

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,
Petitioner

v.

SECURITY PROFILING, LLC,
Patent Owner

IPR2023-00990
U.S. Patent No. 10,893,066

**DECLARATION OF A.L. NARASIMHA REDDY, PH.D.,
UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION
FOR INTER PARTES REVIEW**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	QUALIFICATIONS AND PROFESSIONAL EXPERIENCE	3
III.	LEVEL OF ORDINARY SKILL IN THE ART	6
IV.	RELEVANT LEGAL STANDARDS	7
V.	OVERVIEW OF THE '066 PATENT	9
VI.	STATE OF THE ART	10
	B. Network System Security	11
	C. The Use of Mobile Agents	13
VII.	CLAIM CONSTRUCTION	14
VIII.	IDENTIFICATION OF HOW THE CLAIM IS UNPATENTABLE	14
IX.	THE COMBINATION OF Gupta AND GRAHAM RENDERS OBVIOUS CLAIM 1	15
	A. Summary of Gupta	15
	B. Summary of Graham	24
	C. Motivation to Modify the Teachings of Gupta with the Teachings of Graham	25
	D. Detailed Analysis of Claims	27
	1. Claim 1	27
	a. [1.0] A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:	27
	b. [1.1] receive first vulnerability information from at least one first data storage that is generated	

- utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities; 32
- c.** [1.2] said first vulnerability information generated utilizing the second vulnerability information, by: 38
- d.** [1.3] identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and.....38
- e.** [1.4] determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities; 40
- f.** [1.5] identify an occurrence in connection with at least one of the plurality of devices;.....42
- g.** [1.6] determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and 43
- h.** [1.7] cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; 46

i.	[1.8] wherein the at least one configuration involves at least one operating system.	50
X.	THE COMBINATION OF Gupta AND GRAHAM IN VIEW OF HILL RENDERS OBVIOUS CLAIM 2	51
A.	Summary Of Hill	51
B.	Motivation to Modify the Teachings of Gupta with the Teachings of Hill	53
C.	Detailed Analysis of Claim 2	57
1.	Claim 2	57
a.	[2.0] The non-transitory computer-readable media of claim 1, wherein the at least one actual vulnerability is one of the actual vulnerabilities that are of the at least operating system that is installed on the plurality of devices, the occurrence is at least one of a plurality of occurrences, and the instructions include:.....	58
b.	[2.1] first instructions that, when executed by at least one first processor of the one or more processors of at least one server in communication with the at least one second storage, cause the at least one first processor to	58
c.	[2.2] generate the first vulnerability information utilizing the second vulnerability information, and.....	59
d.	[2.3] communicate, from the at least one server and to the at least one of the plurality of devices over at least one network, the first vulnerability information	60
e.	[2.4] second instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the second instructions are executed by at least one second processor of the one or more	

processors of the at least one of the plurality of
devices, cause the at least one second processor to:.....62

- f. [2.5] receive, from the at least one server and at the
at least one of the plurality of devices over the at
least one network, the first vulnerability
information, store the first vulnerability
information on the at least one first data storage,
and receive the first vulnerability information from
the at least one first data storage, the first
vulnerability information being relevant to the
actual vulnerabilities of the at least one operating
system of the at least one of the plurality of
devices, and excluding at least a portion of the
second vulnerability information that is not
relevant to the actual vulnerabilities of the at least
one operating system of the at least one of the
plurality of devices 64
- g. [2.6] third instructions that are configured to be
stored on the at least one first data storage which is
part of the at least one of the plurality of devices
and that, when the third instructions are executed
by the at least one second processor, cause the at
least one second processor to.....66
- h. [2.7] identify a first portion of the first
vulnerability information that includes data
inspection-related information that is relevant to at
least one of the actual vulnerabilities of the at least
one operating system of the at least one of the
plurality of devices, and that excludes other data
inspection-related information of the second
vulnerability information that is not relevant to the
actual vulnerabilities of the at least one operating
system of the at least one of the plurality of
devices 67

- i. [2.8] identify a first occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and.....68
- j. [2.9] cause a determination whether the at least one of the actual vulnerabilities relevant to the data inspection-related information is susceptible to being taken advantage of by the first occurrence identified in connection with the at least one of the plurality of devices, utilizing the data inspection-related information.....68
- k. [2.10] fourth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fourth instructions are executed by the at least one second processor, cause the at least one second processor to: 69
- l. [2.11] identify a second portion of the first vulnerability information that includes traffic inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other traffic inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, ...70
- m. [2.12] identify a second occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and 71
- n. [2.13] cause a determination whether the at least one of the actual vulnerabilities relevant to the traffic inspection-related information is susceptible to being taken advantage of by the second occurrence identified in connection with the at

- least one of the plurality of devices, utilizing the
traffic inspection-related information.....71
- o.** [2.14] fifth instructions that are configured to be
stored on the at least one first data storage which is
part of the at least one of the plurality of devices
and that, when the fifth instructions are executed
by the at least one second processor, cause the at
least one second processor to: 72
- p.** [2.15] identify a third portion of the first
vulnerability information that includes firewall-
related information that is relevant to at least one
of the actual vulnerabilities of the at least one
operating system of the at least one of the plurality
of devices, and that excludes other firewall-related
information of the second vulnerability
information that is not relevant to the actual
vulnerabilities of the at least one operating system
of the at least one of the plurality of devices.....73
- q.** [2.16] identify a third occurrence of the plurality of
occurrences in connection with the at least one of
the plurality of devices, and.....76
- r.** [2.17] cause a determination whether the at least
one of the actual vulnerabilities relevant to the
firewall-related information is susceptible to being
taken advantage of by the third occurrence
identified in connection with the at least one of the
plurality of devices, utilizing the firewall-related
information; and.....76
- s.** [2.18] sixth instructions that, when executed by at
least one third processor of an administrator
computer, cause the at least one third processor to: 77
- t.** [2.19] in response to administrator action, cause
setting, before the first occurrence, of a first policy
for the third instructions that is applied to a group

including each of the plurality of devices that has
the at least one operating system installed thereon 79

u. [2.20] in response to administrator action, cause
setting, before the second occurrence, of a second
policy for the fourth instructions that is applied to
the group including each of the plurality of devices
that has the at least one operating system installed
thereon 80

v. [2.21] in response to administrator action, cause
setting, before the third occurrence, of a third
policy for the fifth instructions that is applied to
the group including each of the plurality of devices
that has the at least one operating system installed
thereon, and.....81

w. [2.22] cause the utilization of the different
occurrence mitigation actions of the diverse
occurrence mitigation types, including the firewall-
based occurrence mitigation type and the other
occurrence mitigation type, across the plurality of
devices for occurrence mitigation by preventing
the advantage being taken of the actual
vulnerabilities utilizing the different occurrence
mitigation actions of the diverse occurrence
mitigation types across the plurality of devices. 83

XI. CONCLUSION.....i

I, Narasimha Reddy, Ph.D., do hereby declare as follows:

I. INTRODUCTION

1. I am making this declaration at the request of Forcepoint LLC in the matter of the *Inter Partes* Review of U.S. Patent No. 10,893,066 (“the ’066 patent”) to Oliphant et al.

2. I am being compensated for my work in this matter at my standard hourly rate of \$650. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this proceeding. My compensation is not contingent on the outcome of this matter or the specifics of my testimony.

3. I have been asked to provide my opinions regarding whether the subject matter of claims 1 and 2 (“the Challenged Claims”) of the ’066 patent would have been obvious to a person having ordinary skill in the art (“POSITA”) at the time of the alleged invention, in light of the prior art. It is my opinion that the Challenged Claims would have been obvious to a POSITA.

4. In the preparation of this declaration, I have studied:

- a. the ’066 patent, Ex.1001;
- b. the prosecution history of the ’066 patent (“’066 File History”), Ex.1002;

- c. U.S. Patent No. 7,359,962 to Willebeek-LeMair et al. (“W-L”), Ex.1005;
- d. U.S. Patent Publication No. 2003/0004689 to Gupta et al. (“Gupta”), Ex.1006;
- e. U.S. Patent No. 7,237,264 to Graham et al. (“Graham”), Ex.1007;
- f. U.S. Patent No. 6,088,804 to Hill (“Hill”), Ex.1016; and
- g. *Applying Mobile Agents to Intrusions Detection and Response* Jansen, et al, NIST Interim Report (IR) (October 1999) (“Jansen”), Ex.1021.

5. In forming the opinions expressed below, I have considered: the documents listed above; the relevant legal standards, including the standard for obviousness; and my own knowledge and experience based upon my work in the field of network communications and security as described below, as well as portions of the following additional materials:

- a. the prosecution history of U.S. Patent No. 9,117,069 (“’069 File History”), great-grandparent of the ’066 patent, Ex.1008;
- b. the prosecution history of U.S. Patent No. 9,100,431 (“’431 File History”), grandparent of the ’066 patent, Ex.1009;
- c. the prosecution history of U.S. Patent No. 10,050,988 (“’988 File History”), parent of the ’066 patent, Ex.1010; and

d. U.S. Patent No. 6,735,766 to Chamberlain et al.
("Chamberlain"), Ex.1018.

6. Unless otherwise noted, all **emphasis** in any quoted material has been added. Claim terms are *italicized*.

II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE

7. My complete qualifications and professional experience are described in my *Curriculum Vitae*, a copy of which can be found in Exhibit 1004. The following is a brief summary of my relevant qualifications and professional experience.

8. I am currently the J.W. Runyon Professor of Electrical and Computer Engineering at Texas A&M University in College Station, Texas. I have over 25 years of experience in a wide variety of technologies and industries relating to data communications, storage systems, and distributed systems, including packet-switched network communications.

9. My academic credentials include a Bachelor of Technology degree in Electronics and Electrical Communications Engineering from the Indian Institute of Technology, Kharagpur, India, in August 1985. I then received a Master of Science and a Ph.D. in Computer Engineering from the University of Illinois at Urbana-Champaign in May 1987 and August 1990, respectively.

10. I have worked for over 25 years in the field of Electrical Engineering. My primary focus and research interest has been on computer networks, storage systems, multimedia systems, and computer architecture. I have authored and co-authored over a hundred technical papers and several book chapters related to several of these interests, including on such topics as multipath routing, route control, high-speed networks, network congestion, packet management, quality of service regulation, network security, network modeling, differentiated services, storage system enhancements, caching strategies, and multimedia system enhancements to name a few examples. I am listed as an inventor on five U.S. patents in the field of communication networks.

11. My employment history following my graduation from the University of Illinois at Urbana-Champaign began at the IBM Almaden Research Center in San Jose, California in 1990. At IBM, I worked on projects related to disk arrays, multiprocessor communication, hierarchical storage systems and video servers.

12. In 1995, I joined the faculty of the department of Electrical Engineering at Texas A&M University initially as an Associate Professor and was later promoted to full, tenured Professor. At Texas A&M, I was the Associate Agency Director for Strategic Initiatives and Centers for the Texas A&M Engineering Experiment Station (TEES) during 2016-21, which engages in engineering and technology-

oriented research and educational collaborations. I also served as Associate Dean for Research for the College of Engineering during 2016-21.

13. At Texas A&M, I have taught dozens of courses related to computer networking and communications, as well as computer architecture, multimedia systems and networks, topics in networking security, multimedia storage and delivery, as well as networking for multimedia applications. I have done research on various topics of network security including anomaly detection, botnet detection, building mechanisms in routers and switches to improve security, spammer detection in social networks and improving security of cyberphysical systems. I have also served on various committees for the benefit of the scientific community and the Texas A&M University community.

14. I am a member of a number of professional societies, including the Institute of Electrical and Electronic Engineers (IEEE), where I have been elevated to an IEEE Fellow, and the Association for Computing Machinery (ACM). I have been responsible for chairing or co-chairing numerous conferences and programs, as well as presenting research at major IEEE and ACM conferences. For example, I served as program co-chair for the 2008 5th International Conference on Broadband Communications, Networks and Systems, panels co-chair for the 2008 3rd International Conference on Communication Systems Software & Middleware, and panel chair of the IEEE Conference of High Performance Computer Architecture.

15. My presentations include a Keynote speech at International Conference on Information Technology-New Generations in 2013, a Keynote speech at IEEE International Symposium on Computers and Communications 2010, and several invited talks including at Georgia Tech (2013), COMSNETS Conference (2013), Int. Conf. on Networking and Communications (2012), Samsung (2011), Korea University (2011), Aijou University (2011), Catedra Series at University of Carlos III, Madrid (2009), Thomson Research, Paris (2009), Telefonica Research, Barcelona (2009), and a Distinguished Seminar at IBM Austin Research Lab (2008).

16. I have received multiple awards in the field of networks and computer architecture. I received the NSF Career Award from 1996-2000. I received an outstanding professor award by the IEEE student branch at Texas A&M during 1997-1998, an outstanding faculty award by the department of Electrical and Computer Engineering during 2003-2004, a Distinguished Achievement award for teaching from the former students' association of Texas A&M University, and a citation "for one of the most influential papers from the 1st ACM Multimedia conference."

III. LEVEL OF ORDINARY SKILL IN THE ART

17. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the

sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

18. A POSITA in the field of the '066 patent, as of its earliest alleged priority date of July 1, 2003, would have had a working knowledge of the network communications art that is pertinent to the '066 Patent, including network security. A POSITA would have had a bachelor's degree in computer science, computer engineering, or an equivalent, and two years of professional experience relating to network communications. Lack of professional experience can be remedied by additional education, and vice versa.

19. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my own experience and what a POSITA would have understood or known generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the relevant field as of the priority date of the '066 patent.

IV. RELEVANT LEGAL STANDARDS

20. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '066 patent, I am relying on certain basic legal principles that Forcepoint's counsel has explained to me.

21. I understand that prior art to the '066 patent includes patents and printed publications in the relevant art that predate the priority date of the '066 patent. For

purposes of this Declaration, I am applying July 1, 2003, as the priority date of the '066 patent.

22. I have been informed by Forcepoint's counsel that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the claimed invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA. I have also been informed by Forcepoint's counsel that the obviousness analysis considers factual inquiries, including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

23. I have been further informed by Forcepoint's counsel that there are several recognized rationales for combining references or modifying a reference to show obviousness. These rationales include: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led a

POSITA to modify the prior art or to combine prior art teachings to arrive at the claimed invention.

V. OVERVIEW OF THE '066 PATENT

24. The '066 patent focuses on the “management of security of computing and network devices that are connected to other such devices.” '066 patent at 1:23-25. To accomplish this, “technology is provided to meet the following market requirements: integrate network security products to share information; provide system intelligence; and remediate network vulnerabilities.” '066 patent at 11:37-40. Integrating products is done “to intelligently reference and share information from the same vulnerability data set.” '066 patent at 11:41-43.

25. The system in the '066 patent has a “security server 135” which “collects certain information and provides certain data services.” '066 patent at 2:30-38. The server collects data about devices within the network, including operating system information and other configuration and policy settings. '066 patent at 2:43-45. The system in the '066 patent “may easily integrate with and enable network security products such as IDS [intrusion detection system], scanners, or firewalls to intelligently reference and share the same vulnerability data set.” '066 patent at 8:26-33.

