAN Interconnection Via Bridges: Congestion Control Issues," **Proceedings of the Infolan 89, Local Area Network Show and Conference**, 1989.
56. **Jacobson, D. W.**, "Design and Implementation of an Integrated Voice, Data, and Video Services Network," **Proceedings of the IEEE Pacific RIM Conference on Communication, Computers and Signal Processing**, Victoria, BC, Canada, pp. 500-505, June 1-2, 1989.
57. Gaitonde, S., **Jacobson, D. W.**, Pohm, A. V., "Bounding Delay on a Token Ring Network with Voice, Data and Facsimile Applications: a Simulation Study," **Proceedings of the Phoenix Conference on Computers and Communications**, Phoenix, AZ, pp. 201-205, March 22-24, 1989.
58. Ghansah, I. and **Jacobson, D.**, "A Prioritized Reservation Protocol for Fiber Optic Ring Local Area Computer Networks," **Proceedings of the 13th Conference on Local Computer Networks**, Minneapolis, MN, October 10-12, 1988.
59. Lee, J. Y. and **Jacobson, D. W.**, "Design and Implementation of the High Performance Integrated Voice/Data Token Ring Protocol," **Proceedings of COMSAC88**, Chicago, IL, pp. 97-104, October 5-7, 1988.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

60. Ghansah, I. and **Jacobson, D.**, "A State-Oriented Architecture Model for Validation and Performance Prediction of Computer Networking Protocols," Proceedings, Nineteenth Annual Pittsburgh Conference on Simulation and Modeling, Pittsburgh, PA, May 1988.
61. **Jacobson, D. W.**, "Network Performance Analysis using Queuing Model Simulation Techniques," Proceedings Eighteenth Annual Pittsburgh Conference on Simulation and Modeling, Pittsburgh, PA, April 23-24, 1987.
62. **Jacobson, D. W.**, "Network Protocol Verification and Performance Analysis using Discrete Event Simulation," Proceedings Eighteenth Annual Pittsburgh Conference on Simulation and Modeling, Pittsburgh, PA, April 23-24, 1987.
63. **Jacobson, D. W.**, "High Performance Multiple Channel Token Bus Protocol," Proceedings IEEE Pacific RIM Conference on Communications, Computers and Signal Processing, Victoria B.C. Canada, pp. 465-468, June 4-5, 1987.
64. **Jacobson, D. W.**, "Token Bus Interconnection Network for Tightly-Coupled Multiprocessor Systems," Proceedings Phoenix Conference on Computers and Communication, Phoenix, AZ, pp. 18-24, February 25-27, 1987.
65. **Jacobson, D. W.**, "Measurement Technique for an Operating Ethernet Network," Fifteenth Annual Computer Science Conference, Proceedings, pp. 458, St. Louis, MO, February 17-19, 1987.
66. **Jacobson, D. W.**, "High Performance Reliable Token Bus for the MAP Network Architecture," Proceedings Conference on Local Computer Networks, p. 27-33, October 6-8, 1986.
67. **Jacobson, D. W.**, "Network Protocol Analysis," Proceedings of Fourteenth Annual Computer Science Conference, (ACM), p. 426, Cincinnati, OH, February 4-6, 1986.

On-Line Articles and Magazines

1. **D. Jacobson**, "stop-doing-these-4-things-online-immediately " Nerdwallet [Online] <https://www.nerdwallet.com/blog/finance/stop-doing-these-4-things-online-immediately/> [10-16-19]
2. **D. Jacobson**, "The Research Question: Keeping research assets safe," EdTech Magazine, Spring 2017, 47-48.
3. **D. Jacobson**, "Is Bitcoin Safe," WalletHub [Online], <https://wallethub.com/blog/is-bitcoin-safe/32920/#doug-jacobson>, [February 28, 2017]
4. **D. Jacobson** and J.A. Rursch, "Security education: Cyber Defense Competitions a major hit on campus," Information Security [Online], 15 (8), 37-40 <http://searchsecurity.techtarget.com/opinion/Security-education-Cyber-defense-competitions-a-major-hit-on-campus>, [November 15, 2013].
5. **D. Jacobson** and J.A. Rursch, "Attack Security Literacy with Brute Force," Information Security [Online], 15(6), 9-11, <http://searchsecurity.techtarget.com/opinion/Attack-security-literacy-with-brute-force> , [September 15, 2013].
6. **D. Jacobson** and J.A. Rursch, "Is Big Data Education a Big Failure?" Information Security [Online], 15(6), 7-9, <http://searchsecurity.techtarget.com/opinion/Is-big-data-education-a-big-failure>, [August 19, 2013].

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

7. **D. Jacobson** and J.A. Rursch, “IT’s Problems with Security Can Spread”, Information Security [Online], 15(5), 8-9, <http://searchsecurity.techtarget.com/opinion/Staff-infection-IT-security-education-is-contagious>, [June 1, 2013].
8. **D. Jacobson** and J.A. Rursch, “Security Education Climbs Corporate Ladder”, Information Security [Online], 15(4), 10-12, <http://searchsecurity.techtarget.com/opinion/IT-security-education-climbs-the-corporate-ladder>, [May 1, 2013].
9. **D. Jacobson** and J.A. Rursch, “Why information security education isn’t making the grade”, Information Security [Online], 15(3), 11-13, <http://searchsecurity.techtarget.com/opinion/Why-information-security-education-isnt-making-the-grade>, [Apr. 1, 2013].
10. **D. Jacobson** and J.A. Rursch, “Information Security Education Options Galore”, Information Security [Online], 15(2), 4-7, <http://searchsecurity.techtarget.com/opinion/Well-rounded-information-security-education-benefits-IT-professionals>, [Mar. 1, 2013].
11. **D. Jacobson** and J.A. Rursch, “Information assurance training programs create new cadre of IT security pros,” Information Security, [Online], 15(1), 4-7, <http://searchsecurity.techtarget.com/opinion/Information-assurance-training-programs-create-new-cadre-of-IT-security-pros>, [Feb. 5, 2013].

Additional online articles and blog posts

<http://www.iowacyberhub.org/index.php/blog/>
<https://futurumcareers.com/can-we-learn-to-be-safe-online>
<https://www.extension.iastate.edu/smallfarms/farmers-and-cybersecurity>
<http://iowacyber.iac.iastate.edu/index.php/2021/07/14/who-has-your-data/>
<http://www.iowacyberhub.org/index.php/working-from-home-resources/>
<https://www.news.iastate.edu/news/2021/11/04/cybersecuritycoalition>
<https://www.news.iastate.edu/news/2019/10/24/dougjchangeagent>
<https://www.ece.iastate.edu/seminars-and-events/seminar-with-doug-jacobson-why-cyber-security-engineering/>
https://openprairie.sdstate.edu/cgi/viewcontent.cgi?article=1006&context=asee_nmws_2020_pubs

Books or Chapters of Books

1. Sedighi A., **Jacobson D.** (2019) Computational Challenges and Opportunities in Financial Services. In: Qiu M. (eds) Smart Computing and Communication. SmartCom 2019. Lecture Notes in Computer Science, vol 11910. Springer, Cham. https://doi.org/10.1007/978-3-030-34139-8_31
2. **Jacobson, D. W.**, Idziorek, J. " Computer Security Literacy: Staying Safe in a Digital World", Chapman & Hall/CRC November 2012.
3. Rursch, J. **Jacobson, D. W.**, "Cyber Defense Competitions as Learning Tools: Serious Applications for Information Warfare Games", a chapter in a book entitled “Serious Games as Educational, Business, and Research Tools: Development and Design” M.M. Cruz-Cunha, Ed., 2012

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

4. **Jacobson, D. W.**, "Introduction to Network Security", ISBN 1584885432, Chapman & Hall/CRC; 1 edition (November 18, 2008)
5. **Jacobson, D. W.**, "Teaching Large Classes Well: A handbook for Faculty in Higher Education" Contributed a chapter "Getting students in a technical class involved in the classroom", ISBN 1-882982-51-7, pp210-220, Anker Press
6. **Jacobson, D. W.**, "Local Area Network (LAN) Lab Manual," Texas Instruments, Dallas, Texas, 1989.
7. Davis, J. A. and **Jacobson, D. W.** "Processor Design Using Microprogramming and Bit-Slice Techniques," Texas Instruments, Dallas, Texas, 1987.

IX. TECHNICAL PRESENTATIONS

1. **D. Jacobson**, Etal, "The Energy Grid" Panel Member, The Gazette's Iowa Ideas 2021, October 14, 2021, Virtual. Invited
2. **D. Jacobson**, "Cyber Security Threats" Ames Rotary Club, October 13, 2021, Ames IA, Invited
3. **D. Jacobson**, Etal, "Future Tech Workforce Cultivators" Panel Member, Future Ready Iowa Summit 2021, September 16, 2021, Des Moines. Invited
4. **D. Jacobson**, Etal, "CyberSecurity – Top ways to protect your business" Panel Member, West Des Moines Chamber business toolkit series, July 27, 2021, Virtual. Invited
5. **D. Jacobson**, "Cybersecurity Threats," Midwestern Legislative Conference, The council of state governments, MLC Agriculture and Natural Resources Committee, July 11, 2021, Rapid City SD, Invited
6. **D. Jacobson**, "cyber security threats" Ames Lions Club, June 24, 2021, Ames IA, Invited
7. **D. Jacobson**. "Cyber Security" Guest lecture Riinvest College in Pristina, Kosovo, April 26, 2021, Virtual, Invited
8. **D. Jacobson**, Etal, "New Era of Cyber Security: Challenges and opportunities" Panel Member, American Chamber of Commerce in Kosovo, Oct 31, 2020, Virtual. Invited
9. **D. Jacobson**, "Cyber Security for local governments" 2020 Iowa Municipal Professionals Institute and Academy, July 30, 2020, Ames IA, Invited
10. **D. Jacobson**, Etal, "Conversation about Cyber-Deterrence/Security" Panel member, 2020 Deterrence and Assurance Academic Alliance Workshop and Conference, STRATCOM, March 11-12, 2020, Ames. Invited
11. **D. Jacobson**, "Cyber Security", ISU SE Club, Ames, IA., Oct 23, 2019, Invited
12. **D. Jacobson**, "Cyber Security", ISU Open Option engineering students, Ames, IA., Oct 16, 2019, Invited
13. **D. Jacobson**, "Cyber Security", State of Iowa Cyber Security Training Session, Des Moines, IA., Oct 11, 2019, Invited
14. **D. Jacobson**, "Cyber security – Risk management", ISU, Ames, IA June 11 2019
15. **D. Jacobson**, T. La Van, "ISEK Cybersecurity Camp", ISU, Ames, IA June 6 2019
16. **D. Jacobson**, "Cyber security panel", ISU EPRC, Ames, IA., May 21, 2019, invited
17. **D. Jacobson**, "Data Security Protecting data in the new threat environment", IEEE ProCon, Cedar Rapids, IA., May 14, 2019, invited
18. **D. Jacobson**, "Cyber Security Engineering", ABET Symposium, Dallas, TX., April 11, 2019

