

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

Case ~~No. IPR2023~~IPR-2023-00705
U.S. Patent No. 8,990,948

~~PETITION FOR INTER PARTES REVIEW~~
~~OF U.S. PATENT NO. 8,990,948~~

Palo Alto Networks - Exhibit 1003
Palo Alto Networks v. Taasera - IPR2023-00705
Page 1 of 111

DECLARATION OF KEVIN JEFFAY, PH.D.

TABLE OF CONTENTS

Page

I. Introduction.....	1
II. Background and Qualification	2
III. Legal Standards Used in My Analysis.....	6
A. Prior Art.....	6
B. Person of Ordinary Skill in the Art.....	7
C. Obviousness.....	8
IV. The '948 Patent.....	11
A. Overview of the Challenged '948 Patent.....	11
B. Relevant Prosecution History	12
V. Claim Construction.....	13
VI. Summary of Cited Prior Art References	14
A. Das (Ex. 1006).....	14
B. Overcash (Ex. 1007).....	17
VII. Opinions Regarding Unpatentability.	18
A. Ground 1: Claims 1-5 Are Obvious Over Das and Overcash	18
1. Claim 1.....	18
~~I. Introduction.....~~	~~1~~
~~II. Requirements for <i>Inter Partes</i> Review~~	~~2~~
<del> A. Certification.....</del>	~~2~~
<del> B. Identification of Challenges</del>	~~2~~
~~III. The '948 Patent.....~~	~~3~~
<del> A. Effective Filing Date</del>	~~3~~
<del> B. Level of Ordinary Skill in the Art</del>	~~3~~
<del> C. Overview</del>	~~3~~
<del> D. Relevant Prosecution History</del>	~~5~~
~~IV. Claim Construction.....~~	~~5~~
~~V. Detailed Discussion of the Grounds for Unpatentability~~	~~6~~
<del> A. Overview of the Prior Art.....</del>	~~6~~
<del> 1. Das (Ex. 1006)</del>	~~6~~



Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

2. — Overcash (Ex. 1007)	9
B. — Ground 1: Claims 1-5 Would Have Been Obvious Over Das and Overcash-40	
1. — Claim 1	10
a. “A method of providing real-time operational integrity of an application on a native computing environment, the method comprising:” 4018	
a. “monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application;”	11
b. “generating real time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;”	12
c. “correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and”	15
d. “displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.”	17
2. — Claim 2	22
3. — Claim 3	25
a. “The method of claim 1, wherein the event and behavior correlation engine receives one or more of: . . .”	25
b. “monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application;”	19
c. “generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;”	20
d. “correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time	

iv

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

behavior based events; and”	23
e. “displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.”	25
2. Claim 2	30
3. Claim 3	32
a. “The method of claim 1, wherein the event and behavior correlation engine receives one or more of: . . .”	33
b. “system events and infection profiles from a network activity sensor;”	2633
b. “integrity measurement and verification reports of scans from a system configuration sensor;”	
—27“integrity measurement and verification reports of scans from a system configuration sensor;”	35
e. “system events pertaining to processor, network, memory, and storage resource consumption from a resource utilization sensor; and”	29
d. “system events pertaining to image profiles and local execution context from an application integrity sensor.”	31
4. Claim 4	33
5. Claim 5	36
C. No Secondary Considerations Exist	44
VI. Discretionary Factors	44
VII. Mandatory Notices	45
A. Real Parties in Interest	45
B. Related Proceedings	45
C. Lead and Backup Counsel	46
D. Electronic Service	46
VIII. Fees	46
c. Conclusion	47
d. “system events pertaining to processor, network, memory, and storage resource consumption from a resource utilization sensor; and”	37
e. “system events pertaining to image profiles and local execution context from an application integrity sensor.”	39
4. Claim 4	41

~~Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948~~

~~5.~~ <u>Claim 5</u>	<u>43</u>
~~B.~~ <u>No Secondary Considerations Exist</u>	<u>51</u>
~~IV.~~ <u>VIII. Conclusion</u>	<u>51</u>

CITED EXHIBITS

~~vi~~

Palo Alto Networks - Exhibit 1003
Palo Alto Networks v. Taasera - IPR2023-00705
Page 2 of 57

TABLE OF AUTHORITIES

	Page(s)
Statutes	
35 U.S.C. § 103	2, 5
35 U.S.C. § 314(a)	44
Other Authorities	
37 C.F.R. § 42.15	2
37 C.F.R. § 42.22	2
37 C.F.R. § 42.104	2
37 C.F.R. § 42.105	2
37 C.F.R. § 42.106	2

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

PETITIONER'S EXHIBIT LIST

Ex. No.	Brief Description
1001	U.S. Patent No. 8,990,948
1002	File History of U.S. Patent No. 8,990,948
~~1003~~	~~Declaration of Kevin Jeffay, Ph.D.~~
1004	Curriculum Vitae of Kevin Jeffay, Ph.D.
1005	U.S. Provisional Application No. 61/641,007
1006	U.S. Patent App. Pub. No. 2013/0097660 to Das et al.
1007	U.S. Patent App. Pub. No. 2009/0100518 to Overcash

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

I, Kevin Jeffay, declare as follows:

I. Introduction

1. I have been retained by Palo Alto Networks, Inc. (“Petitioner requests”)
in connection with its request for *inter partes* review (“IPR”) of claims 1-5 (“Challenged
Claims”) of U.S. Patent No. 8,990,948 (“the ‘948 Patent”). The Challenged Claims recite
a method for providing real time
A copy of the ‘948 Patent has been marked Ex. 1001. I
have reviewed and am familiar with the ‘948 Patent, which generally relates to
systems and methods for orchestrating runtime operational integrity of.

2. I have been asked to provide my opinions regarding the patentability
of claims 1-5 of the ‘948 Patent (the “challenged claims”). This declaration
discusses my background and qualifications, the legal standards used in my
analysis, an application. See, e.g., Ex. 1001, claim 1. As shown below, all Challenged Claims would
have been obvious to
overview of the ‘948 Patent from the perspective of a person of
ordinary skill in the art (“POSITA”) as of the patent’s alleged priority date of the ‘948
Patent (a “POSITA”), and my opinions regarding the patentability of the
challenged claims.

