

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

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

I.	INTRODUCTION	7
II.	GROUND FOR STANDING	8
III.	NOTE	8
IV.	SUMMARY OF THE '066 PATENT	8
V.	PROSECUTION HISTORY	9
VI.	EFFECTIVE PRIORITY DATE OF THE '066 PATENT	10
VII.	LEVEL OF ORDINARY SKILL IN THE ART	10
VIII.	STATE OF THE ART	11
	A. Network System Security	11
	B. The Use of Mobile Agents	13
VIII.	CLAIM CONSTRUCTION	14
IX.	RELIEF REQUESTED AND REASONS THEREFORE	14
X.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE	14
	A. Statutory Grounds for Challenges	14
	B. Ground 1	16
	1. Summary of Gupta	16
	2. Summary of Graham	23
	3. Motivation to Modify the Teachings of Gupta with the Teachings of Graham	24

4.	Claim 1	25
	[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:.....	25
	EX-1006, FIG. 1 (annotated); EX-1003, ¶61.....	27
	[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;.....	30
	EX-1006, FIG. 15 (annotated); EX-1003, ¶71.....	31
	[1.2] said first vulnerability information generated utilizing the second vulnerability information, by:	37
	[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.....	37
	[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;.....	38
	[1.5] identify an occurrence in connection with at least one of the plurality of devices;	40
	[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.....	40
	[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;.....	42
	[1.8] wherein the at least one configuration involves at least one operating system.	46
C.	Ground 2	47
1.	Summary Of Hill	47
2.	Motivation to Modify the Teachings of Gupta with the Teachings of Hill	49
3.	Claim 2	52
XI.	DISCRETIONARY DENIAL IS INAPPROPRIATE	80
A.	Discretionary denial under 35 U.S.C. § 325(d) is not appropriate	80
B.	Discretionary denial under the <i>Fintiv</i> factors is not appropriate.....	83
I.	MANDATORY NOTICES.....	86
A.	Real party-in-interest	86
B.	Related matters	86
C.	Lead and back-up counsel and service information.....	86
XII.	CONCLUSION.....	88
	CERTIFICATE OF WORD COUNT.....	89
	CERTIFICATE OF SERVICE	90

PETITIONER'S EXHIBIT LIST

EX-1001	U.S. 10,893,066
EX-1002	Prosecution History of U.S. 10,893,066
EX-1003	Declaration of A.L. Narasimha Reddy, Ph.D. under 37 C.F.R. § 1.68
EX-1004	<i>Curriculum Vitae</i> of A.L. Narasimha Reddy, Ph.D.
EX-1005	U.S. 7,359,962 to Willebeek-LeMair et al.
EX-1006	U.S. Pub. 2003/0004689 to Gupta et al.
EX-1007	U.S. 7,237,264 to Graham et al.
EX-1008	Intentionally Left Blank
EX-1009	Intentionally Left Blank
EX-1010	Intentionally Left Blank
EX-1011	IPR2017-02191, Granting Request for Adverse Judgment, Paper 18, September 26, 2018
EX-1012	IPR2017-02192, Final Written Decision, Paper 31, April 8, 2019
EX-1013	Intentionally Left Blank
EX-1014	IPR2022-00035, Institution Decision, Paper 7,(April 19, 2022)
EX-1015	Intentionally Left Blank.
EX-1016	U.S. Pat. No. 6,088,804 (Hill)
EX-1017	Intentionally Left Blank.
EX-1018	Intentionally Left Blank

EX-1019	Intentionally Left Blank
EX- 1020	Intentionally Left Blank
EX-1021	<i>Applying Mobile Agents to Intrusions Detection and Response</i> Jansen, et al, NIST Interim Report (IR) (October 1999) (“Jansen”)

I. INTRODUCTION

Forcepoint LLC, (“Petitioner”) respectfully requests that the Board review and cancel as unpatentable Claims 1 and 2 (hereinafter, the “Challenged Claims”) of U.S. 10,893,066 (the “’066 Patent,” EX-1001).

The ’066 Patent “relates to ... management of security of computing and network devices” connected in a network. EX-1001, 1:18-20. An examiner allowed the claims because the prior art allegedly failed to teach “identifying an occurrence, determining that at least one vulnerability is susceptible to being taken advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.” EX-1002, 564.

However, the Board previously instituted review of Claim 1 of the ’066 Patent in IPR2022-00035 because Gupta in combination with Graham teaches this alleged point of novelty by identifying an occurrence of a packet arriving at a network and determining an associated vulnerability to threats. EX-1014 PP. 37-38 (“Thus, we determine, based on the current record, Gupta teaches ‘a other occurrence mitigation type’ and Graham teaches ‘a firewall-based occurrence mitigation type.’ Moreover, on this record, we determine both Gupta and Graham teach ‘caus[ing] utilization’ of different occurrence mitigation actions receiving packets in traffic and inspecting”).

This Petition also challenges Claim 2, which was not previously challenged

in IPR2022-00035. Claim 2 depends from Claim 1 and is directed to identifying occurrences and taking mitigation actions at devices distributed throughout the network. Claim 2 is obvious over the combination of Gupta and Graham in further view of Hill which discloses the use of security agents distributed throughout the network at computer devices for detecting and mitigating security occurrences.

II. GROUNDS FOR STANDING

Petitioner certifies the '066 Patent is IPR-eligible, and Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

III. NOTE

Petitioner cites to exhibits' original page numbers. **Emphasis** in quoted material has been added. Claim terms are *italicized*. Color annotations are added to the figures.

IV. SUMMARY OF THE '066 PATENT

The '066 Patent “relates to...management of security of computing and network devices.” EX-1001, 1:23-25. The '066 Patent is part of a family of patents and applications, including two patents that had claims cancelled in IPRs. *See generally* EX-1011, 1012.

A “security server 135” collects operating system and other configuration data about devices in the network. EX-1001, 2:30-38, 43-45; *see also* Fig.1 below.

The server determines whether network traffic “is attempting to take advantage of a particular known vulnerability.” EX-1001, 4:9-11, 4:21-29. If so, the server “selects one or more remediation techniques” for the particular vulnerability. EX-1001, 4:62-64; EX-1003, ¶¶25-27.

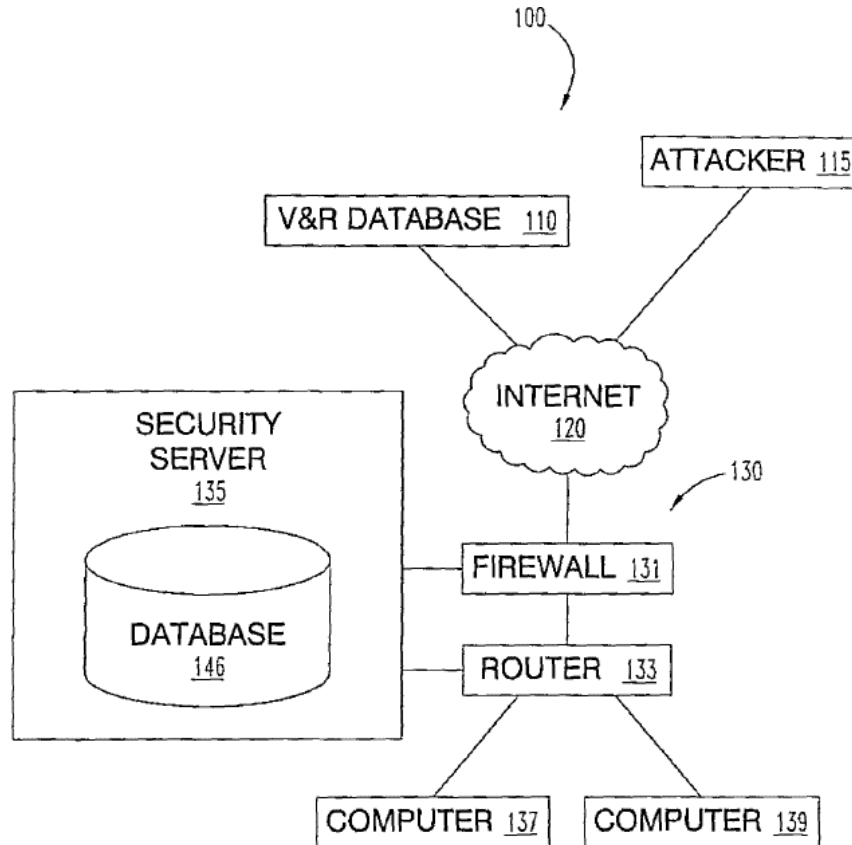


Fig. 1

EX-1001, Fig. 1

V. PROSECUTION HISTORY

The Applicant amended the independent claim for clarification, in order to overcome a rejection under 35 U.S.C. § 101. EX-1002, 538-55. The examiner

indicated the allowability of Claim 1 (Claim 54 during prosecution) explaining that the prior art fails to teach “identifying an occurrence, determining that at least one vulnerability is susceptible to being taken advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.” EX-1002, 564.

The Applicant subsequently filed an RCE with multiple IDS filings and an amendment cancelling all dependent claims and substituting new claims dependent from Claim 1, including Claim 2. The examiner issued a Notice of Allowance identifying the same reason for the allowance of Claim 1 and did not identify any independent reason for the allowance of the newly added dependent claims stating only that they were “allowed by virtue of their dependency.” EX-1002 790.

VI. EFFECTIVE PRIORITY DATE OF THE '066 PATENT

The earliest claimed priority date is July 1, 2003. EX-1001. In prosecution, the Applicant alleged a reduction to practice on October 15, 2002. EX-1002, 281-82. This petition cites prior art predating October 15, 2002. Petitioner does not waive any right or opportunity it may have to dispute the priority date of the '066 Patent in this or another forum where the issue is relevant.

VII. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in The Art (“POSITA”) in July 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. EX-1003, ¶¶17-19.

VIII. STATE OF THE ART

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 POSA, 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).

A. Network System Security

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; EX-1003, ¶¶29.