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

19. **D. Jacobson**, “Why Cyber Security Engineering”, IEEE Central Iowa Section, Ames, IA March 28, 2019, invited
20. **D. Jacobson**, “Cyber Security ”, Simpson College, Indianola, IA., March 5, 2019, invited
21. **D. Jacobson**, “Cyber Security Threats: The threat Landscape”, Tech Talk, Mason City Iowa, IA., August 9, 2018, invited
22. **D. Jacobson**, “Cyber Security”, Central Iowa Antique Tractor group, Huxley, IA., March 13, 2018, invited
23. **D. Jacobson**, “Cyber Security”, Ames Realtor group, Ames, IA., Dec 12, 2017, invited
24. **D. Jacobson**, “Cyber Security for Small Business”, Ames Economic Development Commission Board of Directors, Ames, IA., Oct 27, 2017, invited
25. **D. Jacobson**, “Cyber Security for Small Business”, Ames Chamber of Commerce Board of Directors, Ames, IA., Oct 24, 2017, invited
26. **D. Jacobson**, “Cyber Security Threats”, State of Iowa Cyber Security Training Session, Des Moines, IA., Oct 13, 2017, Invited
27. **D. Jacobson**, “Computer Forensics”, Infragard meeting, Ankeny, IA., July 21, 2017, invited
28. **D. Jacobson**, “Cyber Security Panel”, Global Insurance Symposium, Des Moines, IA., April 26, 2017, invited
29. **D. Jacobson**, “Cyber Security Literacy & Resources”, Iowa Communications Alliance, Cyber Summit, Des Moines, IA., April 24, 2017, invited talk
30. **D. Jacobson**, “Home and Business Security”, Central Iowa Section of IEEE, Ames, IA., February 23, 2017, invited talk
31. **D. Jacobson**, “Data Security: protecting data within an organization”, Data Management Association of Iowa (DAMA) , Des Moines, IA., February 21, 2017, invited talk
32. **D. Jacobson**, “Security Literacy”, K-12 Computer Science Conference, Johnston, IA., Dec 13, 2016
33. **D. Jacobson**, “Privacy and Data Security Conference”, Brown Winick Law firm, Des Moines, IA., Dec 9, 2016, Invited member of Panel
34. **D. Jacobson**, “Cyber Security”, College for Seniors, Ames, IA., Oct 27, 2016
35. **D. Jacobson**, “Cyber Security Threats”, State of Iowa Cyber Security Training Session, Des Moines, IA., Oct 7, 2016
36. **D. Jacobson**, “Cryptography and the Internet”, ISSA Conference, DMACC campus, Ankeny, IA, Oct, 4, 2016
37. **D. Jacobson**, “Cyber Security”, Invited talk, Grinnell College, Grinnell, IA, May 26, 2016
38. **D. Jacobson**, “Cyber Security Threats”, Invited talk, Liberty State Bank, Liberty, IA, Jan 27, 2016
39. **D. Jacobson**, “Cyber Security Challenges and Issues”, Invited talk, DES Moines Partnership, Financial Services Council, West Des Moines, IA, Dec 17, 2015
40. **D. Jacobson**, “Cyber Security”, Invited talk, CFO Council, Des Moines, IA, Nov 18, 2015
41. **D. Jacobson**, “ISERange”, Invited talk, National Guard Cyber Senior Leadership, Camp Dodge, Nov 17, 2015
42. **D. Jacobson**, “Email security”, Invited talk, Senator Grassley's Senate Council, Teleconference, Oct 26, 2015
43. **D. Jacobson**, “Cyber Security”, State of Iowa Cyber Security Training Session, Des Moines, IA., Oct 9, 2015

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

44. **D. Jacobson**, “Security Literacy”, Invited talk, Meeting of community bankers, West Des Moines, IA, Sept 10, 2015
45. **D. Jacobson**, “ISEAGE Testbed”, Invited talk, Pacific Northwest National Labs, Pasco, WA, May 13, 2015
46. **D. Jacobson**, “Data Security: Protecting data within an organization”, Invited talk, Iowa DAMA Chapter Meeting, West Des Moines, IA, March 18, 2015
47. **D. Jacobson**, “Cyber Security: The threat Landscape”, Invited talk, Iowa ISACA Chapter Meeting, West Des Moines, IA, March 17, 2015
48. **D. Jacobson**, “Threat Landscape”, Key note speech, Iowa Winter Cyber Working Group, National Guard Headquarters, Johnston, IA, Jan 30, 2015
49. **D. Jacobson**, “Cyber Security”, State of Iowa Cyber Security Training Session, Des Moines, IA., Oct 20, 2014
50. **D. Jacobson**, “Cyber Security”, Safeguard Iowa partnership webinar, Des Moines, IA., Oct 23, 2014
51. **D. Jacobson**, “SFS Program”, George Washington University, Washington DC., August 13 & 14, 2014
52. **D. Jacobson**, J.A. Rursch and Manimaran Govindarasu, “Cyber Security of the Electric Power Grid with Attacks-Defense Training,” Electric Power Research Center, Iowa State University, Ames, IA, July 15-16, 2014.
53. **D. Jacobson**, “Network Security”, ITEC IT Conference, Ames, IA., March 19 & 20, 2014
54. **D. Jacobson**, “Cyber-Terrorism”, Antiterrorism Advisory Council (ATAC), Des Moines, IA, Dec 3, 2013
55. **D. Jacobson** and J.A. Rursch, “Network Security – Vulnerabilities and Exploitation,” Heartland Area Education Association Tech Coordinators Meeting, Des Moines Area Community College, West Des Moines, IA. Nov. 22, 2013.
56. **D. Jacobson**, “Cyber Security”, State of Iowa Cyber Security Training Session, Des Moines, IA., Oct 25, 2013
57. **D. Jacobson**, “Stopping the hidden threat: common sense cyber security”, Iowa Association of Municipal Utilities Energy 2013 Conference, Oct 3, 2013, Des Moines, IA
58. **D. Jacobson**, “Security Literacy: the future of cyber security education”, IEEE Education fair: Envisioning the Future of Science, Technology, and Engineering Education, Oct 24 2013, worldwide video webcast. (Invited speaker)
59. **D. Jacobson**, J.A. Rursch and Manimaran Govindarasu, “Cyber Security of the Electric Power Grid with Attacks-Defense Training,” Electric Power Research Center, Iowa State University, Ames, IA, July 15-16, 2013.
60. **Jacobson, D.W.**, Julie Rursch, “Cyber Security training and Testing”, Corporate Espionage and Cyber Wars conference, International Traders of Iowa , Cedar Rapids, IA, May. 23, 2013. (Invited)
61. **Jacobson, D.W.** “Cyber Threats”, EmbarkIT Emerging Technology Solutions Summit 2013, Des Moines, IA, May. 1, 2013. (Keynote Speaker)
62. **Jacobson, D.W.** “Computer and Network Forensics: CSI - Ames”, Southern Minnesota IEEE section meeting, Rochester, MN, April. 15, 2013. (Invited)
63. **Jacobson, D.W.** “Programming Robots”, Des Moines Area Community College iWeek, Des Moines, IA, March. 4 & 5, 2013. (Invited)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

64. **Jacobson, D.W.** , Julie Rursch, “Information Warfare: Using software to attack computer systems”, Des Moines Area Community College iWeek, Des Moines, IA, March. 6, 2013. (Invited)
65. **Jacobson, D.W.** “Cyber Security Threats”, Iowa Department of Administrative Services Cyber Security Session, Des Moines, IA, Aug. 12, 2012. (Invited)
66. **Jacobson, D.W.** “Information Warfare from a Hackers point of view”, Southern Minnesota IEEE section meeting, Rochester, MN, May. 21, 2012. (Invited)
67. **Jacobson, D.W.** “Starting a High Tech Company: Going from Idea to Patent to Company”, Des Moines Area Community College iWeek, Des Moines, IA, March. 7, 2012. (Invited)
68. **Jacobson, D.W.** “Next Generation of Computer Security Professionals”, 2011 Information Security Conference, Des Moines, IA, Aug. 16, 2011. (Invited)
69. **Jacobson, D.W.** “A safer Community: Avoid Being a Victim via Technology”, Grundy County IA parent group, Grundy Center, IA, Aug. 27, 2011. (Invited)
70. **Jacobson, D.W.** “Computer Security”, Maryland parent group, Baltimore, MD, Oct. 28, 2010. (Invited)
71. **Jacobson, D.W.**, Idziorek, J. "Computer Security Literacy", IBEA, Cedar Rapids, Iowa, Oct. 8, 2010. (Invited)
72. **Jacobson, D.W.** “Computer Security”, Dallas County Rotary, Dallas Center, Iowa, Sept. 28, 2010. (Invited)
73. **Jacobson, D.W.** “Computer Security”, IEEE Central Iowa Section, Ames, Iowa, April 15, 2010. (Invited)
74. **Jacobson, D.W.** “Computer Security”, Iowa ISACA, Des Moines, Iowa, March 16, 2010. (Invited)
75. **Jacobson, D.W.** “Computer Security”, Story County foster parent group, Ames, Iowa, March 11, 2010. (Invited)
76. **Jacobson, D.W.** “ISEAGE”, Computer Science Department Indiana University Purdue University Indianapolis , Indianapolis, IN, April 30, 2010. (Distinguished speaker, Invited)
77. **Jacobson, D.W.** “Information Warfare”, IEEE Central Iowa Section, Ames, Iowa, April 16, 2009. (Invited)
78. **Jacobson, D.W.** “Computer Security”, Newton Rotary, Eldora, Iowa, April 7, 2009. (Invited)
79. **Jacobson, D.W.** “Academic Support for Cyber Safety”, 2009 Cyber Crime Awareness Conference, DMACC, 2/21/2009 (Invited)
80. **Jacobson, D.W.** “Computer Security”, Hardin County foster parent group, Eldora, Iowa, November 18, 2008. (Invited)
81. **Jacobson, D.W.** , Rursch J, “IT-Adventures, ITEC, Des Moines, IA, October 21, 2008
82. **Jacobson, D.W.** “Cyber Crime”, ISSA, Mankato, MN, March 20, 2008. (Invited)
83. **Jacobson, D.W.** “Computer Security”, Senior Citizen group, Des Moines, Iowa, March 4, 2008. (Invited)
84. **Jacobson, D.W.** “Identity Theft”, IEEE Central Iowa Section, Ames, Iowa, February 28, 2008. (Invited)
85. **Jacobson, D.W.** “Computer security”, Des Moines Lions Club, Des Moines, IA, August, 23, 2007. (Invited)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