The only ground in this Petition relies on Das (Ex. 1006) and Overcash (Ex.
1007), both of which were not before the examiner during prosecution of the ‘948
Patent. As shown in this Petition, the combination of Das and Overcash renders
obvious all Challenged Claims. And as confirmed by Petitioner’s expert declarant,

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~the Challenged Claims merely recite conventional components and features that have been well known and included in commonplace computer network and application security systems prior to the '948 Patent's priority date, as evidenced by the disclosures of Das and Overcash.~~

~~As explained in this Petition, the Challenged Claims would not have been allowed if Das and Overcash had been substantively evaluated by the examiner during prosecution of the '948 Patent. Das discloses a substantially similar computer network and application security system and Overcash discloses a management console used to display real time status indications. Therefore, the Challenged~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

3. ~~Claims should be found~~My work in this proceeding is being charged to
Petitioner at a standard rate of \$800 per hour. My compensation is in no way
contingent on the substance of my opinions or the outcome of this proceeding.
As set forth more fully below, it is my opinion that the challenged claims of the '948
Patent are unpatentable given the strength of the prior art as shown herein.

~~Thus, the Board should institute IPR and cancel the Challenged Claims.~~

I. — Requirements for *Inter Partes* Review

~~This Petition complies with all statutory requirements, as well as 37 C.F.R.~~
~~§§ 42.104, 42.105, and 42.15, and should be accorded a filing date pursuant to 37~~
~~C.F.R. § 42.106. The required fee is being paid electronically through PTAB E2E.~~

A. — Certification

~~Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '948 Patent is~~
~~available for IPR and Petitioner is not barred or estopped from requesting an IPR~~
~~challenging the claims on the grounds identified herein.~~

B. — Identification of Challenges

2.4. Under 37 C.F.R. §§ 42.104(b) and 42.22, Petitioner requests that the Board institute
this IPR on the Challenged Claims of the '948 Patent and cancel those claims as unpatentableas
obvious based on the following ground below:

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

Ground	Claims	Basis for Unpa tenta bility	<u>References</u>
1	1-5	<u>35 U.S.C. § 103</u> <u>(Obviousness)</u>	~~Obvious under 35 U.S.C. § 103~~ ~~over~~ Das (Ex. 1006) in view of Overcash (Ex. 1007)

Inserted Cells

Inserted Cells

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

II. The '948 Patent

A. Effective Filing Date

II. Background and Qualification

5. In formulating my opinions, I have relied upon my knowledge, training, and experience in the relevant art. My qualifications are stated more fully in my curriculum vitae, which has been marked Ex. 1004. I provide a brief summary of my qualifications below.

6. I am currently a tenured professor in the Department of Computer Science at the University of North Carolina at Chapel Hill ("UNC"), where I hold the position of Gillian T. Cell Distinguished Professor of Computer Science. I have been a faculty member at UNC since 1989. From 2014-2022, I served as the Chairman of the Department of Computer Science.

7. I received a Ph.D. in computer science from the University of Washington in 1989. Before that, I received a M.Sc. degree in computer science from the University of Toronto in 1984 and a B.S. degree with Highest Distinction in mathematics from the University of Illinois at Urbana-Champaign in 1982.

8. I have been involved in the research and development of networked computing systems for over 40 years. During this time, I have performed research and taught in the areas of computer networks, computer and network security,

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

distributed systems, real-time systems, operating systems, multimedia networking, network traffic analysis, and network performance evaluation, among others. A major theme of my recent research has been the measurement and analysis of traffic patterns and traffic performance in communications networks. These efforts have been in support of applications such as anomaly and intrusion detection, as well as a broader effort to provide mechanisms and services for quality-of-service provisioning in networks. My work included the design and implementation of network monitoring and analysis devices for passive acquisition and real-time processing of network traffic.

9. Throughout my research and teaching, I have considered problems of the design and implementation of computer networks, including issues of multimedia networking, quality-of-service, network performance measurement and management, and aspects of router design. I have also explored problems in the design and implementation of operating systems. Much of my research has been performed jointly with industry. For example, starting in 2004, in collaboration with Cisco and Cloudshield, my research group experimented with an in-line network packet analysis engine for real-time network intrusion. I have had similar collaborations with IBM, Intel, AT&T, Lucent, and Cabletron/Aprisma, among others.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

10. As part of my research, I regularly build and use clusters of computers interconnected by network switches, bridges, and routers to form and evaluate experimental and production networks. For example, in the late 1990s and early 2000s, my research evolved to consider router-based mechanisms for controlling the performance of network traffic. In much of this research, my students and I built and instrumented network routers and performed large-scale experiments with this equipment. Part of the technology we developed for this research included means for classifying flows within routers and providing differential treatment to flows as a way of providing so-called “better than best effort” forwarding services.

11. The research further included the development of traffic management and scheduling policies and mechanisms to provide guarantees of quality-of-service to packet flows. In addition, part of the experimental infrastructure we developed to support this effort included constructing passive packet-capture devices to classify and monitor the performance of network flows in real time. Based on some of the results of this research, in 2003, my group at UNC won the most prestigious research award for original research in computer networking.

12. I have authored or co-authored over 100 articles in peer-reviewed journals, conference proceedings, texts, and monographs in the aforementioned areas of computer science and others. I have previously served as Editor-in-Chief for the journal *Multimedia Systems* and Associate Editor for the journal *Real-Time*

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

Systems. I have also been an active participant in the Association for Computing Machinery (“ACM”) and the Institute of Electrical and Electronics Engineers (“IEEE”). Specifically, I have been a member of the ACM Special Interest Group on Data Communications (“SIGCOMM”) Steering Committee, the IEEE Technical Committee on Real-Time Systems, and the ACM Special Interest Group on Multimedia. I was also previously involved in the Statistical and Applied Mathematical Sciences Institute (“SAMSI”) program on Network Modeling for the Internet.