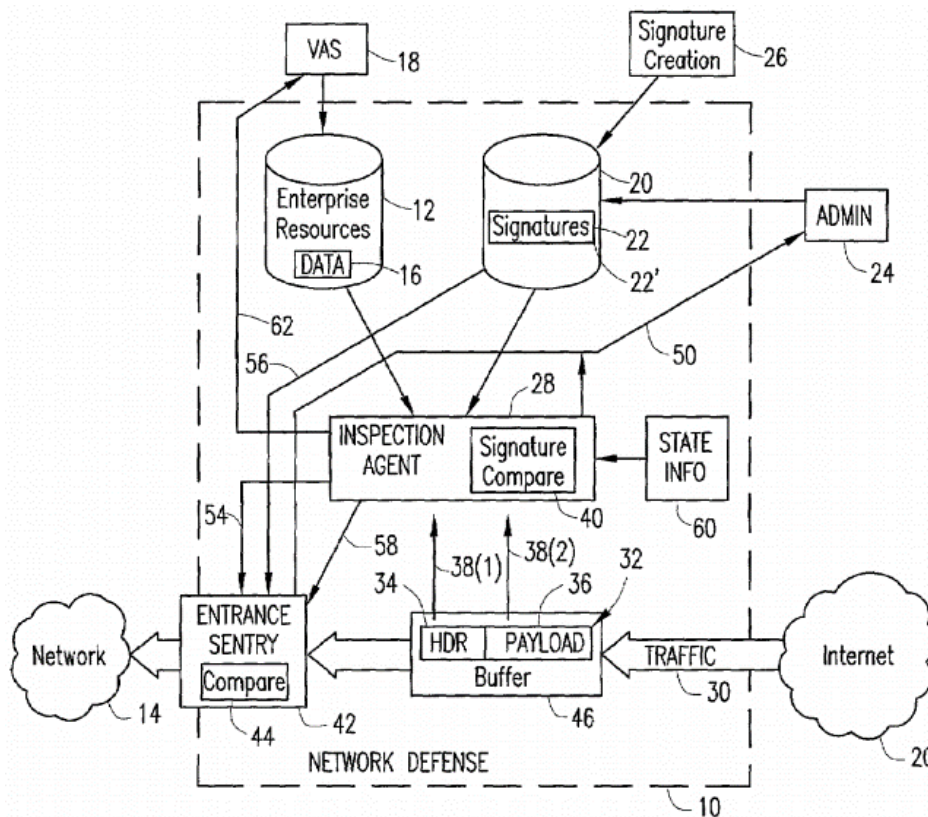


FIG. 1

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: EX-1003, ¶30.

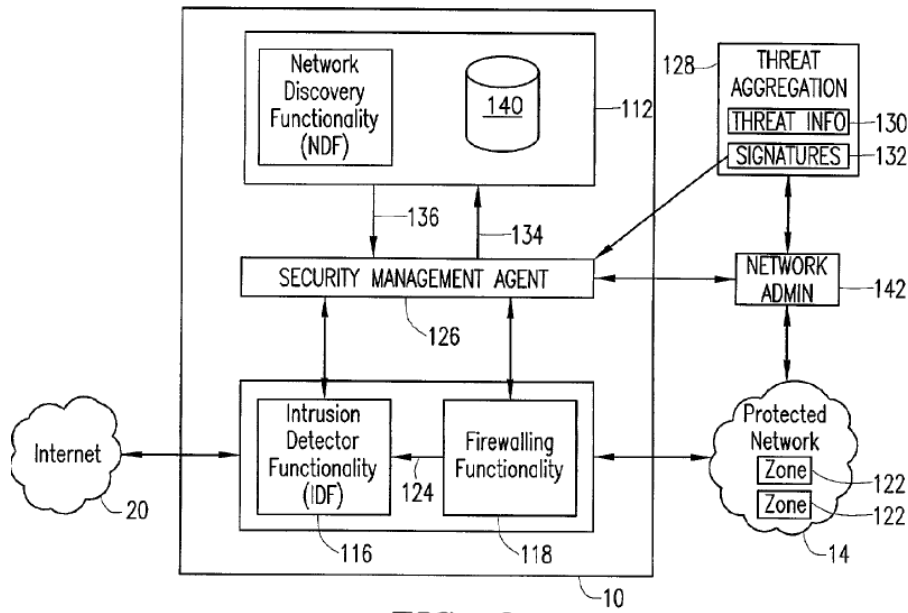


FIG. 2

B. The Use of Mobile Agents

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. EX-1021 pp. 2, 7-8. A POSA 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. EX-

1021 pp. 10-14. 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. EX-1021 p. 21; EX-1003 ¶31

VIII. CLAIM CONSTRUCTION

Petitioner believes that, for purposes of this proceeding and the analysis presented herein, the terms should be given their plain and ordinary meaning. In IPR2022-00035, the Board construed “*instructions that...cause the one or more processors to... 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* as recited in Claim 1, includes network defense systems which provide firewall functionality. We do not exclude those other mitigation types that may be separate from a vulnerable or attacked device.” EX-1014 p. 20. Petitioner agrees that this construction is within the plain and ordinary meaning of the recited limitation.

IX. RELIEF REQUESTED AND REASONS THEREFORE

Petitioner asks that the Board institute a trial for *inter partes* review and cancel the Challenged Claims in view of the analysis below.

X. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Statutory Grounds for Challenges

Grounds	Claims	Basis	References
---------	--------	-------	------------

1	1	§103	Gupta in view of Graham
2	2	§103	Gupta in view of Graham in view of Hill

U.S. Pat. Publication No. 2003/0004689 titled “Hierarchy-Based Method and Apparatus for Detecting Attacks on a Computer System” published on January 2, 2003 based on Application No. 10/172,764 filed June 13, 2002 (“Gupta”)(EX-1006). Gupta is prior art under 35 U.S.C. §§ 102(a) and (e) (pre-AIA) and was not cited by the examiner during prosecution.

U.S. Pat. No. 7,237,264 titled “System and Method for Preventing Network Misuse” issued on June 26, 2007 based on Application No. 09/874,574 filed June 4, 2001 (“Graham”)(EX-1007). Graham is prior art under 35 U.S.C. § 102(e) (pre-AIA) and was not cited by the examiner during prosecution.

U.S. Pat. No. 6,088,804 titled “Adaptive System and Method for Responding to Computer Network Security Attacks” issued on Jul, 11, 2000 from Application No. 09/006,056 filed January 12, 1998 (“Hill”)(EX-1016). Hill is prior art under 35 U.S.C. § 102(a) (pre-AIA) and was not cited by the examiner during prosecution.

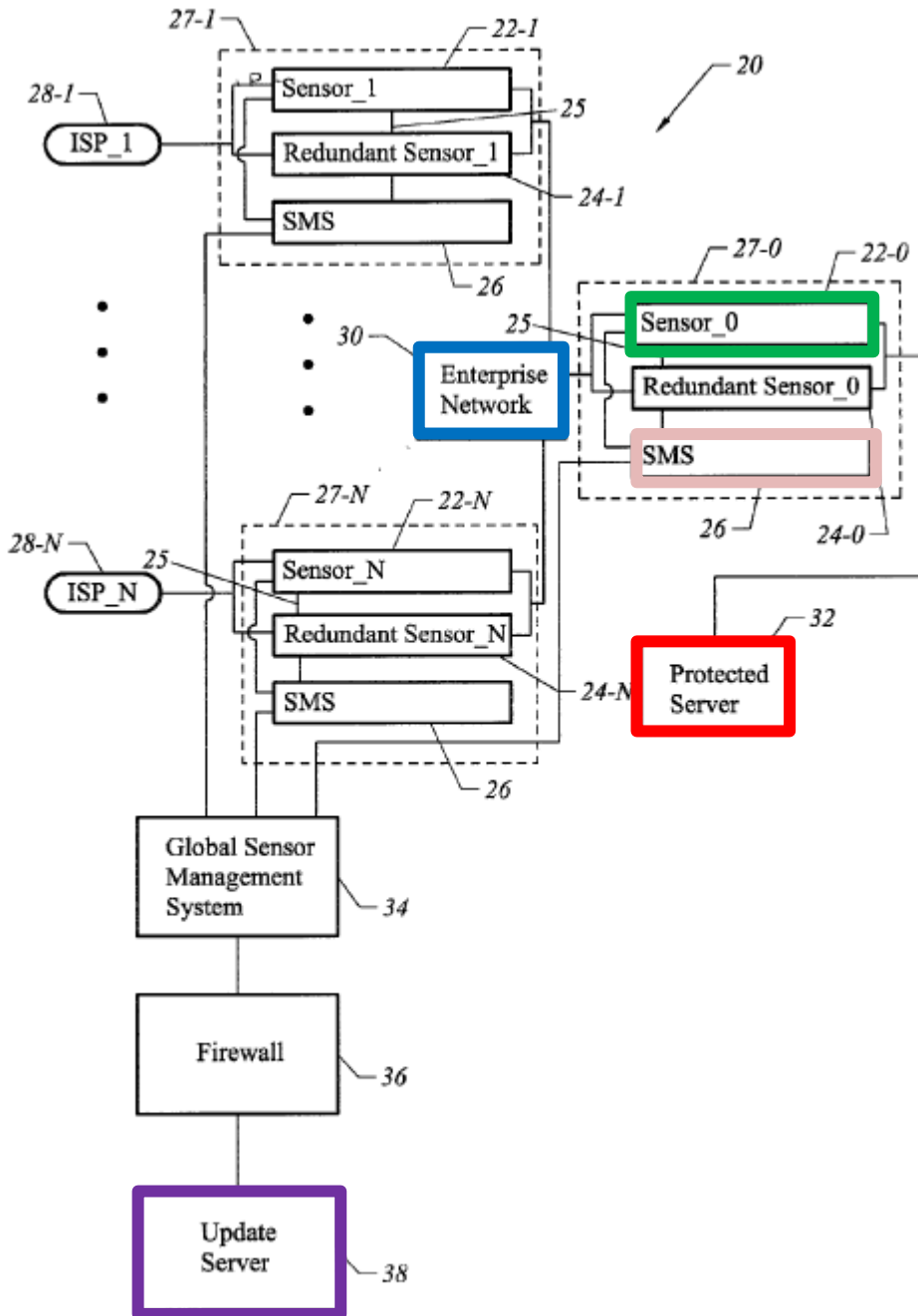
Petitioner’s obviousness grounds rely on the combined teachings of the references and not on a physical incorporation of elements. *See In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); EX-1003, ¶116.

B. Ground 1

1. Summary of Gupta

Gupta discloses a security system that determines actual vulnerabilities, detects occurrences in network traffic that may take advantage of those vulnerabilities, and provides that multiple options for mitigation of those occurrences, including dropping TCP connections, are provided. EX-1006, [0151], [0154], [0164]-[0165]; EX-1003, ¶¶36-48.

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 [0008], Abstract; EX-1003, ¶¶36-39. 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). EX-1006. [0030],[0032]; EX-1003, ¶39.



EX-1006 Fig. 1

The update server 38 (purple) is used to coordinate the delivery of signature and software updates to the local sensor security modules 27. EX-1006 [0034].

The update server 38 is notified by 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. EX-1006 [0138]; EX-1003, ¶40.