86. **Jacobson, D.W.** “What’s Transforming the InfoSec landscape” Panel presentation, SoBIS, Metro State, Minneapolis, Minnesota, April 21, 2006. (Invited)
87. **Jacobson, D.W.** “Protecting Critical Network Assets” SoBIS, Metro State, Minneapolis, Minnesota, April 21, 2006. (Invited)
88. **Jacobson, D.W.** “Palisade Systems” Panel presentation, Innovation Iowa, Iowa Board of Regents, Des Moines, Iowa, February 15, 2006. (Invited)
89. **Jacobson, D.W.** “Computer Forensics”, IEEE Central Iowa Section, Ames, Iowa, February 9, 2006. (Invited)
90. **Jacobson, D.W.** “Information Warfare”, Anti-Terrorism Advisory Council – Northern and Southern Districts of Iowa, Des Moines, Iowa, February 7, 2006 (Invited)
91. **Jacobson, D.W.** “Computer Security – How to stay safe in Cyber Space”, 2005 Midwest Election Officials Conference, Overland Park, KS., December 13, 2005 (Invited)
92. **Jacobson, D.W.** “Computer security”, Des Moines Lions Club, Des Moines, IA, December, 13, 2005. (Invited)
93. **Jacobson, D.W.** “Developing a Comprehensive Security Program – How to Avoid Catastrophic Losses”, Iowa Technology Showcase, Des Moines, IA, October 13, 2005 (Invited)
94. **Jacobson, D.W.** “IT Security”, Iowa HIPAA SNIP Work Group Meeting, Des Moines, IA., October 4, 2005. (Invited)
95. **Jacobson, D.W.** “Security Risks in 2006”, Security Leadership Roundtable, Web conference, September, 22, 2005 (Invited)
96. **Jacobson, D.W.** “Design of a Test-bed network for security research”, IEEE EIT conference, May 23, 2005, Lincoln, NE.
97. **Jacobson, D.W.** “Secure your data with identity management”, Iowa Technology Showcase, Des Moines, IA, October 28 2004. (Invited)
98. **Jacobson, D.W.** “Wireless Security”, Iowa Community Action Association training conference, Des Moines, IA., October, 27 2005 (Invited)
99. **Jacobson, D.W.** “Computer Security”, Iowa Community Conference hosted by Congressman Tom Latham, Iowa State University, Ames, IA, May 27 2004. (Invited)
100. **Jacobson, D.W.** “Information Warfare: What is the role of a university in the battle” BIG XII internal Auditors Conference, May 24, 2004, Ames, IA. (Invited)
101. **Jacobson, D.W.** “Computer Engineering Learning Community” Learning Community Institute, May 11, 2004, ISU, Ames, IA. (Invited)
102. **Jacobson, D.W.** “Future of Information Security”, The Academy of Private Investigators, April 30 2004, Des Moines Area Community College, Ankeny, IA. (Invited)
103. **Jacobson, D.W.** “Computer Security” Simpson College, April 15 2004, Des Moines, IA. (Invited)
104. **Jacobson, D.W.** “Computer Security” INC 500 Annual Conference, March 26 2004, Miami, FL. (Invited)
105. **Jacobson, D.W.** “Technology Solutions: The role of Iowa’s Universities”, The Iowa Partnership for Homeland Security, Iowa Business Council, Des Moines, IA, March 12 2004. (Invited)
106. **Jacobson, D.W.** “Computer Security”, Des Moines Rotary, Des Moines, IA, February 19, 2004. (Invited)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

107. **Jacobson, D.W.** "Computer Forensics", Guest Speaker Chem 619 Special Topics in Analytical Chemistry. Forensic Science ISU , IA, January 24, 2004. (Invited)
108. **Jacobson, D.W.** "Computer Security", Simpson College Computer Science Department, Indianola, IA, November 24, 2003. (Invited)
109. **Jacobson, D.W.** "Securing Your Perimeter: Strategies for Protecting Business Assets", Iowa Technology Showcase, Des Moines, IA, October 22 2003. (Invited)
110. **Jacobson, D.W.** "Computer Security", Ames Rotary, Ames, IA, October 22, 2003. (Invited)
111. **Jacobson, D.W.** "Security problems with peer to peer networks", US Senate Judiciary Committee, September 9 2003
112. **Jacobson, D.W.** "Computer Forensics", Symposium on Information Assurance and Security, St. Cloud State University, St. Cloud, MN., April 18 2003. (Invited)
113. **Jacobson, D.W.** "Computer Security", Clear Lake Economic Development Corporation, Des Moines, IA, December 6 2002. (Invited)
114. **Jacobson, D.W.** "Information Warfare: How do hackers hack", Iowa Technology Showcase, Des Moines, IA, October 24 2002. (Invited)
115. **Jacobson, D.W.** "The care & feeding of a security program: A panel group discussion", Iowa Technology Showcase, Des Moines, IA, October 24 2002. (Invited)
116. **Jacobson, D.W.** "Information Assurance at Iowa State University", InfraGard, Des Moines, IA, September 19 2002. (Invited)
117. **Jacobson, D.W.** "Information Assurance at Iowa State University", State of Iowa Security Staff, Des Moines, IA, June 19 2002. (Invited)
118. **Jacobson, D.W.** "Information Assurance at Iowa State University", Iowa Association of Business and Industry, Ames, IA, May 15 2002. (Invited)
119. **Jacobson, D.W.** "Information Warfare", ISACA meeting, Des Moines, IA, March 19 2002. (Invited)
120. **Jacobson, D.W.** "Serve and Secure Iowa", Iowa legislative meeting, Des Moines, IA, February 28th 2002. (Invited)
121. **Jacobson, D.W.** "Information Warfare", IEEE Central Iowa Section meeting, Ames, IA, February 2002. (Invited)
122. **Jacobson, D.W.** "Computer Security Panel Discussion", Iowa Technology Showcase, Des Moines, IA, October 25 2001. (Invited)
123. Davis, J.A., **Jacobson, D.W.** "Computer Security", State of Iowa Conference on Cyber Terrorism and Critical Infrastructure Assurance, STARC Armory April 25, 2001 (invited)
124. **Jacobson, D.W.** "Computer Security", Software Information Technology of Iowa, Annual meeting, March 6, 2001 (invited)
125. **Jacobson, D.W.** "Faulty Entrepreneurship" Entrepreneurship & Innovation at Iowa State University, ISU Memorial Union, March 29, 2001 (invited)
126. **Jacobson, D.W.** "Computer Security", Security Seminar Des Moines Country Club, March 15, 2001 (invited)
127. **Jacobson, D.W.** "Online Privacy and Security", Personal Privacy Issues Study Committee of the Iowa Legislature, Des Moines Capital Building, January 2, 2001 (invited)
128. **Jacobson, D.W.** "Computer Security at ISU", Cert Conference, Omaha, NE, September 27 2000. (Invited)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

129. **Jacobson, D.W.** "Security and Privacy for a Small Business", Iowa Technology Showcase, Des Moines, IA, November 8 2000. (Invited)
130. **Jacobson, D.W.** "Security and Privacy for a Small Business", Iowa Technology Showcase, Des Moines, IA, November 7 2000. (Invited)
131. **Jacobson D.W.** "Faculty Entrepreneurship Experiences", Entrepreneurship & Innovation at ISU Breakfast & Discussion, Ames, IA, October 24, 2000 (Invited)
132. **Jacobson D.W.** "Computer Security", Iowa CIO Forum, Des Moines, IA, October 16, 2000 (Invited)
133. **Jacobson D.W.** "Securing Your Business: What to Fear from the E", Midwest E-Business Conference, September 18-20, 2000 (Invited)
134. **Jacobson, D.W.**, "Palisade Systems: Entrepreneurial Success in Iowa", Iowa Venture Capital Conference, Des Moines, IA, September 6, 2000 (Invited)
135. **Jacobson, D.W.**, "Computer Security", ISU Computation Center, June 30, 2000 (Invited)
136. **Jacobson, Doug**, Venkata, S.S., "An Active Learning Complex: Can Space be used to foster student interaction?" 2000 ASEE Conference, St. Louis, MO., June 18-21, 2000
137. **Jacobson, Doug**, Licklider, Barb, "Project SUCCESS", 2000 ASEE Conference, St. Louis, MO., June 18-21 2000
138. **Jacobson, D.W.**, "Network Security", Palisade Systems Seminar, Des Moines, IA, May 19, 2000
139. **Jacobson, D.W.** "The Benefits of Starting a Business: A faculty Perspective", Entrepreneur Forum, ISU Pappajohn Center, ISU, March 24, 2000 (Invited)
140. **Jacobson, D.W.** "Computer Security", ISU Unix Users Group, March 8th 2000. (Invited)
141. **Jacobson D.W.** "Information Warfare", ISU Scholars Fair, February 26, 2000
142. **Jacobson, D.W.**, Davis, J.A., "Network Security and ISSL", ISACA meeting February 21st 2000. (Invited)
143. **Jacobson, D.W.**, "Brief history of Palisade Systems", Joint State of Iowa Senate/House Economic Development Appropriations Committee, Des Moines, February 1, 2000 (Invited)
144. **Jacobson, D.W.** "Computer Security", Iowa Technology Showcase, Des Moines, IA, December 16th 1999. (Invited)
145. Davis, J.A., **Jacobson, D.W.** "Overview of NSF security education grant", National Security Agency, September 9th 1999. (Invited)
146. **Jacobson, D.W.** "Productivity Management: Keeping your employees on task", Iowa Technology Showcase, December 16, 1999 (Invited)
147. **Jacobson, D.W.** "Computer Security", ISU Society of Women Engineers, November 8th 1999. (Invited)
148. **Jacobson, D.W.** "Reality Works", ISU New Student Days, August 21st 1999.
149. **Jacobson, D.W.**, Jungst, S. "Experiences with Project LEA/RN", ISU College Teaching Seminar 1999, August 18th 1999. (Invited)
150. Richardson, T., Davis J.A., **Jacobson, D.W.**, "Countermeasures for Denial of Service Attacks", First Annual CERT conference, August 29-31, 1999, Omaha, NE.
151. Richardson, T., Davis J.A., **Jacobson, D.W.**, "Developing a database of vulnerabilities to support the study of denial of service attacks", research talk at the 1999 IEEE Symposium on Security and Privacy, May 10, 1999.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