13. I have edited and co-edited numerous published proceedings of technical conferences and have edited a book of readings in multimedia computing and networking (with Hong-Jiang Zhang), published by Morgan Kaufman. I am a co-author (with Long Le and F. Donelson Smith) of a monograph related to computer network protocols and a co-author (with Jay Aikat and F. Donelson Smith) of a second monograph related to experimental computer networking.

14. I have served on numerous proposal review panels for the National Science Foundation and other international funding agencies in the aforementioned areas of computer science. I have served as a program chair or member of the technical program committee for over 100 professional, international, and technical conferences, workshops, and symposia.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

15. I am a named inventor on four U.S. patents. These patents are generally related to computer networking and the delivery of services over networks.

III. Legal Standards Used in My Analysis

16. I am not a patent attorney, nor have I independently researched patent law. Counsel for Petitioner has explained certain legal standards to me that I have relied upon in forming my opinions set forth in this Declaration. I set forth some of these legal standards below and may set forth additional legal standards in my analysis in later sections of this Declaration.

A. Prior Art

17. I have been informed that the law provides certain categories of information, known as prior art, that may anticipate patent claims or be used to render patent claims obvious. I understand that the references discussed in this Declaration are prior art at least because they would have been available to members of the public as of May 1, 2012, and they are relevant to the subject matter of the '948 Patent.

18. The references discussed in this Declaration are from the same field of endeavor as the claimed invention (even if they address different problems) and/or are reasonably pertinent to the problem faced by the named inventors (even if they are not in the same field of endeavor as the claimed invention).

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

B. Person of Ordinary Skill in the Art

5-19. I understand that the '948 Patent resulted issued from Application No. 13/559,707, (the "707 Application"), filed July 27, 2012. The I also understand that the '948 Patent alleges priority to Provisional Application No. 61/641,007, filed May 1, 2012. Without conceding entitlement to this A copy of the Provisional Application No. 61/641,007 has been marked Ex. 1005. For the purposes of my analysis in this Declaration, I have assumed that the challenged claims are entitled to a priority date, and for purposes of this Petition only, Petitioner has used no earlier than May 1, 2012.

6-20. I understand that the assessment of the patentability of the challenged claims of the '948 Patent must be undertaken from the perspective of a hypothetical POSITA as of the priority date for the Challenged Claims of the '948 Patent. I understand that the POSITA is a hypothetical person who is presumed to have known all the relevant art as of the priority date. I understand factors that may be considered in determining the level of ordinary skill of a POSITA include (i) the types of problems encountered in the art, (ii) prior art solutions to those problems, (iii) rapidity with which innovations are made, (iv) sophistication of the technology, and (v) educational level of active workers in the field. I understand that in a given case, every factor may not be present, and one or more factors may predominate.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

B. — Level of Ordinary Skill in the Art

21. As of May 1, 2012, I understand that the hypothetical POSITA to which the claimed subject matter pertains would have had the capability of understanding the scientific and technological principles applicable to the pertinent art. I further

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

understand that a POSITA is also a person of ordinary skill in the art (“POSITA”) in creativity, not an automaton. Further, I understand that the hypothetical POSITA may comprise a team.

7.22. Based on these factors, my knowledge and expertise, and the prior art to the ’948 Patent’s technical field would have been a person with Patent, it is my opinion that a POSITA at the time of the relevant priority date would have had at least a bachelor’s degree in computer science, computer engineering, or electrical engineering or in a related field and at least three years of experience in computer network security and computer network application security. See Ex. 1003, ¶¶ 19-23.
Someone with less or different technical education but more relevant practical experience, or more relevant education but less practical experience, could also be considered a POSITA. ~~Id. This level of skill in the art is reflected by the references cited in this Petition, the state of the art, and the experience of Kevin Jeffay, Ph.D., as described in his declaration.~~
~~Id.~~

23. I meet this definition of a POSITA today and met this definition by May 1, 2012.

C. Obviousness

24. I have been informed that, even if every element of a claim is not found explicitly or implicitly in a single prior art reference, the claim may still be unpatentable if the differences between the claim and the prior art are such that the claim as a whole would have been obvious to a POSITA at the time the invention

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

was made. For purposes of obviousness, I understand that a POSITA may rely on a single prior art reference or on multiple references in combination.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

25. I have been informed that the following four factors are considered when determining whether a patent claim would have been obvious to a POSITA: (a) the level of ordinary skill in the art; (b) the scope and content of the prior art; (c) the differences between the prior art and the claim; and (d) any “secondary considerations” tending to prove nonobviousness. These secondary considerations, which I understand are also called “objective indicia” or “objective evidence,” may include factors such as: (i) the invention’s satisfaction of a long-felt unmet need in the art; (ii) unexpected results of the invention; (iii) skepticism of the invention by experts; (iv) commercial success of an embodiment of the invention; and (vii) praise by others for the invention. I have also been informed that there must be an adequate nexus or connection between the evidence that is the basis for an asserted secondary consideration and the scope of the invention claimed in the patent.

26. I understand that when every limitation of a claim is disclosed in the cited prior art references, the question of obviousness turns on whether a hypothetical person of ordinary skill in the art would have been motivated to combine those teachings to derive the claimed subject matter with a reasonable expectation of success. Further, I understand that obviousness does not require absolute predictability. Only a reasonable expectation that the beneficial result will be achieved is necessary to show obviousness.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

27. I have been informed that a claimed invention can be rendered obvious by the combination of teachings in the prior art even if there is no explicit teaching to combine them. Instead, any problem known in the field at the time of the alleged invention can provide a sufficient rationale to combine the elements of the prior art in the manner claimed in the patent.