26. The server obtains a list of security vulnerabilities from a vulnerability remediation database 110. '066 patent at 2:46-49. The server also includes a database

146, which maintains remediation techniques for vulnerabilities. '066 patent at 2:56-57, 4:62-64. When traffic arrives at the network, such as at a firewall 131, the security server determines whether the traffic “is attempting to take advantage of a particular known vulnerability” by using the information from the database. '066 patent at 4:9-11, 4:21-29. If an attack is detected, the security server “selects one or more remediation techniques from database 146 that remediate the particular vulnerability.” '066 patent at 4:62-64.

27. As I will explain below, these concepts were well known as of the priority date of the '066 patent.

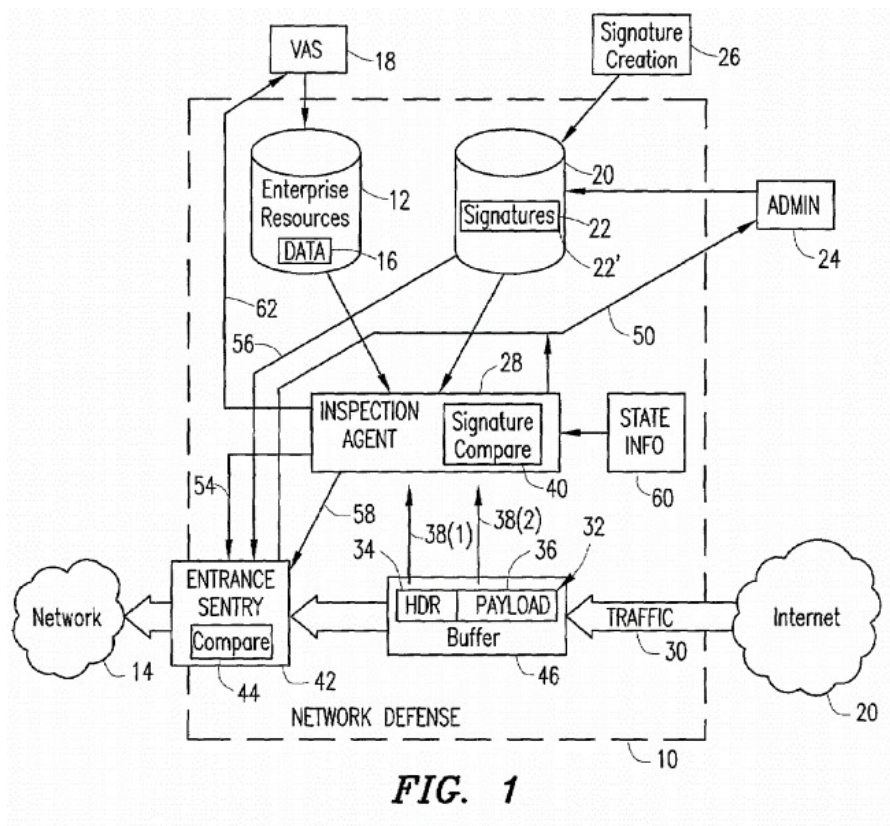
VI. STATE OF THE ART

28. The following section describes the state of the art for network security systems as of July 2003. The prior art references, and the discussions of what was known to a POSITA, provide the factual support for the general description of the state of the art at the time of the invention, provide contemporaneous context to support assertions regarding what a POSITA would have understood from the prior art in the grounds and provide the motivation to modify or combine the references. Accordingly, these references should be considered by the Board. See *Yeda Research v. Mylan Pharm. Inc.*, 906 F.3d 1031, 1041- 1042 (Fed. Cir. 2018) (affirming the use of “supporting evidence relied upon to support the challenge”); 37 C.F.R. § 42.104(b); see also *K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d

1362, 1365-66 (Fed. Cir. 2014); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1363 (Fed. Cir. 2016).

B. Network System Security

29. By July 2003 it was known that network security included “the functionalities performed by a firewall, IDS [intrusion detection system] and [vulnerability assessment scanner] for network security into one system.” EX-1005 3:14-18. Such a unified system 10 is illustrated in Figure 1. EX-1005 4:37-39. It includes “an enterprise resource database” with data identifying potential “vulnerabilities associated with” hosts in the network. EX-1005 5:9-15. A “signature database” stores “detection signatures,” which include “security rules, policies and algorithms” to “mitigate or avert network damage from detected vulnerabilities.” EX-1005, 5:20-24.



30. As shown in Figure 2, reproduced below, the system 10 includes an “agent 126 that functions to configure, tune and monitor the operation of the intrusion detector functionality 116 and the firewalling functionality 118.” EX-1005 9:36-41.

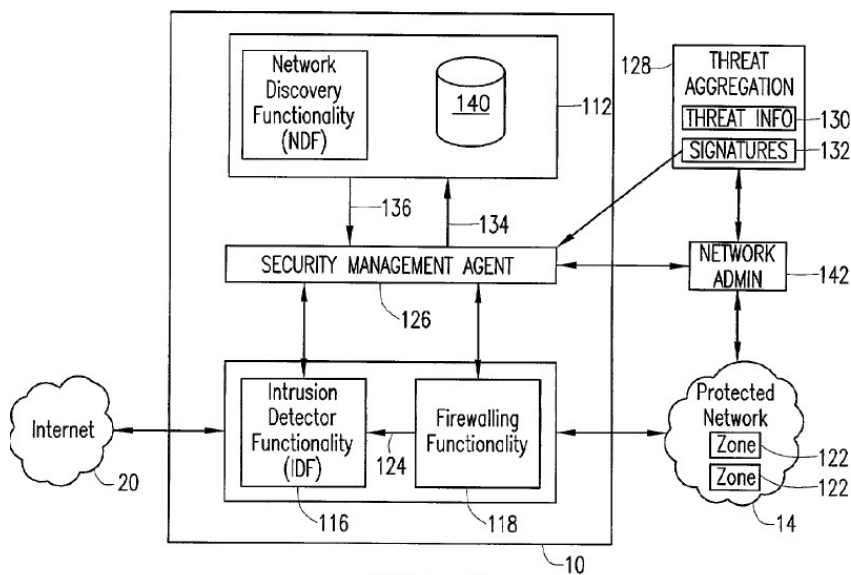


FIG. 2

C. The Use of Mobile Agents

31. By July 2003, intrusion detection systems had adopted the use of mobile agents. A mobile agent is a software agent that is distributed at each host to provide intrusion detection and automatic response. Jansen pp. 5, 10-11. A POSITA understood that the use of mobile agents in an architecture for highly distributed intrusion detection systems provided several advantages over centralized intrusion detection systems including overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. Jansen pp. 13-17. In addition, a layered approach in which a hierarchical IDS where a mobile agent backs each node up and restores any lost functionality provides redundancy for the security of the network. Jensen p. 24.

VII. CLAIM CONSTRUCTION

32. It is my understanding that in order to properly evaluate the '066 patent, the terms of the claims must first be interpreted. It is my understanding that for the purposes of this *inter partes* review, the claims are to be construed under the so-called *Phillips* standard, under which claim terms are given their ordinary and customary meaning as would have been understood by a POSITA in light of the specification and prosecution history, unless the inventor has set forth a special meaning for a term. I have also been informed that claim terms only need to be construed to the extent necessary to resolve the obviousness inquiry. I have reviewed the entirety of the '066 patent, as well as its prosecution history. It is my opinion that for purposes of applying the prior art presented herein to evaluate the patentability of the Challenged Claims, no terms require express construction.

VIII. IDENTIFICATION OF HOW THE CLAIM IS UNPATENTABLE

33. The discussion in this Declaration provides a detailed analysis of how the asserted prior art references teach each limitation of the Challenged Claims.

34. As part of my analysis, I have considered, and discuss in detail, the scope and content of the prior art and any differences between the alleged invention and the prior art.

35. It is my opinion that the alleged invention recited in the Challenged Claim would have been obvious in view of the teachings of the asserted prior art and the knowledge of a POSITA.

IX. THE COMBINATION OF Gupta AND GRAHAM RENDERS OBVIOUS CLAIM 1

A. Summary of Gupta

36. U.S. Patent Application No. 2003/0004689 to Gupta (Ex. 1006, “Gupta”), entitled “Hierarchy-based Method and Apparatus for Detecting Attacks on a Computer System,” is directed toward a hierarchical organization of threat/vulnerability information, which represents potential vulnerabilities. This potential information is matched against device configuration data in order to produce actual vulnerability data. As stated in the abstract:

A method of provisioning a computer against computer attacks includes constructing a **hierarchy characterizing different computer attacks** and counter measures, and traversing this hierarchy to **identify computer attacks and countermeasures relevant to a target platform**. Detection and protection measures are collected in response to this traversing. These detection and protection measures are then downloaded to a security sensor associated with the target platform.

Gupta, Abstract.

37. In more detail, Gupta discloses creating customized “attack files” designed to protect a specific target.

Detection and protection measures for the target platform are then collected (block 164). This can result in an attack file 149. A sensor is then supplied, through a download, with the protective software (e.g., the attack file) for the target platform (block 166).

The hierarchical approach of the invention allows one to clearly describe, in one data structure, what attacks a given environment is vulnerable to, what protection means (mechanisms and signatures) are available, and how detection alerts are correlated.

Gupta, [0164]-[0165].

38. The identified protection measures are used to protect the system and include IPS-based mitigation actions such as dropping the connection:

The response processor 54 responds to AIDs. The response processor 54 generates alerts that provide notification of an attack. The response processor 54 also attempts to prevent the attack. Short-term responses include terminating TCP connections.

Gupta, [0087].

39. Gupta describes “provisioning a computer against computer attacks” by “constructing a hierarchy characterizing different computer attacks and counter

measures, and traversing this hierarchy to identify computer attacks and counter measures relevant to a target platform.” Gupta [0008], Abstract. Gupta explains that its system provides “security operations” via network security sensors 22 in a computer network 20 incorporating network security devices and processes associated with the invention. The combination of the sensor 22 (green), redundant sensor 24, and sensor management system 26 (pink) is referred to as a local sensor security module 27. As shown in FIG. 1, local sensor security modules 27 may be distributed throughout a network. In this example, a local sensor (green) in a local sensor security module 27-0 is positioned between the enterprise network 30 (blue) and a protected server 32 (red). Gupta. [0030],[0032]

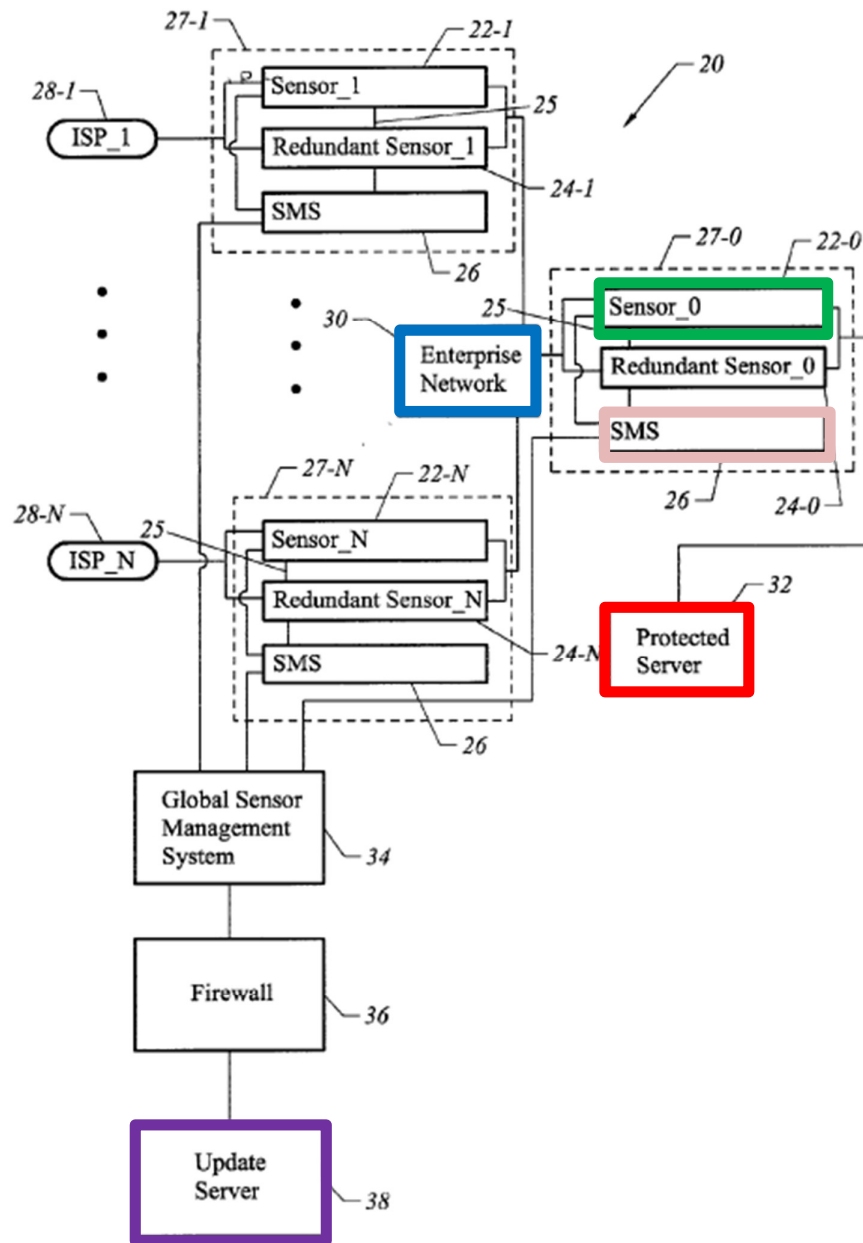


FIG. 1

Gupta FIG. 1 (Annotated)

40. The update server 38 (purple) is used to coordinate the delivery of signature and software updates to the local sensor security modules 27. Gupta [0034]. The update server 38 notifies users of new software or network intrusion signature updates and provides them for download to the sensors. The sensor 22 performs signature matching against network traffic and generates responses in case of intrusions. A sensor 22 accepts configuration and control messages and sends intrusion alerts and/or events to the sensor management system 26. Gupta [0138].

41. As shown in FIG. 2, network security sensors include a “memory 50, which includes primary and/or secondary memory” and “memory 50 stores a set of executable programs utilized to implement functions of the invention.” Gupta [0036], [0037].