152. **Jacobson, D.W.** "Computer Security in Schools", ICN course for school administrators, April 24th 1999 (invited)
153. **Jacobson D.W.**, Stewart, J "Computer Crime", 1999 International Association of Campus Law Enforcement Administrator's (IACLEA) Region 6 Conference, May 5, 1999 (invited)
154. **Jacobson, D.W.** Davis, J.A., "Hackers, Viruses and Worms (Oh MY!)", Iowa Government Management Information Sciences, April 22, 1999, Gateway - Ames. (Invited)
155. **Jacobson, D.W.** "Computer Security in Schools", ICN course for school administrators, April 24th 1999
156. **Jacobson, Doug**, Davis James, Licklider, Barb, "See one, do one, teach one Two faculty member's path through student-centered learning", 1998 Frontiers in Education Conference, Nov 1998
157. **Jacobson, Doug**, Davis James, Licklider, Barb, "Ten Myths of Cooperative Learning in Engineering Education", 1998 Frontiers in Education Conference, Nov 1998
158. **Jacobson, D.W.**, "Computer & Network Security" IEEE Central Iowa Section, September 10, 1998 (invited)
159. **D. Jacobson**, S. Bridges " Hiring a lifeguard: Keeping your kids safe while surfing the Internet", Techlaunch 2010, Sioux City, IA, September 18, 1997.
160. Davis, J.A., **Jacobson, D.**, "MLS Access method", INFOSEC Research and Technology Transfer Conference, Baltimore, MA, August 6-8, 1996
161. **Jacobson, D.W.** "X.500 / X.509" ISU Comp Center, 1996
162. **Jacobson, D. W.**, Davis, J. A. "Network security" Vet Med College May 6th 1996
163. **Jacobson, D. W.**, Davis, J. A. "Network security" Ames Laboratory, June 5th 1996
164. **Jacobson, D. W.**, "Design and Implementation of an Integrated Voice, Data, and Video Services Network," IEEE Pacific RIM Conference on Communication, Computers and Signal Processing, Victoria, BC, Canada, June 1-2, 1989.
165. Ahuja, R. P. S., Gaitonde, S. S., and **Jacobson, D. W.**, "Internetworking of Token Ring and Ethernet," Iowa Academy of Science, One-Hundredth Annual Meeting, April 23, 1988.
166. Gaitonde, S. S., Ahuja, R. P. S., and **Jacobson, D. W.**, "Performance Investigation of a Document Retrieval System on an Integrated Voice/Data Token Ring," Iowa Academy of Science, One-Hundredth Annual Meeting, April 23, 1988.
167. **Jacobson, D. W.**, "Network Performance Analysis using Queuing Model Simulation Techniques," Eighteenth Annual Pittsburgh Conference on Simulation and Modeling, Pittsburgh, PA, April 23-24, 1987.
168. **Jacobson, D. W.**, "Network Protocol Verification and Performance Analysis using Discrete Event Simulation," Eighteenth Annual Pittsburgh Conference on Simulation and Modeling, Pittsburgh, PA, April 23-24, 1987.
169. **Jacobson, D. W.**, "High Performance Multiple Channel Token Bus Protocol, "IEEE Pacific RIM Conference on Communications, Computers and Signal Processing, Victoria B.C. Canada, June 4-5, 1987.
170. **Jacobson, D. W.**, "Token Bus Interconnection Network for Tightly-Coupled Multiprocessor Systems," Phoenix Conference on Computers and Communication, Phoenix, AZ, February 25-27, 1987.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

171. **Jacobson, D. W.**, "Measurement Technique for an Operating Ethernet Network," Fifteenth Annual Computer Science Conference, Proceedings, St. Louis, MO, February 17-19, 1987.
172. **Jacobson, D. W.**, "High Performance Reliable Token Bus for the MAP Network Architecture," Conference on Local Computer Networks, October 6-8, 1986.
173. **Jacobson, D. W.**, "Network Protocol Analysis," Fourteenth Annual Computer Science Conference, (ACM), Cincinnati, OH, February 4-6, 1986.

X. OUTREACH ACTIVITIES

XIV. Off Campus Courses

National Technological University (NTU) 1996-2004, 24 courses taught.

Engineering Outreach

CprE 530 Advanced Protocols and Network Security	2001 through 2021
CprE 532 Information warfare	1996 through 2021
CprE 587 Local Area Network	F88
CprE 580 Advanced Computer Networks	1986 through 2000
CprE 489 Computer Networks	F86, F87, F91

XV. Tutorials & workshops

1. Gilman U.S. Future Leaders Topical Seminar, Dec 10-11, 2020. US Department of State
2. **D. Jacobson**, "Computer security literacy professional development workshop", Johnston, IA, Jun 10 & 20, 2016
3. **D. Jacobson**, "Cyber Security Curriculum, presented to Iowa High schools", Ames, IA, Aug 10-12, 2015
4. **D. Jacobson**, "Computer Security Literacy workshop for middle school teachers", AEA 11, Johnston, IA, Aug 3-4, 2015.
5. **D. Jacobson**, "National Guard Training exercise", Ames, IA, July 11-12, 2015.
6. **D. Jacobson**, J.A. Rursch and J. Idziorek, "Teaching Computer Security Literacy to the Masses: A Practical Approach," workshop for Frontiers in Education, Seattle, WA, Oct. 3-6, 2012.
7. **D. Jacobson**, J.A. Rursch and J. Idziorek, "Teaching Computer Security Literacy to the Masses: A Practical Approach," workshop for Frontiers in Education, Seattle, WA, Oct. 3-6, 2012.
8. **D. Jacobson** and J.A. Rursch, "Iowa Community College Information Assurance and Computer Security Training," National Science Foundation Scholarship for Service program, Ames, IA, June 4-8, 2012.

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

9. **D. Jacobson** and J.A. Rursch, "Information Warfare," National Science Foundation Scholarship for Service program, Ames, IA, semester long online course for community college faculty, Jan.-May, 2012.
10. **D. Jacobson** and J.A. Rursch, "Iowa Community College Information Assurance and Computer Security Training," National Science Foundation Scholarship for Service program, Ames, IA, June 6-10, 2011.
11. **D. Jacobson** and J.A. Rursch, "Advanced Protocols and Network Security," National Science Foundation Scholarship for Service program, Ames, IA, semester long online course for community college faculty, Jan.-May, 2011.
12. **Jacobson, D.W.** & Rursch, J.A. "Community College Cyber Security Workshop," ISU, June 6-9, 2011
13. **Jacobson, D.W.** & Rursch, J.A. "Cyber Security Workshop," presented at DMACC, (Des Moines, IA, March 4, 2010)
14. **Jacobson, D.W.** & Rursch, J.A. "Cyber Intrusion Workshop," presented at Working Connections IT Conference, (Council Bluffs, IA, June 22-26, 2009)
15. **Jacobson, D.W.** & Rursch, J.A. "Workshop - Using Cyber Defense Competitions (CDCs) to Engage and Recruit Students with IT: How to Organize and Run Your Own Cyber Defense Competition," in *Proc. Frontiers in Education* (San Antonio, TX, Oct. 18-21, 2009).
16. **Jacobson, D.W.** "Computer security", ISACA, May 30 – June 1 2007
17. **Jacobson, D.W.** "Authentication Methods", ISU ADP July 31, August 2,4 2000 (Invited)
18. **Jacobson, D.W.** "Authentication Methods", ISU ADP July 31, August 2,4 2000 (Invited)
19. **Jacobson, D.W.** "Authentication Methods", ISU Computation Center July 26, 27, 28 2000 (Invited)
20. **Jacobson, D. W.** and Davis, J. A., "Current technology in Computer Security" (IEEE), ICC 98, Atlanta, GA, June 11, 1998.
21. **Jacobson, D. W.** and Davis, J. A., "Introduction to Computer Security and Current Technology in Computer Systems Security" (IEEE), Phoenix Conference on Computers and Communication, Phoenix, AZ, March 27, 1996.
22. **Jacobson, D. W.** and Davis, J. A., "Internetwork Systems," (IEEE), Phoenix Conference on Computers and Communication, Phoenix, AZ, March 16, 1988.
23. **Jacobson, D. W.** and Davis, J. A., "Internetworking," 12th Conference on Local Computer Networks, Minneapolis, MN, October 5, 1987.

XI. PATENTS

1. **Jacobson, D.W.** and J.A. Davis. "Network Connection Blocker, Method, and Computer Readable Memory for Monitoring Connections in a Computer Network and Blocking the Unwanted Connections." US Patent #6,044,402, awarded March 28, 2000
2. **Jacobson, Douglas,** "Network Security Bridge and associated method." US Patent #5,548,649, Awarded Aug 20, 1996

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

XII. GRADUATE STUDENTS

XVI. MS Non-Thesis Degrees

1	2021	Enhancing Cyber Insurance Underwriting Through Existing Security Frameworks *	Garza, Christopher
2	2021	A Defense in Depth Architecture for Cloud Security	Dickman, Eric
3	2021	Splunk, ISERink integration	Adb Elmaji, Fatima
4	2020	Research work on cybersecurity frameworks	Raza, Haider
5	2020	Network Management: Developing a Training Curriculum	Newton, Keegan
6	2020	Using Message Precedencies Similarity to Detect Message Inject in in-vehicle network *	Jedh, Mubrak
7	2020	Splunk, ISEAGE integration	Hurst, Shanell
8	2020	Hackerville	Hasstedt, Joshua
9	2020	Hackerville	Brimingham, Alec
10	2019	Log Analysis in Cyber Threat Detection	Awotipe, Oluwaseur
11	2019	Utilizing Cloud Computing Log Events for Security Automation	Farrag, Khalid
12	2019	MFAProxy: A reverse proxy for multi-factor authentication	Schmitz, Alan
13	2019	Internet of Things	Balakrishna Rao, Vismayashree
14	2019	Utilizing Cloud Computing Log Events for Security Automation	Farrag, Khalid
15	2019	Existence of Dependency-Based Attacks in NodeJS Environment *	Patel, Prachi R
16	2019	Aggregation, indexing and visualization using the ELK Stack	Beadle, Bradlee
17	2019	A cyber focused table top exercise for Iowa State University	Garrison, Christopher
18	2019	An analysis of the evolution of botnets	Stephan, Cole
19	2019	Upgrades to ISEFlow: Offloading ARP and supporting IPv6	May, Joel
20	2019	Cyber Defense Competition Card Game	Luckinbill, Ryan
21	2019	Literature survey on IPv6 over Low-power Wireless Personal Area Networks	Mathew, Roshan
22	2018	A simple moving target defense for power grid security using network address translation"	Ulrich, Jacob
23	2018	ISEMan: A management and deployment interface for lab-based activities within ISERink	Luehm, Alex
24	2018	Implementation of an Information Security Program for a City Government	Tran, Minh
25	2018	Creating a Malware Analysis Lab and Basic Malware Analysis	Peppers, Joseph
26	2018	A Survey of the Vulnerabilities and Performance Issues with the Internet of Things	Hayden, Ben

