

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET, INC.,
Petitioner,

v.

BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY,
Patent Owner.

IPR2019-01327
Patent 7,370,358 B2

Before KEVIN C. TROCK, MONICA S. ULLAGADDI, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

TROCK, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Fortinet, Inc. (“Petitioner”) filed a Petition, Paper 1 (“Pet.” or “Petition”), to institute an *inter partes* review of claims 1, 2, 4–6, 14–18, 21, 23, 26, 27, 29–31, 34, 39–43, 46, and 48 (the “challenged claims”) of U.S. Patent No. 7,370,358 B2 (Ex. 1001, “the ’358 patent”). British Telecommunications Public Limited Company (“Patent Owner”) timely filed a Preliminary Response, Paper 6 (“Prelim. Resp.”), contending the Petition should be denied as to all challenged claims. Pursuant to an Order, Paper 8, authorizing Petitioner to file a Reply to Patent Owner’s Preliminary Response and Patent Owner to file a Sur-reply, Petitioner filed a Reply, Paper 9 (“Reply”), addressing Patent Owner’s arguments that IPR2019-01327 and IPR2019-01328 are duplicative, and Patent Owner filed a Sur-reply, Paper 10 (“Sur-reply”), regarding the alleged duplication of Petitions.

We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). A decision to institute under 35 U.S.C. § 314 may not institute on fewer than all claims challenged in the petition. *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018).

Upon consideration of the arguments presented by the parties and the evidence of record, we determine that Petitioner has not shown a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we do not institute an *inter partes* review.

B. Real Party-In-Interest

Petitioner identifies Fortinet, Inc. as the real party-in-interest. Pet. 2.

C. Related Proceedings

Petitioner and Patent Owner state that the '358 patent is the subject of the following action: *British Telecommunications PLC and BT Americas, Inc. v. Fortinet, Inc.*, C.A. No. 18-1018-CFC-MPT (D. Del). Pet. 2; Paper 5, 1. Petitioner and Patent Owner further state the '358 patent is the subject of a second Petition to institute an *inter partes* review (IPR2019-01328), challenging claims 1–4, 7–13, 19, 20, 24–29, 32–38, 44, 45, 49, and 50 of the '358 patent. Pet. 2; Paper 5, 1.

D. The '358 Patent (Ex. 1001)

The '358 patent, titled “Agent-based Intrusion Detection System,” is directed to a “computer security system [that] uses a plurality of co-operating software agents to protect a network against attack.” Ex. 1001, codes (54), (57). According to the '358 patent, the advent of increasingly powerful macro viruses with port-scanning capabilities “has demonstrated the inadequacies of most current static and manually-controlled security mechanisms for protecting computer systems,” the current mechanisms being “insufficiently flexible, scalable or reactive to be able to deal effectively with new and potentially unknown security threats.” *Id.* at 1:19–28. The '358 patent discloses an “intrusion detection system (IDS) for use within a computer network, and particularly to such a system that makes use of co-operative software agents” for “maintaining and tracking a groupwide measure of agent status or behavior . . . and determining that a security threat does or may exist when the actual behaviour patterns diverge from normal behaviour patterns.” *Id.* at 1:14–17, 2:32–40. One application of the '358

patent's IDS is for defending peer to peer (P2P) networks, which are "difficult to secure using existing network security models as they bypass traditional firewall mechanisms, and they may span multiple corporate networks." *Id.* at 8:1–7.

Figure 1 of the '358 patent, reproduced below, depicts a computer security system comprising software agents for determining the existence of a security threat.

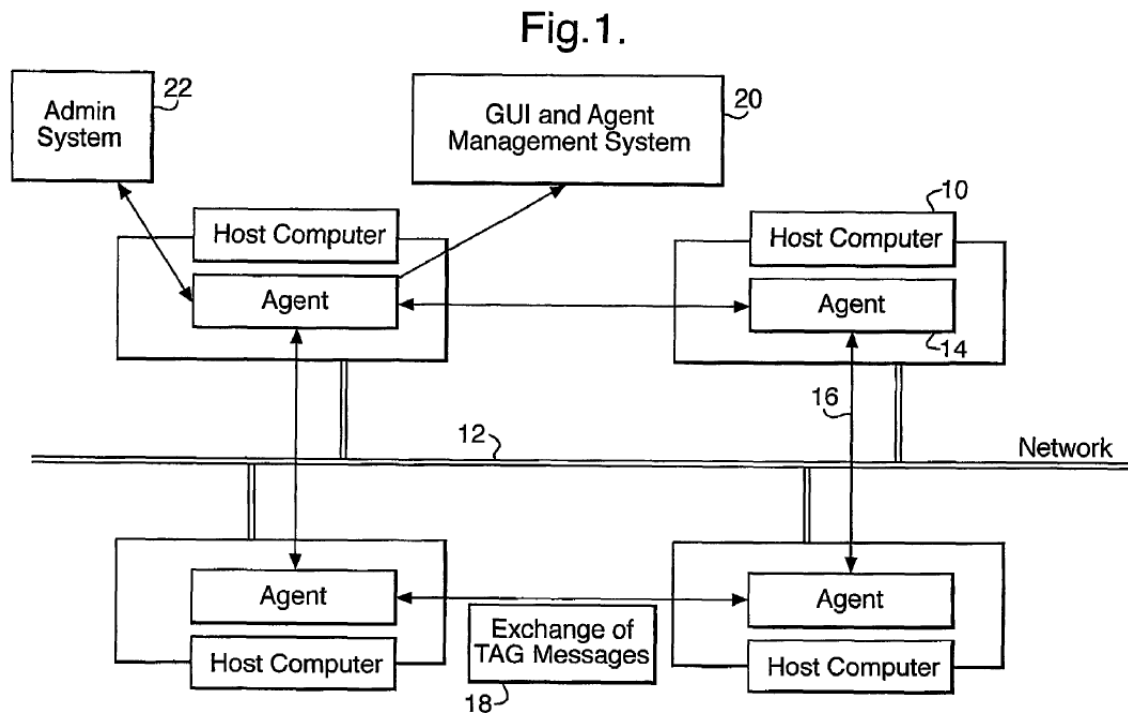


Figure 1, above, shows a computer security system designed to protect host computers 10 linked together by a network 12. *Id.* at 3:65–4:7. Protection is achieved by a population of distributed software agents 14 residing on the host computers, and acting as smart monitors of hostile behaviors, attacks, and intrusions on the network. *Id.* at 4:2–7. The computer security system maintains and tracks a groupwide measure of agent status or behavior, comparing actual behavior patterns of the measure with known normal behavior patterns, and determining that a security threat

does or may exist when the actual behavior patterns diverge from normal behavior patterns. *Id.* at 2:32–40, 4:6–19.

Agents 14 communicate with each other by exchanging tag messages 18, which allow information exchange and agent identification. *Id.* at 4:6–10. A virtual private network 16 may provide secure inter-agent communication. *Id.* at 4:9–19. Each agent has sensors for making “local measurements, some of which may relate to the local state of the physical network 12 and some . . . to the local state of the agent itself or to the virtual private network 16.” *Id.* at 4:33–37. The sensors’ measurements may include “local CPU utilisation, local network traffic rates, local memory usage, agent’s internal state (e.g. the ‘health’ of the agent), level of trade with other agents, [and] agent’s success rate at communicating with other agents.” *Id.* at 4:37–42. The sensors “allow agents to detect, either individually or in combination with other agents, anomalous behaviour on the network, such as for example that which might be symptomatic of a virus attack, a worm attack, or a denial of service attack.” *Id.* at 4:42–47.

Some patterns of anomalous activity may not be easily detectable by a single agent, such that macro-scale measurements are also made across agents or across the virtual private network to trigger alerts or initiate defensive actions. *Id.* at 4:54–60. For example, each agent may have a “metabolic rate” which can be considered representative of the agent’s “health” or “energy level,” and “[o]ne or more user-nominated agents across the network records and measures variations in the average or collective metabolic rate of the entire agent population. . . . [and] then compare[s] the measured metabolic rate over a specific time interval to previously recorded patterns known to represent healthy network states.” *Id.* at 4:54–5:1. In addition, user-nominated agents may monitor a frequency of inter-agent

messages to detect variations in this traffic. *Id.* at 5:5–8. Such variations can be used as indications of attacks on other agents, to indicate that the virtual private network may have been compromised, or to indicate attacks on the network resources of the host machines. *Id.* at 5:5–12. Agents may also compare patterns representative of some anomalous activity to stored lists of known anomalous patterns or signatures. *Id.* at 5:27–46. These “anomaly patterns” may indicate viral or worm infections, or other known threat processes. *Id.* at 5:32–35. Agents may also transmit anomaly patterns/signatures to other agents by tag messages 18 to “rapidly distribute[] knowledge of the potential threat throughout the community of agents.” *Id.* at 5:44–48. By exchanging shared anomaly patterns, the agents create “a group immune system which is far more resistant to attack than a collection of isolated detection systems.” *Id.* at 5:55–58.