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.” EX-1006 [0036],[0037]; EX-1003, ¶41.

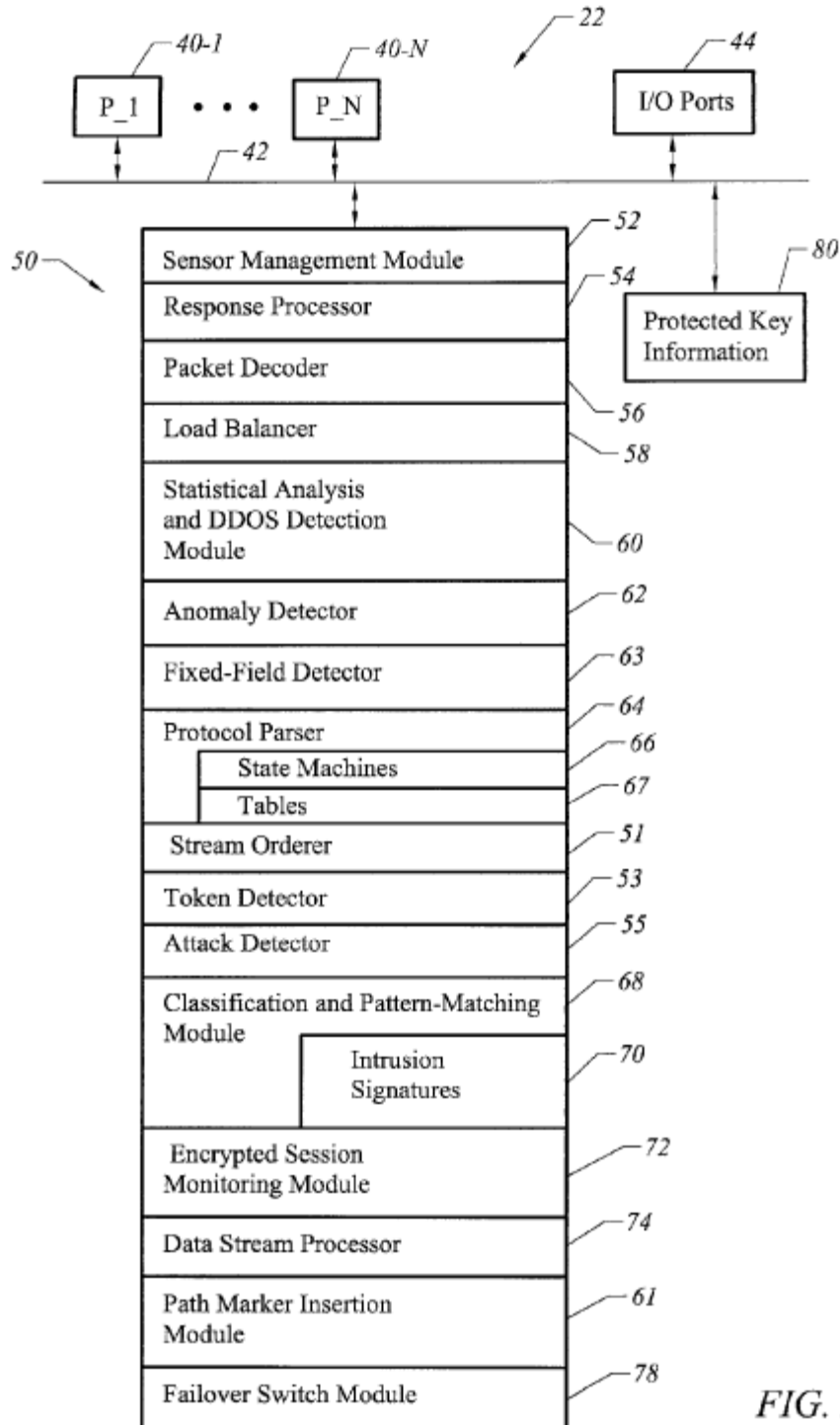


FIG. 2

EX-1006 FIG. 2.

Further, “memory 50 also stores a classification and pattern-matching module 68” which “has an associated set of intrusion signatures 70” (EX-1006

[0042]) and those intrusion signatures 70 are stored in an “attack file” which “specifies attacks and counter measures.” EX-1006 [0151]; EX-1003, ¶42.

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); EX-1003, ¶43.

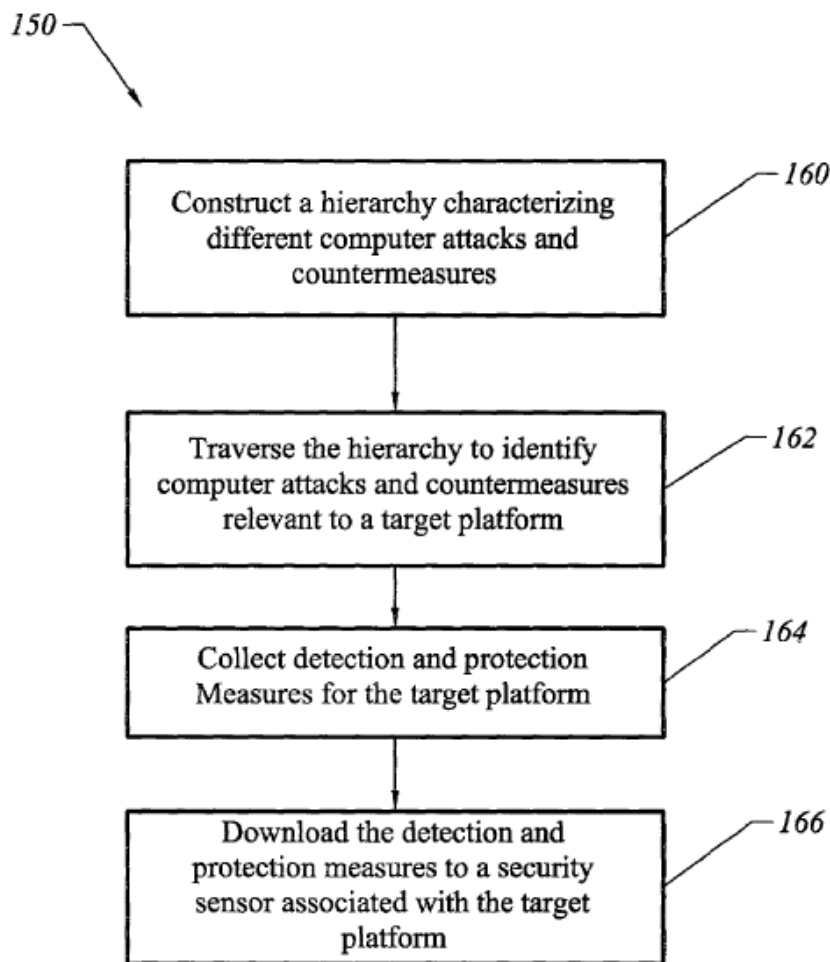


FIG. 17

EX-1006 FIG. 17.

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). EX-1006 [0164]; EX-1003, ¶44.

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.” EX-1006 [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.” EX-1006 [0087]; EX-1003, ¶45.

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; EX-1003, ¶46.

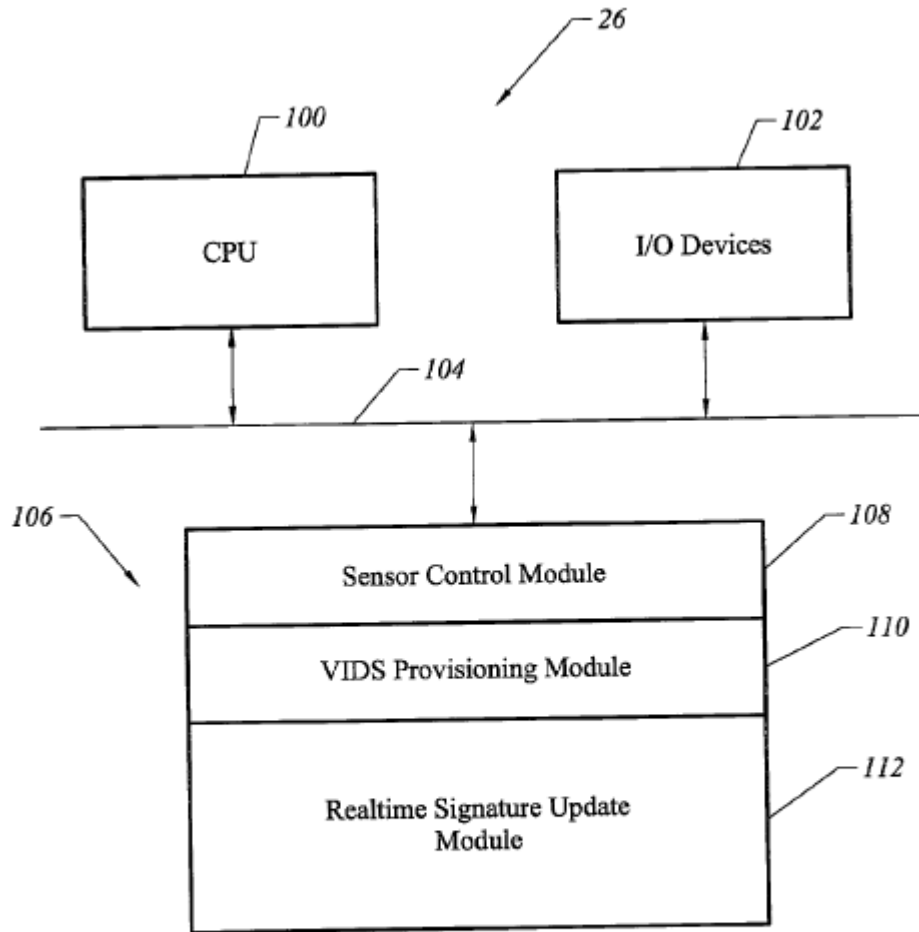


FIG. 13

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. EX-1006 [0132]; EX-1003, ¶47.

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. EX-1006 [0138]; EX-1003, ¶48.

2. Summary of Graham

Graham is directed to “analyzing and preventing unauthorized use of data network resources” by “evaluat[ing] potential network misuse signatures” to make a “misuse determination.” EX-1007 1:7-10, 2:51-56. For example, “several successive transmissions of an invalid user ID or password from a suspect node to a target may indicate that an unauthorized user is attempting to gain access to [a] target.” EX-1007 4:40-43. Graham describes identifying potential vulnerability information and deriving actual vulnerability data from it, by 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.**” EX-1007, 7:14-19. Graham also discloses using firewall-based mitigation actions to prevent an attack from taking advantage of an actual vulnerability, including taking “certain precautionary measures” such as

attempting “to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so).” EX-1007, 7:58-67; EX-1003, ¶¶49-50.