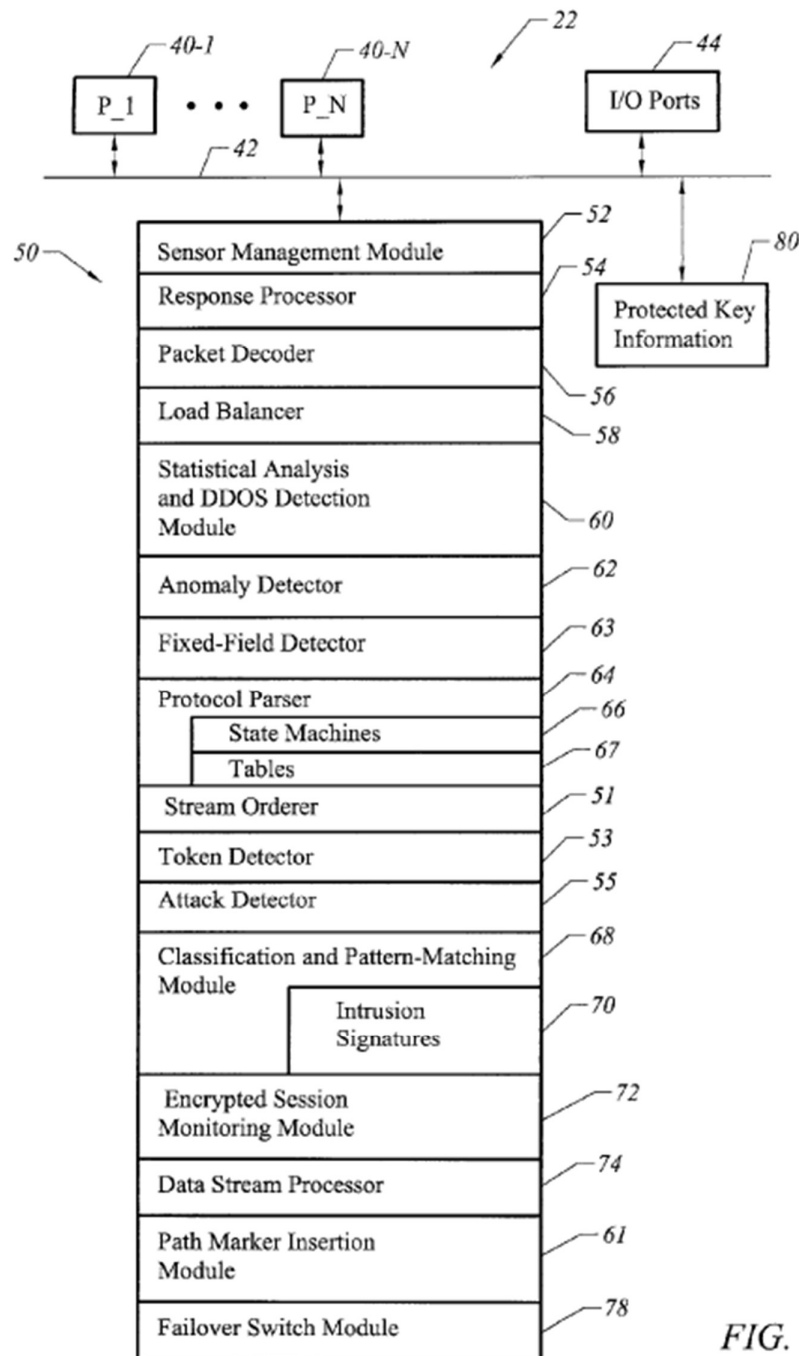


FIG. 2

Gupta FIG. 2.

42. Further, “memory 50 also stores a classification and pattern-matching module 68” which “has an associated set of intrusion signatures 70” (Gupta [0042])

and those intrusion signatures 70 are stored in an “attack file” which “specifies attacks and counter measures.” Gupta [0151].

43. As illustrated in FIG. 17, the attack file is generated by the hierarchical categorization module in the update server, which initially constructs a hierarchy characterizing different computer attacks and countermeasures (block 160).

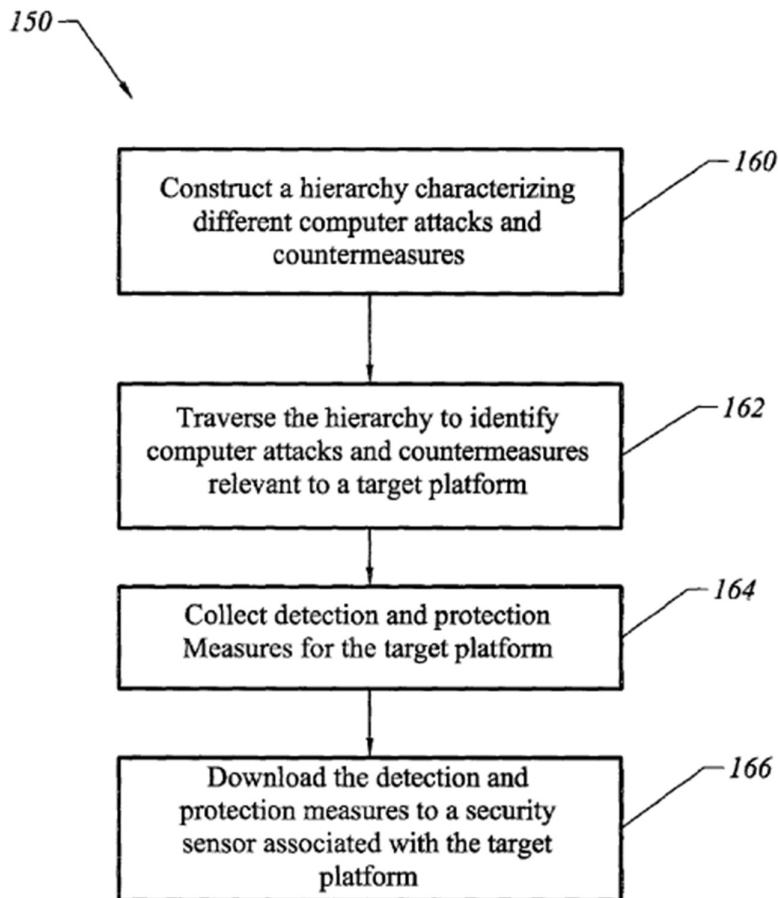


FIG. 17

Gupta FIG. 17.

44. The hierarchy is then traversed to identify computer attacks and countermeasures relevant to the target platform (block 162). Detection and protection measures for the target platform are then collected (block 164). This can result in an attack file 149 and a sensor is then supplied, through a download, with the protective software (e.g., the attack file) for the target platform (block 166). Gupta [0164].

45. To detect an attack the sensor uses, a “signature processing system . . . look[s] for signatures that are specific combinations of patterns (e.g., numerical field values, string matches, and the like) existing in monitored network traffic.” Gupta [0083]. When an attack is found, “response processor 54 . . . attempts to prevent the attack. Short-term responses include terminating TCP connections. Long-term responses include packet logging for further analysis to improve detection and response.” Gupta [0087].

46. As shown in FIG. 13, the sensor management system 26 includes a virtual intrusion detection system (VIDS) provisioning module 110 and a real-time signature update module 112.

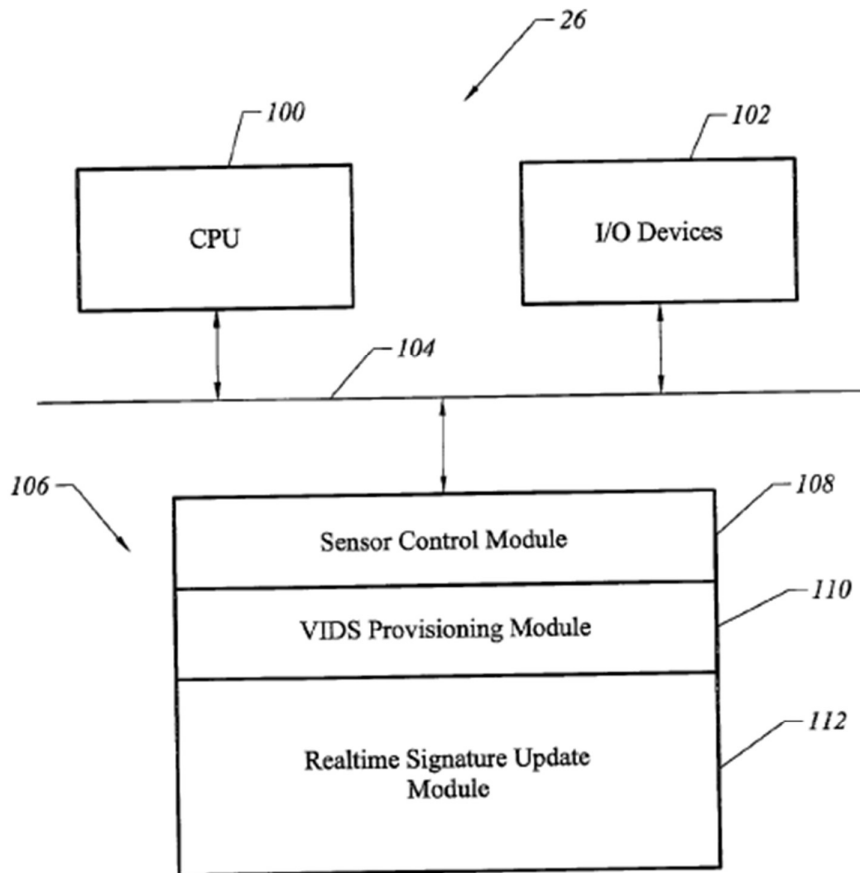


FIG. 13

Gupta FIG. 13

47. This realtime signature update module coordinates the delivery of intrusion signatures 70 to sensors 22. This module is responsive to control signals from the update server 38. Gupta [0132].

48. The VIDS provisioning module operates in conjunction with a sensor 22 and the update server 38. As previously discussed, the sensor 22 performs

signature matchings against network traffic and generates responses in case of intrusions. A sensor 22 accepts configuration and control messages and sends intrusion alerts and/or events to the sensor management system 26. Since each VIDS can customize the response in the face of an intrusion, a sensor must be able to generate VIDS specific responses. In addition, the sensor 22 labels all alerts and events sent to the sensor management system 34 with VIDS identifiers so that the sensor management system 34 does not have to spend extra computer resources in filtering VIDS events. Gupta [0138].

B. Summary of Graham

49. U.S. Patent No. 7,237,264 to Graham et al. (Ex. Graham, “Graham”), entitled “System and Method for Preventing Network Misuse,” is also directed to identifying potential vulnerability information and deriving actual vulnerability data from it. Graham teaches correlating “target fingerprint data ... with the context-based and/or state-based data signature (as indicated at 255) **to determine whether the target is actually vulnerable to the suspicious data signature.**” Graham at 7:14-19.

50. Graham also discloses using firewall-based mitigation actions to prevent an attack from taking advantage of an actual vulnerability.

If the system determines that the target is not vulnerable,
one embodiment of the system generates a low-level alert

and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). **If the system determines that the target is vulnerable**, however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or **may take certain precautionary measures** (at 235). For example, at this stage **the system may attempt to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so)**.

Graham at 7:58-67.

One embodiment of the system factors in the targets response to the detected data signature to further evaluate the probability of network misuse.

Graham at 8:3-5.

C. Motivation to Modify the Teachings of Gupta with the Teachings of Graham

51. One of ordinary skill in the art would have been motivated to combine Gupta and Graham. Both disclosures are directed towards the same problem, and they share a number of common elements in their solutions. For example, both disclosures make use of potential vulnerability data to determine actual vulnerability data.

52. Gupta, however, is broader in its view of vulnerabilities. While it discloses software vulnerabilities (*see, e.g.*, buffer overflow attacks, Gupta, [0156]), it also discloses protocol and network vulnerabilities as well. Graham discloses greater detail and specificity with remediating and mitigating such weaknesses. One of ordinary skill in the art as of July 2003 would have looked to a reference, such as Graham, to provide details appropriate to their technological environment. Such a combination is almost mandated by Gupta's disclosure to identify target-specific attacks. Graham enables the skilled artisan, in possession of Gupta, to employ a wider range of mitigations and more clearly identify actual vulnerability data within its narrower purview.

53. Gupta discloses a security system that identifies devices with actual vulnerabilities, determines attacks directed to the identified devices, and presents options to a user for mitigating the attacks. Gupta, [0151], [0154], [0164]-[0165]. Graham discloses a security system that identifies attacks against vulnerable systems and takes precautionary measures including blocking data transmissions with a firewall. Graham, 7:58-67.

54. Gupta does not expressly recite that it uses firewall functionality, but a POSITA understood that firewall functionality was a well-known mitigation technology for preventing attacks, as discussed in the State of the Art section. EX 1005 9:36-41. Thus, a POSITA would have been motivated to modify the teachings

of Gupta to implement the additional corrective actions disclosed in Graham of using a firewall for any identified vulnerabilities by combining the teachings according to known methods to yield predictable results

55. Further, the combination permits but does not require physical incorporation of elements from Graham into Gupta.

D. Detailed Analysis of Claims

1. Claim 1

- a.** *[1.0] A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:*

56. To the extent that the preamble is limiting, Gupta discloses this limitation.

57. First, Gupta discloses a non-transitory computer-readable media that stores instructions.

58. Gupta describes “an exemplary computer network 20” which “includes a set of network security sensors 22 configured in accordance with the invention ... to implement local and distributed security operations.” Gupta, [0030]. A “sensor management system 26 ... provides supervisory control of a sensor 22,” and together also with a redundant sensor 24 “is referred to as a local sensor security module 27.” Gupta, [0031]-[0032].

59. The sensor 22 includes a “memory 50” which “stores a set of executable programs utilized to implement functions of the invention.” Gupta, [0037]. Gupta alternatively discloses that “the executable programs are stored in memory associated with each processor that executes a program.” Gupta, [0037]. The programs are examples of instructions.

60. More generally, Gupta discloses that the various distributed components (e.g., computer security sensors, statistical analysis engines, etc.) include computer-readable media that store instructions. *See* Gupta, [0037]; *see also* [0130] (sensor management system 26 “memory 106 stores a set of executable programs utilized to implement features of the invention”), [0150] (sensor management system 34 includes memory 146, which “stores a set of executable programs to implement the functions of the update server”).