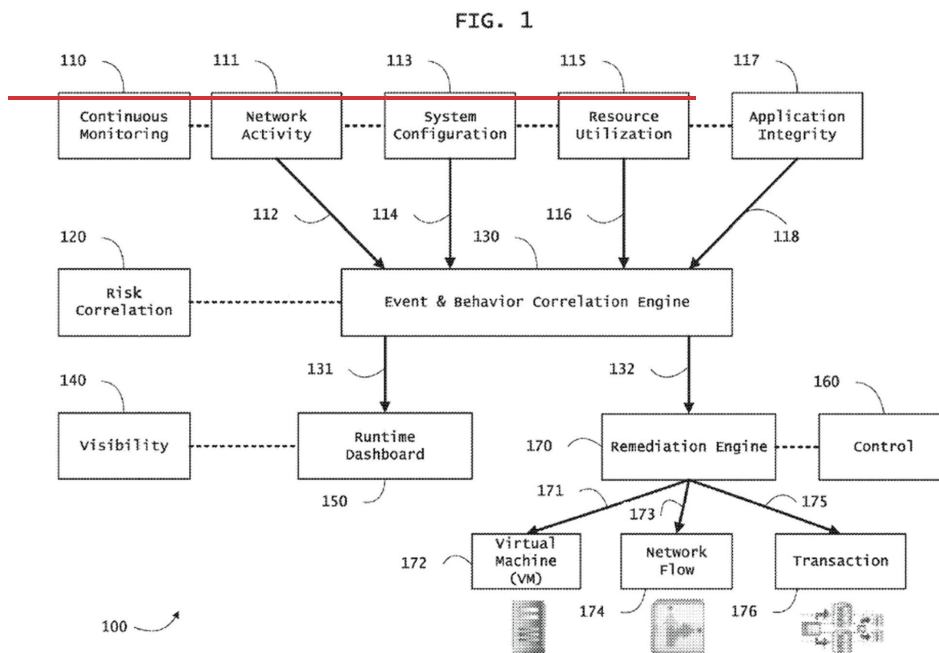
28. I have been informed that examples of sufficient rationales for establishing obviousness include the following:

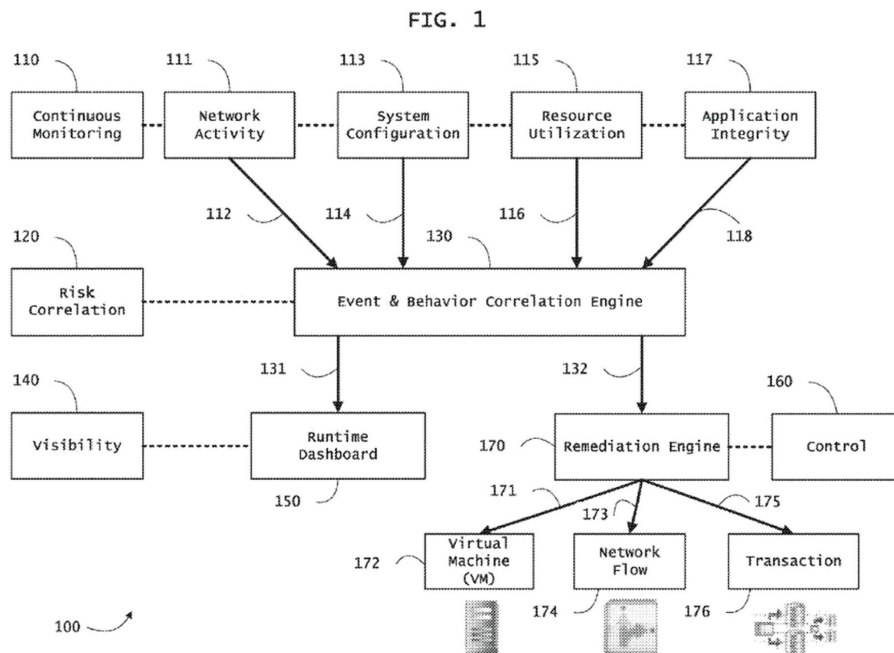
- combining prior art elements according to known methods to yield predictable results;
- substituting known elements for other known elements to obtain predictable results;
- using a known technique to improve similar devices, methods, or products in the same way;
- choosing from a finite number of identified, predictable solutions that would be obvious to try; and
- providing some teaching, suggestion, or motivation to modify the prior art reference or to combine teachings in prior art references to arrive at the claimed invention.

IV. The '948 Patent

A. Overview of the Challenged '948 Patent

8-29. The '948 Patent describes systems and methods for orchestrating runtime operational integrity. Ex. 1001, Title. The '948 Patent discloses that a computer network security system can be “configured to continuously monitor and dynamically analyze events and network activity to ascertain the integrity of a monitored system (i.e., a target system).” *Id.*, 8:6-8. Figure 1 shows an example computer network security system:





Id., Fig. 1. The security system can also be configured “for continuously monitoring one or more systems and/or to correlate events and behavior of systems

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

on an instrumented target platform at runtime using or based on a plurality of assertions (or statements).” *Id.*, 4:28-32.

9-30. The security system can further include an “administration console interface comprising various dashboards for displaying data related to operational integrity, resource utilization, application integrity, and network activity, in accordance with embodiments of the invention.” *Id.*, 26:42-46.

B. Relevant Prosecution History

31. I have reviewed and considered the prosecution history of the '948 Patent, which is marked Ex. 1002. Below, I provide a brief summary of certain key events during the prosecution of the '948 Patent.

10-32. During prosecution, the first substantive action issued by the examiner was a restriction requirement. Ex. 1002, 116-122. In response, Applicant elected (without traverse) five claims. *Id.*, 113.

11-33. The Examiner subsequently rejected the elected claims under 35 U.S.C. § 103, relying on U.S. Pat. App. Pub. No. 2008/0175266 (Alperovitch), U.S. Pat. App. Pub. No. 2011/0145711 (Njemanze), and U.S. Patent No. 5,604,862 (Midgely) for the obviousness rejections. *Id.*, 66-84.

12-34. In response, Applicant amended all the pending claims. *Id.*, 38-56. After receiving authorization in a telephone interview with Applicant to cancel the withdrawn claims, the examiner issued a Notice of Allowance. *Id.*, 8-18.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~13-35.~~ Das and Overcash, the prior art cited in this Petition, were not cited, nor are they cumulative of anything cited, during prosecution.

36. As discussed below, the challenged claims that were allowed to issue in the '948 Patent are taught by the Das and Overcash prior art references. Das and Overcash, cited in this Declaration, were not considered during prosecution and are not cumulative of anything cited during prosecution. As discussed below, it is my opinion that Das and Overcash teach all limitations of the '948 patent's claims.