Some agents 14 may be members of a single group, capable of talking to each other, while other agents 14 form other groups “with the agents of one group being able to communicate between themselves but not with the agents of a second group.” *Id.* at 6:13–19; *see also* 2:57–64 (“agents . . . divided up into a plurality of agent groups, each agent corresponding with other agents in its respective group, but not agents in other groups, by a message-exchange system including the exchange of group-specific tags”). By maintaining “the internal cohesion of each group, the [agents’] groups become better able to distinguish between ‘self’ and ‘non-self’, and therefore better able to identify messages from spurious non-friendly agents which might have infiltrated the virtual private network.” *Id.* at 6:18–23. Tag messages 18 enhance the agents’ cohesion and identification processes within a group. *Id.* at 6:5–12 and 30–35. Tag messages 18 may be

encrypted (as, e.g., hashed encoded objects), and decryptable only within one agent's group. *Id.* at 6:10–12, 29–30, and 46–49.

E. Challenged Claims

Petitioner challenges claims 1, 2, 4–6, 14–18, 21, 23, 26, 27, 29–31, 34, 39–43, 46, and 48 of the '358 patent. Pet. 1, 23–24. Claims 1, 16, 26, and 41 are independent.

Claims 1 and 26 are set out below.

1. [1.p] A computer security system comprising:
 - [1.1] a plurality of inter-communicating computers including software agents together forming a plurality of agent groups, each agent corresponding with other agents in its respective group but not with agents in other groups via a message-exchange system including the exchange of group specific tags;
 - [1.2] means for maintaining and tracking groupwide measures of agent status or behavior; and
 - [1.3] means for comparing actual behavior patterns of the measure for a given group with known normal behavior patterns and determining that a security threat does or may exist when the actual behavior patterns diverge from normal behavior patterns.

26. [26.p] A method providing computer security among a plurality of inter-communicating computers having associated software agents, said method comprising:
 - [26.1] dividing a plurality of said agents into plural groups, each agent corresponding with other agents in its respective group but not with agents in other groups, a message-exchange system including the exchange of group specific tags;
 - [26.2] maintaining and tracking groupwide measures of agent status or behavior comparing actual behavior patterns of the measure for a given group with known normal behavior patterns; and
 - [26.3] determining that a security threat does or may exist when the actual behavior patterns diverge from normal behavior patterns.

Ex. 1001, 10:50–63, 11:53–12:5 (bracketed numbering added).

F. Prior Art References

Petitioner relies upon the following prior art references:

(1) Porras et al., *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 20th National Information Systems Security Conference (NISSC) on October 9, 1997, 353–365. (“EMERALD97”)¹ (Ex. 1004);

(2) U.S. Patent No. 6,321,338 B1, issued Nov. 20, 2001 (“EMERALD-Patent”) (Ex. 1005);

(3) Porras et al., *Live Traffic Analysis of TCP/IP Gateways*, Internet Society’s Networks and Distributed Systems Security Symposium of March 1998. (“EMERALD98”) (Ex. 1006);

(4) Crosbie et al., *Defending a Computer System Using Autonomous Agents*, Proceedings of the 18th National Information Systems Security Conference on October 10–13, 1995, Vol. II, 549–558. (“Crosbie1”) (Ex. 1009);

(5) Crosbie et al., *Applying Genetic Programming to Intrusion Detection*, Association for the Advancement of Artificial Intelligence (AAAI) Technical Report FS-95-01 of November 1995, 1–8. (“Crosbie2”) (Ex. 1010); and

(6) Schnackenberg et al., *Infrastructure for Intrusion Detection and Response*, DARPA Information Survivability Conference & Exposition (DISCEX ’00) on January 25–27, 2000, Vol. II, 3–11. (“IDIP”) (Ex. 1011).

Petitioner also relies on the Declaration of Dr. Stuart Staniford. Ex. 1003.

¹ We employ the reference labels selected by the Petitioner. See Pet. iv (Petitioner’s Exhibit List).

G. Asserted Grounds of Unpatentability

Claims Challenged	35 U.S.C. §	References
1, 2, 4, 6, 14, 15, 21, 26, 27, 29, 31, 34, 39, 40, 46	103	EMERALD97, EMERALD- Patent, EMERALD98 (the “EMERALD References”) ² , IDIP
5, 17, 18, 30, 42, 43	103	EMERALD References, IDIP, Crosbie2
23, 48	103	EMERALD References, IDIP, Crosbie1
16, 41	103	EMERALD References, Crosbie2

Pet. 23–24.

II. ANALYSIS

A. Level of Ordinary Skill

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991).

Petitioner contends that a person having ordinary skill in the art (“POSA”) would have had

a working knowledge of engineering intrusion detection systems including distributed intrusion detection systems. . . . [and] would have gained knowledge of these concepts through a

² Petitioner collectively refers to EMERALD97, the EMERALD-Patent, and EMERALD98 as the “EMERALD References.” Pet. 25.

mixture of training and work experience, such as by having a bachelor's degree in computer science, computer engineering, or an equivalent, and four years of industry experience in intrusion detection; or by obtaining a Master's degree in these subjects with two years experience; or by having no formal education but industry experience in intrusion detection of at least six years.

Pet. 18 (citing Ex. 1003 ¶ 23). Patent Owner does not contest Petitioner's definition of a person of ordinary skill in the art at this stage. *See* Prelim. Resp. 20.

For purposes of this Decision, because the parties do not dispute the level of ordinary skill, we adopt Petitioner's proposed description of the person of ordinary skill in the art, which appears to be commensurate with the level of skill contemplated by the prior art. The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

B. Claim Construction

For petitions filed after November 13, 2018, a claim shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings before the Patent Trial and Appeal Board*, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (codified at 37 C.F.R. § 42.100 (2019)). The Petition was accorded a filing date of July 11, 2019. Paper 3. Thus, we apply the claim construction

standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Under *Phillips*, claim terms are generally given their ordinary and customary meaning as would be understood by one with ordinary skill in the art in the context of the specification, the prosecution history, other claims, and even extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Phillips*, 415 F.3d at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

The specification may reveal a special definition given to a claim term by the patentee, or the specification may reveal an intentional disclaimer or disavowal of claim scope by the inventor. *Id.* at 1316. If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). The disavowal, if any, can be effectuated by language in the specification or the prosecution history. *Poly-America, L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016). “In either case, the standard for disavowal is exacting, requiring clear and unequivocal evidence that the claimed invention includes or does not include a particular feature.” *Id.*

Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017); see *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

Petitioner proposes constructions for several claim terms, including “agent” and “group specific tags.” Pet. 16–17. In particular, Petitioner contends that “agent” means “a piece of software running on a computer system,” and “group specific tags” means “information exchanged between agents that enables a member of a group of agents to distinguish other group members from non-group members.” *Id.*

In addition, some of the claims, such as independent claims 1 and 16, have “means-plus-function” limitations. Petitioner asserts that “[e]ach of the means-plus-function terms is directed to software running on a computer to perform the recited functions.” Pet. 15 (citing Ex. 1003 ¶¶ 105–106). Petitioner argues that “[b]ecause the cited art includes these structures, the construction of these limitations is not material.” *Id.* Nonetheless, Petitioner identifies structure in the ’358 Specification that corresponds to the “means” limitations in claims 1 and 16. *See* Pet. 15–16 (citing Ex. 1003 ¶¶ 107–117).

Patent Owner “does not dispute Petitioner’s proposed constructions” and submits, “at this stage, no claim term requires express construction.” Prelim. Resp. 26–27.

For purposes of this Decision, we do not construe any of the claim terms expressly nor assess Petitioner’s proposed corresponding structures for the “means-plus-function” limitations, because the parties do not dispute any of the terms. *See Vivid Techs.*, 200 F.3d at 803 (only terms that are in controversy need to be construed, and “only to the extent necessary to resolve the controversy”).

C. Patentability Challenges

1. Principles of Law on Obviousness

Section 103(a) forbids issuance of a patent when “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” In *Graham*, the Supreme Court set out a framework for applying the statutory language of Section 103: the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. *Graham*, 383 U.S. at 17.