61. Gupta’s FIG. 1 depicts a local security module 27 which includes a sensor 22 and a sensor management system 26, and a global sensor management system 34, all of which are connected to an update server 38, each of which include processors executing instructions stored on non-transitory computer readable media. Gupta, FIG. 1, [0032]-[0033]. Gupta further discloses that the update server 38 includes “standard computer components” including a CPU 140 and a “memory 146” storing “a set of executable programs to implement the functions of the update server.” Gupta, [0150]

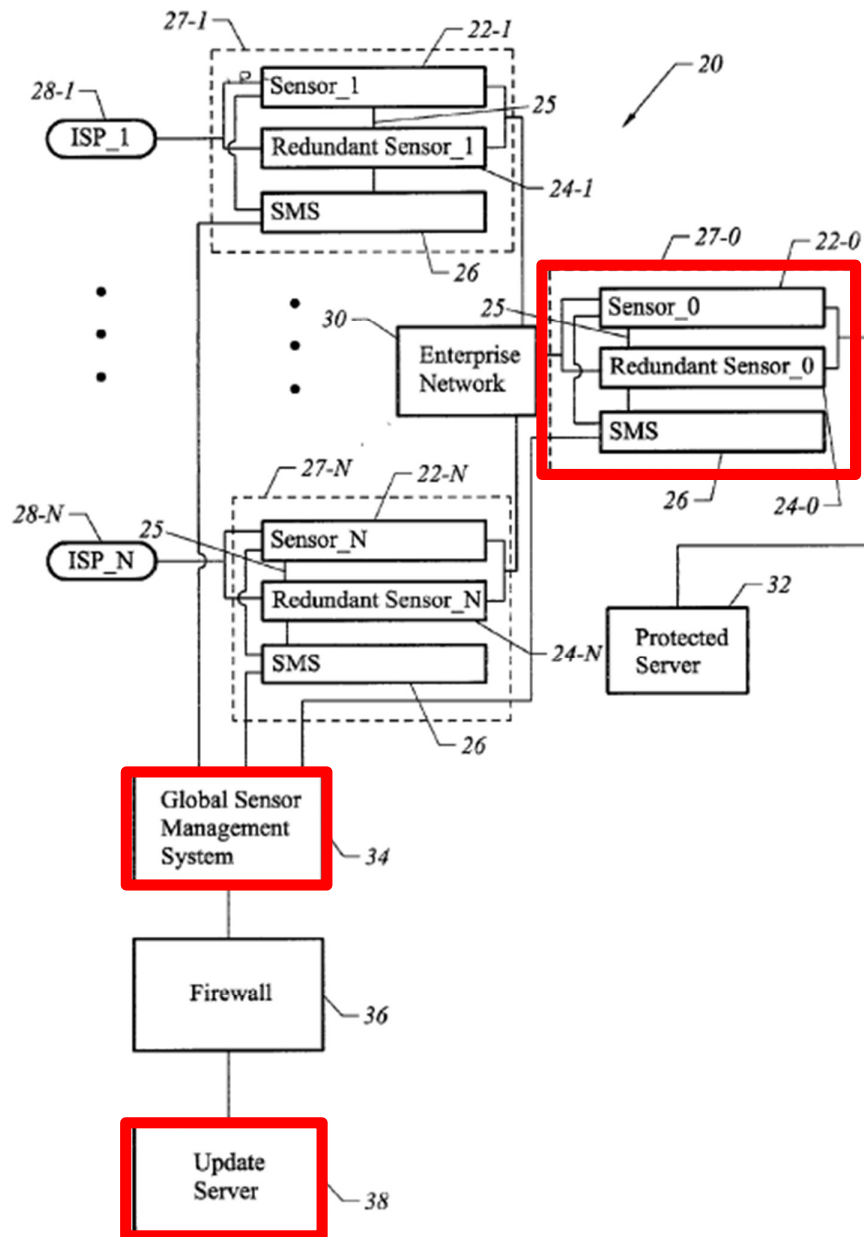


FIG. 1

Gupta FIG. 1 (Annotated)

62. **Second**, Gupta discloses executing the instructions by one or more processors.

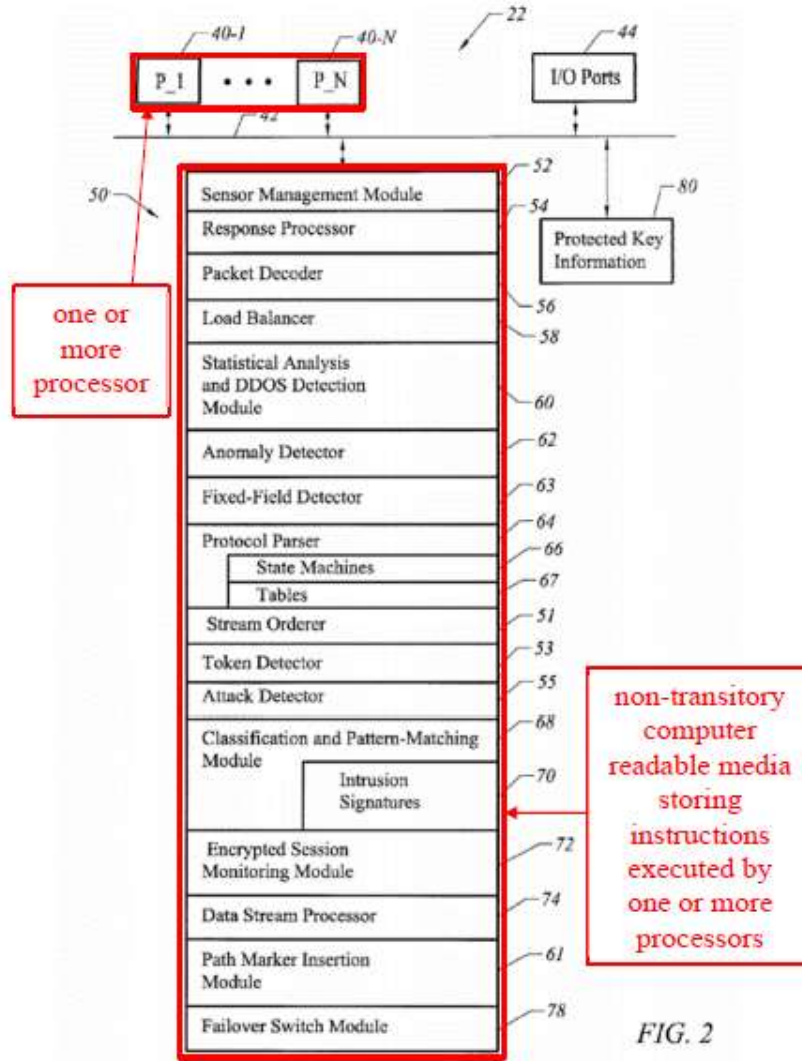
63. Gupta further discloses *instructions* stored at the update server 38 are downloaded to the local security module 27 and global sensor management system 34. For example, Gupta discloses the update server 38 “coordinate[s] the delivery” of “**software updates** to the local sensor security module 27.” Gupta [0034].

64. Gupta further discloses the update server is “used to notify customers of **new software**,” and “provides the **software images** and signature files **for download**.” Gupta [0138]. It is well known in the art that computing devices can download and install software from a software update server (a “download server downloads updating files to the client” computer and the “desired revised software product is then installed on the client computer”). EX-1014, Abstract.

65. Therefore, a POSITA would understand that Gupta’s update server 38 stores software (*instructions*) that is downloadable by local security module 27 and global management system 34.

66. Gupta further discloses executing the *instructions* downloaded from update server 38 by “processor[s] 40_1 through 40_N,” CPU 100 of the sensor management system 26, and CPU 120 of the global management system 34. Gupta, [0036], [0129], [0133]. As illustrated in FIG. 2, the processors 40 are connected to the memory 50 (storing the downloaded software from update server 38) via a

system bus, and therefore the executable programs in memory 50 are executed by “one or more processors” 40. Gupta, [0036]-[0037].



Gupta, FIG. 2 (annotated)

67. Similarly, as illustrated in FIG. 13, Gupta discloses the “sensor management system 26” is in the “form of a general-purpose computer, including a central processing unit 100” and a “memory 106” storing “a set of executable

programs utilized to implement features of the invention,” which are connected via a “system bus 104.” Gupta, [0129]-[0130]. Likewise, as illustrated in FIG. 14, the “global sensor management system 34” is also “in the form of a general-purpose computer, including a central processing unit 120” and a “memory 126.” Gupta, [0133]-[0134]. Thus, a POSITA would understand that processors (40-1 thru 40-N) or the central processing unit 100 or 120 (*one more processors*) executes software *instructions* downloaded from update server 38 to memory 50 or 106 or 126, respectively.

68. Therefore, Gupta discloses “*a non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to,*” as claimed.

- b. **[1.1] *receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;***

69. Gupta renders obvious this limitation. Gupta discloses two data storages, including one that contains potential vulnerabilities and one that contains actual vulnerabilities. Gupta further discloses receiving the first vulnerability information. See, e.g., Gupta, claim 1.

70. Gupta discloses an attack file identifying potential vulnerabilities and devices susceptible to those vulnerabilities (*first vulnerability information*) that is

generated based on a hierarchy of different computer attacks and countermeasures (*second vulnerability information*) stored in a hierarchical attack categorization module 150 (i.e., *a second data storage*). Gupta discloses “*first vulnerability information*” by disclosing an “attack file” that identifies “computer attacks and counter measures relevant” to the network. Gupta, [0151], [0164]. Thus, a POSITA would understand that the “attack file” in Gupta contains “*first vulnerability information*” as recited in this claim limitation.

71. Gupta further discloses that the attack file is generated using a broader set of potential vulnerability information (*second vulnerability information*) from Gupta’s hierarchical attack categorization module (*second data storage*), that identifies a plurality of potential vulnerabilities as recited in this claim limitation. For example, with reference to the update server illustrated in Figure 15, Gupta discloses “[t]he attack file 149 may be formed utilizing the hierarchical attack categorization module 150 of the invention. The hierarchical attack categorization module 150 is used to develop, deploy and manage information on different computer attacks and countermeasures.” Gupta, [0154].

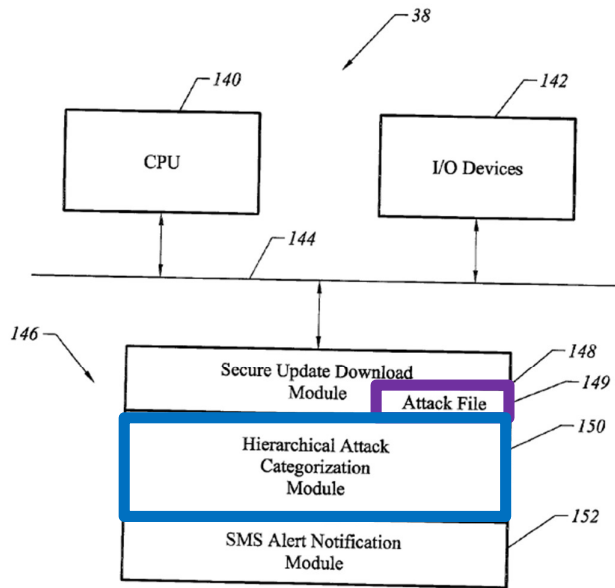


FIG. 15

Gupta, FIG. 15 (annotated)

72. Gupta discloses that this hierarchical attack categorization module creates a hierarchy of potential vulnerabilities and attacks; the hierarchy is then used to generate actual vulnerability information for the target platform that is then stored in the attack file. *See* Gupta, [0164]. As illustrated in FIG. 17, Gupta discloses that this hierarchical attack categorization module creates a hierarchy of different potential vulnerabilities and attacks; the hierarchy is then used to generate actual vulnerability information for the target platform stored in the attack file:

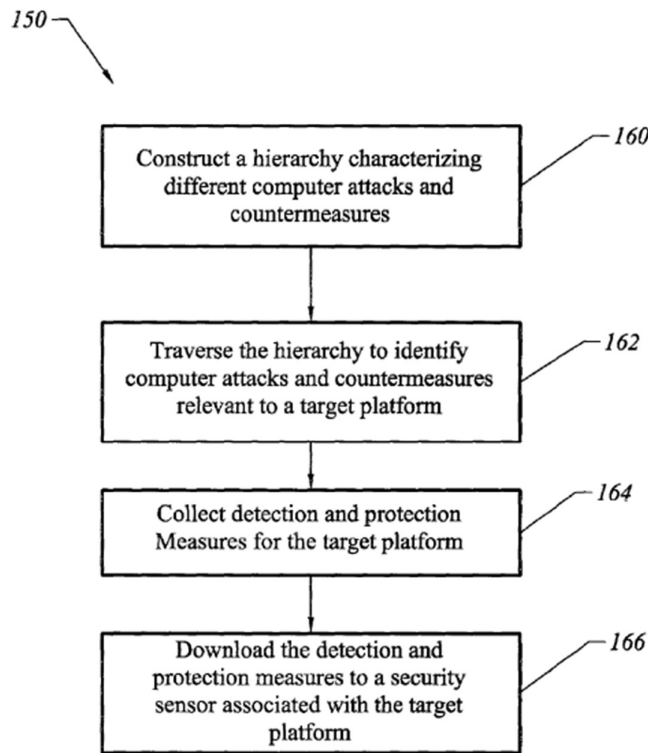


FIG. 17

Gupta FIG. 17

The module initially constructs a hierarchy characterizing different computer attacks and countermeasures (block 160) ... **The hierarchy is then traversed to identify computer attacks and countermeasures relevant to the target platform (block 162). Detection and protection measures for the target platform are then collected (block 164). This can result in an attack file 149. A sensor is then supplied, through a download, with the protective software (e.g., the attack file) for the target platform (block 166).**

Gupta [0164].

73. The attack file “clearly describe[s], in one data structure”, what attacks a given environment is vulnerable to, what protection mechanisms and signatures are available, and how detection alerts are correlated. Gupta [0165].

74. Gupta further discloses that the secure update download module 148 of the update server includes executable code executed by CPU 140 to download an attack file 149 to a sensor management system 26. The attack file 149 specifies attacks and counter measures and includes information forming the intrusion signatures 70 processed by the classification and pattern-matching module 68 stored in memory 50 of the network sensor 22. Gupta [0151]. Gupta further discloses the processors 40 are connected to the memory 50 (storing the downloaded software from update server 38) via a system bus, and therefore the executable programs in memory 50 are executed by “*one or more processors*” 40 (red). Gupta, [0036]-[0037]. Thus, Gupta further discloses processors 40 *receiving first vulnerability information* (purple) in the attack file stored in memory 50 (*first data storage*)(blue). Gupta, [0151].