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.” EX-1007 8:3-5. Thus, 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.” EX-1007 7:65-67; EX-1003, ¶50.

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

A POSITA would have been motivated to modify the teachings of Gupta with the teachings of Graham because both Gupta and Graham are directed to identifying vulnerabilities and applying corrective actions to protect against identified vulnerabilities. More specifically, 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. EX-1006, [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. EX-1007, 7:58-67. EX-1003, ¶¶ 51-55.

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. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007). In other words, such a combination is merely applying a known technique (implementing firewall functionality for identified vulnerabilities) to a known method (identifying vulnerabilities) with the predictable outcome of identifying and implementing corrective action for the identified vulnerabilities. *KSR*, 550 U.S. at 417. The combination also merely represents using a known technique (firewall functionality) to improve a similar system (Gupta’s network of devices) in the same way (“preventing unauthorized use of data network resources,” EX-1007, 1:7-10). *KSR*, 550 U.S. at 417; EX-1003, ¶54.

4. Claim 1

[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:*

Gupta discloses several examples of a non-transitory computer-readable media that stores instructions. For example, 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. EX-1006, 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.” EX-1006, [0150]; EX-1003, ¶¶56-68

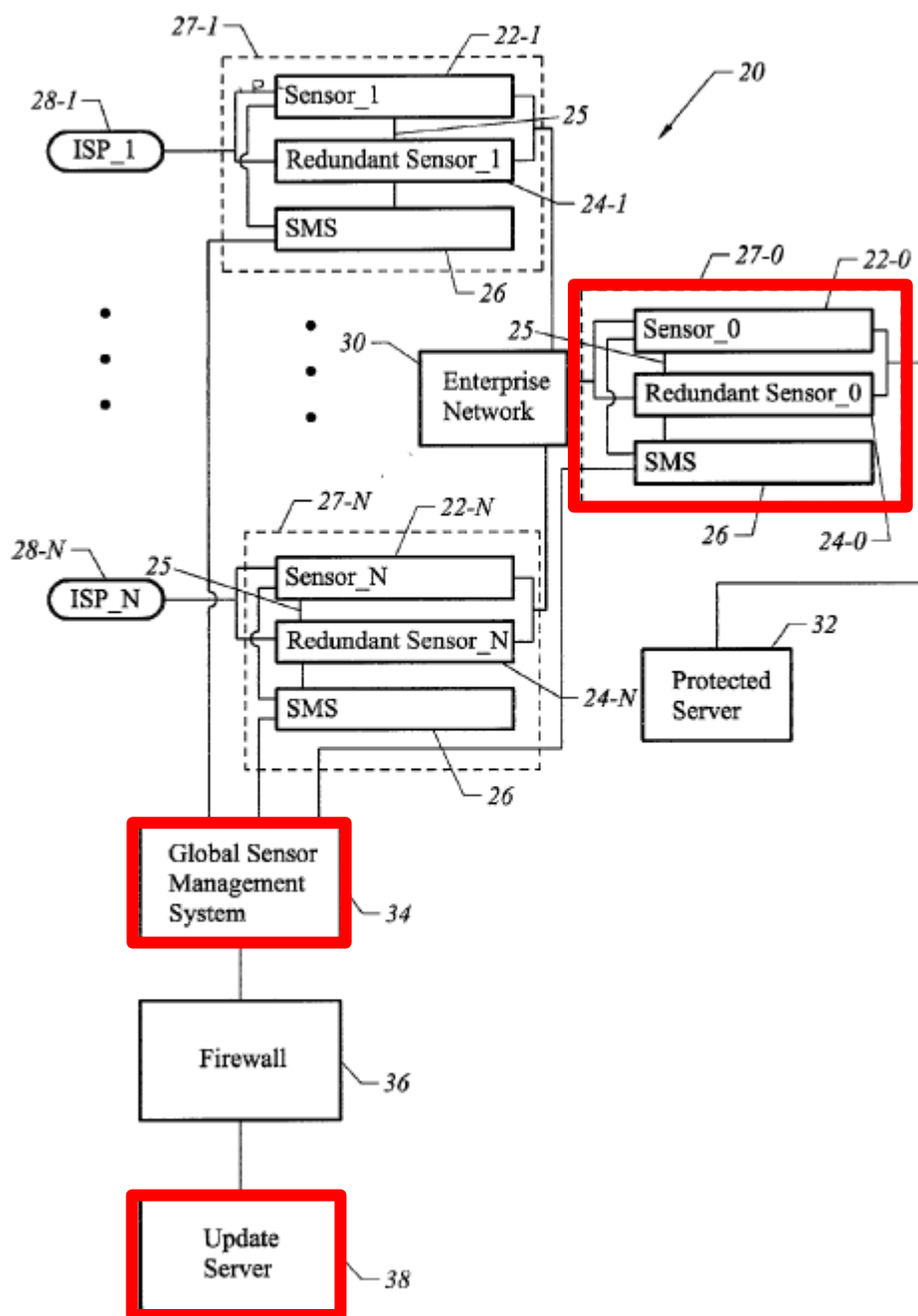


FIG. 1

EX-1006, FIG. 1 (annotated); EX-1003, ¶61

Gupta further discloses *instructions* stored at the update server 38 are

downloaded to the local security module 27 and global sensor management system

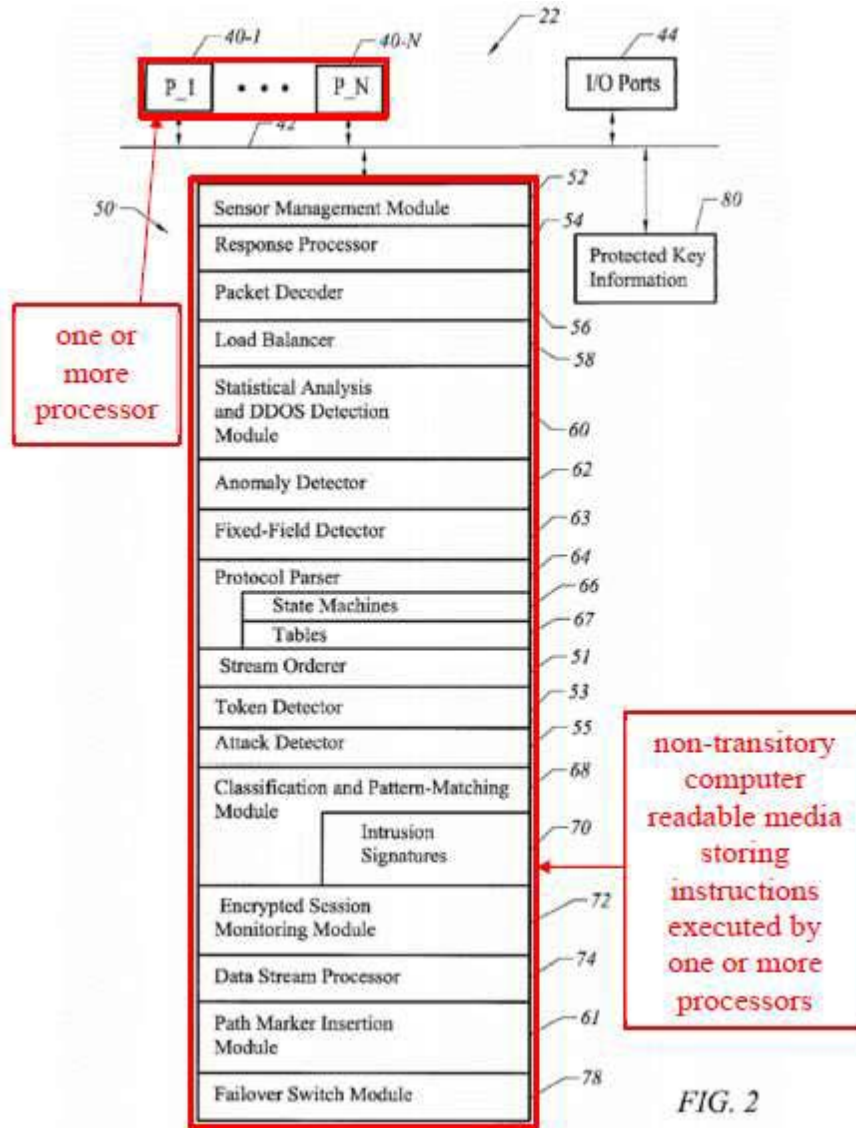
34. For example, Gupta discloses the update server 38 “coordinate[s] the delivery” of “**software updates** to the local sensor security module 27.” EX-1006 [0034]; EX-1003, ¶63.

Gupta further discloses the update server is “used to notify customers of **new software**,” and “provides the **software images** and signature files **for download**.” EX-1006 [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; EX-1003, ¶64.

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. EX-1003, ¶65.

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. EX-1006, [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. EX-1006, [0036]-[0037]. EX-1003,

¶ 66.



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.” EX-1006, [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.” EX-1006, [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. EX-1003, ¶67.

Therefore, Gupta discloses [10.0]. EX-1003, ¶64.

[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;

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. EX-1006, [0151], [0164]. Thus, a POSITA would understand that the “attack file” in Gupta contains “*first vulnerability information*” as recited in this claim limitation. EX-1003, ¶¶69-76.

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." EX-1006, [0154]. EX-1003, ¶71.

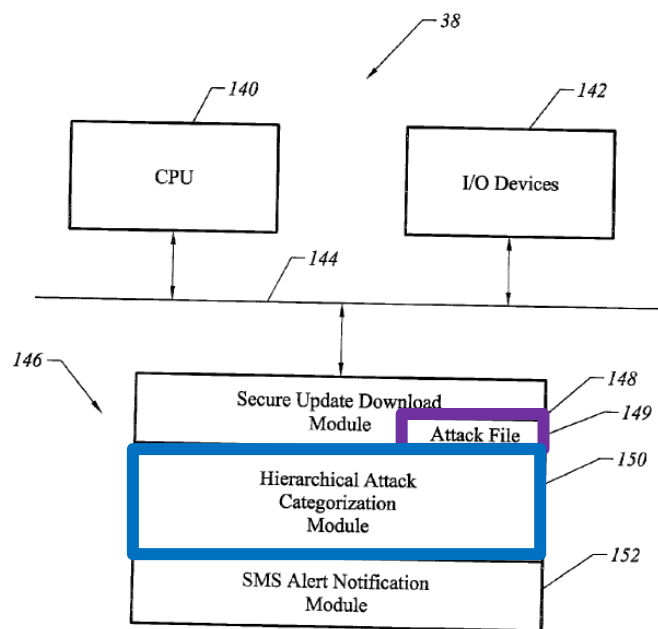


FIG. 15

EX-1006, FIG. 15 (annotated); EX-1003, ¶71.