The Supreme Court has made clear that we apply “an expansive and flexible approach” to the question of obviousness. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 415 (2007). Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *KSR*, 550 U.S. at 417. Reaching this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.*

2. Relevant Prior Art

a. EMERALD97 (Ex. 1004)

EMERALD97, titled “EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances,” describes “a distributed scalable tool suite for tracking malicious activity through and across large networks,” using “highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically at various abstract layers in a large network.” Ex. 1004, 1, Abstr. The techniques in EMERALD97 are applicable to “a large enterprise network with thousands of users connected in a federation of independent administrative *domains*” that seeks to “provide real-time detection of patterns in network operations that may indicate anomalous or malicious activity, and to respond to this activity through automated countermeasures.” *Id.* at 2, § 2.

EMERALD97 employs “a building-block architectural strategy using independent distributed surveillance monitors that can analyze and respond to malicious activity on local targets, and can interoperate to form an analysis hierarchy” which provides a framework for recognizing global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across entire network enterprises. *Id.* at 3, § 2. EMERALD97’s monitors include: (i) “dynamically deployable, highly distributed, and independently tunable *service monitors* . . . dynamically deployed within a domain to provide localized real-time analysis of infrastructure (e.g., routers or gateways) and services (privileged subsystems with network interfaces)”; (ii) “[*d*]omain monitors” that are “responsible for surveillance over all or part of the domain” and “correlate intrusion reports disseminated by individual service monitors, providing a domain-wide perspective of malicious activity (or patterns of activity)”; and (iii)

“[e]nterprise-layer monitors correlat[ing] activity reports produced across the set of monitored domains” such that “reports of problems found by one monitor may propagate to other monitors throughout the network.” *Id.* at 3–4, § 3. Information correlated by a service monitor can be “disseminated to other EMERALD monitors through a *subscription*-based communication scheme” enabling “monitor interoperation.” *Id.* at 3, § 3. Meanwhile, the domain monitors are responsible for “interfacing with other monitors beyond the domain, and reporting threats against the domain to administrators.” *Id.* at 3–4, § 3.

Figure 1 of EMERALD97, reproduced below, illustrates a generic monitor architecture.

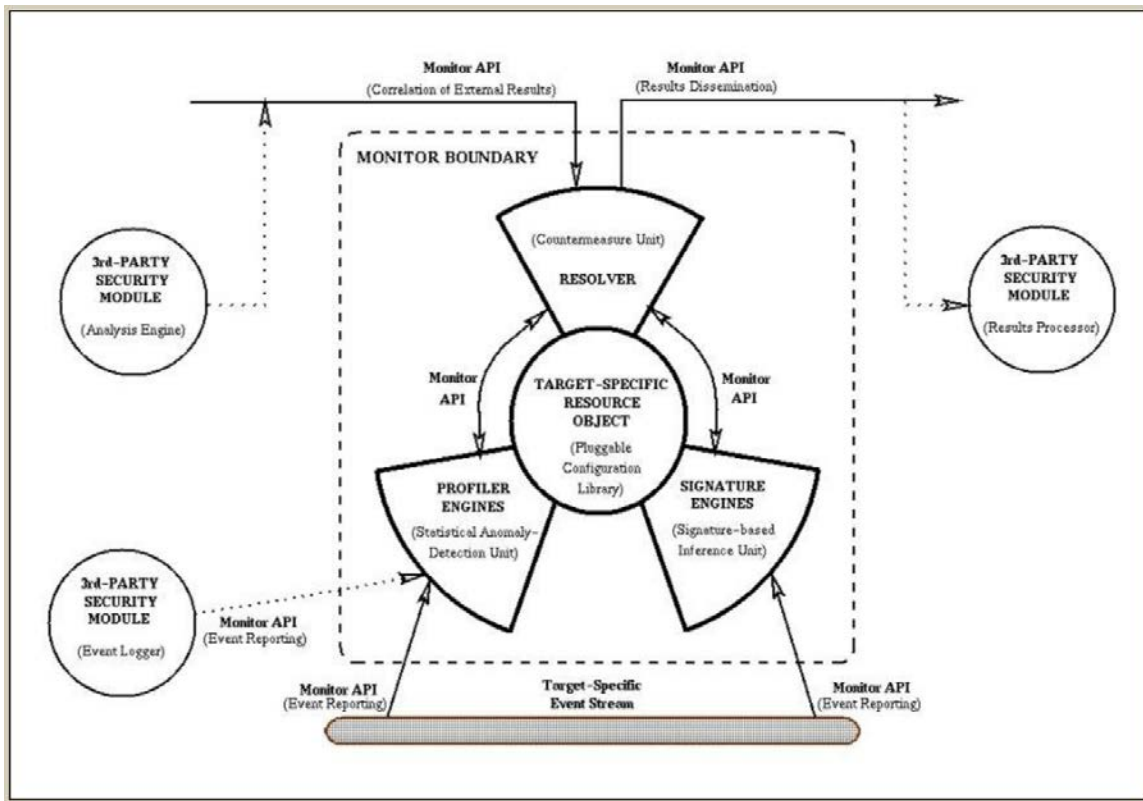


Figure 1 illustrates a generic EMERALD monitor architecture.
Id. at 5, § 3.1.

EMERALD97's Figure 1, above, illustrates a generic monitor architecture that enables a "flexible introduction and deletion of analysis engines from the monitor boundary as necessary." *Id.* at 4, § 3.1. The monitor architecture includes (1) a "*profiler engine* [that] performs statistical profile-based anomaly detection given a generalized event stream of an analysis target" and (2) a "*signature engine* [that] requires minimal state-management and employs a rule-coding scheme that breaks from traditional expert-system techniques to provide a more focused and distributed signature-analysis model." *Id.* at 5, § 3.1. The monitor architecture also includes (3) "a *resource object*. . . [that] is a pluggable library of target-specific configuration data and methods that allows the monitor code-base to remain independent from the analysis target to which it is deployed," (4) a "resolver implementing a response policy based on intrusion summaries produced by other EMERALD monitors," and (5) an "application programmers' interface that enhances the[] [monitor's] ability to interoperate with the analysis target, and with other third-party intrusion-detection tools." *Id.* at 4–5, § 3.1. A monitor's resolver may "correlate analysis results produced externally by other analysis engines to which it subscribes, and it may be bound to one or more analysis engines within the monitor boundary." *Id.* at 5, § 3.1.

EMERALD97 explains that "[i]nteroperability is especially critical to EMERALD's decentralized monitoring scheme, and extends within EMERALD's own architectural scope as well as to third-party modules,"

and “[t]o support interoperability, EMERALD monitors incorporate a bidirectional messaging system.” *Id.* at 5–6, § 3.1.

b. EMERALD-Patent (Ex. 1005)

The EMERALD-Patent, titled “Network Surveillance,” describes network surveillance techniques including “receiving network packets handled by a network entity and building at least one long-term and a least one short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections” to determine suspicious network activity. Ex. 1005, codes (54), (57). EMERALD-Patent’s Figure 1, reproduced below, illustrates network monitors deployed in an enterprise. *Id.* at 3:2–3.

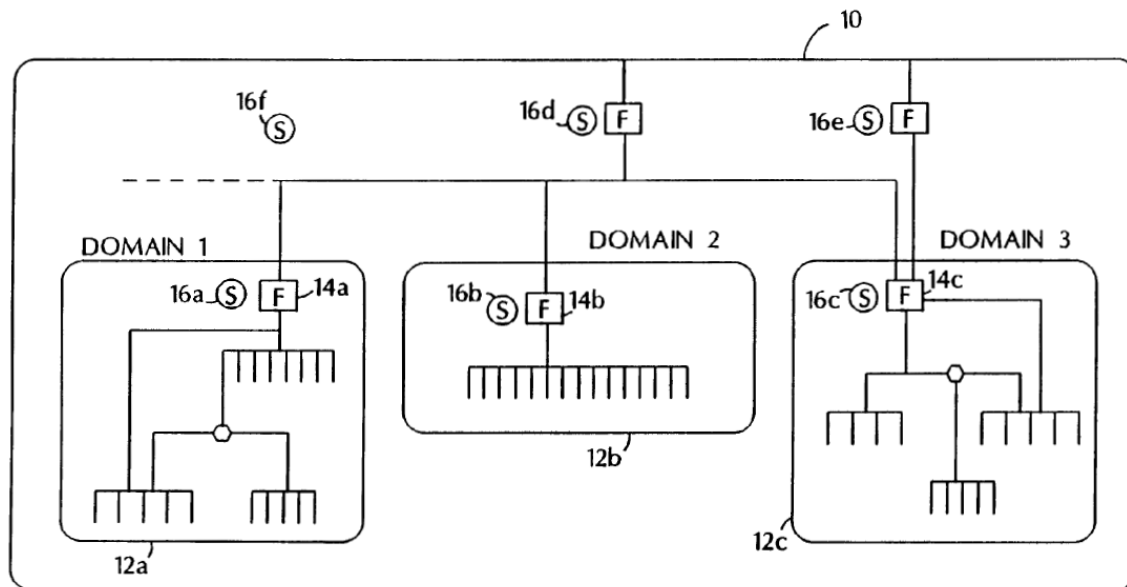


FIG. 1

Figure 1 is a diagram of network monitors 16a–16f deployed in an enterprise 10. *Id.* at 3:2–3 and 16–35.