H.V. Claim Construction

~~The Board construes claims under the same standard used in civil actions in federal district court. Counsel for Petitioner submits~~has informed me ~~that for the purposes of this Petition, the~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~Board does not need to explicitly construe any language in a patent claim term, should be construed in accordance with the ordinary and there are no known customary meaning of such claim construction disputes that affect the outcome as understood by a POSITA in light of this Petition.¹~~

~~14.37. Detailed Discussion the specification and prosecution history of the Grounds for Unpatentability patent at the time of the alleged invention.~~

~~38. Overview of the Counsel for Petitioner has also informed me that only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.~~

~~39. For purposes of my opinions of unpatentability in this Declaration, no claim construction is necessary because, in my opinion, the challenged claims would have been rendered obvious over the cited reference under any reasonable construction and based on their plain and ordinary meaning to a POSITA as of the '948 Patent's alleged priority date.~~

III.VI. Summary of Cited Prior Art References

40. The prior art references Das and Overcash that are relevant to my analysis are briefly summarized below. I discuss additional elements of Das and Overcash in my analysis of how the combination of Das and Overcash invalidates the challenged claims.

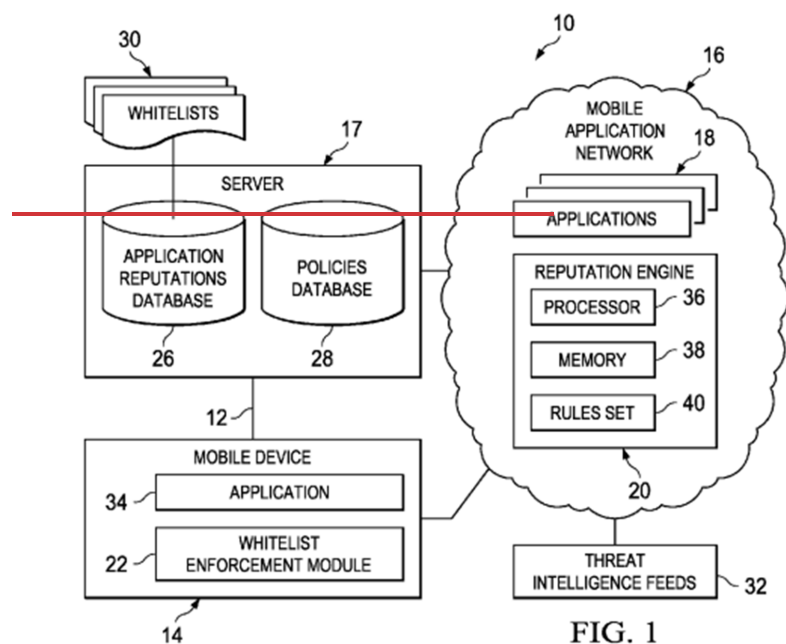
A. Das (Ex. 1006)

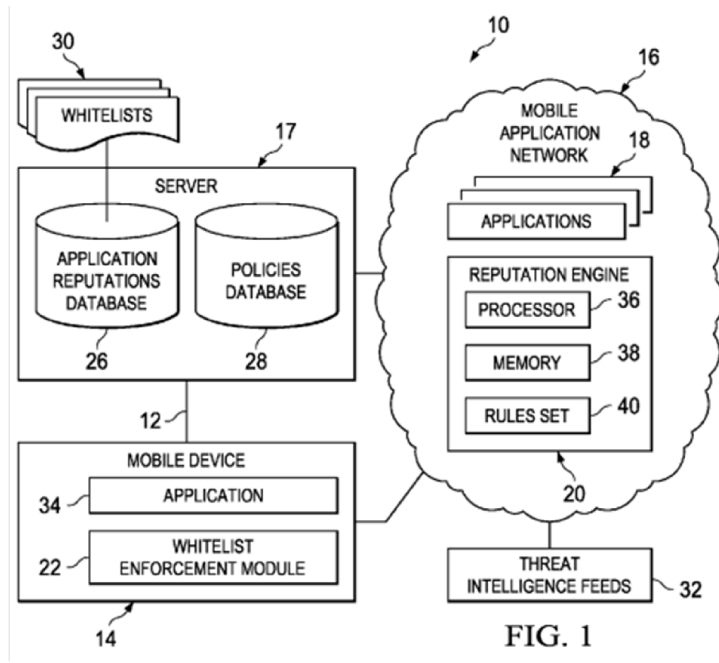
41. U.S. I understand that Das is prior art to the '948 Patent Application-Publication No. 2013/0097660 to Das et al. ("Das") at least because it was filed on October 17, 2011 and published on April 18, 2013. Ex. 1006.

42. Das is titled "System and Method for Whitelisting Applications in a Mobile Network Environment." Ex. is prior art under at least § 102(e), 1006, Title. Das's disclosure relates disclosures relate to computer network/application security systems. Ex. 1006, [0001]-[0002], Ex. 1003, ¶ 42. Figure 1 of Das (shown below) illustrates relevant aspects of Das's computer network/application security "system 10." Ex. 1006, [0016], Ex. 1003, ¶ 42.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

⁺~~This claim construction analysis is not a concession as to the scope of any claim term in litigation or a waiver of any argument in any proceeding that claim terms are indefinite, invalid, or unpatentable.~~





Ex. 1006, FIG. 1.

System 10 includes “mobile device 14” where applications, such as “applications 34,” execute. Ex. 1006, [0024]; ~~Ex. 1003, ¶ 43~~. Das discloses that applications “include native applications pre-installed on the mobile device.” Ex. 1006, [0018]; ~~Ex. 1003, ¶ 43~~. System 10 also includes “one or more sources internal or external to network 12” that provide “threat information,” including “network threat information,” via “threat intelligence feeds 32.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 43~~. System 10 also includes a “server 17 [that] may be an enterprise server managing security and policies of a particular enterprise.” Ex. 1006, [0058]; ~~Ex. 1003, ¶ 43~~.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

1003, ¶ 43.