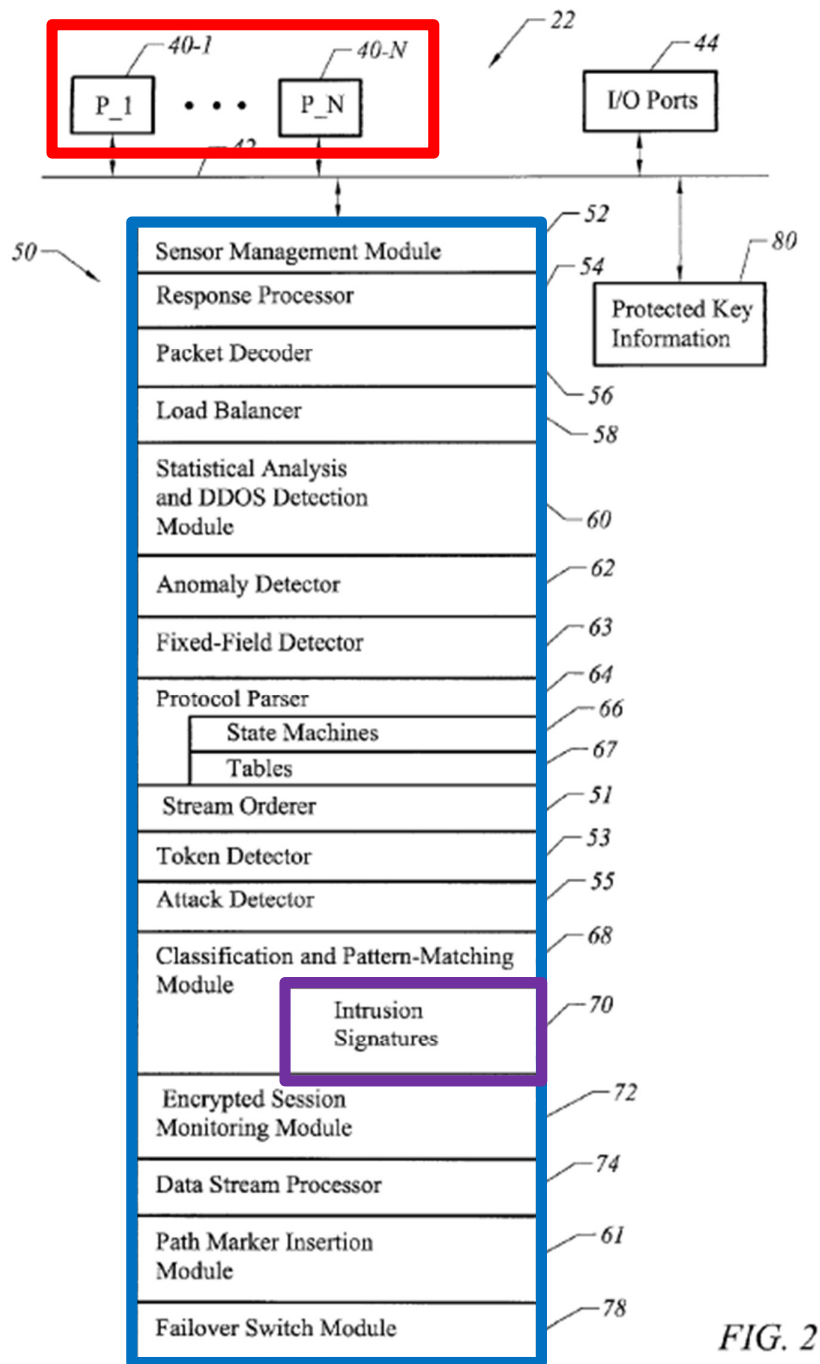


FIG. 2

Gupta FIG. 2 (Annotated)

75. Therefore, Gupta discloses [1.1].

76. Therefore, Gupta renders obvious “*receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities,*” as claimed.

c. **[1.2] *said first vulnerability information generated utilizing the second vulnerability information, by:***

77. As discussed with respect to [1.1], Gupta discloses that the attack file (*first vulnerability information*) is generated utilizing hierarchy of different computer attacks and countermeasures (*second vulnerability information.*).

d. **[1.3] *identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and***

78. Gupta renders obvious this limitation.

79. Gupta discloses *identifying at least one configuration* by disclosing an attack file that includes configuration information of a device or a target platform. Gupta [0164]-[0165]. Gupta discloses that the attack file includes information for a “target platform” or computing “environment” that identifies a “*configuration.*” For example, Gupta discloses that the vulnerabilities in an attack file may be categorized based on device configurations including “**operating system (e.g., Solaris, Linux, MAC OS).**” Gupta [0160]. Thus, Gupta disclosing categorizing attacks based on

the device configurations which meets the claim limitation of *identifying at least one configuration*.

80. A POSITA understood that Gupta's reference to categorizing an attack file based on the configuration of a "target platform" or computing "environment" would be associated "*with a plurality of devices.*" For example, Gupta expressly discloses protecting enterprise networks which a POSITA understood would include networks with at least three different devices. *See, e.g.,* Gupta, [0032] (an "enterprise network"), [0057] ("enterprise network" different than a "single host/server"), [0068] ("The target system can be a whole enterprise network, an individual server or host machine ...").

81. Gupta further discloses the "attack file" is generated by *identifying* the *configuration*. The attack file is created at the "hierarchical attack categorization module 150" which belongs to the memory 146 of update server 38: "[d]etection and protection measures for the target platform are then collected (block 164)," which "result in an attack file." Gupta [0150], [0164]. Based on Gupta's statement that the hierarchy of known attacks is traversed to identify those that are "relevant" to a particular target platform, and its teaching of categorizing attacks based on the operating system of the target platforms, a POSITA understood Gupta would identify configuration information such as the operating system of the computers to be protected to determine if a known attack is "relevant." *See* Gupta, [0164].

Therefore, a POSITA understood that the resulting “attack file” includes “detection and protection measures for the target platform,” which is based on *identifying... configuration* information of the target platform (e.g., an enterprise network including “a plurality of devices”).

82. Therefore, Gupta renders obvious “*identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device*,” as claimed.

- e. **[1.4] *determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;***

83. Gupta renders obvious determining that the plurality of devices is actually vulnerable to an actual vulnerability based on the configuration.

84. Gupta discloses that *accurately identified vulnerability information* in the attack file is identified using Gupta’s hierarchical attack categorization module 150 of *second vulnerability information*. For example, Gupta discloses that the update server 38 contains a hierarchical attack categorization module 150 (contains *second vulnerability information*), which generates the attack file. Gupta [0154] (“[t]he attack file 149 may be formed utilizing the hierarchical attack categorization module 150”).

85. Gupta further discloses determining that *a plurality of devices are vulnerable to attacks (at least one accurately identified vulnerability)*. Gupta [0165] (“describe... what attacks a given environment is vulnerable to”). Gupta further describes how an attack file is generated to contain “computer attacks and countermeasures **relevant** to the target platform.” Gupta [0164]. As previously discussed in [1.3], a POSITA understood that Gupta’s attack file includes information for a “target platform” or computing “environment” that identifies a *configuration associated with a plurality of devices*, i.e., the target platform or the computing “environment” are within an “enterprise network 30.” Gupta, FIG. 1, [0032].

86. Therefore, a POSITA would have recognized that the attack file is directed to a target platform that includes different devices within the enterprise network. Thus, a POSITA understood that Gupta discloses determining the different devices are vulnerable to attacks based on the configuration information in the attack file.

87. Therefore, Gupta renders obvious “*determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities,*” as claimed.

f. [1.5] *identify an occurrence in connection with at least one of the plurality of devices;*

88. Gupta discloses this limitation.

89. First, Gupta discloses performing intrusion detection to identify an occurrence. According to Gupta,

The anomaly detector 62 is one mechanism utilized by the invention to prevent attacks. Another mechanism utilized in accordance with the invention is signature processing. The signature processing system detects attacks by looking for signatures that are specific combinations of patterns (e.g., numerical field values, string matches, and the like) existing in monitored network traffic.

Gupta, [0083].

90. Gupta provides additional details about how these signatures lead to the identification of an AttackID (AID):

Both the fixed-field detector and the protocol parser 64 generate Signature Sub-IDs (SSIDs) that indicate the presence of subsets of the patterns required for detection of a particular signature. The classification and pattern matching module 68 accepts the SSIDs in the order in which they occur and determines if all the SSIDs required to form the complete pattern of a signature occurred. The pattern signatures are stored as intrusion signatures 70. For each complete signature, the classification and pattern

matching module 68 raises an AttackID (AID) that indicates the attack that was found in the communications being monitored.

Gupta, [0086].

91. This describes identifying a presently occurring attempt to take advantage of a vulnerability in connection with devices being protected on the network.

92. Further, Gupta teaches that these actions, with respect to individual sensors 22, are “used to implement a shared-resource virtual intrusion detection system.” Gupta, [0031]. Gupta further teaches implementing a “global shared-resource virtual intrusion detection system” with the “global sensor management system 34.” Gupta, [0033].

93. Therefore, Gupta discloses “*identify an occurrence in connection with at least one of the plurality of devices,*” as claimed.

g. **[1.6] *determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and***

94. Gupta discloses this limitation.

95. Gupta discloses using an attack file provided to a sensor that identifies actual vulnerabilities of devices on the network. The sensor determines the detected

occurrence may take advantage of at least one accurately identified vulnerability, which a POSITA understood as determining if an accurately identified vulnerability of a device is susceptible to an “*occurrence*” based on “*first vulnerability information*.” For example, Gupta discloses that the sensor is provided with an attack profile for the target platform which identifies what attacks a given environment is vulnerable to, what protection mechanisms and signatures are available, and how detection alerts are correlated. Gupta [0164]-[0165]. Gupta further discloses several methods of threat detection of an actual vulnerability. For example, Gupta teaches implementing the threat detection by the sensors for a packet analysis, by way of “looking for signatures that are specified combinations of patterns ... existing in monitored network traffic.” Gupta, [0083]; *see also* [0086] (generating SSIDs in response to comparing signatures to the contents of packets). Based on this packet analysis, the system determines when “*at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence*” using the signatures (“*utilizing the first vulnerability information*”).

96. By way of further example, Gupta discloses an anomaly detector 62 to identify computer attacks. The detector looks for any event, state, or behavior that is considered to be abnormal by certain pre-defined standards defined in the attack file. Gupta [0051].

97. Gupta explains that anomaly-based intrusion detection approaches complement the signature-based approaches by offering a means to detect attacks whose signatures are not yet known or attacks that exhibit modified behavior (e.g., intentionally stealthy attacks or variants of existing attacks in new environments). Gupta [0052].

98. Gupta further discloses that the update server 38 updates sensors with updated attack signatures, anomaly profiles, and the like. The various attack detection methods (i.e., anomaly-based, signature-based, etc.) can also be performed on information decrypted by the various decryption methods. Gupta [0166].

99. Thus, Gupta discloses several different ways for determining when “*at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence*” using the attack file (“*utilizing the first vulnerability information*”).

100. Therefore, Gupta discloses “*determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information,*” as claimed.

- h. [1.7] *cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;***

101. Gupta in combination with Graham renders obvious this limitation.

102. Gupta discloses providing a user with the ability to select between different occurrence mitigation actions of diverse occurrence mitigation types. For example, Gupta discloses that the VIDS 130 in the global sensor management system 34 “implements a graphical user interface (GUI)” that “enables the subscriber to... manage and monitor the VIDS” and the “GUI can be implemented within a browser, either as an applet or using HTML. Gupta, [10131], [0143]. The VIDS 130 supports “different security policies, protection objectives, and security management preferences.” Gupta, [0136]. A POSITA understood that the availability of multiple “security policies, protection objectives, and security management preferences” demonstrates that Gupta’s teachings apply to a variety of *different occurrence mitigation actions* in response to different threats and attacks.

103. Gupta discloses providing one or more options to selectively utilize different occurrence mitigation actions, including terminating TCP connections, which a POSITA understood to be *an intrusion prevention system-based occurrence*

mitigation technique as recited in this claim. For example, Gupta discloses that sensor 22 include a response processor 54 that responds to an attack ID (AID) and “generates alerts that provide notification of an attack. The response processor 54 also attempts to prevent the attack. **Short-term responses include terminating TCP connections.** Long-term responses include packet logging for further analysis to improve detection and response.” Gupta [0087]. Thus, Gupta discloses terminating TCP connections, which a POSITA understood to be an “*intrusion prevention system-based occurrence mitigation type*.”

104. Gupta also suggests a *firewall-based occurrence mitigation type*. For example, Gupta’s sensor 22 includes a “fixed-field detector 63” that “[o]nce the packet is received by the sensor 22,” scans the “the source and destination address fields” of a packet “for attacks that leave characteristic traces in certain specific fields.” Gupta [0084], [0101]. “A web server suddenly seeing a lot of requests from new IP addresses may also be considered an anomaly.” [0051]. A POSITA would understand that the best way to prevent such DOS attacks is to drop these packets at the Firewall.

105. To the extent that Patent Owner asserts that Gupta does not expressly disclose a “firewall-based” occurrence mitigation type, Graham discloses providing occurrence mitigation actions, including the use of techniques known in the art, including firewall techniques, that a POSITA understood could beneficially be

utilized among the plurality of mitigation options provided in Gupta. For example, Graham teaches providing different occurrence mitigation actions:

If the system determines that the target is not vulnerable, one embodiment of the system generates a low-level alert and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). If the system determines that the target is vulnerable, however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or may take certain precautionary measures (at 235)

Graham at 7:58–65.

106. Graham provides an example:

If the system determines that the target is not vulnerable, one embodiment of the system generates a low-level alert and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). **If the system determines that the target is vulnerable**, however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or **may take certain precautionary measures** (at 235). For example, at this stage **the system may attempt to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so).**

Graham at 7:58-67.

107. Graham further discloses that a factor considered by the system is “the target’s response to the detected data signature to further evaluate the probability of

network misuse.” Graham 8:3–5. Thus, a POSITA understood that Graham teaches occurrence mitigation actions, one of which is a firewall-based occurrence mitigation type — the firewall blocking incoming data transmission from a suspect node. Graham at 7:65–67.

108. Thus, the combined teachings of Gupta and Graham disclose this limitation. As discussed in the Motivation to Modify the Teachings of Gupta with the Teachings of Graham section, it would have been obvious to a POSITA to modify the teachings of Gupta with the firewall mitigation technique taught by Graham because both references teach the use of multiple, known mitigation techniques and the benefit of using the technique that best fits the circumstances of a given occurrence or device, and would be assured of its success.

109. Gupta further teaches that a user is able to manage and monitor the virtual intrusion detection system (VIDS) provisioning module 110 for a plurality of devices being monitored by a sensor. Gupta [0131], [0143]. In particular, Gupta teaches:

The VIDS provisioning module 130 facilitates protection for multiple traffic streams for different subscribers using a Single Sensor platform while maintaining security separation. The module 130 supports different security policies, protection objectives, and security management preferences effectively and efficiently.

Gupta [0136].

110. Thus, Gupta describes the occurrence mitigation actions are facilitated by the VIDS provisioning module that “facilitates protection for multiple traffic streams for different subscribers” which a POSITA understood teaches *utilization of . . . occurrence mitigation actions . . . across the plurality of devices* as recited.

111. Therefore, Gupta in combination with Graham renders obvious “*cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices,*” as claimed.

i. [1.8] wherein the at least one configuration involves at least one operating system.

112. Gupta discloses this limitation.

113. As noted at [1.3], the configuration may be an operating system configuration for target platforms.

In addition to defining attack categories, it is useful to define attack target platforms. In one embodiment of the invention, the following hierarchy is identified: (1) vendor (e.g., SUN, IBM, HP, SGI, CISCO), (2) device (e.g., workstation, server, router, firewall), (3) **operating**

system (e.g., Solaris, Linux, MAC OS), and (4)
version/revisions.