EMERALD-Patent’s Figure 1 illustrates an enterprise 10 including domains 12a–12c, each domain 12a–12c including one or more computers

offering local and network services. *Id.* at 3:16–23. Enterprise 10 further includes dynamically deployed network monitors 16a–16f (including service monitors 16a–16c, domain monitors 16d–16e, and enterprise monitors 16f), which “analyze and respond to network activity and can interoperate to form an analysis hierarchy. . . . [that] provides a framework for the recognition of more global threats to interdomain connectivity, including coordinated attempts to infiltrate or destroy connectivity across an entire network enterprise.” *Id.* at 3:31–43.

Service monitors 16a–16c provide local real-time analysis of network packets (e.g., TCP/IP packets) handled by network entities 14a–14c, while information gathered by a service monitor can be disseminated to other monitors 16a–16f such that monitors 16a–16f “are able to efficiently disseminate reports of malicious activity without requiring the overhead of synchronous polling.” *Id.* at 3:42–65. Domain monitors 16d–16e perform surveillance over all or part of a domain 12a–12c, correlate intrusion reports disseminated by individual service monitors 16a–16c, and disseminate analysis reports to enterprise monitors 16f for global correlation. *Id.* at 3:66–4:18. Enterprise monitors 16f correlate activity reports produced across the set of monitored domains 12a–12c. *Id.* at 4:19–22. Enterprise monitor 16f subscribes “to various domain monitors 16d–16e, just as the domain monitors 16d–16e subscribed to various service monitors 16a–16c.” *Id.* at 4:27–31. “Through correlation and sharing of analysis reports, reports of problems found by one monitor 16a–16f may propagate to other monitors 16a–16f throughout the network” to “address[] more global, information attacks against the entire enterprise.” *Id.* at 4:42–47.

c. EMERALD98 (Ex. 1006)

EMERALD98, titled “Live Traffic Analysis of TCP/IP Gateways,” describes “techniques to analyze TCP/IP packet streams that flow through network gateways for signs of malicious activity, nonmalicious failures, and other exceptional events” to demonstrate “the utility of introducing gateway surveillance mechanisms to monitor network traffic.” Ex. 1006 1, Abstr. Network traffic may be continuously measured to monitor the network’s health and status for connectivity and throughput. *Id.* at 6, § 4.2. For example, an “instantaneous measure of traffic volume maintained by a gateway monitor can detect a sudden and unexpected loss in the data rate of received packets, when this volume falls outside historical norms for the gateway.” *Id.* EMERALD98’s monitoring techniques also use “volume analyses to help detect the introduction of malicious traffic, such as traffic intended to cause service denials or perform intelligence gathering,” whereby a sharp increase in the overall volume of discarded packets may indicate maliciously intended transmissions such as scanning of UDP ports, and malformed packets resulting from poor line quality or internal errors in neighboring hosts. *Id.* at 7, § 4.3.

EMERALD98’s monitoring techniques may also monitor event-distribution measures (meta-measures that monitor which measures are affected by particular events) using a “Monitor of Monitors” approach by which “each monitor contributes to an aggregate event stream for the domain of [a] correlation monitor.” *Id.* at 7, § 4.4. Significant events may be generated “only when the individual monitor decides that the recent behavior is anomalous,” whereby an overall intensity of event streams and a “distribution of which monitors and which measures are anomalous” may indicate a correlated attack. *Id.* Monitors include “individual traffic

monitors dispersed to the various entry points of external traffic into local network domains” and enterprise-layer monitors that “correlate[] the distributed results into a meta-event stream.” *Id.* at 9, § 6.

d. IDIP (Ex. 1011)

IDIP, titled “Infrastructure for Intrusion Detection and Response,” describes an “Intruder Detection and Isolation Protocol (IDIP) architecture” that “supports the need for an intrusion detection and response infrastructure.” Ex. 1011, 9, Abstr. Figure 1 of IDIP, reproduced below, illustrates systems organized into IDIP communities.

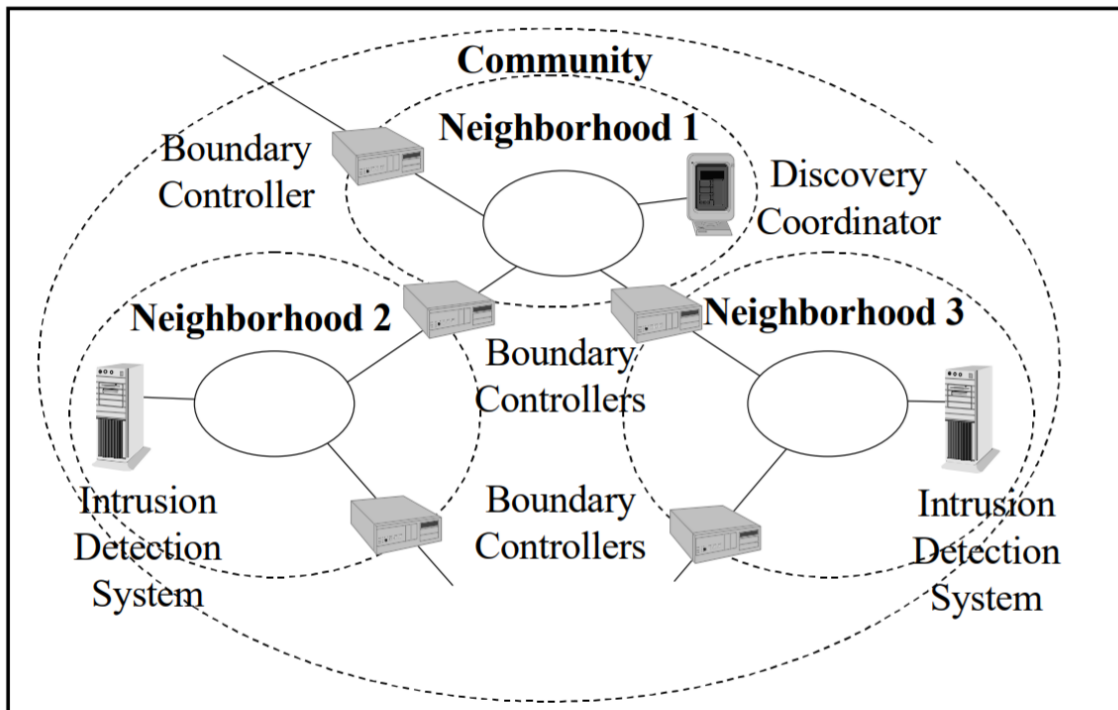


Figure 1: IDIP communities

Figure 1 illustrates an IDIP communities’ infrastructure for intrusion tracking and isolation. *Id.* at 10, § 2.

IDIP’s Figure 1, above, illustrates IDIP systems organized into IDIP communities, each IDIP community being an administrative domain, with intrusion detection and response functions managed by a component called

“Discovery Coordinator.” *Id.* at 10, § 2. The communities are further organized into IDIP neighborhoods representing collections of components with no other IDIP component between them, where boundary control devices are members of multiple IDIP neighborhoods. *Id.* An intrusion response is accomplished by IDIP nodes, such that “when an attack traverses an IDIP-protected network, each IDIP node along the path is responsible for auditing the connection” and “when a component detects an intrusion attempt, the detector distributes an attack report to its neighbors who can then help trace the attack path and respond to the intrusion.” *Id.* This enables the IDIP protocol to trace the attack back to the edge of the IDIP-protected system, taking appropriate responses at each IDIP node along the attack path. *Id.*

Some IDIP nodes may be “significantly less ‘trustworthy’ than others because they may have a number of vulnerabilities available for an attacker to use,” and therefore such IDIP nodes may be compromised and potentially used against the system. *Id.* at 11, § 2. To address this problem, the IDIP protocol distinguishes less trustworthy components from more trustworthy components. *Id.* For example, the Discovery Coordinator has access to system-wide information including topology, component vulnerabilities, neighbor lists, as well as status and status changes for each IDIP neighbor. *Id.* at 13, § 5.1, 15, § 5.2.3. Additionally, the IDIP protocol includes “[e]fficient cryptography for messages . . . that must be sent to each node in a neighborhood,” using encryption, generation of integrity checksums for IDIP messages, and multicast key distribution. *Id.* at 12, § 4.

e. Crosbie1 (Ex. 1009)

Crosbie1, titled “Defending a Computer System using Autonomous Agents,” describes “a prototype architecture of a defense mechanism for

computer systems” using “small, independent agents [that] monitor the system. . . . [and] are taught how to recognize intrusive behavior.” Ex. 1009, 549, Abstr. The agents’ learning mechanism is built using genetic programming so that an “agent should do one job well, do it in cooperation with the other agents, and do it as efficiently as possible.” *Id.* at 549, 553, §

4. Crosbie1 explains the agents’ architecture and operation as follows:

Each agent will be structured to monitor audit logs and other system data streams for a small subset (possibly even one) of activities. When an activity is detected (e.g. a login attempt, a network connection, excessive CPU usage etc.), the agent will simply inform the other agents on the system that it suspects an intrusion. Naturally this agent could be mistaken. However, the other agents will take this into account in their own operation. Once these broadcasts exceed some threshold, a message can be sent to a human operator via some monitoring process.