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~17.44.~~ System 10 further includes a “reputation engine 20” and a “processor 36” that is used by “reputation engine 20.” Ex. 1006, [0024], [0055~~;~~ Ex. 1003, ¶ 44.]. Das discloses that system 10 “can detect security events relating to particular applications and application activities and report such events to reputation engine 20 or other modules for use in determining the trustworthiness of such applications and application activities.” Ex. 1006, [0055~~;~~ Ex. 1003, ¶ 44.]. For example, Das teaches that as part of the operations that reputation engine 20 performs to “determin[e] the trustworthiness of [] applications and application activities,” “knowledge gained from monitoring application activity on any one mobile device may be aggregated and analyzed against information about similar activity obtained from other mobile devices, and correlated with data from other vectors (e.g., file, web, message, network connections, and manual efforts) for substantially comprehensive information about the application.” Ex. 1006, [0055~~;~~ Ex. 1003, ¶ 44.]. Das further teaches that “reputation engine 20 may incorporate and adjust reputation scores with each additional data point.” Ex. 1006, [0055~~;~~ Ex. 1003, ¶ 44.]. Das also discloses that “reputation engine 20” can “analyz[e] each application . . . against a rules set 40.” Ex. 1006, [0024~~;~~ Ex. 1003, ¶ 44.]. “In some embodiments, evaluation of applications to determine their respective trust status is performed in real-time for applications associated with an execution attempt in mobile device.” Ex. 1006, [0048].

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~18-45.~~ System 10 also includes a “whitelist enforcement module 22” that includes “event detection capabilities, communication interfaces, policy manager, etc.” for “collect[ing] identification information (e.g., application manifest) of applications to be downloaded (or already downloaded) to mobile device 14, and monitor[ing] behavior and activities of any one or more applications already installed on mobile device 14.” Ex. 1006, [0052]-[0053]; ~~Ex. 1003, ¶ 45.~~

~~19-46.~~ Das further discloses “risk categories of the applications” that include at least “low risk,” “medium risk,” and “high risk.” Ex. 1006, [0077]-[0078] and FIG. 7; ~~Ex. 1003, ¶ 46.~~

B. Overcash (Ex. 1007)

~~47. U.S. Patent Application Publication No. 2009/0100518 to~~ I understand that Overcash ~~(“Overcash”)~~ is prior art to the ’948 Patent at least because it was published on April 16, 2009. ~~Ex. 1007.~~

Overcash is titled “System and Method for Detecting Security Defects in Applications.” Ex. is prior art under at least §

~~20-48. 102(b). 1007, Title.~~ Overcash’s disclosure relates to computer network/application security systems. Ex. 1007, [0008], [0020]; ~~Ex. 1003, ¶ 48.~~ Overcash’s system includes “application defect detection” that “occur[s] in real-time” through “continuous monitoring [of application operations] for defects as they are exposed through usage.” Ex. 1007, [0020]; ~~Ex. 1003, ¶ 48.~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~21.49.~~ Overcash discloses a “management console” that is used to “generate displays of information to a network administrator,” e.g., “to enable intuitive- application security management.” Ex. 1007, [0068]; Ex. 1003, ¶ 49. Overcash discloses that the

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

application security management.” Ex. 1007, [0068]. Overcash discloses that the
displays of the management console are used to display real-time application
defect detection information, e.g., via an event viewer display 602 that includes a
real-time event analysis module. Ex. 1007, [0020], [0062], [0068]-[0079], [0229]-
[0230], FIGS. 4-6 and 8-9; Ex. 1003, ¶ 49. For example, Overcash explains
that “[t]he event viewer display 602 includes an event detection window 604 with
a list of events detected by the Web application security system.” Ex. 1007,
[0077]; Ex. 1003, ¶ 49. Figures 4-6 and 8-9 of Overcash are examples of the
displays that can be generated by Overcash’s system. Overcash, FIGS. 4-6 and 8-
9; Ex. 1003, ¶ 49.

VII. Opinions Regarding Unpatentability

50. In my opinion, the challenged claims are unpatentable based upon one
ground. Claims 1-5 are obvious over Das and Overcash.

A. Ground 1: Claims 1-5 ~~Would Have Been~~ Are Obvious Over Das and Overcash

1. Claim 1

22-51. The As set forth below, it is my opinion that the combination of Das
and Overcash discloses ~~and/or~~ renders obvious all ~~elements~~ limitations of claim 1 of
the ’948 Patent.

- a. **“A method of providing real-time operational integrity of an application on a native computing environment, the method comprising:”**

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~23-52~~. To the extent the Board considers the preamble a limitation, Das discloses this limitation. ~~Ex. 1003, ¶ 52~~. Das discloses that “evaluation of applications to determine their respective trust status is performed in real-time for applications

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

associated with an execution attempt in mobile device 14” (*“providing real-time operational integrity of an application”*). Ex. 1006, [0048]. A POSITA would have understood that the real-time trust status is for the *“operational integrity of an application”* based on Das’s disclosure that an application execution attempt refers to an application operation, “includ[ing] any software process or instruction with an execute request and any attempt to access resources (e.g., processor, memory, camera, microphone, etc.) in the mobile device.” Ex. 1006, [0048]; ~~Ex. 1003, ¶ 52.~~ Das also discloses that the applications “include native applications pre-installed on the mobile device” (*“application on a native computing environment”*). Ex. 1006, [0018]; ~~Ex. 1003, ¶ 52.~~ Das further discloses “trust evaluation techniques” for determining the “real-time” “trust status” of those native applications associated with execution attempts (*“[a] method of providing real-time operational integrity of an application on a native computing environment”*). Ex. 1006, [0048]; ~~Ex. 1003, ¶ 52.~~

~~24-53.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 53.~~

- b. **“monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application;”**

~~25-54. This claim element is taught by Das.~~ Das discloses *“monitoring[] by a plurality of sensory inputs”* in the form of a “whitelist enforcement module 22”

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

that includes “event detection capabilities, communication interfaces, policy manager, etc.” for “collect[ing]

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

identification information (e.g., application manifest) of applications to be downloaded (or already downloaded) to mobile device 14, and monitor[ing] behavior and activities of any one or more applications already installed on mobile device 14.” Ex. 1006, [0052]-[0053]; ~~Ex. 1003, ¶ 54.~~ Das discloses that the monitoring of behavior and activities of applications can include the monitoring of “one or more of” an application’s “network activity” (“*network dialogs of the application*”), an application’s “network connectivity” or activation of a “camera” or a “phone” (“*system operations initiated by the application*”), the “ports and protocols actually used by the application” (“*runtime configuration of the application*”), an application’s “requests for resources” and/or usage of “computing resources” (“*resource utilization by the application*”), and the “real-time” “trust status” of applications (“*integrity of the application*”). Ex. 1006, [0022], [0033], [0048], ~~[0051]-[0052], [0055], [0073]; Ex. 1003, ¶ 54.~~ [0051]-[0052], [0055], [0073].