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

27	2018	Dynamic and System Agnostic Malware Detection Via Machine Learning	Sgroi, Michael
28	2018	Using Blockchain to Maintain the Integrity of Legal Documents and Evidence	Henely, Eric
29	2018	Redbot: an automated and distributed red team and traffic generation system	O’Kelly, Keanne
30	2018	Building Blocks of Commercial Crypto-Technologies Solutions	Kincaid, William
31	2018	Vulnerability Assessment of Skybell HD Doorbell	Miller, Travis
32	2017	Current Firewall Technologies and: Proposal for a Threat Intelligence Correlation and Rule Engine	Eberle, Eric
33	2017	RATs, Techniques and mitigations in the Enterprise	Bowcut, Jeremy
34	2017	A Raspberry PI 3 Device used as Hardware for Snort Intrusion Detection Software	Groom, Jerry
35	2017	P2P Botnet Communications Testing	Wilson, Joseph
36	2017	Malware Analysis and Mitigations in the Enterprise	Clancy, Patrick
37	2016	Automated Virtual Network Creation System	Wiemers, Ben
38	2016	Browser hacking Methodology	Giampa, John
39	2016	Implementing Effective Information Security Governance in a Decentralized Local Government Institution	Lafosse, Ricardo
40	2016	Network Defense Risk-Assessment through Aggregation of Established Attack Graph Methodologies	Poczatek, Alec
41	2016	The Design and Implementation of a CPS-CDC for ISEAGE	Pfister, Paul
42	2015	Design of a Cyber-Physical Systems Cyber Defense Competition	Weidman, Matthew
43	2015	Creating a social engineering teaching tool	Rodine, Eric A
44	2015	Analysis of DoS attacks and Mitigations: In relation to common game network models	Farrington, Christopher
45	2014	The Utility and Limitations of Radio Frequency Identification	Cisek, Lukas
46	2013	Exploit Avoidance Training	Koster, David M
47	2013	Security in Curriculum	Fredrickson, Christian
48	2013	Design and defense of the Guilder network and attacks	Miller, Brad M
49	2013	Modeling SELinux type enforcement security in AADL	Morrissey, Patrick J
50	2013	Cookie Cadger: An Auditing Tool for Wi-Fi or Wired Ethernet Connections	Sullivan, Matthew E
51	2013	Security in Curriculum	Fredrickson, Christian
52	2012	Online Banking Authentication Augmentation	Williams, Jeffery
53	2012	Ninja CTF: The Community Driven Capture the Flag Site	Melvin, Jeffrey
54	2012	Modernizing 532 Corp	Kirwin, Kevin
55	2012	ISECatch: A Framework to Capture, Filter and Monitor	Li, Dan

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

		Network Traffic for ISEAGE	
56	2012	Creating an Agile Software Framework to Increase the Effectiveness of Information Assurance Education	McAllister, Josh
57	2011	Network-enabled entertainment devices and their security implications	Hart, Shelly
58	2011	Examining crucial aspects of National Computer Incident Response Team establishment in developing countries	Mangaali, Nelson
59	2010	ISEStorm: An implementation of many unique virtual access points on a single platform	Risse, Daniel
60	2010	Cryptographic s-box analysis, design and implementation	Minyard, Nancy
61	2010	Random Automated Scanning Utility	Rabe, Mark
62	2010	Using WebGoat to understand web security: examining vulnerabilities, exploits, and countermeasures	Goodwyn, Ron
63	2010		Chan, Jenny
64	2010	CostumeDB	Tinkham, Josh
65	2009	Green IT & Security	Liu, Shuer
66	2009	Cyber security of industrial control systems with assessment of HART industrial protocol	Gade, Mahesh
67	2009	ServPass” Server-Based Password management	Moerk, Mike
68	2009	Secure Computing via Security-Enhanced Linux	Smith, Ryan
69	2009	Engineering Secure Software Systems	Kirkhhoff, Jason
70	2009	Analysis of Information Security Exercise Architectures	Kruse, Brian
71	2009	Secondary User Authentication Methods based on Wireless LAN Location Tagging by Wireless Mobile Devices	Chen, Min-Hsao
72	2008	Enterprise-wide Information Security Compliance Management	Williams, Megan
73	2008	Primary Direct Healthcare Provider Performance: Compiling, Warehousing, Securing, and Presenting Data	Williams, Jeremy
74	2008	Auto Red Team (ART): A network attack automation framework based on decision learning tree	Lu, Song
75	2008	Mobile Ad Hoc Network Security	Rolfes, Mark
76	2007	Certification of Industrial Security	Burkhardt, Bryan
77	2007	A high bandwidth to low bandwidth network appliance for legacy communication infrastructures in remote industrial control applications	Bryngelson, Ryan
78	2007	An architecture for secure command encryption and telemetry decryption	McVicker, Kenneth
79	2007	The use of digital forensics in investigating corporate system attacks	Musa, Fadl
80	2007	A study of performance and characteristics of computer security experimental testbeds	Haddush, Nesreen
81	2007	KIDO.S. Operating System for Kids	Coughlin, Brian
82	2006	A scalable – business enabling framework for strategic malware threat and incident mitigation within an	Alexander, Brylan

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

	organization	
83	2006 Using Electronic Design Automation Tool Integration Environment for Static Timing Analysis	Corbett, Matthew
84	2006 Anatomy of an Insecure Web Application	David Linder
85	2006 Cellular Automata: An Application in Cryptography	Susan Helser
86	2005 Analysis of InfiniBand Security	Bailey, Dave
87	2005 Real-time UART control in ADA	Rowenhorst, Bruce
88	2003 A study of Information Assurance Technologies related to Networking	Ray, Niloy
89	2003 Commercial Integrated Modular Avionics*	Daley-Fell, Adam
90	2003 Safety-Critical Systems design in a UML Model-Based Environment	Jacobowitz, Brian
91	2002 Client-server based Internet Communication & analyzing software for NIR instrumentation	Dzupin, Robert
92	2002 Enhancing wireless network security IEEE 802.1X	Qleibo, Haider
93	2002 Reducing SIP Call Setup Latency in CDMA 2000 Networks	Bergan, Patrick
94	2002 Lifecycle of a LINUX cluster	Orman, David
95	2001 Task Analysis Tool	Mueggenberg, Craig
96	2001 Software Requirements for Avionics Systems	Feldkamp, Keith
97	2001 Structural Coverage Analysis of a Dynamic Device Driver*	Radack, David
98	2001 Performance Comparison and a new QoS routing protocol for Ad Hoc Networks	Lin, Bin
99	2001 767 Desktop Simulation	Dineen, Tom
100	2000 Web Server Development Using Java	Jiang, Shuguang
101	2000 Security Impact of Changes on the Internet	Buhr, Orlin
102	2000 The Love-Bug and ways to Avoid Future Virus Attacks	Li, Tianshi
103	2000 Hardware and Software Design for the Control of a New Scanning Pulsed Eddy-Current System	Xu, Wen
104	2000 Prospective Applications of Java Language and Java Platforms in Embedded and Real-time Systems	Yang, Jinchao
105	2000 Secure Socket Layer	Zhong, Jie
106	2000 Virtual Private Network Technology	Chen, Jinyuan
107	1999 Security on the World Wide Web	Lam, Loius
108	1999 Integrated security models in an Unix and NT environment	Cheng, Xiaohua
109	1999 Remote Sharing of Applications across platforms	Zhang, Lei
110	1999 DLXV: A vector Architecture Extension for DLX	Sama, Kiran
111	1999 WINSOCK2 Quality of Service Application Programming Interface	Haverkamp, David
112	1999 Mobile Agent Technology for distributed network computing: information retrieval	Aji, Pandu
113	1999 Security on the World Wide Web	Zhang, Benqun
114	1998 An implementation of a distributed multilevel access control system	Richmand, Colin
115	1998 Detection of DNS probes	Michael, Scott

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

116	1998	ATM Signaling	Ansari, Muhammad
117	1998	X.500 Directory Service	Zhang, Jing
118	1998	HTTP traffic analyzer	Bull, Axel
119	1998	Effective System Functional Testing	Bejarno, Anthony
120	1998	Tomographic Inspection System Redesign and Remote Control	Yang, Zhou
121	1998	Overview of SS7 (MTP level2 & Level 3)	Chahal, Ajay
122	1998	Intrusion Detection Systems	Xu, Lianlian
123	1998	Security using Audit files	Yu, Jingchu
124	1997	Desktop network topologies related to Ethernet upgrades & ATM networks	Chen, Wei
125	1997	Integration of DNSSEC (keyserver) with SSH application	Dash, Sunita
126	1997	Packet Editor / Responder	John, Tara
127	1997	A framework for achieving non-reputability of web based transactions in electronic commerce	Apsani, Lavanya
128	1997	Low-cost Link Encrypter	Rajesh Gandhi
129	1996	Fault tolerant Communications in a railroad environment	Haag, Robert
130	1996	Network Security Topologies	Cheng, Xinhong
131	1996	Logic programming and Deductive database	Tang, Yanguo
132	1996	A world Wide Web Search Engine	Balsara, Cyrus
133	1996	Network security - protocols	Morampudi, Chandra
134	1995	Business on the Internet: the next step	McClellan, Paul
135	1995	Network Security -- Firewall	Chen, Zai
136	1992	Microprocessor Based Baler Controller	Zacharia, Pavlos
137	1991	Vincent Network Analysis	Willoz, Aimee
138	1989	Interconnecting of Ideal Area Networks	Sadrerafi, Ezzatollah
139	1988	PRISM: Fault Tolerant Data Communications for Multiprocessing Applications	McGahee, Kevin

Masters Degree Theses

1.	2020	Implementation of Network Moving Target Defense in Embedded Systems	Finstad, Robert
2.	2020	Distributed Public Key Based Computing: The Super Virtual Computer	Monaghan, Zachary
3.	2019	Regsym – Dataflow Analysis of Linear x86 Code *	Foudree, Grant
4.	2018	Security Awareness Training in a Corporate Setting	Dugan, Nichole
5.	2018	Virtual ICS Test Bed	Brooks, Roxanne
6.	2018	A rotational moving target defense solution for web servers	Bisinger, Steffanie
7.	2017	Detecting Drones using Machine Learning	Waylon Scheller
8.	2017	ISEConf: A management tool for the ISEAGE Environment to allow users to create a custom mock internet for testbed research	Neel, Jeff
9.	2017	Markov Chain Analysis of packet sequence for intrusion	Bockholt, Chad

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

		detection *	
10.	2016	Device fingerprinting identification and authentication: A two-fold use in multi-factor access control schemes	Manning, Paul
11.	2016	Hackerville: A laboratory environment for security literacy	Van Roekel, John
12.	2016	Application of Active Device Authentication Mechanisms	Schlue, Matthew
13.	2016	A User driven cloud based multisystem malware	Cain, Brian
14.	2015	A Cruel Angel's Thesis: A Quantitative Study of Online Privacy Values Dependent on Social Factors	Czalbowski, Arielle
15.	2013	Mobile Device Policy Framework	Putney, Curtis
16.	2012	The CDC in a box Project	Cross, Jason
17.	2012	First Responder Assistance tool for Mobile Device Forensics	Kallal, Benjamin
18.	2012	Design and Evaluation of delay based FPGA physically unclonable function *	Mills, Aaron
19.	2011	SCADA Honeynets: The attractiveness of honeynets as critical infrastructure security tools for the detection and analysis of advanced threats	Wade, Susan
20.	2011	Greater Sustained throughput in IEEE 802.11 and contention elimination with DS-CDMA*	Plass, Bryan
21.	2011	Network-enabled entertainment devices and their security implications	Hart, Shelly
22.	2011	Virtualized guest live migration profiling and detection	Nirschl, Joey
23.	2010	A low-cost connection aware, load-balancing solution for distributing Gigabit Ethernet traffic between two intrusion detection systems	Jackson, Adam
24.	2010	Integrating Modern business methodologies and behavior factors to better apply information technology security practices with the organization	Edwards, Brian
25.	2008	Web Application vulnerability detection using automated tools	Johnson, Eric
26.	2008	Crawler 2.0: A search tool to assist law enforcement with investigations	Harkness, Dan
27.	2008	SnoScan: An Iterative functionality scanner for large networks	Murphy, Jon
28.	2008	High Performance password cracking by implementing rainbow tables on nVidia graphics cards	Graves, Russell
29.	2008	Condenser: A custom tool for capturing and summarizing network traffic for avalanche and ISEAGE	Maughan, Jason
30.	2008	Cryptic backup: A framework for automated compression, encryption, and backup of data.	Hoff, Christopher
31.	2008	ISEHARVEST: TCP packet data re-assembler framework for network traffic content	Eilers, Stephen
32.	2008	Intercept system to edit, control, and analyze packets (ISECAP)	Btinkmeyer, Grant