This illustrates how a intrusion decision is reached. No one agent has the final vote to decide on a potential intrusion. It is a collective consensus among all the agents on the system. If only one agent suspects an intrusion, then it will be ignored. If many of them suspect anomalous behavior, then there probably is a potential intrusion. Certain events may be more “important” in this scheme than others—for example 50 failed login attempts on root would be more significant than an ftp connection from a machine outside the domain. If two separate agents detect these events, the message from the first agent detecting failed login attempts could be given more “weight” than that of the second. Other agents would then react differently to seeing the more “important” message—possibly monitoring for slightly different activities as a result.

Id. at 553, § 4.

f. Crosbie2 (Ex. 1010)

Crosbie2, titled “Applying Genetic Programming to Intrusion Detection,” describes an intrusion detection system implemented using

autonomous agents built by genetic programming. Ex. 1010, 1, Abstr. The agents, which may run simultaneously and in parallel to perform intrusion detection, may be placed in a computer system's kernel. *Id.* at 2. Each agent performs computations based on contents of audit records and "reports a *suspicion value* which indicates whether the agent considers the system (as viewed through the audit log records) under the threat of an intrusion." *Id.* at 2–3. Each agent reports its suspicion value to an upper multiplexor, which combines individual suspicion values into an overall suspicion report (with, e.g., an average of suspicion values) to be passed up to a system security officer. *Id.* at 3.

3. *Independent Claims 1 and 26*

Petitioner contends independent claims 1 and 26 are obvious over the combined teachings of the EMERALD References and IDIP. Pet. 27–49. All of the dependent claims of the '358 patent depend from either claim 1 or claim 26. Claims 1 and 26 are similar, where claim 1 recites a computer security system and claim 26 recites a method for providing computer security. Claim 1, however, recites two "means for" limitations, whereas claim 26 does not. To support its position on obviousness with respect to claim 26, Petitioner relies on the evidence and arguments it uses to support its position for claim 1. *See* Pet. 50. Patent Owner does not provide arguments directed separately to claim 26. *See* Prelim. Resp. 28–53. We address limitation 1.1 below, but our consideration of limitation 1.1 also applies to limitation 26.1, which recites similar critical language.

- a. [1.1] a plurality of inter-communicating computers including software agents together forming a plurality of agent groups, each agent corresponding with other agents in its respective group but not with agents in other groups via a message-exchange system including the exchange of group specific tags

Petitioner relies on the combined teachings of EMERALD97 (Ex. 1004), the EMERALD-Patent (Ex. 1005), and IDIP (Ex. 1011) to meet this limitation. See Pet. 40–44. Petitioner asserts the EMERALD References teach “a hierarchical framework in which a ‘domain’ monitor (16d, 16e) and several ‘service’ monitors (e.g., for each service/router in the domain) (16a, 16b, 16c) were deployed on respective computers in each ‘domain’ (12a, 12b, 12c) of the network.” *Id.* at 40–41 (citing *id.* at § VIII.A.1, § VIII.A.2; Ex. 1004, 2–3; Ex. 1005, Fig. 1, 3:16–27, 3:31–45, 3:66–4:3, 4:6–7; Claim [1.i]; Ex. 1003 ¶ 161). Petitioner’s annotated Figure 1 from the EMERALD-Patent is shown below.

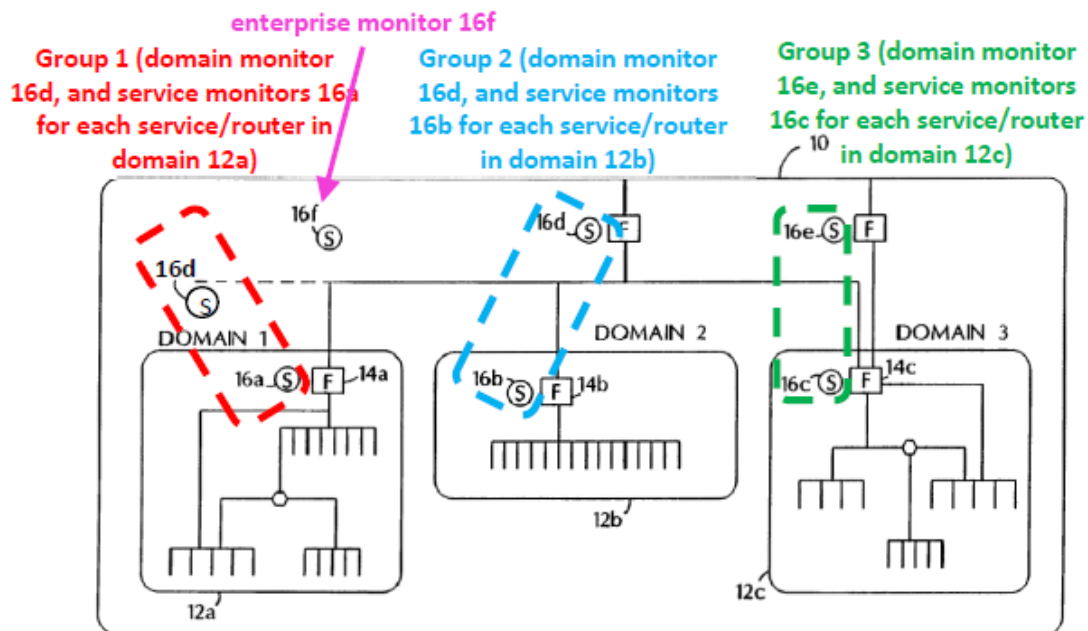


FIG. 1

Petitioner’s annotated Figure 1 from the EMERALD-Patent, shown above, depicts a diagram of network monitors, 16a–16f, and Domains 1–3, in an enterprise. Ex. 1005, 3:2–3; Fig. 1.

Petitioner asserts, “EMERALD97 teaches that monitors only exchanged messages with trusted monitors (identified in their ‘subscription list’) and that the trust relationship (which bounded each subscriber group) could vary domain-to-domain, including being restricted to the monitors in a single domain.” Pet. 41 (citing *id.* at § VIII.A.1; Ex. 1004, 2 (“Some domains may share trust relationships with other domains . . . Other domains may operate in complete mistrust of all others.”), 6–7, 9–10, Fig. 2; Ex. 1003 ¶ 162).

Petitioner also asserts EMERALD97 “teaches mutual authentication, and message confidentiality and integrity, as ‘essential’ to its subscription-based messaging scheme, and teaches the use of cryptographic, key-based techniques to ensure only trusted subscriber monitors understood a given monitor’s communications.” *Id.* at 42 (citing *id.* at § VIII.A.1; Ex. 1004, 7, 11; Ex. 1003 ¶ 163). Thus, Petitioner concludes, “EMERALD97 in view of EMERALD-Patent teaches a plurality of inter-communicating computers including software agents (monitors) together forming a plurality of agent groups (trusted monitor groups).” *Id.* (citing Ex. 1003 ¶ 164).

Petitioner further concludes that

EMERALD97 in view [of] EMERALD-Patent teaches a plurality of agent groups (trusted monitor groups) where each agent (monitor) corresponds with other monitors in its trusted monitor group, but not with untrusted, non-subscriber monitors, via a bi-directional, subscription-based messaging scheme in which cryptographic, key-based techniques were used to ensure only trusted subscriber monitors understood a given monitor’s communications.

Id. at 43 (citing Ex. 1003 ¶ 168).