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* EX-1006, [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. EX-1003, ¶72.

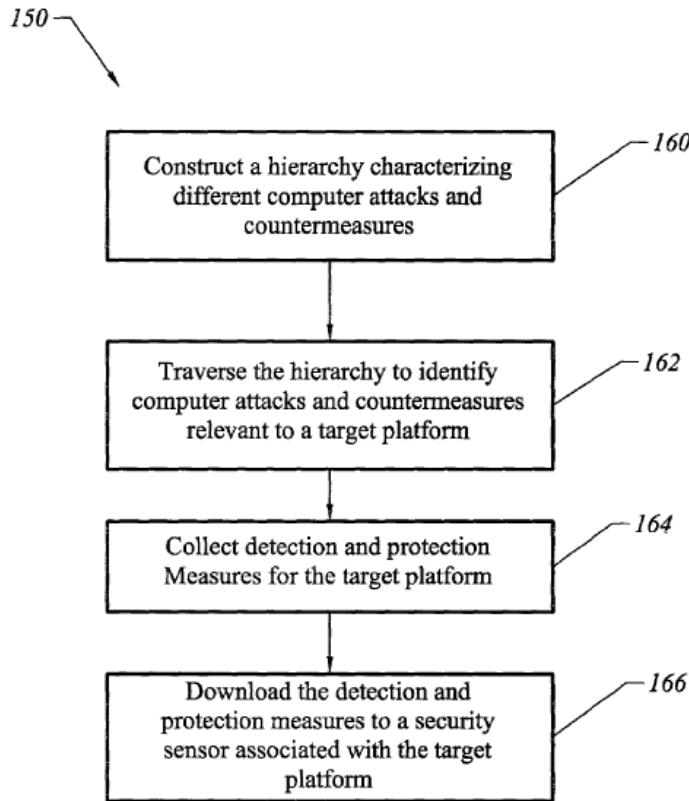


FIG. 17

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).

EX-1006 [0164].

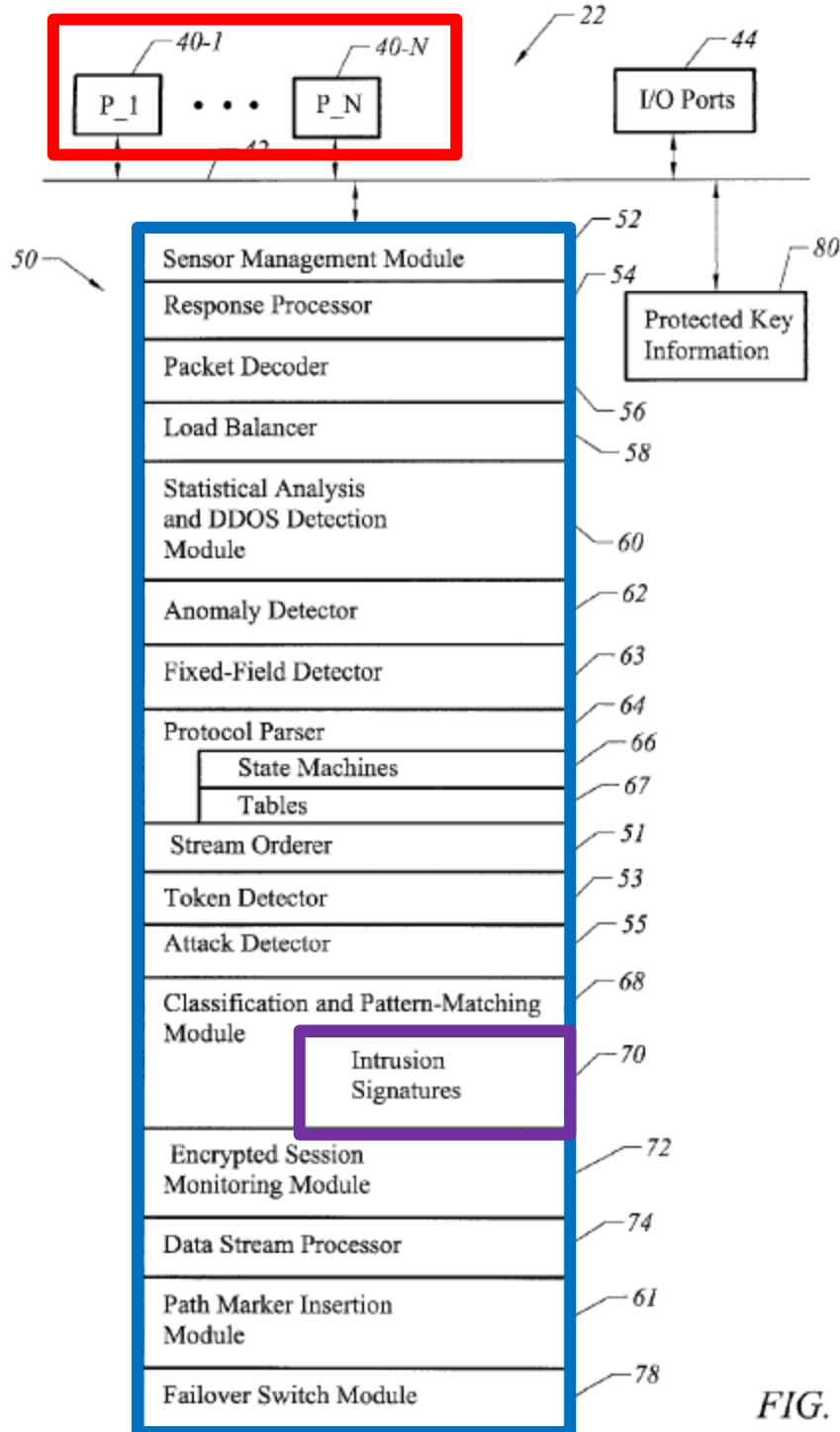
The attack file “clearly describe[s], in one data structure”, what attacks a

given environment is vulnerable to, what protection mechanisms and signatures are available, and how detection alerts are correlated. EX-1006 [0165] ; EX-1003, ¶73.

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. EX-1006 [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). EX-1006, [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). EX-1006, [0151] ; EX-1003, ¶74.¹

¹ In IPR2023-00989 challenging the U.S. Pat. No. 10,609,063, Petitioner asserts that the Secure Update Download Module 148 of Gupta satisfies *first data storage* limitation recited in Claim 10. In the present Petition, the Secure Update Download Module 148 could, alternately, satisfy the *first data storage* limitation

recited in Claim 1. However, because dependent Claim 2 of the '066 Patent includes additional limitations regarding the *first data storage*, the current Petition uses memory 50 as the *first data storage*.



Therefore, Gupta discloses [1.1]. EX-1003, ¶¶75-76.

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

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*). EX-1003, ¶77.

[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

Gupta discloses *identifying at least one configuration* by disclosing an attack file that includes configuration information of a device or a target platform. EX-1006 [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)**.” EX-1006 [0160]. Thus, Gupta disclosing categorizing attacks based on the device configurations which meets the claim limitation of *identifying at least one configuration*. EX-1003, ¶¶78-82.

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.*, EX-1006, [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 ...”); EX-1003, ¶80.

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.” EX-1006 [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* EX-1006, [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”). EX-1003, ¶¶81082.

Therefore, Gupta discloses [10.3]. EX-1003, ¶82

[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;*

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. EX-1006 [0154] (“[t]he attack file 149 may be formed utilizing the hierarchical attack categorization module 150; EX-1003, ¶83-87).

Gupta further discloses determining that *a plurality of devices are vulnerable to attacks (at least one accurately identified vulnerability)*. EX-1006 [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.” EX-1006 [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.” EX-1006, FIG. 1, [0032]; EX-1003, ¶85.

Therefore, a POSITA would have recognized that the attack file is directed to a target platform that includes different devices within the enterprise network. EX-1003, ¶86. Thus, a POSITA understood that Gupta discloses determining the

different devices are vulnerable to attacks based on the configuration information in the attack file. EX-1003, ¶86.

Therefore, Gupta discloses obvious [1.4]. EX-1003, ¶87.

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

Gupta discloses detecting attacks against devices within a network, which a POSITA understood to be an “*occurrence in connection with at least one of the plurality of devices.*” For example, Gupta discloses that the sensor 22 detects attacks through its anomaly detector 62. EX-1006, [0083] (“detect[ing] 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”). EX-1003, ¶¶88-93.

By way of another example, Gupta discloses “[a]nother 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.**” EX-1006, [0083]; EX-1003, ¶89.

Therefore, Gupta discloses [1.5]. EX-1003, ¶¶93.

[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

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. EX-1006 [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.” EX-1006, [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*”). EX-1003, ¶¶94-100.

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. EX-1006 [0051].

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). EX-1006 [0052] ; EX-1003, ¶96.

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. EX-1006 [0166] ; EX-1003, ¶97.

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*”). EX-1003, ¶99.

Therefore, Gupta discloses [1.6]. EX-1003, ¶¶94-100.

[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;*

Gupta discloses providing a user with the ability to select between different

occurrence mitigation actions of diverse occurrence mitigation types. EX-1003 [0194]. 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. EX-1006, [10131], [0143]. The VIDS 130 supports “different security policies, protection objectives, and security management preferences.” EX-1006, [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. EX-1003, ¶¶101-111.

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.” EX-1006 [0087]. Thus, Gupta discloses

terminating TCP connections, which a POSITA understood to be an “*intrusion prevention system-based occurrence mitigation type*.” EX-1003, ¶103.

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.” EX- 1006, [0084], [0101]. Therefore, a POSITA would understand that the best way to prevent such DOS attacks is to drop these packets at the Firewall. EX-1003, ¶104.

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)

EX-1007, 7:58–65; EX-1003, ¶105.

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)**.

EX-1007 7:58-67; EX-1003, ¶106.

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.” EX-1007 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. EX-1007 7:65–67; EX-1003, ¶107.

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; EX-1003, ¶108.

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. EX-1006 [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.

EX-1006 [0136]; EX-1003, ¶109.

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. EX-1003, ¶110.

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

EX-1003, ¶111.