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

33.	2007	Internet Scale Endpoint Management	Gillispie, Thad
34.	2007	Polymorphic malware detection	Shanklin, Teresa
35.	2007	DeepFreeze: a management interface for ISEAGE	Karstens, Nathan
36.	2007	Automation in digital photo management	Brady, Benjamin
37.	2007	Security Integrated Messaging – a protocol for secure electronic mail	Hoernecke, Andrew
38.	2007	Customization and Automation in the future of digital forensics: Live OS forensics with FENIX (Forensic Examiner UNIX)	Howard, Sean
39.	2007	The Intrusion Collector and Emulator	Wilden, Matthew
40.	2007	Designing an interactive visualization for intrusion detection systems with video game theory and technology	Paustain, Shane
41.	2006	ISECUBE – A portable ISEAGE	Rathje, Ryan
42.	2006	Network Services for Large Scale Distributed Science Instruments	Metzger, Joe
43.	2006	Advanced Packet Obfuscation and Control Program (APOC)	Hahn, Adam
44.	2006	Medium Resolution computed Tomography through Phosphor Screen Detector and 3D Image Analysis*	Sheikh, Nadia
45.	2005	Network Centric Operations Infrastructure Considerations	Clark, Joe
46.	2005	Secure Group Communications Protocol and Implementation for JetMeeting, an Application Based on P2P	Li, Yan
47.	2005	Hiding out in plaintext: covert messaging with bitwise summations	Perkins, Michael
48.	2005	A Modular Architecture for Critical Events (MACE)	Openshaw, Pascal
49.	2005	A definitive way to block unsolicited Internet e-mail	Davis, Justin
50.	2005	Roaming user-based distributed firewalls	Luse, Andrew
51.	2005	An Autonomous Approach to Proactive Computer Crime Investigation	Korba, Noah
52.	2005	Using Nodes in a Cluster Efficiently *	Li, Ying
53.	2005	Design and Development of Network Traffic Simulator	Houghton, Douglas
54.	2004	Benchmark with Small Business Database Module	Zhu, Yancong
55.	2004	The design and development of SNIP (simple network imitator program)	Myers, Brett
56.	2004	A Method for Classifying Attack Implementations Based Upon its Primary Objective *	Ryon, Luke
57.	2003	A Comparative study of routing protocols in MANETs*	Ali, Muhammad
58.	2003	Wireless Security for Secure Facilities	Mitchell, DeAntrious
59.	2003	A systematic security analysis of the AODV protocol*	Jones, Ben
60.	2003	Development of a high resolution 3D computed tomography system: data acquisition, reconstruction and visualization*	Zhang, Jie
61.	2002	FileAccessManager: A Key Management Program	Whitaker, Katherine

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

		Including an Implementation of RFC 2945: The SRP Authentication and Key Exchange System	
62.	2002	Blocking API calls for security	Truckenmiller, James
63.	2002	Deadlock detection in MPI programs *	Zou, Yan
64.	2001	Three-Dimensional free-hand Ultrasound imaging system for medical applications*	Wang, Bo
65.	2001	Establishing security and privacy policies for an on-line auction	Meiners, Michael
66.	2001	High-resolution CT data acquisition software and 3D visualization tool	Fan, Peng
67.	2001	Design and implementation of real time image acquisition and processing systems	Liu, Junhong
68.	2001	Scanning macro virus in Microsoft Word files macros under UNIX operating system	Zhang, Wei
69.	2001	System Security for Windows for Personal Computers (WINDS)	Khan, Tauquir
70.	2000	Implementation of Integrated Computer Control for X-ray Material Characterization Systems*	Lu, Huaifu
71.	1999	Implementation of a site survey application	Hammer, Terry
72.	1999	Portable networking software for near-infrared instrument	Siska, Juraj
73.	1998	Test-case Development for an Industrial, Multi-Tasking, Embedded Operating System via Reverse Engineering, Equivalence Partitioning, and Boundary Value Testing	Zhu, Zhaobin
74.	1997	Creation of an advanced network embedded system software environment	Schwadrer, Curtis
75.	1996	Automation of real time X-Ray Scans *	Midhe, Madhushdhan
76.	1996	A novel Inspection systems for aircraft engine turbine disks *	Bohra, Naveen
77.	1996	An implementation of multi-level security for distributed applications using X.500/X.509	Bridges, Stephanie
78.	1996	Fault tolerant distributed computing system for heterogeneous network: application to non-destructive testing *	Gadiyar, Vivek
79.	1996	Mplayer: A software-only design and analysis of a MPEG-1 systems player	Kaas, Gerald
80.	1996	Network Protocol guard	Omdahl, Svein-Tore
81.	1995	Home Automation via a Telephone Line	Waters, Tim
82.	1995	An Internet Information Browser for use in a Digital-Audio/Video Interactive-Decoder Environment	Thompson, Brent
83.	1995	Performance Model of AFS Using OPNET	Morampudi, Chandra
84.	1995	Stereography for Flaw Inspection *	Nutakki, Gangdhar
85.	1995	Multimedia Presentation in a Distributed Environment	Prasad, A. N.
86.	1995	Remote control of X-Ray Hardware *	Puvvadi, Sudha
87.	1994	Remote Service on a Mid-Range Computer System	Sokhey, Sarab

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

88.	1995	Design and Implementation of Networked NEEDS Database	239.50	Xioug, Siqiang
89.	1994	High Speed Computer Tomography System		Kasiviswanathan, Rangarajan
90.	1994	Performance Measurement of NFS Using OPNET		Seetharaman, Dhiraviam
91.	1994	LAN Interconnection Using ATM		Damm, Kurt
92.	1994	Practical Network Security		Kroymann, Kenneth
93.	1994	Distributed Instrumentation System on a Local Area Network		Arsikere, Amarnath
94.	1994	Methods of Multiple Access to an Aeronautical Satellite Communications Network: Simplifying Multiple Access Software		Lessman, Ronald
95.	1994	Design and implementation of an automated scheme for an Eddy current scanning system *		Hebdalae, Chetan
96.	1994	Advanced Land Transportation Communication System		Freeland, Joe
97.	1994	Administration of a Hetrogeneous UNIX Network		Detterman, Jeff
98.	1993	Hierarchical Distributed Network Monitor for a Heterogeneous Network		Urali, Prem
99.	1993	Server Program for File Retrieving and Transferring with Internet		Ding, Shujin
100.	1993	Interconnection of Ethernet Using ISDN		Vardharajan, Satya
101.	1993	The Design of an Ethernet to Ethernet Bridge		Chen, Yue
102.	1993	Distributed Computing Using C-Linda		Wijaya, Valentina
103.	1993	Simulation and Performance Analysis of an FDDI Backbone		Viswanathan, Gautham
104.	1993	Computer Network to Control and Monitor a Remote Process		Dhawan, Rakesh
105.	1993	Software design and implementation of a contactless surface scanning NDE Scanning System *		Bugar, Alexandru
106.	1993	High Speed Switch for High Speed Networks		Al-Khatib, Mohammad
107.	1992	PC Based ISND Central Office		Dongre, Suresh
108.	1991	A Data Communication Study on ATCS, Advance Train Control Systems, as Define by ARINC Standards		Birkenberger, Lisa
109.	1991	Enhancements to the ARINC 629 Avionics Bus		Tietz, Randy
110.	1991	Design of a B-channel Multiplexer for Integrated Services Digital Network		Rajasekaran, Bharathi
111.	1991	Design of an ISDN Central Office, U-interface		Toillion, Tim
112.	1991	Design of a PC-Based ISDN Central Office		Bradley, Angela
113.	1991	Vincent Network Analysis		Willoz, Aimee
114.	1990	Development of a monitoring system for FDDI campus and local area network *		Christiansen, Lynn
115.	1990	Performance analysis of interconnected networks using decomposition techniques		Varadachari, Anand

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

116.	1990	Dynamic Server Selection in a Multithreaded Network Computing Environment	Stapleton, Joseph
117.	1990	Design and Implementation of a PC Token Bus Network Interface Card	Lin, Chih-Hung
118.	1990	The Design of a Token Ring Local Area Network Bridge	Freeman, Paul
119.	1990	Design of a Central Office for an ISDN System	Venkataraman, Geetha
120.	1989	Design of a Token Ring to ISDN Gateway	Kim, Jangkyung
121.	1989	Local Area Network Monitoring Between Token-Ring and Ethernet	Kang, Hun
122.	1989	Design and Implementation of an ISDN Telephone	Zhang, Xiao
123.	1989	The Core Fault Tolerant Computer Architecture for Advanced Aviation Flight Control	Ambros, Martin
124.	1988	Design of a Token Ring ETHERNET Bridge	Ahuja, Ratinder
125.	1988	Graphical Computer Network Performance Simulation	Prayugo, Murniwati
126.	1988	Implementation of Voice/Data Integration on a Token Ring Network	Lioe, Hidayat
127.	1988	Network Monitor Based on Token Ring	Tzeng, Shun-Ren

XVII.

XVIII. Ph.D. Degree Dissertations

1.	2022	Exploring the Feasibility of leveraging a firewall as a Moving Target Defense mechanism for web services	Wright-Hamor, Cimone
2.	2019	A framework towards fusing multisensory cyber security data utilizing graph databases	Murray, Lori
3.	2016	Dissertation Identity Theft Education: Comparison of Text-Based and Game-Based Learning	Helser, Susan
4.	2013	Business impact visualization for information security and compliance events	Tannian, Mark
5.	2012	Exploiting Cloud Utility Models for Profit and Ruin	Idziorek, Joseph
6.	2012	Cyberprints: Identifying Cyber Attackers by Feature Analysis	Blakely, Ben
7.	2010	Information technology social engineering: an academic definition and study of social engineering-analyzing the human firewall	Evans, Nate
8.	2010	Exploring utilization of visualization for computer and network security *	Luse, Andrew
9.	2009	Wireless Sensor Network Integrity Model	Qleibo, Haider
10.	2007	Performance and security measures of clustering protocols for sensor networks	Banerjee, Pubali
11.	2006	Security Enhancement in Passive Optical Networks through Wavelength Sequences Cycling Technique*	Walid Shawbaki
12.	2005	Incorporating TQM and CQI techniques into evaluation tools	Freeman, Richard

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

	for a computer engineering learning community	
13.	2004 MAC-Level Approaches for security and performance enhancement in IEEE 802.11	Wang, Haoli
14.	1999 Test suite development using a structured framework*	Hastings, Nelson
15.	1999 Bandwidth Allocation and Routing in Virtual Path based ATM Networks	Ahn, Byungjan
16.	1995 A Continuous Media Transport Protocol	Freeman, Paul
17.	1993 Multimedia Synchronization on a High Speed Transport Layer	Kang, Hun
18.	1992 Design of a multiprocessor High Bandwidth Communication Gateway Based on a Protocol Processor Pool Architecture	Jangkyung, Kim
19.	1990 Transport Interoperability Using a Virtual Transport Layer	Ahuja, Ratinder
20.	1989 Design and Analysis of a Medium Access and Control Strategy for Extending ISDN Services to LAN Users	Shafiq, Muhammad
21.	1988 Performance Investigation of a Document Retrieval System on a Voice/Data Integrated Token Ring Local Area Network	Gaitonde, Sunil
22.	1987 Performance Analysis of Token Bus Protocol with Maintenance Functions *	Kim, Joon-Nyun
23.	1986 A Distributed Channel-Sense Non-Preemptive Static Priority Ring for Local Area Computer Networks and its Performance *	Ghansah, Isaac
24.	1986 Design and Performance Analysis of an Integrated Voice-Data (IVD) Protocol for a Token Ring Network *	Lee, Jai

Note: * indicates co-major professor.