Petitioner argues, “grouping agents (monitors) into mutually independent groups to achieve the benefit of reducing the risk of an attack in one group from impacting other agent groups (trusted monitor groups) was a well-known solution” to a person of ordinary skill in the art. *Id.* (citing *id.* at § VI.F.3; Ex. 1003 ¶ 169).

Petitioner also argues, a person of ordinary skill in the art “would understand ‘group-specific tags’ means ‘information exchanged between agents that enables a member of a group of agents to distinguish other group members from non-group members.’” *Id.* (citing *id.* at § VI.C.3; Ex. 1003 ¶¶ 170, 120–123). Petitioner asserts,

IDIP discloses the exchange of information that accomplishes this same function (enables a member of a group of agents to distinguish other group members from non-group members) by distributing and managing group-specific (neighborhood/sub-neighborhood-specific) multicast keys, and using such group specific keys to secure messages exchanged between intrusion detection components within a given group.

Id. at 43–44 (citing *id.* at § VIII.A.5; Ex. 1011, 3–5, Figs. 1, 3; Ex. 1003 ¶ 170).

Petitioner argues a person of ordinary skill in the art

would be motivated to use IDIP’s group-specific multicast keys in EMERALD’s subscription-based messaging scheme because doing so would involve nothing more than applying a known technique to a known device that is ready for improvement, and thereby achieve (i) EMERALD97’s ‘essential’ security requirements, (ii) the well-known benefits of preventing untrusted, nonsubscriber monitors from understanding messages exchanged in a trusted monitor group, and (iii) a reduction of the risk that an attack in one monitor group will impact other monitor groups.

Id. at 44 (citing *id.* at §§ VIII.A.6; VI.F.3; Ex. 1003 ¶ 171). A person of ordinary skill in the art, Petitioner argues, “would also be confident of the success of the modification especially given EMERALD monitors already used subscription lists and key-based cryptography to render messages unintelligible to untrusted monitors, and IDIP explicitly identifies that EMERALD monitors had already been integrated with IDIP.” *Id.* (citing Ex. 1004, 7, 11; Ex. 1011, 8, Table 1; Ex. 1003 ¶ 172).

Patent Owner challenges Petitioner’s assertion that EMERALD’s monitors are equivalent to the agents recited in claim 1. *See, e.g.*, Prelim. Resp. 29. Patent Owner argues that the EMERALD References organize monitors into a hierarchy rather than organizing agents into groups. *Id.* Further, Patent Owner argues,

a statement about whether domains operate in complete mistrust of one another is not clearly indicative of whether domain monitors operate in complete mistrust of one another, much less whether the monitors in the hierarchy are limited to exchanging messages within the annotated ‘groups’ of monitors and no monitors outside of those annotated ‘groups.’” *Id.* at 31–32. Patent Owner asserts, “no EMERALD reference clearly states that an untrusting domain—let alone an ‘untrusting domain monitor’ (a concept not even explicitly contemplated in any EMERALD reference)—will not provide any outgoing connections and will not receive any incoming connections.

Id. at 32 (citing Ex. 2001 ¶ 96).

To illustrate its argument, Patent Owner modifies Petitioner’s annotated Figure 1 from the EMERALD-Patent by overlaying a similar Figure 1 from EMERALD98. Patent Owner’s modified Figure 1 is shown below. *Id.* at 34.

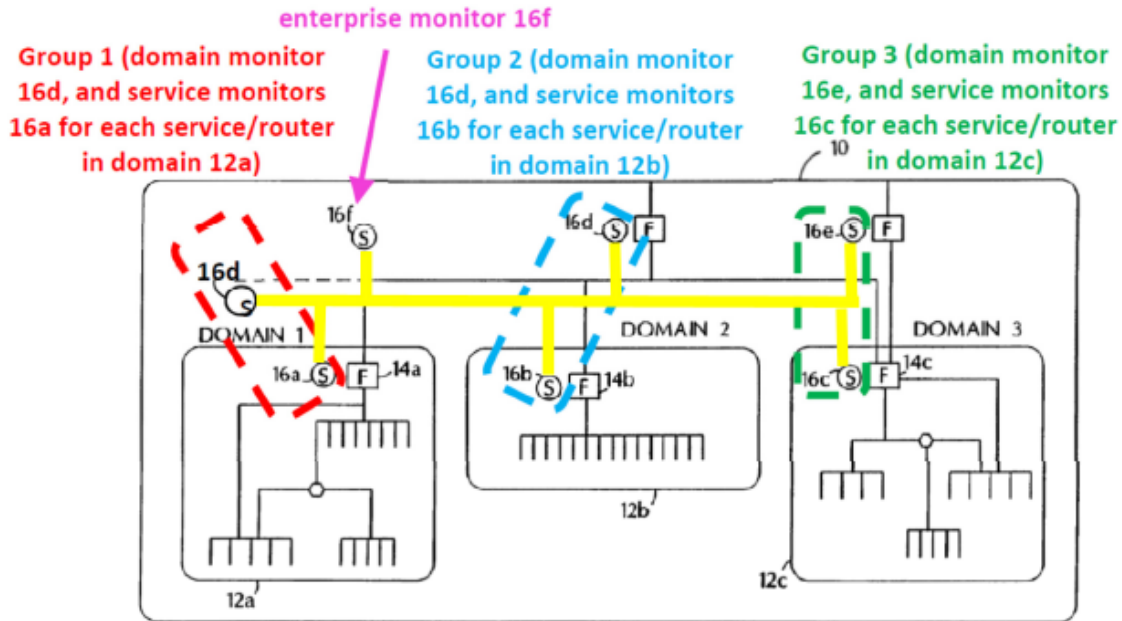


FIG. 1

Patent Owner's modified Figure 1, above, has a yellow line "added to correspond to the communications channel shown visually in Fig. 1 of EMERALD98 and discussed in EMERALD97 and EMERALD-Patent." *Id.* (citing Ex. 2001 ¶¶ 99–101). Patent Owner argues, "the communications channel exists, connecting the service-level monitors 16a-16c, domain-level monitors 16d-16e, and enterprise monitor 16f." *Id.* The communications channel must exist, Patent Owner argues, "because it is through the 'correlation and sharing of analysis results [that] reports of problems found by one monitor may propagate to other monitors throughout the network.'" *Id.* at 34–35 (citing Ex. 1004, 4; Ex. 1005, 4:42–47; Ex. 1006, 8–9; Ex. 2001 ¶¶ 99–101).

Patent Owner argues, "[t]he communications channel shown in yellow above is used by the domain monitors, as each 'domain monitor is responsible for . . . interfacing with other monitors beyond the domain, and

reporting threats against the domain to administrators.” *Id.* at 35 (citing Ex. 1004, 3–4).

Moreover, Patent Owner argues, “each of the three EMERALD references clearly establishes that at least one monitor in each of the three annotated groups will correspond not only with other agents in its respective group but also with at least one agent in at least one other group.” *Id.* at 36 (citing Ex. 2001 ¶ 103). In particular, Patent Owner argues, “each domain-level monitor will necessarily communicate with the enterprise monitor 16f,” which, Patent Owner asserts, “exists in its own ‘group.’” *Id.* “Because enterprise monitor 16f does not exist in any of the annotated groups,” Patent Owner argues, “it must exist in a separate group (either alone or with other monitors).” *Id.* at 37 (citing Ex. 2001 ¶ 104). Indeed, Patent Owner argues, “[d]omain monitors . . . disseminate intrusion reports to enterprise monitors for global correlation.” *Id.* (quoting Ex. 1004 at 11).

We are not persuaded that Petitioner has met its burden. Limitations 1.1 and 26.1 require, in pertinent part, “*each agent corresponding with other agents in its respective group but not with agents in other groups.*” Ex. 1001, 10:53–54, 12:63–65 (emphasis added). Petitioner maps the recited “agents” to EMERALD’s “monitors” and maps the recited “groups” to EMERALD’s “trusted monitor groups.” See Pet. 42 (“EMERALD97 in view of EMERALD-Patent teaches a plurality of inter-communicating computers including software agents (monitors) together forming a plurality of agent groups (trusted monitor groups).”).

Petitioner asserts, “EMERALD97 teaches that monitors only exchanged messages with trusted monitors (identified in their ‘subscription list’) and that the trust relationship (which bounded each subscriber group) could vary domain-to-domain, including being restricted to the monitors in a

single domain.” Pet. 41 (citing Ex. 1004, 2 (“Some domains may share trust relationships with other domains . . . Other domains may operate in complete mistrust of all others.”), 6–7, 9–10, Fig. 2; Ex. 1003 ¶ 162). The implication in Petitioner’s argument, however, is that *a domain* operating in “complete mistrust of all others” is able to restrict *a domain monitor* to “corresponding with other agents (monitors) in its respective group but not with agents in other groups.” Petitioner has not identified or explained with particularity where in the prior art this concept is taught or suggested.