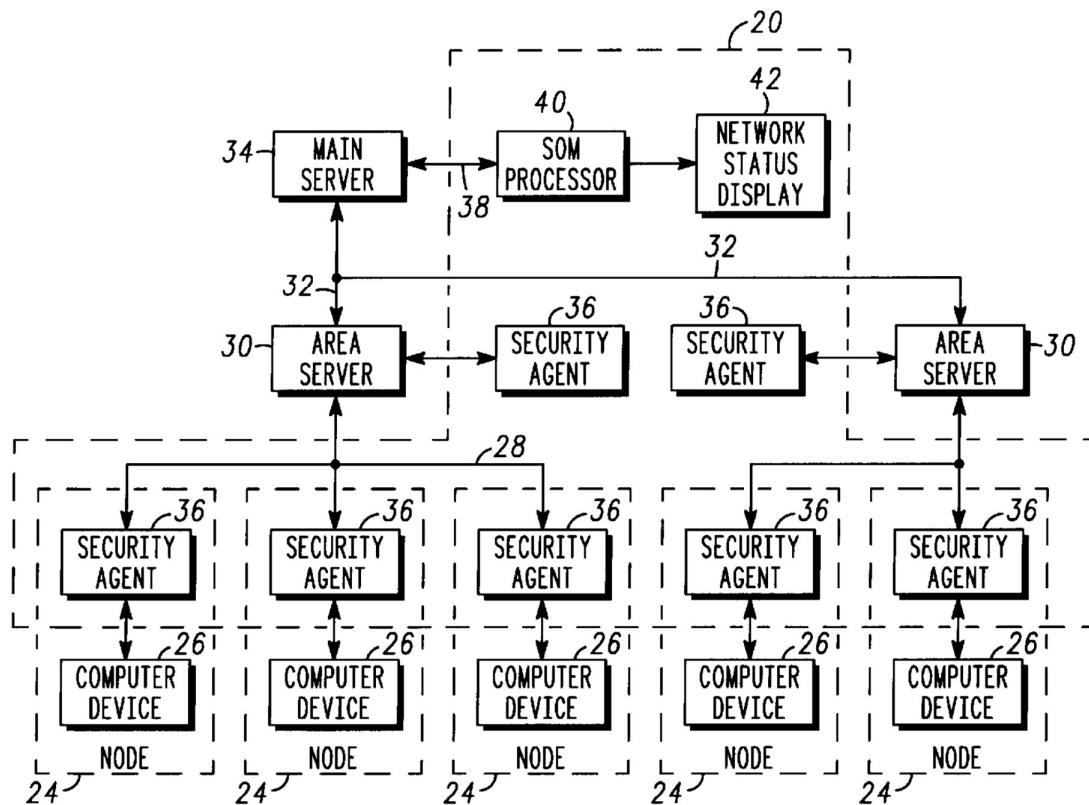
Gupta, [0160].

114. Gupta therefore discloses “*wherein the at least one configuration involves at least one operating system,*” as claimed.

**X. THE COMBINATION OF Gupta AND GRAHAM IN VIEW OF HILL
RENDERS OBVIOUS CLAIM 2**

A. Summary Of Hill

115. Hill discloses a network security system for responding to a security attack on a computer network having a plurality of computer nodes, each having a security agent protecting a computer device as illustrated in FIG. 1. Hill Abstract



Hill FIG. 1

116. Dynamic network security system 20 includes a plurality of security agents 36 each of which is associated with one or more nodes 24. Security agents 36 are configured to concurrently detect occurrences of security events on associated computer nodes 24. Security agents 36 are software programs located at nodes 24 and area servers 30 that identify security events as they appear at the nodal level. Security events may include port scans, malicious software, penetration attempts,

and others that are identified through either a specific code signature or through actions or attempts at actions. Hill 4:31-41.

117. Hill discloses that security events can include destructive virus, snooping virus, worm, Trojan horse, FTP requests, network overload and/or additional evolving types of security events relative to the computer network for which the dynamic network security system is used. Hill 5:58-65.

118. Hill discloses that the node autonomously detects and repulses or at least attempts to repulse security events 50 (FIG. 3) at the nodes using conventional software tools installed on computer devices 26 such as virus detectors, firewalls, and the like. Hill 7:64-8:3.

B. Motivation to Modify the Teachings of Gupta with the Teachings of Hill

119. A POSITA would have been motivated to modify the teachings of Gupta with the teaching of Hill because both Gupta and Hill are directed to identifying vulnerabilities and applying corrective actions to protect against identified vulnerabilities. More specifically, Gupta discloses a security system that utilized a sensor security module to detect and repulse attacks. Like Hill, the security sensor module of Gupta includes a set of software in the form of executable programs utilized to implement the functions of detecting and repulsing attacks as illustrated in

FIG. 2. FIG. 1 of Gupta teaches that a security module 27 (yellow) can be utilized to protect protected server (red).

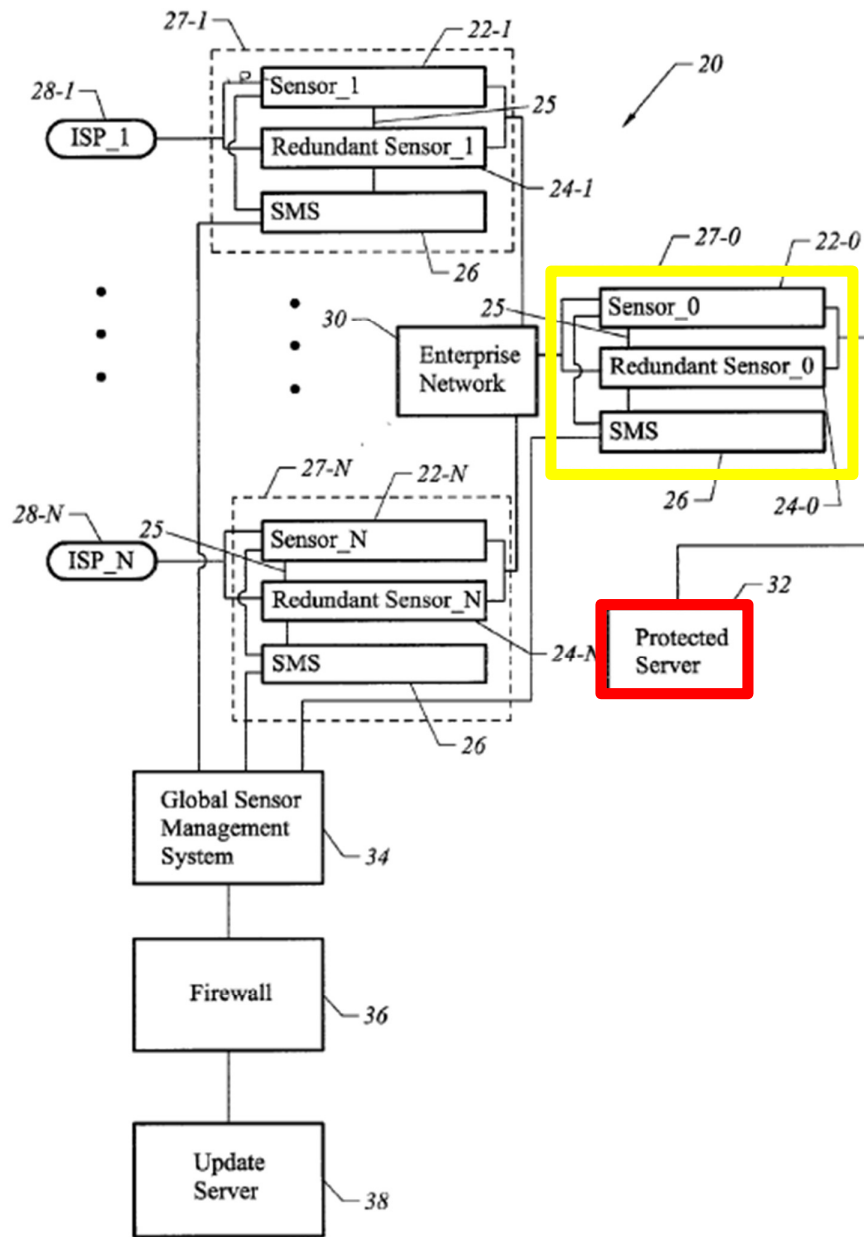
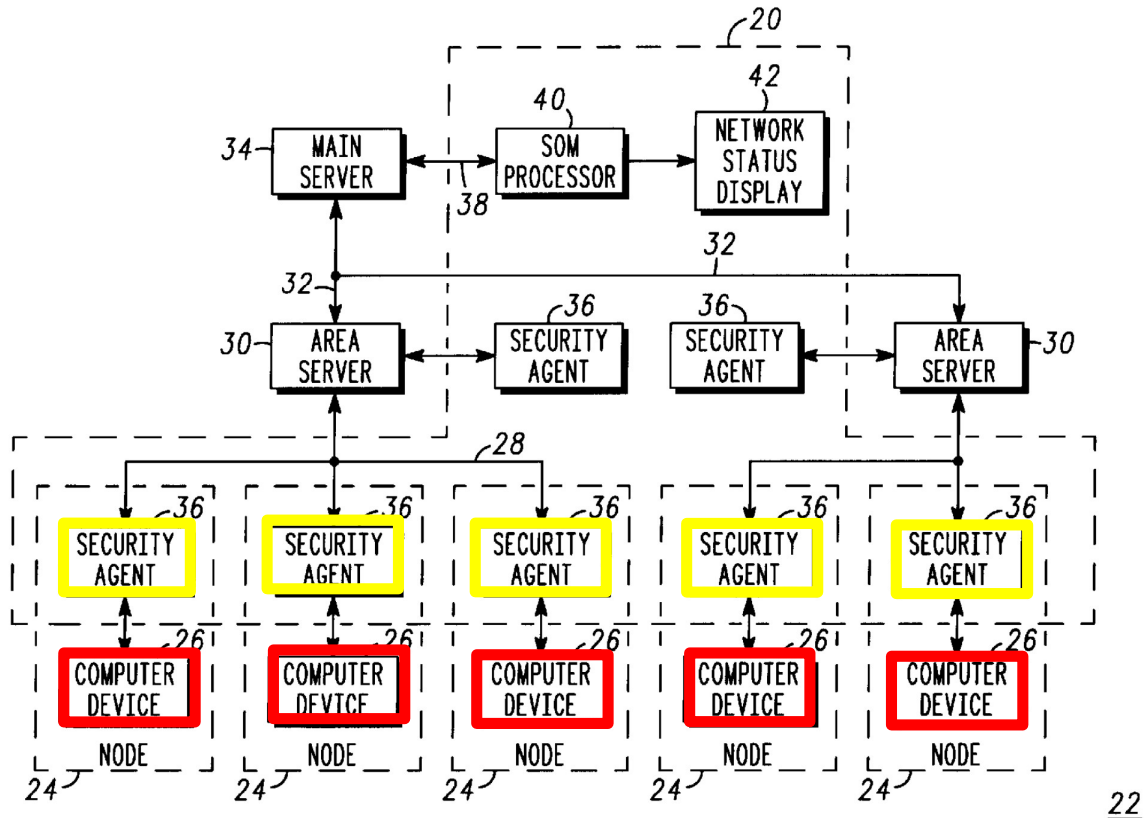


FIG. 1

Gupta FIG. 1 (Annotated)

120. Gupta does not expressly disclose utilizing a security module at each computer device, nor does it discourage the use of a security module at each computer device. On the other hand, Hill expressly discloses using a security agent at each computer device.



Hill FIG. 1 (Annotated)

121. As discussed in the State of the Art section, by July 2003, the benefits of using distributed mobile agents for detecting vulnerabilities and automatically responding to such vulnerabilities was well-known, including overcoming network latency, reducing network load, executing asynchronously and autonomously,

adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. EX-2021 pp. 10-14. In addition, a POSA understood that layered security can be provided with a hierarchical IDS where a mobile agent backs each node up and restores any lost functionality to provide redundancy for the security of the network. EX-1021 p. 21. Thus, a POSITA would have been motivated to modify the teachings of Gupta to include a security module for detecting and automatically responding to vulnerabilities at each computer device as taught by Hill.

C. Detailed Analysis of Claim 2

1. Claim 2

122. Claim 2 depends from Claim 1 and generally recites that the non-transitory computer-readable media includes first instructions for a first processor, second through fifth instructions stored at a network device for a second processor and sixth instructions for a third processor at an administrative computer. As set forth in more detail below, Ground 2 relies on the same combination of Gupta and Graham, and modifies the teaching of Gupta with the teachings of Hill to disclose that the second through fifth instructions are stored at the local sensor security module of Gupta distributed at each computer device as taught by Hill.

- a. ***[2.0] The non-transitory computer-readable media of claim 1, wherein the at least one actual vulnerability is one of the actual vulnerabilities that are of the at least operating system that is installed on the plurality of devices, the occurrence is at least one of a plurality of occurrences, and the instructions include:***

123. Gupta discloses this limitation for the reasons discussed with respect to limitation [1.4] and [1.7]. Specifically, Gupta discloses that the actual vulnerability is associated with a “target platform” or computing “environment” having an identified configuration, and the occurrence can include a firewall-based occurrence and an intrusion detector functionality occurrence.

- b. ***[2.1] first instructions that, when executed by at least one first processor of the one or more processors of at least one server in communication with the at least one second storage, cause the at least one first processor to***

124. Gupta discloses that the update server 38 (*at least one server*) includes CPU 140 (*first processor*) and the hierarchical attack characterization module 150 (*one second storage*) in memory 146.

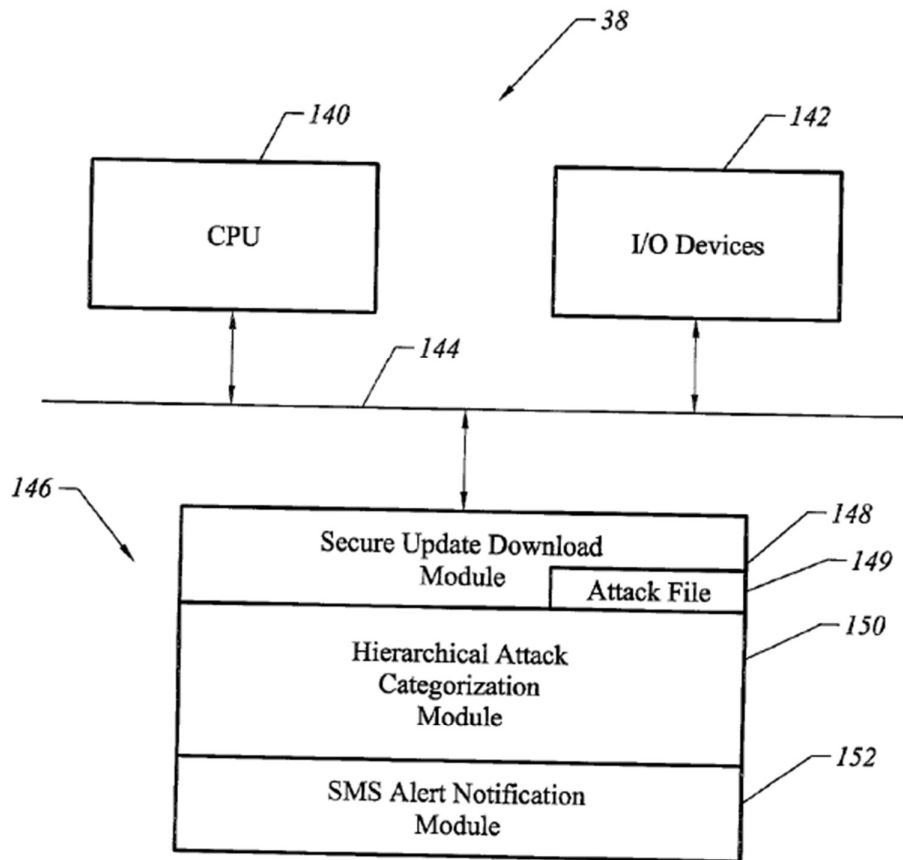


FIG. 15

Gupta FIG. 15.