XIII. PROFESSIONAL ACTIVITIES

2019 - 2025		ABET Team Chair
2020	Member	State of Iowa Computer Science working group
2020	Member	Cyber.org committee to develop K-12 standards
2019 – present	editor	Elsevier Computers & Security Journal
2017 – present	Member	Central College Engineering advisory board
2015 – present	Member	DMACC IT & Cyber security pathway committee
2015 – present	Member	DMACC IT – Partnership (co-chair cyber security group)
2015 – present	Member	IEEE CEAA
2015 – present	Member	Iowa National Guard Cyber Senior Leadership
2016 – present	Member	Iowa Information Technology Program Management Committee (Iowa Dept. of Ed)
2012-2020	Member	North Central Iowa STEM Hub Advisory Board
2010-2013	Member	TAI Education and Workforce committee
2010-2011	Member	Iowa IT-Sector planning group
2010 – present		Member Southwestern CC advisory board
2009 -		IEEE ABET Program Evaluator
2007-2011	Member	IT Career Pathways Sector Board
2007-2010	Member	IDED IT Council
2005-2010	Member	Advisory board CMNet

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

2004-2018		Certified Computer Forensic Examiner
2004-2018	Member	The International Association of Computer Investigative Specialists
2001-present	Member	InfraGard
2000-2001	Member	International Advisory Board, Software and Internet Quality Week Conference
1991- Present	Member	ASEE
1991- Present	Member	Internet Society
1990-1991	Chairman	IEEE Central Iowa Section
2011-present	Fellow	IEEE
1990-2011	Senior Member	IEEE
1989	Member	IEEE 802.10 Standards Committee
1989-1990	Vice Chairman	IEEE Central Iowa Section
1988-1989	Sec/Treas	IEEE Central Iowa Section
1987	Member	SME
1987	Member	MAP/TOP Users Group
1986	Member	ACM
1979-1990	Member	IEEE

Expert Testimony:

- 1) September 9th 2003, I testified in front of the U.S. Senate Judiciary Committee on the uses of peer-to-peer protocols.
- 2) February 23 2007, I gave a deposition in the case UMG Recordings v. Marie Lindor, Case No. 05-cv-1095 (E.D.N.Y.).
- 3) October 1 & 2 2007, I testified at the trial in the case of Virgin Records v. Jammie Thomas, Case No. 06-cv-1497 (D. Minn.).
- 4) April 2 2009, I gave a deposition in the case of Atlantic Recording Corp. v. Jenna Raleigh, Case No. 06-cv-01708 (E.D. MO).
- 5) June 3 2009, I gave a deposition in the case of Tanya Andersen v. Atlantic Recording Corp, Case Bo. 07-cv-934 (OR)
- 6) June 16 2009, I testified at the trial in the case of Virgin Records v. Jammie Thomas, Case No. 06-cv-1497 (D. Minn.).
- 7) July 29 2009, I testified at the trial in the case of Sony BMG Music v. Joel Tenenbaum, Case No. 03-cv-11446 (D. MA.).
- 8) Nov 2 2010, I testified at the trial in the case of Virgin Records v. Jammie Thomas, Case No. 06-cv-1497 (D. Minn.).
- 9) September 19 2018, I gave a deposition in the case Centripetal Networks, Inc. v. Keysight Technologies, Inc. and Ixia, Case No. 2:17-cv-383-HCM

Active Learning Activities:

In addition to modifying courses to included cooperative learning methods, Dr. Jacobson has participated in the following activities:

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

May 2001	Attended and presented the ISU Learning Communities workshop
May 1999	Attended Wakonse teaching conference
May 1999	Attended ISU learning community workshop
November 1998	Attended and presented at a Learning Communities workshop
August 1998	Facilitator at the Engineering College "Foundations for effective Assessment workshop
August 1998	Helped facilitate one session of cooperative learning workshop
Summer 1998	Helped facilitate one session of cooperative learning workshop
May 1998	Attended and presented at a Learning Communities workshop
May 1998	Attended a Leadership & Ethics Workshop
April 1998	Attended learning centered syllabi workshop
February 1998	Presentation at active learning workshop
January 1998	Helped facilitate one day cooperative learning workshop
January 1998	Helped facilitate one session of cooperative learning workshop
AY 1997 - 1998	Co-facilitated bi-weekly student athletes leadership training workshop
October 1997	Helped facilitate one session of cooperative learning workshop
Summer 1997	Participated in a four day cooperative learning workshop
Summer 1997	Participated in a four day advanced cooperative learning workshop
1997- 2000	Facilitator of a bi-weekly faculty development workshop (project LEA/RN)
1996 - 2002	Participant in bi-weekly faculty development workshop (project LEA/RN)

XIV. UNIVERSITY ACTIVITIES

University Committees & activities

2021		On-Line learning task force
2017 - 2021		Teaching Technology Advisory Committee
2020 – 2021		Faculty Senate Curriculum Committee
2020 – 2023	Chair	Faculty Senate IT Committee
2020 – 2023		Faculty Senate Resource Policy and Allocation Council
2018 – 2021		Technology Enterprise Advisory Committee
2014 – 2020	Chair	Faculty Senate Curriculum Committee
2014 – 2020		Faculty Senate Academic Affairs Committee
2012 – 2014		Faculty Senate Curriculum Committee
2012-		STEM Advisory Council
2012 - 2021		Inventors Advisory Council
2010- present		Computer curriculum coordination committee
2004 - 2008		Council of Institute and Center Directors
2004 -		Interdepartmental Programs committee
2003		Information Security Task Force
2002-2005		Faculty Senate Curriculum Committee
2001		Graduate Curriculum and catalog committee
2000		Authentication Committee

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

1999-2000		Faculty Spring Conference Planning Committee
1999-2002		Goldwater Scholarship nominating committee
1999		Reviewer for carver trust grants
1998		Summer orientation panel 6/2/98 & 6/29/98
1998-2001		Learning Communities advisory Committee
1998		Reviewer for Carver Trust Grants
1997-2000		University Computer Security Policy Group
1997-98		Academic Information Technology Director Search
1996-97		Teaching Building
1995-2000		Computer Advisory
1995-97	Chair	Computation Center Advisory
1992-93		Distributed Computing Planning
1992		Email Planning
1992		WOI Review
1991		Review of Vice President/Office for Business and Finance
1990-1996		Project Vincent Implementation Group
1989	Chair	Ad-Hoc Computer Science/Computer Engineering Program Review

College Committees

2012-2021	Chair	Curriculum Committee
2004-present		ABET Committee (formally the Student Learning Task Force)
2002-2005	Chair	Curriculum Committee
2003		EE/CPRE department chair search committee
2001-2004		Academic Quality management team
2001-present		Curriculum Committee
1998-2000		ABET Task Force
1998-2001		Learning Communities Task Group
1998		ABET Assessment planning group
1998		College retreat to review college plan
1997		Undergraduate Program Task Group
1996		Basic Program Review
1996	Chair	Engineering Computer Services and Policy Task Group - Computer Plan subgroup
1995- 2000		Engineering Computer Services & Policy Task Group
1995		EE/CPRE DEO Search
1991-1995	Chair	Ad Hoc Network Planning
1991-1991		Computer Policy
1991-1995		NSF Coalition
1990-1992		Engineering Extension, (Chairman 1991)
1990		OES Review
1990		EE/CPRE DEO Search
1988-1989		Engineering Network Planning
1987-1988		Engineering Research

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

Department Committees

2013-present	Chair: Assessment Committee
2019-present	Curriculum Committee
2010 -2015	Chair Student recruitment and retention committee
2007- 2008	Chair ECpE 100 th year celebration committee
2004-2010	Chair Building Committee
2004-2011	Administrative Committee
1999-2000	Ad-Hoc ABET task group
1998-2002	Student recruitment and retention advisory board
1996-2009	Chair Information Security and Networking group
1996-2001	Advisory
1990-2017	Curriculum (chair 2004)
1991-1992	Computer Planning
1990-1993	Long Range Planning
1987-1989	Faculty Governance
1988-1990, 1994-1996	Graduate
1986-1991	Research
1986-Present	Computer Area

Other Professional Activities

Book Reviews

2003	TCP/IP Protocol Suite	Forouzan	McGraw-Hill
2001	TCP/IP Protocol Suite	Forouzan	McGraw-Hill
1998	Computer Networks: A systems Approach	Larry Peterson and Bruce Davie	Morgan Kaufmann
1998	Information Security	Neil Rowe	Morgan Kaufmann
1997	Communications Networks	Jean Walrand	McGraw-Hill
1995	Data and Computer Communications	Stallings	Prentice Hall
1995	Advanced Data and Computer Communications	Stallings	Prentice Hall (Book Proposal)
1993	Scientific C++: A primer for Engineers and Scientists	Salmon	MacMillan Publishing (Book Proposal)
1993	Data Communications and Object Orientation: Concepts and Implementations	Anil Ananthaswamy	Addison-Welsey (Book Proposal)
1993	Data Communications, Computer Networks, and Open Systems, Third edition	Fred Halsall	Addison-Wesley
1993	Mathematical toolkit in C++	Lawrence Williamson	MacMillan Publishing

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

1992	Open for Business: Introducing the open Systems Movement	Howard Berkowitz	Addison-Wesley
1992	Distributed Systems Software Development	Aggarwal & Kintala	Addison-Wesley (Book proposal)
1989	Digital Logic and Computer Design	Stephen Ben-Avi	Saunders College Publishing
1989	An Introduction to Distributed Operating Systems	Andrzej Goscinski	Addison-Wesley
1988	Local Area Networks	Keiser	McGraw-Hill