Petitioner annotates Figure 1 from the EMERALD-Patent (shown below), and explains, “a ‘domain’ monitor (16d, 16e) and several ‘service’ monitors (e.g., for each service/router in the domain) (16a, 16b, 16c) were deployed on respective computers in each ‘domain’ (12a, 12b, 12c) of the network.” Pet. 40–41.

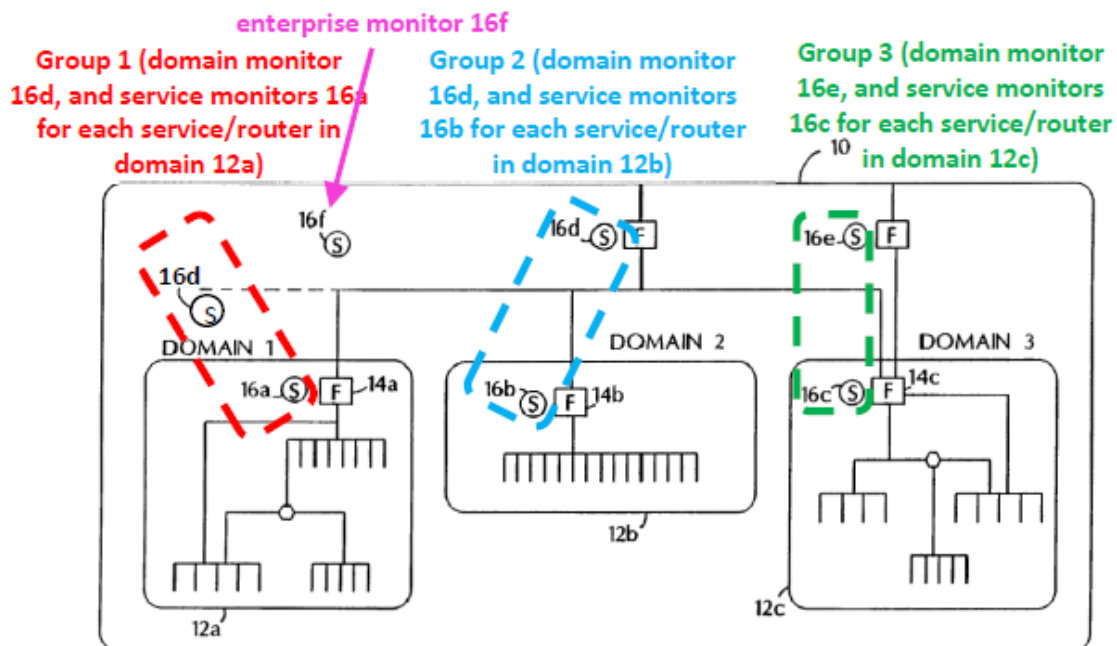


FIG. 1

Petitioner's annotated Figure 1, above, shows three different domains, DOMAIN 1 (12a), DOMAIN 2 (12b), and DOMAIN 3 (12c). *See* Ex. 1004, 3:16–17 (“Referring to FIG.1, an enterprise 10 includes different domains 12a–12c.”). The EMERALD-Patent, similar to EMERALD97, explains that “domains 12a–12c may operate in complete mistrust of all others, providing outgoing connections only or severely restricting incoming connections.” *Id.* at 3:25–27 (emphasis added).

Petitioner's annotation to Figure 1 includes three colored rectangles, red, blue, and green, that extend outside of DOMAINS 1 (12a), 2 (12b), and 3 (12c), respectively. Petitioner provides annotated text (also colored), describing “Group 1 (domain monitor 16d, and service monitors 16a for each service/router in domain 12a)” in red; “Group 2 (domain monitor 16d, and service monitor 16b for each service/router in domain 12b)” in blue; and “Group 3 (domain monitor 16e, and service monitors 16c for each service/router in domain 12c)” in green. In a footnote, Petitioner explains that its “annotations include a domain monitor 16d for domain 12a as described in EMERALD97 and EMERALD Patent.” Pet. 34, n.3 (citing *id.* at § VIII.A.1; Ex. 1005, 3:66–4:3; Ex. 1003 ¶ 144).

The Petition does not expressly state, but appears to imply from annotated Figure 1, that Group 1 (comprising domain monitor 16d, and service monitors 16a for each service/router in domain 12a) shown in red is a mapped “trusted monitor group” and that Group 2 (blue) and Group 3 (green) are different mapped “trusted monitor groups.” For Petitioner's “trusted monitor groups” 1, 2, and 3 to meet limitation 1.1 or 26.1, the monitors in each of these groups may “*correspond[] with other agents (monitors) in its respective group but not with agents (monitors) in other groups.*”

The Petition provides no explanation of how an Emerald *domain*, operating in “complete mistrust” of all other *domains*, would be able to restrict *monitors* in one group from corresponding with *monitors* in another group. Petitioner’s argument appears to imply that if a *domain* operates in “complete mistrust” of other *domains* then any *monitor* operating in that *domain* would be precluded from corresponding with other *monitors* operating outside of that *domain*. But Petitioner’s argument appears to conflate an Emerald *domain* with a *trusted monitor group*, which Petitioner mapped specifically to the recited “group” in claims 1 and 26.

For example, the Petition does not explain, nor does it even address, how a domain operating in “complete mistrust of all others,” yet still “providing outgoing connections only or severely restricting incoming connections,” complies with the requirement of “*corresponding with other agents (monitors) in its respective group but not with agents (monitors) in other groups.*” At best, “providing outgoing connections” or “severely restricting incoming connections” suggests reducing, but not prohibiting or eliminating, connections. The Petition does not address whether this restriction or reduction in connections applies to *monitors* or whether it affects or prohibits *monitors* in one group from corresponding with *monitors* in another group.

The Petition also does not explain the apparent communication channel Figure 1 shows between Domains 1 (12a), 2 (12b) and 3 (12c), which appears to allow monitors 16a and 16d, which Petitioner places in Group 1, to correspond with monitors 16b and 16d in Group 2, along with monitors 16c and 16e in Group 3, as well as with enterprise monitor 16f. Patent Owner argues that when a similar Figure 1 from EMERALD98 is overlaid on Petitioner’s annotated Figure 1, the communication channel

connecting these monitors is shown in yellow. See Prelim. Resp. 34; Ex. 1006, 9; Ex. 2001 ¶ 99–101. The existence of this communication channel appears to be supported by the EMERALD References. For example, EMERALD97 states that the “domain monitor is responsible for . . . interfacing with other monitors *beyond the domain*, and reporting threats against the domain to administrators.” See Ex. 1004 at 3–4 (emphasis added). EMERALD98 also explains, in reference to its Figure 1,

EMERALD surveillance monitors are represented by the S-circles, and are deployed to the various entry points of the enterprise and domains. EMERALD surveillance modules develop analysis results *that are then directed up to an enterprise-layer monitor*, which correlates the distributed results into a meta-event stream. The enterprise monitor is identical to the individual gateway monitors (i.e., they use the same code base), except that it is configured to correlate activity reports produced by the gateway monitors.

Ex. 1006, 9 (emphasis added).

The Petition also does not address statements in the EMERALD-Patent that suggest monitors may correspond with other monitors outside of their domain. For example, the EMERALD-Patent explains, “domain monitors 16a–16c can . . . *interface with other monitors beyond a domain*, and report threats against a domain 12a–12c to administrators.” Ex. 1005, 4:4–7 (emphasis added). The EMERALD-Patent also explains that “[t]hrough correlation and sharing of analysis reports, *reports of problems found by one monitor 16a-16f may propagate to other monitors 16a-16f throughout the network.*” *Id.* at 4:42–45 (emphasis added). Taken together, these statements appear to show that domain monitors are not prohibited from corresponding or communicating with monitors outside of their own

domain, as Petitioner asserts. Nonetheless, the Petition fails to address these statements.

Finally, the Petition does not address the apparent ability of the Emerald service and domain monitors (i.e., 16a/16d in Group 1 (red), 16b/16d in Group 2 (blue), and 16c/16e in Group 3 (green)), to correspond or communicate with enterprise monitor 16f, which is not shown to be part of any of Petitioner's designated "Groups" in annotated Figure 1. See Pet. 41, Fig. 1. Based on Petitioner's annotated Figure 1, any correspondence or communication between any of the domain monitors in Groups 1–3 with enterprise monitor 16f would appear to be correspondence or communication with a monitor outside of Petitioner's designated "Group."