[1.8] wherein the at least one configuration involves at least one operating

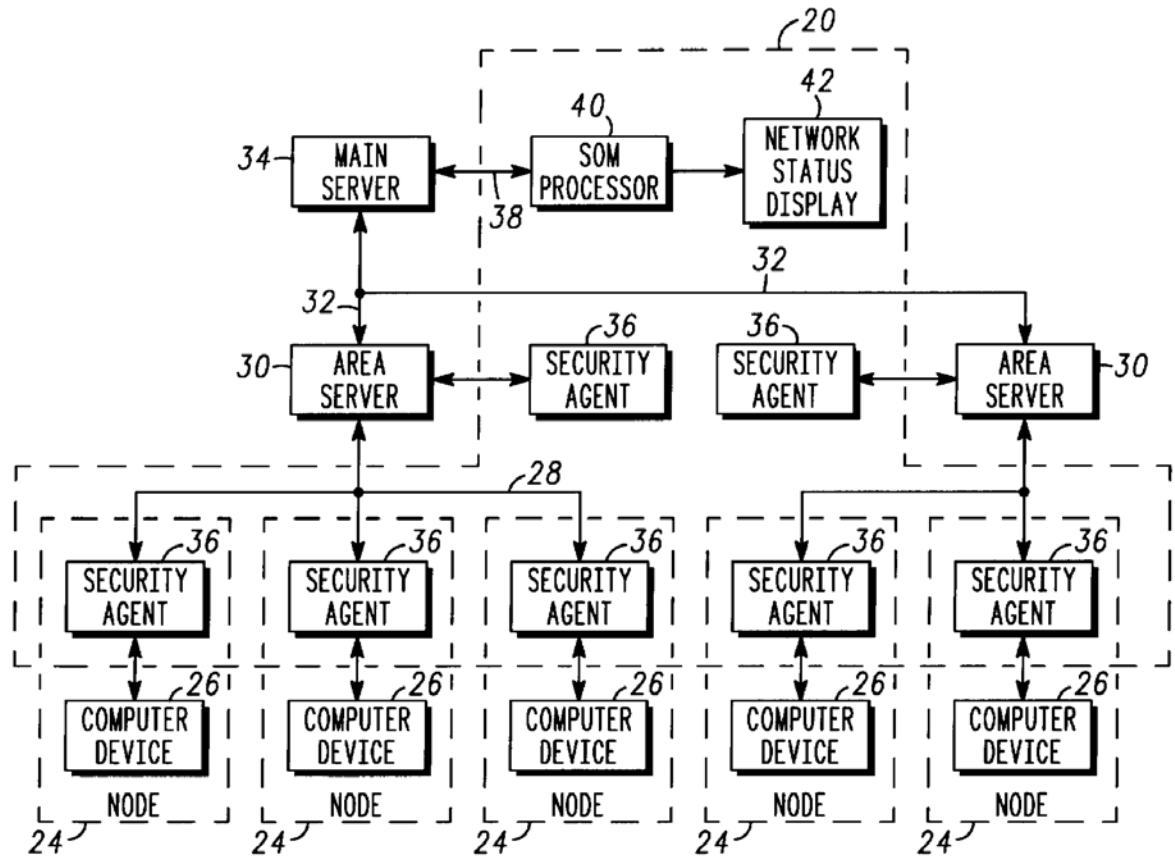
system.

As noted at [1.3], the configuration may be an operating system configuration for target platforms. *See* EX-1006, [0160] (target platforms identified, including “operating system”). Therefore, Gupta discloses [1.8]. EX-1003, ¶¶112-114.

C. Ground 2

1. Summary Of Hill

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. EX-1016 Abstract; EX-1003, ¶115.



22

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. EX-1016 4:31-41; EX-1003, ¶116.

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. EX-1016 5:58-65; EX-1003, ¶117.

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. EX-1016 7:64-8:3; EX-1003, ¶118.

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

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). EX-1003, ¶119.

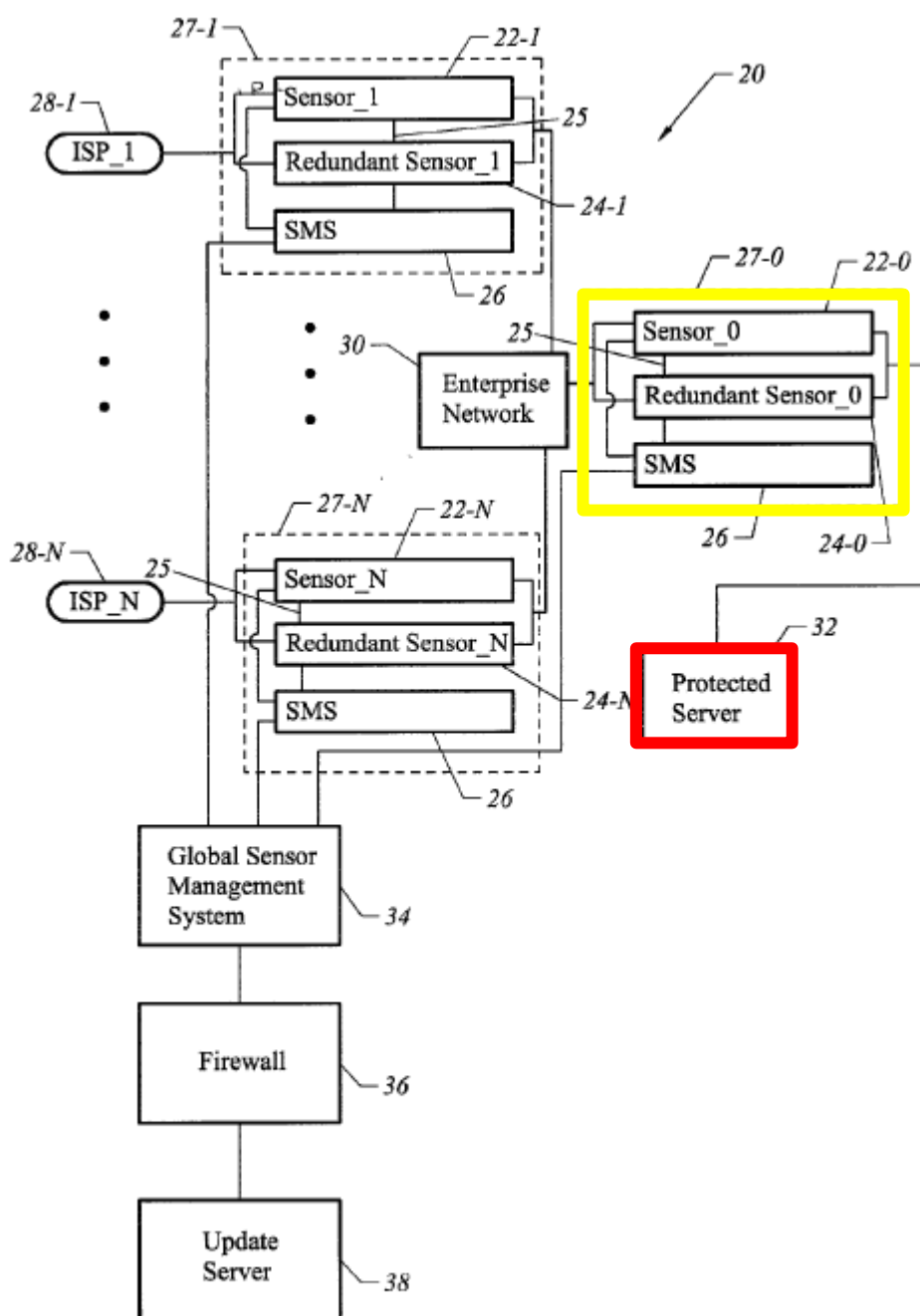
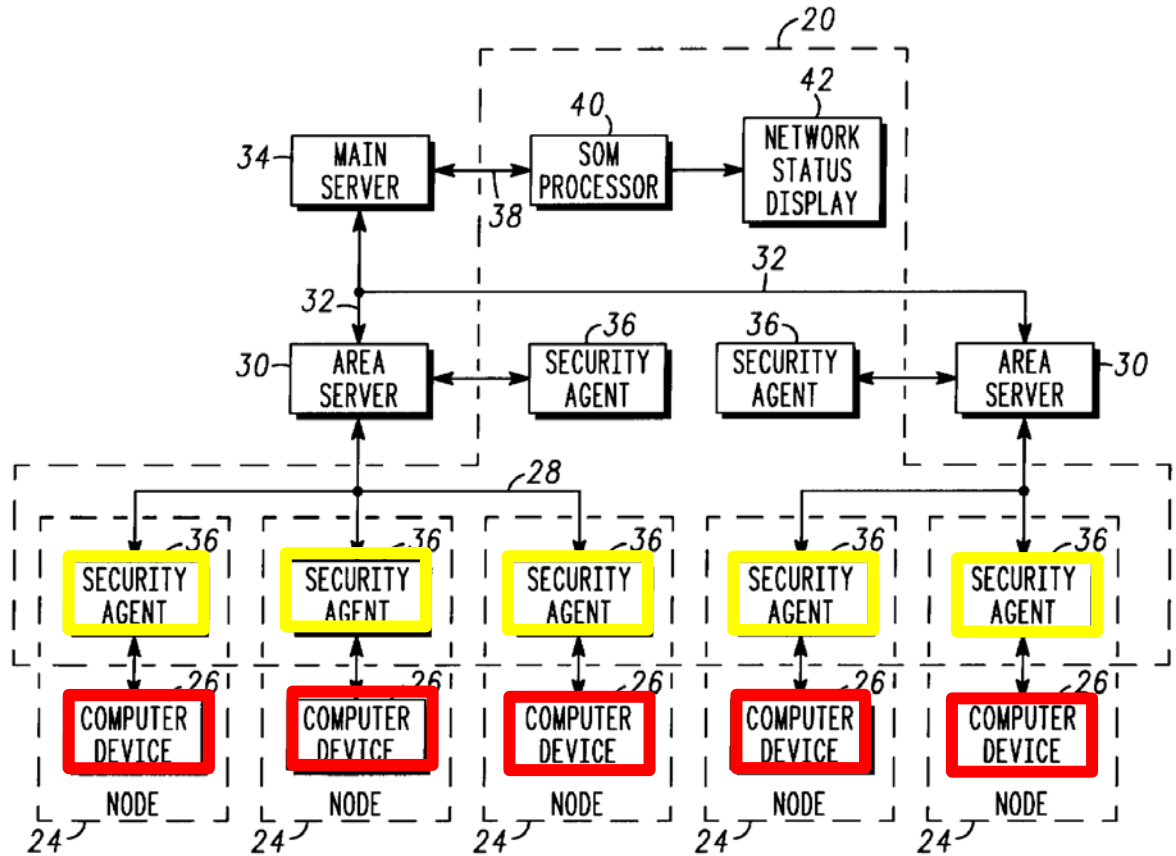


FIG. 1

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. EX-1003, ¶120.



22

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. EX-1003, ¶121.