- c. *[2.2] generate the first vulnerability information utilizing the second vulnerability information, and*

125. Gupta discloses this limitation for the same reasons as discussed with respect to limitation [1.2]

- d. ***[2.3] communicate, from the at least one server and to the at least one of the plurality of devices over at least one network, the first vulnerability information***

126. Gupta discloses that the update server communicates the attack file that identifies “computer attacks and counter measures relevant” for the network (*first vulnerability information*) to a local security sensor module (*one of a plurality of devices*) as discussed with respect to limitation [1.1].

127. To the extent that PO asserts that *at least one of the plurality of devices* must be an endpoint computer device and argues that the local security sensor module is not located at the endpoint computer device, Hill discloses locating the local security sensor module at an endpoint computer device. A person would be motivated to modify the teachings of Gupta with the teachings of Hill for several reasons.

128. First, the teachings of Gupta are broad enough to suggest to a POSITA that the local security sensor module would be co-located with a host computer device. Specifically, FIG 1 illustrates that local security sensor module 27-0 is positioned between the enterprise network 30 and a protected server 32, and in-line with the server such that it monitors traffic on the physical link connecting the protected server 32 to the enterprise network 30. EX-1006 [0032], [0145]. Further, Gupta discloses that the targeted platform to be protected can be a host machine or

a particular user on a machine. EX-1006 [0068]. In addition, Gupta's use of the term "local" security sensor module describes the intended distributed nature of the modules to be used with host computer devices.

129. Second, as discussed in the State of the Art section, a POSITA understood that security agents distributed at computer device provided advantages over more centralized network security systems. EX-1021 pp. 10-14.

130. Third, Hill provides an example of security software for detecting and repulsing attacks (security agent) being distributed at nodes 24 containing computer devices 26. Hill FIG. 1.

131. Fourth, Hills' disclosure of using inline software agents is consistent with the '066 Patent description of using inline agents and sensors to monitor the computer devices in the network. EX-1001 FIG. 11.

132. Thus, a POSITA would be motivated to modify the teachings of Gupta to locate the local sensor security module at the computer device as taught by Hill. Further, because Hill teaches that the security agent located at the computer device is implemented in software to detect and repel intrusions, a POSITA would be confident of the success modifying the teachings of Gupta because the local security sensor is likewise implemented in software as illustrated in FIG. 2 of Gupta.

- e. *[2.4] second instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the second instructions are executed by at least one second processor of the one or more processors of the at least one of the plurality of devices, cause the at least one second processor to:*

133. Gupta discloses that second instructions are stored in memory 50 (*first data storage*) (blue) which is part of the local security sensor module (*one of the plurality of devices*) and are executed by P_1 (40-1)...P_N (40-N) processors (*by at least one second processor of the one or more plurality of processors*) (green) as illustrated in FIG 2:

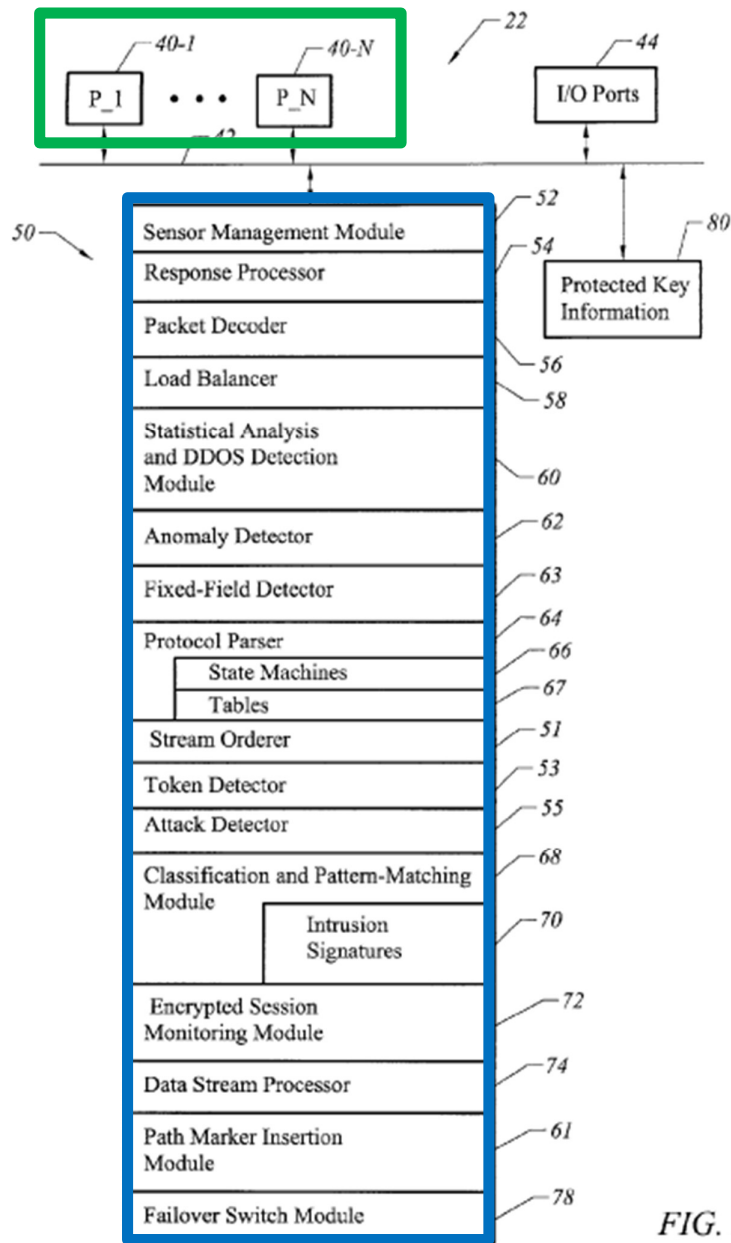


FIG. 2

Gupta FIG. 2 (Annotated)

134. To the extent that PO asserts that *at least one of the plurality of devices* must be an endpoint computer device, a POSITA would be motivated to modify the teachings of Gupta to locate the local security sensor module at the endpoint

computer device as taught by Hill for the reasons described in limitation [2.3], and thus the steps below performed by the second instruction would be performed at the endpoint computer device.

- f. ***[2.5] receive, from the at least one server and at the at least one of the plurality of devices over the at least one network, the first vulnerability information, store the first vulnerability information on the at least one first data storage, and receive the first vulnerability information from the at least one first data storage, the first vulnerability information being relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and excluding at least a portion of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices***

135. Gupta discloses that the update server (*at least one server*) provides an attack file that includes intrusion signatures (*first vulnerability*) that is received at the local sensor security module (*at least one of the plurality of devices*) and stores the intrusion signatures 70 in memory 50 (*at least one first data storage*). Specifically, the secure update download module 148 in update server 38 includes executable code to download an attack file 149 to a sensor management system 26. The attack file 149 specifies attacks and countermeasures. Preferably, the file also identifies unknown attacks and suggests responses for such attacks. The attack file

149 includes information forming the intrusion signatures 70 processed by the classification and pattern-matching module 68. EX-1006 [0151].

136. Further, Gupta describes “provisioning a computer against computer attacks” by “constructing a hierarchy characterizing different computer attacks and counter measures, and traversing this hierarchy to identify computer attacks and counter measures **relevant** to a target platform.” EX-1006 Abstract, [0008], [0164], Claim 1.

137. Gupta discloses that the first vulnerability being relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices in the attack file is identified using Gupta’s hierarchical attack categorization module 150 of second vulnerability information. For example, Gupta discloses that the update server 38 contains a hierarchical attack categorization module 150 (contains second vulnerability information), which generates the attack file. GUPTA, [0154] (“[t]he attack file 149 may be formed utilizing the hierarchical attack categorization module 150). Gupta discloses that the attack file includes information for a “target platform” or computing “environment” that identifies a “configuration.” For example, Gupta discloses that the vulnerabilities in an attack file may be categorized based on device configurations including “operating system (e.g., Solaris, Linux, MAC OS).” Gupta, [0160]. Thus, in order to determine the computer attacks and countermeasures relevant to a

platform, Gupta considers the operating system of the device of the computer environment. A POSITA understood that because Gupta describes that the attack file includes only computer attacks and counter measures **relevant** to a target platform, the attack file would exclude computer attacks and counter measures that are **not relevant** to a target platforms.

- g. *[2.6] third instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the third instructions are executed by the at least one second processor, cause the at least one second processor to*

138. For the same reasons as described with respect to limitation [2.4], Gupta discloses that third instructions are stored in memory 50 (*first data storage*) (blue) which is part of the local security sensor module (*one of the plurality of devices*) and are executed by P_1 (40-1)...P_N (40-N) processors (*by at least one second processor of the one or more plurality of processors*) (green) as illustrated in FIG 2.

139. To the extent that PO asserts that *at least one of the plurality of devices* must be an endpoint computer device, a POSITA would be motivated to modify the teachings of Gupta to locate the local security sensor module at the endpoint computer device as taught by Hill for the reasons described in limitation [2.3], and thus the steps below performed by the third instructions would be performed at the endpoint computer device.

- h. [2.7] identify a first portion of the first vulnerability information that includes data inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other data inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices**

140. Gupta discloses memory 50 stores an anomaly detector 62, which is used to identify network traffic anomalies indicative of an attack based on “anomaly profiles” (*a first portion of the first vulnerability information that includes data inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices*) which are included in the attack profile provided by the update server. EX-1006 [0041], [0166]. For example, Gupta discloses keeping anomaly profiles, and the sensor 22 contains an anomaly detector 62 that detects attacks by packet analysis and identifies several different anomalies, e.g., by “keeping a run-time count of request and response packets separately”; “the existence of a remote root shell on a system that only expected console root login”, “based upon the normal traffic profile of a target domain, which may be a single host/sever, a sub-net, or an enterprise network.” Gupta, [0041], [0044], [0051], [0057],[0081], [0166]. Gupta’s disclosure is consistent with the ’066 Patent disclosure that *data inspection-related information* includes “anomalies”. Gupta Claim 44.

141. As discussed with respect to limitation [2.5] Gupta discloses that the attack file only include specific attacks and countermeasures, e.g., anomaly profiles (*a first portion of the first vulnerability information*) that are relevant to the targeted platform or computing environment and would exclude vulnerability information that is not relevant (*excludes other data inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of device.*)

- i.** *[2.8] identify a first occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and*

142. Gupta discloses this limitation for the same reason as discussed with limitation [2.7] because an anomaly would be *a first occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices.*

- j.** *[2.9] cause a determination whether the at least one of the actual vulnerabilities relevant to the data inspection-related information is susceptible to being taken advantage of by the first occurrence identified in connection with the at least one of the plurality of devices, utilizing the data inspection-related information*

143. Gupta discloses this limitation for the same reason as discussed with limitation [2.7] because identifying network traffic anomalies indicative of an attack

is a determination that an actual vulnerability is susceptible to being taken advantage of.

- k. *[2.10] fourth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fourth instructions are executed by the at least one second processor, cause the at least one second processor to:*

144. For the same reasons as described with respect to limitation [2.4], Gupta discloses that fourth instructions are stored in memory 50 (*first data storage*) (blue) which is part of the local security sensor module (*one of the plurality of devices*) and are executed by P_1 (40-1)...P_N (40-N) processors (*by at least one second processor of the one or more plurality of processors*) (green) as illustrated in FIG 2.

145. To the extent that PO asserts that *at least one of the plurality of devices* must be an endpoint computer device, a POSITA would be motivated to modify the teachings of Gupta to locate the local security sensor module at the endpoint computer device as taught by Hill for the reasons described in limitation [2.3], and thus the steps below performed by the fourth instructions would be performed at the endpoint computer device.

1. ***[2.11] identify a second portion of the first vulnerability information that includes traffic inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other traffic inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices,***

146. Gupta discloses memory 50 stores a classification and pattern matching module 68, and an associated set of intrusion signatures 70 (*a second portion of the first vulnerability information that includes traffic inspection-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices*) used to compare incoming network traffic with the set of intrusion signatures 70 which are included in the attack profile provided by the update server is indicative of an attack. EX-1006 [0042], [0086]. For example, Gupta discloses that the attack file 149 includes information forming the intrusion signatures 70 processed by the classification and pattern-matching module 68. Gupta [0151].

147. As discussed with respect to limitation [2.5] Gupta discloses that the attack file only include specific attacks and countermeasures, e.g., intrusions signatures (*a second portion of the first vulnerability information*) that are relevant to the targeted platform and would exclude vulnerability information that is not relevant (*excludes other traffic inspection-related information of the second*

vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of device.)

- m. [2.12] identify a second occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and**

148. Gupta discloses this limitation for the same reason as discussed with limitation [2.11] because an intrusion would be *a second occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices*

- n. [2.13] cause a determination whether the at least one of the actual vulnerabilities relevant to the traffic inspection-related information is susceptible to being taken advantage of by the second occurrence identified in connection with the at least one of the plurality of devices, utilizing the traffic inspection-related information**

149. Gupta discloses this limitation for the same reason as discussed with limitation [2.11] because matching traffic signatures with the stored intrusion signatures is indicative of an attack, and thus a determination that an actual vulnerability is susceptible to being taken advantage of.

- o.** *[2.14] fifth instructions that are configured to be stored on the at least one first data storage which is part of the at least one of the plurality of devices and that, when the fifth instructions are executed by the at least one second processor, cause the at least one second processor to:*

150. For the same reasons as described with respect to limitation [2.4], Gupta discloses that fifth instructions are stored in memory 50 (*first data storage*) (blue) which is part of the local security sensor module (*one of the plurality of devices*) and are executed by P_1 (40-1)...P_N (40-N) processors (*by at least one second processor of the one or more plurality of processors*) (green) as illustrated in FIG 2.

151. To the extent that PO asserts that *at least one of the plurality of devices* must be an endpoint computer device, a POSITA would be motivated to modify the teachings of Gupta to locate the local security sensor module at the endpoint computer device as taught by Hill for the reasons described in limitation [2.3], and thus the steps below performed by the fifth instructions would be performed at the endpoint computer device.

- p. *[2.15] identify a third portion of the first vulnerability information that includes firewall-related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices, and that excludes other firewall-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices*

152. Gupta discloses memory 50 stores information for the attack file that can be considered firewall related information. For example, as discussed with respect to limitation 2.7, inspection related information identifying anomalies can also be considered firewall-related information. For example, the anomaly detector can use a range of source or destination IP addresses, and identify as an anomaly and received packets having a source destination address outside the range. Gupta [0064], [0075].