The ability of Petitioner's "Group" monitors to correspond or communicate with enterprise monitor 16f is discussed by the EMERALD References, but is not addressed in the Petition. For example, EMERALD98 states, "[t]he enterprise monitor is identical to the individual gateway [domain] monitors . . . except that it is configured to correlate activity reports produced by the gateway [domain] monitors." Ex. 1006, 9. EMERALD97 states, "Enterprise-layer monitors correlate activity reports produced across the set of monitored domains." Ex. 1004, 4. The EMERALD-Patent states, "[a] domain monitor 16d–16e . . . propagates its own analytical reports to its parent enterprise monitor 16f." Ex. 1005, 9:64–10:1 (*see also id.* at 10:4–6 ("Domain monitors 16d–16e operate as servers to the enterprise monitors 16f.")). Taken together, these statements appear inconsistent with Petitioner's assertion that monitors in Groups 1–3 do not correspond with monitors outside their group, yet the Petition fails to address these statements.

Based on this record, we are not persuaded that Petitioner has demonstrated sufficiently that the combination of EMERALD97, the EMERALD-Patent, and IDIP teaches or suggests “each agent corresponding with other agents in its respective group but not with agents in other groups,” as recited in limitations 1.1 and 26.1. We are, therefore, not persuaded that Petitioner has demonstrated a reasonable likelihood it would prevail in showing that independent claims 1 and 26 would have been obvious over the combined teachings of the Emerald references and IDIP.

4. Dependent Claims 2, 4–6, 14, 15, 17, 18, 21, 23, 27, 29–31, 34, 39, 40, 42, 43, 46, 48

Petitioner contends dependent claims 2, 4–6, 14, 15, 17, 18, 21, 23, 27, 29–31, 34, 39, 40, 42, 43, 46, and 48 would have been obvious over different combinations of the EMERALD References, IDIP, Crosbie1 or Crosbie2. *See* Pet. 50–71. Because these dependent claims incorporate all the limitations of independent claims 1 or 26, Petitioner’s arguments and evidence presented with respect to these dependent claims do not remedy the deficiencies with respect to claims 1 and 26 discussed above.

We are, therefore, not persuaded that Petitioner has demonstrated a reasonable likelihood it would prevail in showing that dependent claims 2, 4–6, 14, 15, 17, 18, 21, 23, 27, 29–31, 34, 39, 40, 42, 43, 46, and 48 would have been obvious over the combination of the Emerald References, IDIP, Crosbie1, or Crosbie2.

5. Independent Claims 16, 41

Petitioner contends independent claims 16 and 41 would have been obvious over the combination of the EMERALD References and Crosbie2. Pet. 71–74. Claims 16 and 41 are similar, where claim 16 recites a computer security system and claim 41 recites a method for providing computer

security. Claim 16, however, recites a number of “means for” limitations, whereas claim 41 does not.

To support its position on obviousness with respect to claim 16, Petitioner relies in large part on the evidence and arguments it uses to support its position for claims 1, 4, 14, and 15. *See* Pet. 72–73. To support its position on obviousness with respect to claim 41, Petitioner relies on the evidence and arguments it uses to support its position for claims 1, 14, 15, and 16. *See* Pet. 73–74. We address limitation 16.8, but our consideration of this limitation also applies to limitation 41.6, which recites identical language. Claims 16 and 41 are set out below.

16. [16.p] A computer security system comprising:
 - [16.1] a plurality of inter-communicating computers including software agents together forming an agent group;
 - [16.2] means for maintaining and tracking a groupwide measure of agent status or behavior;
 - [16.3] means for comparing actual behavior patterns of the measure with known normal behavior patterns; and
 - [16.4] means for determining that a security threat does or may exist when the actual behavior patterns diverge from normal behavior patterns;
 - [16.5] wherein each agent, individually attempts to detect anomalous behavior;
 - [16.6] wherein detected anomalous behavior is converted into an anomaly pattern which the agent attempts to match against a local record of known anomaly patterns;
 - [16.7] wherein the value is indicative of a notional metabolic rate of the agents within the group; and
 - [16.8] wherein, if the match fails and the agent cannot recognize the anomaly pattern its metabolic rate is increased, or its life expectancy or notional energy is decreased.

Ex. 1001, 11:53–12:5.

41. [41.p] A method providing computer security among a plurality of inter-communicating software agents together forming an agent group, said method comprising:
- [41.1] maintaining and tracking a groupwide measure of agent status or behavior;
 - [41.2] comparing actual behavior patterns of the measure with known normal behavior patterns; and
 - [41.3] determining that a security threat does or may exist when the actual behavior patterns diverge from normal behavior patterns;
 - [41.4] wherein each agent, individually, attempts to detect anomalous behavior;
 - [41.5] wherein detected anomalous behavior is converted into an anomaly pattern which the agent attempts to match against a local record of known anomaly patterns; and
 - [41.6] wherein, if the match fails and the agent cannot recognize the anomaly pattern its metabolic rate is increased, or its life expectancy or notional energy is decreased.

Ex. 1001, 13:56–14:9.

- a. [16.8] [41.6] if the match fails and the agent cannot recognize the anomaly pattern its metabolic rate is increased, or its life expectancy or notional energy is decreased*

Petitioner asserts the combination of the EMERALD References and Crosbie2 discloses this limitation. Pet. 72–73 (citing *id.* at § VIII.B.1–2; Ex. 1003 ¶¶ 342–345). Petitioner argues, “Crosbie2’s ‘fitness score’ computation is an obvious variant of the ’358’s ‘life expectancy’ computation, and the ’358 presumes and relies upon the knowledge of a POSA of how to raise or lower the ‘life expectancy’ value as the totality of its disclosure regarding such value is minimal and identified at Claim [5] above.” *Id.* at 73 (citing Ex. 1003 ¶ 343). Petitioner also argues, “the ’358 acknowledges there are no specific technology changes needed to

accommodate one measurement (*e.g.*, life expectancy) over another (*e.g.*, traffic rates).” *Id.* (citing Ex. 1003 ¶ 343).

Thus, Petitioner argues,

it is simply a design choice for a POSA to select a known “fitness score” measure from a finite number of known status/behavior measurements as a design choice to achieve a predictable solution with a reasonable expectation of success and with expressly stated benefits because doing so would involve nothing more than applying a known technique to a known device ready for improvement.

Id. (citing Ex. 1003 ¶ 344).

Patent Owner argues the Petition, and Petitioner’s expert, fail to address the conditional nature of this limitation, i.e., adjusting one of the listed values (metabolic rate, life expectancy, or notional energy) in response to the predicate being satisfied (match failure and inability to recognize an anomaly pattern). Indeed, the Petition does not point to any of the relied upon prior art as teaching or suggestion this limitation. And none of the citations provided by Petitioner address the conditional aspect of this limitation either. Petitioner’s argument, that Crosbie2’s “fitness score” computation is an obvious variant of the recited “life expectancy,” and that it would simply be a matter of design choice to select a known fitness score measure from a finite number of known measurements, fails to address the conditional nature of this limitation as well.

It is Petitioner’s responsibility to describe with particularity each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim. Without some discussion from Petitioner directing us to where in the prior art this limitation is taught or suggested, some explanation as to how a person of ordinary skill in the art would know to make this particular feature

conditional as recited, Petitioner has failed to provide persuasive support for its contentions with respect to claims 16 and 41.

For these reasons, we are not persuaded Petitioner has demonstrated a reasonable likelihood it would prevail in showing that independent claims 16 and 41 would have been obvious over the combined teachings of the Emerald references and Crosbie2.

III. CONCLUSION

For the reasons set forth above, we determine Petitioner has not demonstrated a reasonable likelihood of prevailing in showing that any one of the challenged claims is unpatentable. Because we find no reasonable likelihood Petitioner would prevail, we need not reach the issue of duplicative petitions raised by Patent Owner in the Preliminary Response. *See* Prelim. Resp. 21–25. Accordingly, we do not institute an *inter partes* review.

IV. ORDER

Therefore, it is

ORDERED that the Petition is denied as to all challenged claims of the '358 patent and no trial is instituted.

PETITIONER:

Christopher J. Tyson
Patrick D. McPherson
D. Joseph English
Patrick C. Muldoon
Paul H. Belnap
DUANE MORRIS LLP
cjtyson@duanemorris.com
pdmcperson@duanemorris.com
djenglish@duanemorris.com
pcmuloon@duanemorris.com
phbelnap@duanemorris.com

PATENT OWNER:

Joseph A. Rhoa
Jonathan A. Roberts
Raymond Y. Mah
NIXON & VANDERHYE P.C.
jar@nixonvan.com
jr@nixonvan.com
rym@nixonvan.com