Journals and Conferences reviews

2019-	Editor COSE
2012	CISSE 2012
2012	2012 ASEE Conference
2011	CISSE 2011
2010/11	2011 ASEE Conference
2009	2010 FIE conference
2006	ASEE Conference
2005	International Journal of Computers and Applications
2005	SDCS 2005 Conference
2005	2005 IEEE EIT conference
2005	2 nd international workshop on security in distributed systems
2001	ASEE Conference
2000	Software Quality Week 2000
1999	IEEE transactions on Education
1998	Infocom
1997	Electronics and Telecommunications Research Institute journal
1997	12 Articles on network installation for Electrical Contractor
1996	Electronics and Telecommunications Research Institute journal
1992	IEEE Transactions on Systems, Man and Cybernetics
1991	IEEE Transactions on Knowledge and Data Engineering
1990	International Journal of Microcomputer Applications
1989	IEEE Software

Proposal Review

2010	NSF	ATE proposal review panel
2005	NSF	CRI proposal review panel
2004	South Dakota	Reviewer for South Dakota 2010 Initiative
2002	NSF	SBIR proposal review panel
1987	NSF	Division of networking and communications

Other

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

IEEE CEAA committee member (ABET) 2016- 2020
IEEE EAC Team Chair (ABET) 2019-2024
Attended NSF sponsored “Information Assurance Education and Workforce Development workshop, Washington D.C., Oct 13-15, 2010.
Planning committee for Information Assurance Education and Workforce Development workshop, 2010.
ABET Evaluator, 2008-2021
Program Chair Annual Conference on Education in Information Security September 2006
Program committee for 2005 University Synergy Program International Conference
Program committee for SDCS 2005 conference
Program committee for 2nd international workshop on security in distributed systems
Program committee for 2005 Electro/Information Technology Conference
Steering Committee “NSF Cyber Defense Exercise Workshop”, 2004
Attended “NSF Cyber Defense Workshop”, February 26-28 2004, San Antonio TX.
Planning committee Partnership for Homeland Security, Iowa Business Council, Infrastructure interdependencies table top exercise (Amber waves), 2004
Attended the CRA “Grand Challenges in Computer Security Workshop” November 16-19 2003, Airlie Center, Warrenton Virginia
Participated in a NSF workshop on Cyber Infrastructure hosted by the engineering directorate. June 5 & 6, 2003. (invited)
Coordinated and developed curriculum material for the ISU summer connections program, Summer 1999.
Program review for MS program in Computer Science at Winona State University, March 1998
Detailed study of State Fiber Optic Network for State Auditor
Attended and helped organize the local viewing of the IEEE Video Conference on the Interdisciplinary World of Computing, 1989
Voting Member in the IEEE 802.10 Network Security Standardization Committee, 1989-92
Voting member in the IEEE P1003 UNIX standardization committee, 1987-1989

XV. OTHER INFORMATION

Senior design projects:

Year	Project	Number of students
2015	ISEStorm – cyber test-bed	4
2015	SCADA honey pot	4
2011	Wireless security lab development	3
2009-10	Science Center 3	4
2008-09	NCAA compliance system	4
2008-09	Science Center 2	4
2007-08	Science Center	4

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

2005-06	Attack database for ISEAGE	4
2005-06	Network Specification and Report System for ISEAGE	4
2004-05	Attack Collector/Watcher/Replayer for ISEAGE	4
2004-05	Network Specification and Report System for ISEAGE	4
2004-05	Optical Encoder for a Game Steering Wheel	4
2004	Personal Record Keeper	4
2003-04	Travel Software for Kids for Laptop or PDA	4
2003	CyberSim	4
2002-03	Smart Appliance	5
2002-03	Serial port to serial port switch	4
2002	A secure wireless interface between PDAs	4
2000-01	Java Embedded Network Intrusion Security	6
2000-01	Smart Digital Valve Control Simulator	4
2000-01	MP3-Based Digital Record and Playback device	6
2000-01	One time passwords using Biometrics	4
2000-01	Computer Security	4
1999-00	CD-ROM Based Portable MP3 Player	4
1999-00	Graphical Output Package for Industrial Sensors	5
1999-00	Java Embedded Network Intrusion Security	4
1999-00	Transportation and Logistics Simulator	3
1999-00	One time passwords using Biometrics	4
1999-00	Generator based backup system	4
1998-99	STREAMS Compatibility API for mwSoftStax	5
1998-99	Temperature monitoring Systems	3
1998-99	Child Monitoring Device	3
1997-98	Microelectromechanical Systems (MEMS) flow injection Analysis	3
1997-98	Graphical Keyboard Display	3
1997-98	Automated Livestock feeder	3
1997-98	Secure Network Monitor System	4
1996-97	ScopeBoy	2
1996-97	Smart Answering Machine	4
1996	Design of an ISDN switch	5
1996	Digital Design lab for CprE 211	6
1995	Virtual Orchestra Project	3
1995	Real Time Programming - Robotic Tanks	5
1994-95	ISDN Central Office Design	4
1994	Car Navigator	7
1994	Weather Station Project	4
1994	Real time programming Platform Project	9
1991-92	ISDN software design	4
1991-92	Motorola Graphical User interface of Cell Phone design	5
1990	ISDN phone	5

Appendix B

LIST OF EXHIBITS

EX1001	U.S. Patent No. 9,917,856 (“’856”)
EX1002	File History of U.S. Patent No. 9,917,856 (“’856 FH”)
EX1004	U.S. Patent No. 9,680,795 (“Buruganahalli”)
EX1005	U.S. Patent No. 5,878,231 (“Baehr”)
EX1006	Reserved
EX1007	Barry M. Leiner et al., “A Brief History of the Internet,” Internet Society, 1997, available at: https://www.internetsociety.org/internet/history-internet/brief-historyinternet/ (“Leiner”)
EX1008	U.S. Pat. No. 7,032,031 (“Jungck ’06”)
EX1009	E. H. Spafford, “The Internet Worm Program: An Analysis,” Purdue Technical Report CSD-TR-823, 1988. (“Spafford”)
EX1010	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 (“Eichin”)
EX1011	T. Eisenberg et al., “The Cornell Commission: On Morris and the Worm,” Communications of the ACM, Volume 32 Number 6, June 1989 (“Eisenberg”)
EX1012	J. C. Mogul, “Simple and Flexible Datagram Access Controls for Unixbased Gateways,” Digital Western Research Laboratory Technical Report No. 89/4, 1989 (“Mogul”)
EX1013	“FireWall-1 User Interface from 3.0,” PhoneBoy’s Security Theater, archived at the Internet Archive Wayback Machine on January 2, 2014 at https://web.archive.org/web/20140102143305/http://phoneboy.net/ (“FireWall-1”)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

EX1014	“SonicWALL Global Management System: Centralized Network Monitoring and Management Solution”, 2008, archived at the Internet Archive Wayback Machine on December 7, 2008 at https://web.archive.org/web/20081207003303/http://www.sonicwall.com/downloads/EC_GMS_DS_US.pdf (“SonicWALL GMS”)
EX1015	“SonicWALL ViewPoint 6.0 Administrator’s Guide”, 2010, archived at the Internet Archive Wayback Machine on August 21, 2010 at https://web.archive.org/web/20100821022839/http://www.sonicwall.com:80/downloads/SonicWALL_ViewPoint_6_0_Admin_Guide.pdf (“SonicWALL ViewPoint”)
EX1016	Heberlein, L. T.L, et al., “A Network Security Monitor,” Proceedings, 1990 IEEE Computer Society Symposium on Security and Privacy, 1990 (“Heberlein”)
EX1017	“NetRanger Network Security Management System User Guide”. v1.3.1 Wheelgroup Corporation, 1997 (“NetRanger”)
EX1018	Roesch, M., “Snort: Lightweight Intrusion Detection for Networks,” Lisa (Vol. 99, No. 1, pp. 229-238), 1999 (“Roesch”)
EX1019	U.S. Pat. No. 8,370,936 (“Zuk”)
EX1020	W32.hllw.Doomjuice Technical Description, Symantec Security Center, updated February 13, 2007, available at: https://www.symantec.com/security-center/writeup/2004-020909-2916-99 (“Doomjuice”)
EX1021	“(Vendor Issues Fix) Re: Helix Universal Server and RealServer URL Parsing Flaw in View Source Plug-in Lets Remote Users Execute Arbitrary Code with Root Privileges” Security Tracker, September 13, 2003, available at: https://securitytracker.com/id/1007692 (“Helix”)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

EX1022	“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 (“RFC 793”)
EX1023	“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
EX1024	“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 (“RFC 765”)
EX1025	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 (“T.B. Lee”)
EX1026	<i>Cisco System Inc. v. Centripetal Networks, Inc.</i> , IPR2018- 01760, Paper 41 (PTAB May 18, 2020)
EX1027	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case No. 2:18-cv-00094 (E.D. Va.), Dkt. No. 621 (Opinion and Order Regarding Findings of Fact and Conclusions of Law)
EX1028	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case 2021- 1888 (Fed. Cir.), Dkt. No. 18 (Non-Confidential Brief for Defendant-Appellant Cisco Systems, Inc.)
EX1029	<i>Centripetal Networks, Inc. v. Cisco Systems, Inc.</i> , Case No. 2:18-cv-00094 (E.D. Va.), Dkt. No. 548 (June 10, 2020 Trial Transcript)
EX1030	<i>Centripetal Networks, Inc. v. Keysight Techs., Inc.</i> , Case No. 2:17-cv-383 (E.D. Va.), Dkt No. 484 (“Keysight Markman”)

Declaration of Dr. Doug W. Jacobson in Support of
Petition for *Inter Partes* Review of
U.S. Patent No. 9,917,856

EX1031	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 (“Turner”)
EX1032	I. Ristic, “SSL/TLS and PKI History,” April 2018, available from https://www.feistyduck.com/ssl-tls-and-pki-history/ (“Ristic”)
EX1033	U.S. Pat. Appl. Pub. No. 2007/0271605 (“Le Pennek”)
EX1034	U.S. Patent No. 8,504,822 (“Wang”)
EX1035	U.S. Patent No. 7,793,342 (“Ebrahimi”)
EX1036	J. Wack et al., <i>Guidelines on Firewalls and Firewall Policy</i> , National Institute of Standards and Technology (“NIST”)
EX1037	U.S. Patent No. 8,813,228 (“Magee”)
EX1038	Reserved
EX1039	Reserved
EX1040	U.S. Patent Appl. Pub. No. 2014/0283004 (“Moore”)
EX1041	U.S. Patent Appl. Pub. No. 2015/0207809 (“Macaulay”)
EX1042	U.S. Patent Appl. Pub. No. 2014/0089661 (“Mahadik”)
EX1043	U.S. Patent No. 7,849,502 (“Bloch”)
EX1044	U.S. Patent No. 7,584,352 (“Boivie”)
EX1045	Young-Ho Kim, et al., <i>Design of Firewall in Router using Network Processor</i> , IEEE (Jul. 11, 2005) (“Kim”)
EX1047	Declaration of Dr. Jon Weissman (IPR2022-00182 EX1003)