~~26-55.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 55.~~

- c. **“generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;”**

~~27-56. This claim element is taught by Das.~~ Das discloses detecting and reporting real-time application activity security events (“*generating real-time behavior*

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

based events”) for performing a ~~real-time “evaluation of applications [associated with an execution attempt in mobile device 14] to determine their respective trust status”~~
real-time “evaluation of applications [associated with an execution attempt in

mobile device 14] to determine their respective trust status” (“for determining the real-time operational integrity of the application”). Ex. 1006, [0048], [0055~~;~~ Ex. 1003, ¶ 56.]. Das also discloses that the applications “include native applications pre-installed on the mobile device” and are “associated with an execution attempt in mobile device 14,” “includ[ing] any software process or instruction with an execute request and any attempt to access resources (e.g., processor, memory, camera, microphone, etc.) in the mobile device.” (“application executing on the native computing environment”). Ex. 1006, [0018], [0048~~;~~ Ex. 1003, ¶ 56.].

28-57. Figure 1 of Das (shown below) illustrates the relevant aspects of system 10 (“native computing environment”). ~~Ex. 1003, ¶ 57.~~

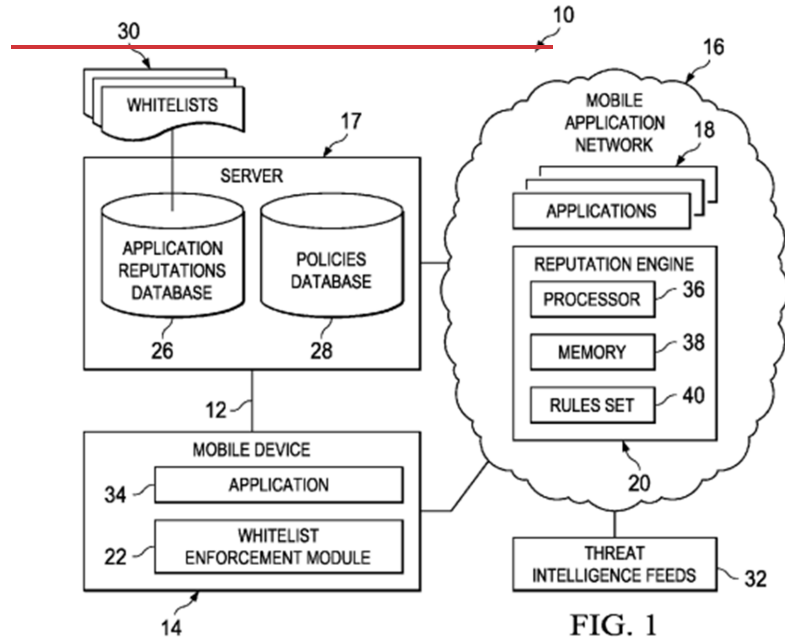
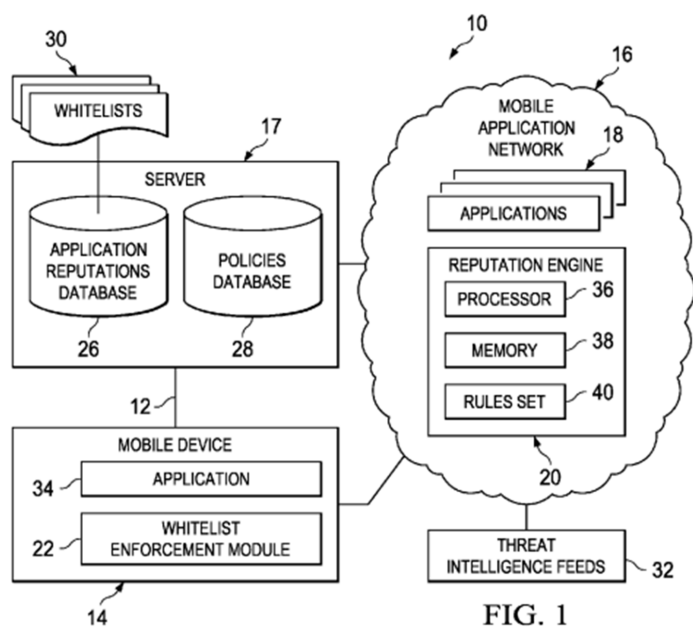


FIG. 1

32



Petition for Inter Partes Review of U.S. Patent No. 8,990,948

Ex. 1006, FIG. 1. As shown in figure 1, system 10 (“*native computing environment*”) includes the mobile device 14 where applications, such as applications 34, execute. ~~Ex. 1003, ¶ 57.~~ System 10 also includes “*a network analyzer*” in the form of “one or more sources internal or external to network 12” that provide “threat information,” including “network threat information,” via “threat intelligence feeds 32.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 57.~~ System 10 further includes “*an integrity processor*” in the form of a “processor 36” that is used by “reputation engine 20” to “determin[e] the trustworthiness of [] applications and application activities.” Ex. 1006, [0024], [0055]; ~~Ex. 1003, ¶ 57.~~ System 10 also includes “*a trust supervisor*” in the form of a “server 17 [that] may be an enterprise server managing security and policies of a particular enterprise.” Ex. 1006, [0058]; ~~Ex. 1003, ¶ 57.~~ System 10 further includes “*an event correlation matrix*” and “*a risk correlation matrix*” in the form of a “reputation engine 20” that correlates events associated with applications and risks associated with applications to “determin[e] the trustworthiness of [] applications and application activities.” Ex. 1006, [0055]; ~~Ex. 1003, ¶ 57.~~ For example, Das teaches that as part of the operations that reputation engine 20 performs to “determin[e] the trustworthiness of [] applications and application activities,” “knowledge gained from monitoring application activity on any one mobile device may be aggregated and analyzed