153. By way of further example, Gupta also teaches sensor 22 includes a “fixed-field detector 63” that “[o]nce the packet is received by the sensor 22,” scans the packet “for attacks that leave characteristic traces in certain specific fields.” One specific field checked is the source and destination IP address. Gupta, [0084], [0101]. Therefore, a POSITA would understand that Gupta’s fixed-field detector implements a firewall-based application, e.g., to inspect every received packet.

154. Thus, Gupta’s disclosure of the anomaly detector or fixed field detector and associated IP addresses (a third portion of the first vulnerability information that includes firewall related information that is relevant to at least one of the actual vulnerabilities of the at least one operating system of the at least one of the plurality of devices) used to identify IP addresses from which traffic associated therewith should be identified as a vulnerability indicative of an attack. EX-1006 [0042], [0086]. This is consistent with the ’066 Patents disclosure that the data inspection-related information, the traffic inspection-related information, and the firewall-related information are relevant to a same one of the actual vulnerabilities. Gupta, Claim 4.

155. As discussed with respect to limitation [2.5] Gupta discloses that the attack file only include specific attacks and countermeasures, e.g., range of IP addresses (*a third portion of the first vulnerability information*) that are relevant to the targeted platform and would exclude vulnerability information that is not relevant (*excludes other traffic inspection-related information of the second vulnerability information that is not relevant to the actual vulnerabilities of the at least one operating system of the at least one of the plurality of device.*)

156. To the extent that Patent Owner asserts that Gupta does not expressly recite a “firewall-related information”, for the same reasons as discussed with respect to limitation [1.7], Graham discloses using *firewall related information that is relevant to at least one of the actual vulnerabilities of the at least one operating*

system of the at least one of the plurality of devices, including the use of techniques known in the art, including firewall techniques, that a POSITA understood could beneficially be utilized among the plurality of mitigation options provided in Gupta. For example, Graham teaches providing a listing of acceptable source and destination addresses for network traffic. Traffic addressed to an unlisted source or destination will be filtered out and discarded by the firewall. Graham at 1:39-43; 7:58–65. Graham provides an example:

If the system determines that the target is not vulnerable, one embodiment of the system generates a low-level alert and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). **If the system determines that the target is vulnerable**, however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or **may take certain precautionary measures** (at 235). For example, at this stage **the system may attempt to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so)**.

Graham at 7:58-67.

157. Graham further discloses that a factor considered by the system is “the target’s response to the detected data signature to further evaluate the probability of network misuse.” Graham at 8:3–5. Thus, a POSITA understood that Graham

teaches the use of firewall related information to identify an actual vulnerability that is indicative of an attack.

158. Thus, the combined teachings of Gupta and Graham disclose this limitation. As discussed in the Motivation to Modify the Teachings of Gupta with the Teachings of Graham above, it would have been obvious to a POSITA to modify the teachings of Gupta with the firewall mitigation technique taught by Graham because both references teach the use of multiple, known mitigation techniques and the benefit of using the technique that best fits the circumstances of a given occurrence or device, and would be assured of its success.

- q.** *[2.16] identify a third occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices, and*

159. Gupta discloses this limitation for the same reason as discussed with limitation [2.15] because a vulnerability associated with a source or destination IP address would be *a third occurrence of the plurality of occurrences in connection with the at least one of the plurality of devices*

- r.** *[2.17] cause a determination whether the at least one of the actual vulnerabilities relevant to the firewall-related information is susceptible to being taken advantage of by the third occurrence identified in connection with the at least one of the plurality of devices, utilizing the firewall-related information; and*

160. Gupta discloses this limitation for the same reason as discussed with limitation [2.15] because matching IP addresses with the stored source and destination IP addresses is indicative of an attack, and thus a determination that an actual vulnerability is susceptible to being taken advantage of.

- s. *[2.18] sixth instructions that, when executed by at least one third processor of an administrator computer, cause the at least one third processor to:*

161. Gupta discloses that sixth instructions when executed by CPU 120 (purple) of the global sensor management system 34 (*at least one third processor of an administrator computer*) cause the CPU to execute the modules stored in memory 146 (pink). as illustrated in FIG 14:

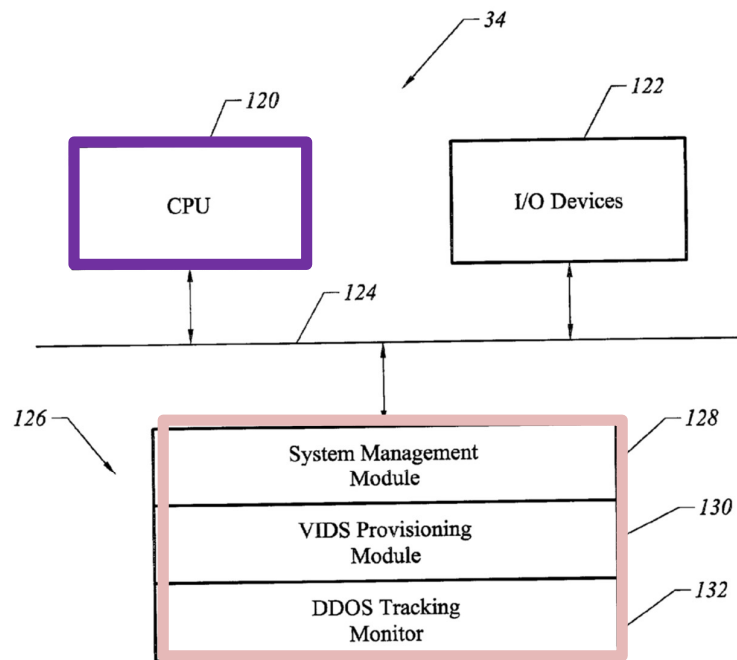


FIG. 14

Gupta FIG. 14 (Annotated)

162. Gupta discloses that anyone with a sensor management system role is automatically mapped to all system-wide operations. The VIDS provisioning module 130 enforces security. Gupta defines the roles that a user may play in the operation of the security system, and although Gupta defines the role of a “system administrator” narrowly, a POSITA understood that all of the roles are to be performed by an administrator of the system. Gupta, [0041]-[0042]. Gupta discloses that the global sensor management system allows a user to manage and

monitor the intrusion detection system and allows configuration of the response processor at each sensor and thus would include an administrator computer. For example, the global sensor management system 34 “implements a graphical user interface (GUI)” that “enables the subscriber to... manage and monitor the VIDS” and the “GUI can be implemented within a browser, either as an applet or using HTML.” GUPTA, [10131], [0143]. The VIDS 130 supports “different security policies, protection objectives, and security management preferences.” GUPTA, [0136]. Gupta further discloses that the “[t]he response processor 54 is configured by the system administrator.” Gupta, [0048]. A POSITA understood that the availability of multiple “security policies, protection objectives, and security management preferences” and configuration of the response detector demonstrates that Gupta’s global sensor management systems carries out the policies set forth below, including an anomaly based policy (*first policy*), a signature based policy (*second policy*), and a firewall based policy (*third policy*).

- t. ***[2.19] in response to administrator action, cause setting, before the first occurrence, of a first policy for the third instructions that is applied to a group including each of the plurality of devices that has the at least one operating system installed thereon***

163. As discussed with respect to limitation [2.6] - [2.9], the third instructions are related to data inspection-related information and the first

occurrence is an anomaly based attack for a device with the installed operating system.

164. As discussed with respect to limitation [2.18], Gupta discloses that the *setting of a first policy* related to an anomaly based attack *is caused* by an administrator using the global sensor management system (*in response to administrator action*) and is subsequently applied by providing relevant local security sensor modules with an attack file that includes anomaly profiles as discussed with respect to limitation [2.6]-[2.9].

165. A POSITA understood that the downloading of the attack file with anomaly profiles at each local security sensor module for which the attack file is relevant would occur before the anomaly profiles would be used to identify an attack (*before the first occurrence*).

- u.** *[2.20] in response to administrator action, cause setting, before the second occurrence, of a second policy for the fourth instructions that is applied to the group including each of the plurality of devices that has the at least one operating system installed thereon*

166. As discussed with respect to limitation [2.10] - [2.13], the fourth instructions are related to traffic inspection-related information and the second

occurrence is an intrusion signature based attack for a device with the installed operating system.

167. As discussed with respect to limitation [2.18], Gupta discloses that the *setting of a second policy* related to an intrusion based attack *is caused* by an administrator using the global sensor management system (*in response to administrator action*) and is subsequently applied by providing relevant local security sensor modules with an attack file that includes intrusion signatures.

168. A POSITA understood that the downloading of the attack file with intrusion signatures at each local security sensor module for which the attack file is relevant would occur before the intrusion signatures would be used to identify an attack (*before the second occurrence*).

- v. ***[2.21] in response to administrator action, cause setting, before the third occurrence, of a third policy for the fifth instructions that is applied to the group including each of the plurality of devices that has the at least one operating system installed thereon, and***

169. As discussed with respect to limitation [2.14] - [2.17], the fifth instructions are related to firewall-related information and the third occurrence is indicative of an attack based on IP addresses from which traffic associated therewith should be identified as a vulnerability for a device with the installed operating system.

170. As discussed with respect to limitation [2.18], Gupta discloses *setting of a third policy* related to an IP addresses based attack *is caused* by an administrator using the global sensor management system (*in response to administrator action*) and is subsequently applied by providing relevant local security sensor modules with an attack file that includes a range of IP source and destination addresses as discussed with respect to limitation [2.14]-[2.17].

171. Gupta also teaches a *firewall-based occurrence mitigation type*. For example, Gupta's sensor 22 includes a "fixed-field detector 63" that "[o]nce the packet is received by the sensor 22," scans the packet "for attacks that leave characteristic traces in certain specific fields." Gupta, [0084], [0101]. Therefore, a POSITA would understand that Gupta's fixed-field detector implements a firewall-based application, e.g., to inspect every received packet.

172. As discussed with respect to limitation [2.15] Gupta also teaches a *firewall-based occurrence mitigation type*. For example, Gupta's sensor 22 includes a "fixed-field detector 63" that "[o]nce the packet is received by the sensor 22," scans the packet "for attacks that leave characteristic traces in certain specific fields." Gupta, [0084], [0101]. Therefore, a POSITA would understand that Gupta's fixed-field detector implements a firewall-based application, e.g., to inspect every received packet.

173. A POSA understood that the downloading of the attack file with IP addresses at each local security sensor module for which the attack file is relevant would occur before the IP addresses would be used to identify an attack (*before the third occurrence*).

- w. ***[2.22] cause the utilization of the different occurrence mitigation actions of the diverse occurrence mitigation types, including the firewall-based occurrence mitigation type and the other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing the advantage being taken of the actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.***

174. Gupta discloses providing a user with the ability to select between different occurrence mitigation actions of diverse occurrence mitigation types. For example, Gupta discloses that the VIDS 130 in the global sensor management system 34 “implements a graphical user interface (GUI)” that “enables the subscriber to... manage and monitor the VIDS” and the “GUI can be implemented within a browser, either as an applet or using HTML. Gupta, [10131], [0143]. The VIDS 130 supports “different security policies, protection objectives, and security management preferences.” Gupta, [0136]. A POSITA understood that the availability of multiple “security policies, protection objectives, and security management preferences” demonstrates that Gupta’s teachings apply to a variety of *different occurrence mitigation actions* in response to different threats and attacks.

175. Gupta discloses providing one or more options to selectively utilize different occurrence mitigation actions, including terminating TCP connections, which a POSITA understood to be *an intrusion prevention system-based occurrence mitigation technique* as recited in this claim. For example, Gupta discloses that sensor 22 include a response processor 54 that responds to an attack ID (AID) and “generates alerts that provide notification of an attack. The response processor 54 also attempts to prevent the attack. **Short-term responses include terminating TCP connections.** Long-term responses include packet logging for further analysis to improve detection and response.” Gupta, [0087]. Thus, Gupta discloses terminating TCP connections, which a POSITA understood to be an “*intrusion prevention system-based occurrence mitigation type*.”

176. Gupta also teaches a *firewall-based occurrence mitigation type*. For example, Gupta’s sensor 22 includes a “fixed-field detector 63” that “[o]nce the packet is received by the sensor 22,” scans the packet “for attacks that leave characteristic traces in certain specific fields.” Gupta, [0084], [0101]. Therefore, a POSITA would understand that Gupta’s fixed-field detector implements a firewall-based application, e.g., to inspect every received packet.

177. To the extent that Patent Owner asserts that Gupta does not expressly disclose a “firewall-based” occurrence mitigation type, Graham discloses providing occurrence mitigation actions, including the use of techniques known in the art,

including firewall techniques, that a POSITA understood could beneficially be utilized among the plurality of mitigation options provided in Gupta. For example, Graham teaches providing different occurrence mitigation actions:

If the system determines that the target is not vulnerable, one embodiment of the system generates a low-level alert and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). If the system determines that the target is vulnerable, however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or may take certain precautionary measures (at 235)

Graham at 7:58–65.

178. Graham provides an example:

If the system determines that the target is not vulnerable, one embodiment of the system generates a low-level alert and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). **If the system determines that the target is vulnerable,** however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or **may take certain precautionary measures** (at 235). For example, at this stage **the system may attempt to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so).**

Graham at 7:58-67.

179. Graham further discloses that a factor considered by the system is “the target’s response to the detected data signature to further evaluate the probability of network misuse.” Graham at 8:3–5. Thus, a POSITA understood that Graham teaches occurrence mitigation actions, one of which is a firewall-based occurrence mitigation type — the firewall blocking incoming data transmission from a suspect node. Graham at 7:65–67.

180. Thus, the combined teachings of Gupta and Graham disclose this limitation. As discussed in the Motivation to Modify the Teachings of Gupta with the Teachings of Graham section, it would have been obvious to a POSITA to modify the teachings of Gupta with the firewall mitigation technique taught by Graham because both references teach the use of multiple, known mitigation techniques and the benefit of using the technique that best fits the circumstances of a given occurrence or device, and would be assured of its success.

181. Gupta further teaches that a user is able to manage and monitor the virtual intrusion detection system (VIDS) provisioning module 110 for a plurality of devices being monitored by a sensor. Gupta [0131], [0143]. In particular, Gupta teaches:

The VIDS provisioning module 130 facilitates protection for multiple traffic streams for different subscribers using a Single

Sensor platform while maintaining security separation. The module 130 supports different security policies, protection objectives, and security management preferences effectively and efficiently.

Gupta, [0136].

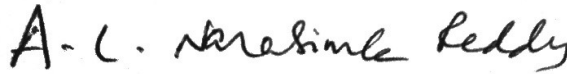
182. Thus, Gupta describes the occurrence mitigation actions are facilitated by the VIDS provisioning module that “facilitates protection for multiple traffic streams for different subscribers” which a POSITA understood teaches *utilization of . . . occurrence mitigation actions . . . across the plurality of devices* as recited.

183. Therefore, Gupta in combination with Graham renders obvious [1.7].

XI. CONCLUSION

184. I 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 that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Dated: June 7, 2023

A handwritten signature in black ink that reads "A. C. Narasimha Reddy". The signature is written in a cursive, flowing style.

Narasimha Reddy, Ph.D.