3. Claim 2

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. EX-1003, ¶122.

[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:*

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. EX-1003, ¶123.

[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*

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. EX-1003, ¶124.

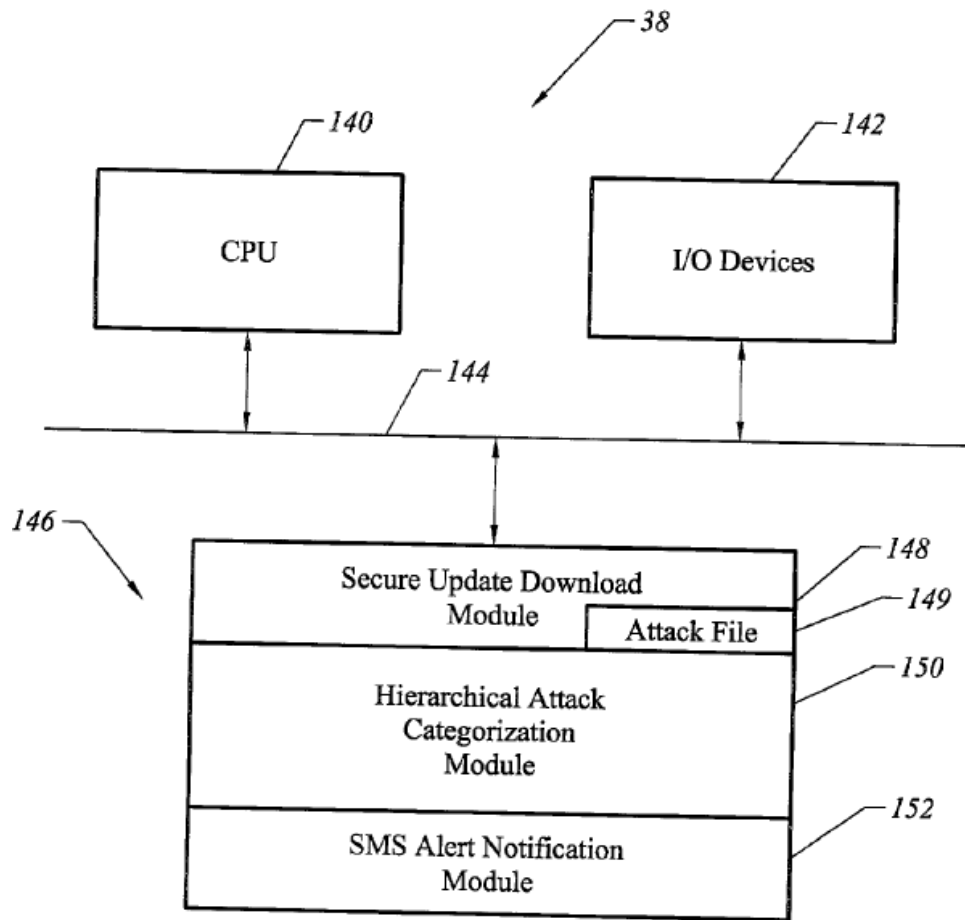


FIG. 15

EX-1006 FIG. 15; EX-1003, ¶124.

[2.2] generate the first vulnerability information utilizing the second vulnerability information, and

Gupta discloses this limitation for the same reasons as discussed with respect to limitation [1.2]. EX-1003, ¶125.

[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

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]. EX-1003, ¶126.

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. EX-1003, ¶127.

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. EX-1003, ¶128.

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; EX-1003, ¶129.

Third, Hill provides an example of security software for detecting and repulsing attacks (security agent) being distributed at nodes 24 containing computer devices 26. EX-1016 FIG. 1; EX-1003, ¶130.

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; EX-1003, ¶131.

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. EX-1003, ¶132.

[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:

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:

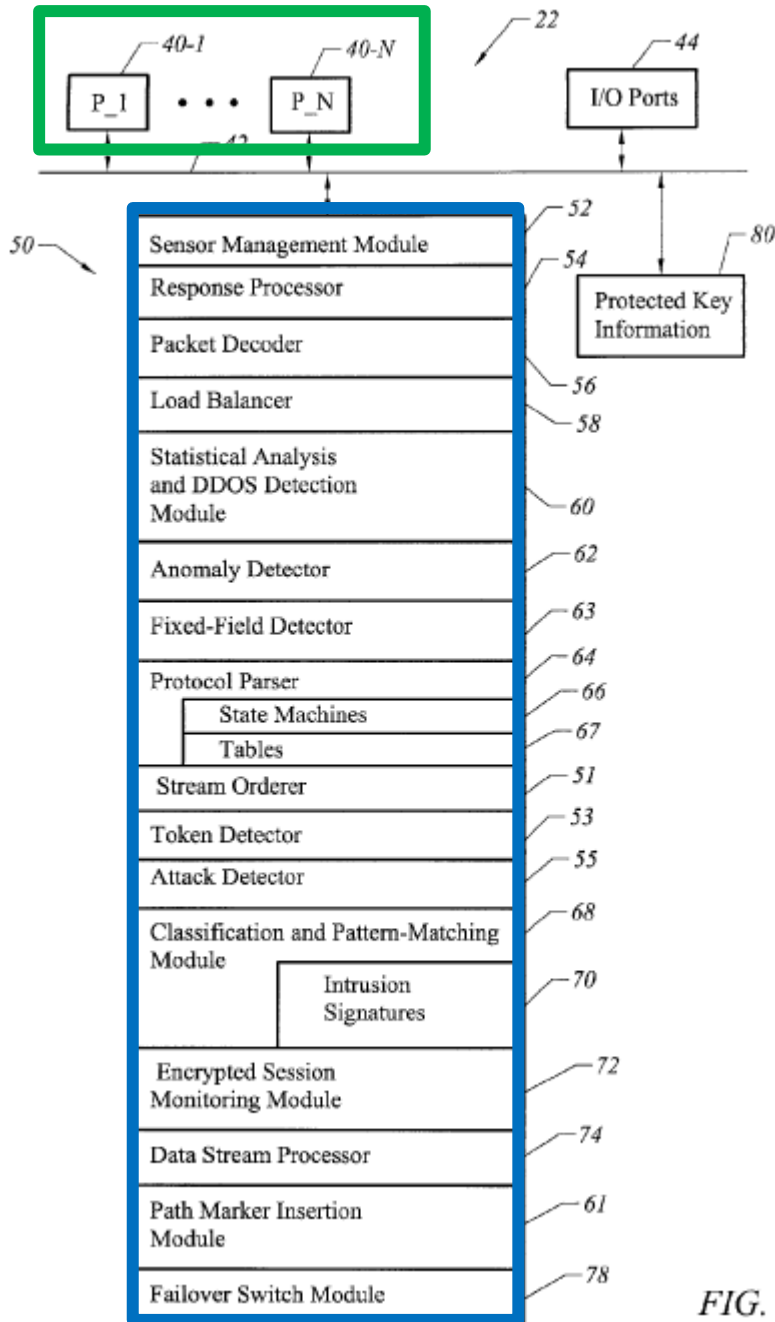


FIG. 2

EX-1006 FIG. 2; EX-1003, ¶133.

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. EX-1003, ¶134.

[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

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]; EX-1003, ¶135.

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; EX-1003, ¶136.

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*. EX-1003, ¶137.

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. EX-1006, [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)**.” EX-1006 [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 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. EX-1003, ¶137.

[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*

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. EX-1003, ¶138.

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. EX-1003, ¶139.

[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

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.”. EX-1006, [0041], [0044], [0051], [0057],[0081], [0166]. Gupta’s disclosure is consistent with the ’066 Patent disclosure that *data inspection-related information* includes “anomalies”. EX-1006 Claim 44; EX-1003, ¶140.

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.*) EX-1003, ¶141.

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

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.* EX-1003, ¶142.

[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*

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. EX-1003, ¶143.

[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:

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. EX-1003, ¶144.

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. EX-1003, ¶145.

[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,

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. EX-1006 [0151]; EX-1003, ¶46.

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.*) EX-1003, ¶147.

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

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*. EX-1003, ¶148.

[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

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. EX-1003, ¶149.

[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:

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. EX-1003, ¶150.

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. EX-1003, ¶151.

[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

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. EX-1006 [0064], [0075]; EX-1003, ¶152.

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. EX- 1006, [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. EX- 1003 [0198]; EX-1003, ¶153.

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. EX-1006 Claim 4. EX-1003, ¶154.

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.*) EX-1003, ¶155.

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. EX- 1007 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).**

EX-1007 7:58-67; EX-1003, ¶156.

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.” EX-1007 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. EX-1003, ¶157.

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. EX-1003, ¶158.

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

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*. EX-1003, ¶159.

[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

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. EX-1003, ¶160.

[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:*

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:

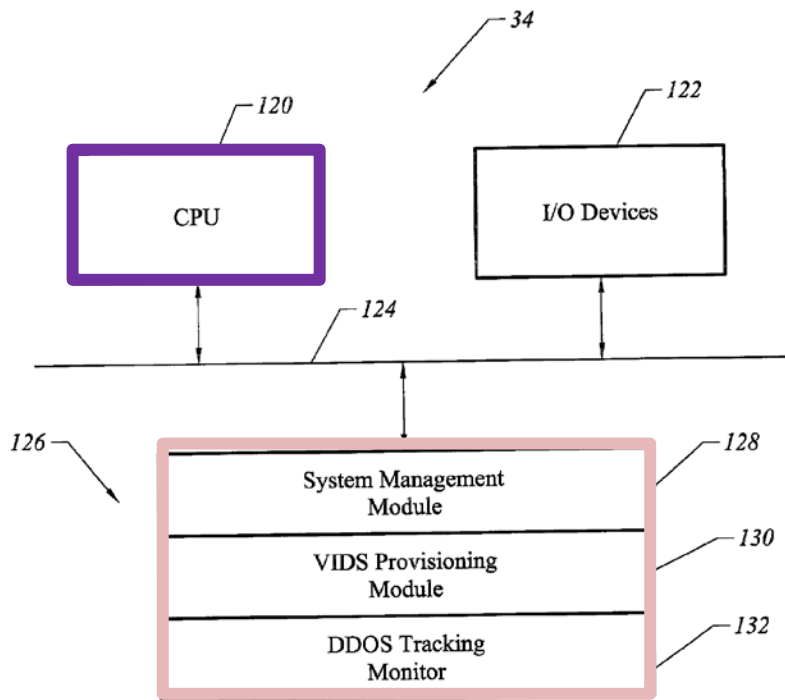


FIG. 14

EX-1006 FIG 14; EX-1003, ¶161

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. EX-1006 [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.” EX-1006, [10131], [0143]. The VIDS 130 supports “different security policies, protection objectives, "and security management preferences.” EX-1006, [0136]. Gupta further discloses that the “[t]he response processor 54 is configured by the system administrator.” EX-1006 [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*). EX-1003, ¶162.

[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*

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. EX-1003, ¶163.

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]. EX-1003, ¶164.

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*). EX-1003, ¶165.

[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*

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. EX-1003, ¶166.

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. EX-1003, ¶167.

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*). EX-1003, ¶168.

[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*

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. EX-1003, ¶169.

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]. EX-1003, ¶170.

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." EX- 1006, [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. EX-1003 ¶171.

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." EX-

1006, [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. EX-1003 ¶172.

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*). EX-1003, ¶173.

[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.*

Gupta discloses providing a user with the ability to select between different occurrence mitigation actions of diverse occurrence mitigation types. EX-1003 [0194]. 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. EX-1006, [10131], [0143]. The VIDS 130 supports “different security policies, protection objectives, and security management preferences.” EX-1006, [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. EX-1003, ¶174.

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.” EX-1006 [0087]. Thus, Gupta discloses terminating TCP connections, which a POSITA understood to be an “*intrusion prevention system-based occurrence mitigation type*.” EX-1003 ¶175.

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.” EX- 1006, [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. EX-1003 ¶176.

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)

EX-1007, 7:58–65; EX-1003, ¶177.

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).**

EX-1007 7:58-67; EX-1003, ¶178.

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.” EX-1007 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. EX-1007 7:65–67; EX-1003, ¶179.

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. EX-1003, ¶180.

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. EX-1006 [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.

EX-1006 [0136]; EX-1003, ¶181.

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. EX-1003, ¶182.

Therefore, Gupta in combination with Graham renders obvious [1.7].
EX-1003, ¶183.

XI. DISCRETIONARY DENIAL IS INAPPROPRIATE

A. Discretionary denial under 35 U.S.C. § 325(d) is not appropriate

Ground 1 is based on Gupta and Graham, and Ground 2 is based on Gupta, Graham and Hill. Graham was not cited or applied during prosecution of the '066 Patent. Both Gupta and Hill were identified on the face of the '066 Patent, but neither were effectively before the office as described in more detail below.

During prosecution, the examiner issued a Notice of Allowance of Claim 1 (Claim 54 during prosecution) and the dependent claims, explaining that the prior art fails to teach “identifying an occurrence, determining that at least one vulnerability is susceptible to being taken advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.” EX-1002, 564. Several months later, the Applicant submitted Information Disclosure Statements identifying over 775 references, including Gupta and Hill, but without any description of the relevancy of any of the references to allowed Claim 1. EX-1022 (7/20/20 IDS). Two months later, the Applicant cancelled all dependent claims and substituted a new set of dependent claims, including Challenged Claim 2, without any explanation of how the claims were patentable over the recently identified 775 references. In response, the examiner issued a new Notice of Allowance for all claims, identifying the same reason for the allowance of Claim 1 and did not identify any independent reason for the allowance of the newly

added dependent claims stating only “allowed by virtue of their dependency.”

EX-1002 790.

The grounds based on Gupta and Hill disfavors denial, because Gupta and Hill were not properly considered by the Office. The *Advanced Bionics* framework strongly disfavors discretionary denial because the “Office erred in a manner material” to patentability by overlooking the relevance of Gupta and Hill to the ’066 Patent claims. *Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH*, IPR2019-01469, Paper 6, 8-9 (Feb. 13, 2020). Analysis of this issue is guided by factors (c), (e), and (f) enumerated in *Becton*. *Advanced Bionics* at 9-10.

Regarding *Becton* factor (c) (the extent to which the asserted art was evaluated during examination), neither Gupta nor Hill were not the basis of any rejection for the ’066 Patent, which weighs strongly against exercising discretion. *See Cellco Partnership v. Huawei Device Co.*, IPR2020-01117, Paper 10, 13 (Feb. 3, 2021). As noted above, Gupta and Hill were cited as part of almost a dozen IDS filings on the same day (and after Claim 1 had already been examined and allowed), totaling over 750 references. There is no record of the Examiner’s evaluation of the merits of Gupta or Hill—particularly those presented in this petition—when also considering the hundreds of other documents cited. The Examiner’s evaluation may have been merely cursory, particularly in view of the

previously issued Notice of Allowance.

Regarding *Becton* factors (e) (Petitioner's identification of examiner error) and (f) (other facts and evidence presented in the petition), this petition specifically points out and explains how Gupta, as combined with Graham and Hill, renders obvious every limitation of Claims 1 and 2.

Moreover, in IPR2022-00035, the Board previously instituted review of Claim 1 on the merely identical grounds of Gupta in combination with Graham, which demonstrates a material error in prosecution. Thus, contrary to the Examiner's assertions in the Notice of Allowance regarding the prior art, Gupta identifies an occurrence (monitored network traffic), and determines that a vulnerability is susceptible to an attack in the packet (a given environment is vulnerable to an attack).

In summary, the Examiner erred in a material way by allowing the claims instead of rejecting them based on Gupta, Graham and Hill. Thus, under the second prong of *Advanced Bionics*, discretionary denial under § 325(d) is not appropriate on the basis of the Gupta ground.

B. Discretionary denial under the *Fintiv* factors is not appropriate

The Board has discretion to deny *inter partes* review under 35 U.S.C. § 314(a). In *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential), the Board set forth six non-dispositive factors intended to guide that discretionary decision of whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, 2022, the Director issued interim procedure regarding application of the *Fintiv* factors (“Interim Procedure”). The Interim Procedure states that “the PTAB will not deny institution of an IPR ... under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” Interim Procedure 9. Here, the Petition presents compelling evidence of unpatentability of the Challenged Claims. Specifically, the Board previously instituted trial for the Challenged Claim 1 based on the identical grounds in IPR2022-00035. Thus, the evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.

Further, Petitioner hereby issues a Sotera stipulation that should the board institute review, the Petitioner stipulates not to pursue in the parallel district court proceeding the same grounds as in the Petition or any grounds that could have reasonably been raised in the Petition. Thus, under the Interim Procedure, the Board should not deny institution.

Nevertheless, a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

Under factor 2, the trial date has not yet been set in the Related Litigation. Nonetheless, according to the most recent statistics on median time-to-trial for civil actions in W.D. Texas, the median time from filing to trial is 27 months. (<https://www.uscourts.gov/statistics/table/na/federalcourt-management-statistics/2022/03/31-1>). The Related Litigation was filed on January 10, 2023 and thus would be expected to go to trial shortly after April 2025 according to the median time to trial statistics. A Final Written Decision is expected in December 2024. Considering the inherent uncertainties of litigation scheduling, particularly where multiple trials are scheduled for the same date this factor weighs against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. A Scheduling Order has not yet issued in the case.

Under factor 4, Petitioner stipulates that if the IPR is instituted, it will not pursue the same grounds as in the Petition or any grounds that could have reasonably been raised in the Petition.

Under factor 5, Petitioner is a defendant in the Related Litigation.

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are strong and supported by compelling evidence of unpatentability. For example, in IPR2022-00035, the Board instituted trial finding that it was reasonably likely that the petitioner would be able to show that Claim 1 was unpatentable over Gupta in combination with Graham.

When viewed holistically, the timing of the present Petition was reasonable, there has been relatively limited investment in the related litigation, and there is minimal overlap between the present IPR and the Related Litigation. Thus, the efficiency and integrity of the IPR process is best served by instituting review.

C. Discretionary denial under the *General Plastic* factors is not appropriate

The *General Plastic* factors do not apply to this Petition because this is the first and only IPR petition filed by Petitioner challenging claims of the '066 Patent. Although the '066 Patent was previously challenged in IPR2022-00035, Petitioner was not involved in those IPRs. IPR2022-00035 was directed only to Claim 1, but the IPR settled shortly after the Board issued an institution decision. Thus, the Board never had the opportunity to review the Challenged Claims and issue a final written decision, and thus any concerns of serial petitions are largely outweighed by the benefits to the patent system of improving patent quality by reviewing the merits of the challenges raised in this petition, which have not been finally addressed to date. *Code200, UAB v. Bright Data, Ltd.*, IPR2022-00861, Paper 18 5-6 (P.T.A.B. Aug. 23, 2022) (precedential).

I. MANDATORY NOTICES

A. Real party-in-interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is Forcepoint LLC.

B. Related matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '066 Patent is or was involved in the following cases:

Case Heading	Number	Court	Status
<i>SecurityProfiling, LLC v. Cisco Systems, Inc.</i>	6-21-cv-00337	W.D. TEX-	Dismissed
<i>SecurityProfiling, LLC v. Trend Micro Incorporated</i>	6-21-cv-00330	W.D. TEX-	Dismissed
<i>SecurityProfiling, LLC v. Forcepoint LLC</i>	6:23-cv-00014	W.D.TEX	Pending Filed 1/10/230

The '066 Patent was involved in the following *Inter Partes Review* proceeding:

Case Heading	Number	Court	StatusFiled
<i>Cisco Systems, Inc. v. SecurityProfiling, LLC</i>	IPR2021-01428	PTAB	Institution Denied
<i>Cisco Systems, Inc. v. SecurityProfiling, LLC</i>	IPR2022-00259	PTAB	Settled after Trial Instituted

C. Lead and back-up counsel and service information

Lead Counsel:

Patrick McPherson, USPTO Reg. 46,255
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-5214; F: (202) 776-7801; PDMcPherson@duanemorris.com

Back-Up Counsel:

Patrick Muldoon USPTO Reg. 47,343
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-7840; F: (202) 776-7801; PCMuldoon@duanemorris.com

Paul H. Belnap, USPTO Reg. 73,106
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-7879; F: (202) 776-7801; PHBelnap@duanemorris.com

Please address all correspondence in this proceeding to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

XII. CONCLUSION

Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable.

Respectfully submitted,

Dated: June 8th 2023

/Patrick D. McPherson/
Patrick D. McPherson
Lead Counsel for Petitioner
Registration No. 46,255
901 New York Ave. NW
Suite 700 East
Washington DC 20001

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,635. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Respectfully submitted,

Dated: June 8th, 2023 _____

/Patrick D. McPherson/
Patrick D. McPherson
Lead Counsel for Petitioner
Registration No. 46,255

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

The Caldwell Firm, LLC
PATRICK CALDWELL
G. GORDON
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229
UNITED STATES

Respectfully submitted,

Dated: June 8th 2023

/Patrick D. McPherson/
Patrick D. McPherson
Lead Counsel for Petitioner
Registration No. 46,255