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

against information about similar activity obtained from other mobile devices, and correlated with data from other vectors (e.g., file, web, message, network

~~web, message, network~~ connections, and manual efforts) for substantially comprehensive information about the application.” Ex. 1006, [0055]; ~~Ex. 1003, ¶ 57.].~~ Das further teaches that “reputation engine 20 may incorporate and adjust reputation scores with each additional data point.” Ex. 1006, [0055]; ~~Ex. 1003, ¶ 57.].~~

~~29-58.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 58.~~

- d. **“correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and”**

~~30-59.~~ This claim element is taught by Das. Das discloses “risk categories of the applications” (“*threat classifications*”) that include at least “low risk,” “medium risk,” and “high risk.” Ex. 1006, [0077]-[0078] and FIG. ~~7; Ex. 1003, ¶ 59].~~

~~31-60.~~ Das also discloses that “reputation engine 20” (“*the event and risk correlation matrix*”) can “analyz[e] each application . . . against a rules set 40,” e.g., to determine “the trustworthiness of such applications and application activities,” thereby establishing a relationship between the “risk categories of the applications” (“*correlating, by the event and risk correlation matrix, threat classifications*”). Ex. 1006, [0024], [0055], [0077]-[0078]; ~~Ex. 1003, ¶ 60.].~~ For example, “reputation engine 20 may analyze applications[and] characterize applications and application functions and other actions as trusted or untrusted” to correlate and categorize the “risk categories of the applications” such that a “high

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

risk” ~~application is deemed to~~

application is deemed to be an application that includes “suspicious behavior,” and

a “low risk” application is deemed to be an application that does not include “suspicious behavior.” Ex. 1006, [0020], [0043]-[0044], [0077]-[0078]; ~~Ex. 1003, ¶ 60.~~

~~32-61.~~ Das further discloses that the correlation, by the reputation engine 20, of the risk categories of the applications (“*correlating, by the event and risk correlation matrix, threat classifications*”) is based on the temporal “order” in which the detected and reported real-time application activity security events are performed (“*based on the temporal sequence of the generated real-time behavior based events*”). Ex. 1006, [0043]-[0044]; ~~Ex. 1003, ¶ 61.~~ For example, Das discloses that if an application “records audio,” “sends SMS text message,” “reads contact list,” and “contacts an Internet server,” “*in that order*, the application may be exhibiting suspicious behavior.” Ex. 1006, [0043]-[0044] (emphasis added); ~~Ex. 1003, ¶ 61.~~ Das also discloses that if, on the other hand, the application “sends SMS text message,” “reads contact list,” and “contacts an Internet server,” in that order, but does not “record[] audio,” “the application may not be exhibiting suspicious behavior.” Ex. 1006, [0043]-[0044]; ~~Ex. 1003, ¶ 61.~~ Here, the detected and reported real-time application activity security events (“*generated real-time behavior based events*”) are the foregoing application actions that implicate application security and are reported to the reputation engine 20 to correlate the risk categories of the applications, such as the “records audio,” “sends SMS text

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

message,” “reads contact list,” and “contacts an Internet server” application activities. Ex. 1006, [0043]-[0044].

~~list,” and “contacts an Internet server” application activities. Ex. 1006, [0043]-[0044]; Ex. 1003, ¶ 61.~~

~~33-62.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 62.~~

- e. **“displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.”**

~~34-63.~~ Das does not explicitly disclose “*displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application,*” but it would have been obvious, in light of Overcash, to include those features in the system of Das. ~~Ex. 1003, ¶ 63.~~

~~35-64.~~ In particular, the foregoing features of the “displaying . . .” element of claim 1 were well-known in the art by the ’948 Patent’s priority date. ~~Id., ¶ 64.~~ For example, Overcash discloses a “management console” that “generate[s] displays of information to a network administrator” (“*administrative console of the computing environment*”). Ex. 1007, [0068]; ~~Ex. 1003, ¶ 64.~~

~~36-65.~~ Regarding “*runtime dashboards of an administrative console of the computing environment,*” the ’948 Patent uses the terms “dashboard” and “window” interchangeably to refer to the same display of information. *See, e.g.,* Ex. 1001, 27:59-66 (referring to display “1450” as either “dashboard 1450” or ~~“window~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

“window 1450”), 28:35-41 (same for display “1550”), 28:58-62 (same for display “1650”), 29:12-16 (same for display “1750”), 29:33-37 (same for display “1850”); Ex. 1003, ¶ 65.”). Additionally, a POSITA would have understood that the term “*runtime*” is interchangeable with the term “real-time.” Ex. 1003, ¶ 65. Indeed, the ’948 Patent suggests that the

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

term “runtime” is interchangeable or synonymous with the term “real-time.” See, e.g., Ex. 1001, Abstract, 8:17-22, 9:43-48, 28:16-20, 35:41-43; ~~Ex. 1003, ¶ 65.~~

Overcash discloses that the “management console” (“*administrative console of the computing environment*”) includes a plurality of real-time “runtime” displays/windows (“*plurality of runtime dashboards*”) to display various real-time “runtime” “information” obtained from the “continuous monitoring [of applications] for defects as they are exposed through usage.” Ex. 1007, [0020], [0062], [0068]–~~37-66. f.]~~ [0079], [0229]–[0230], FIGS. 4-6 and 8-9 (each figure showing a plurality of windows); ~~Ex. 1003, ¶ 66.~~ Going further, Overcash discloses that the plurality of runtime displays/windows of the “management console” (“*plurality of runtime dashboards of an administrative console of the computing environment*”) are used to “display” (“*displaying*”) “real-time” “application defect detection” “information” (“*real-time status indications for operational integrity of the application*”) via an “event viewer display 602” that includes “a real-time event analysis module.” Ex. 1007, [0020], [0062], [0068]–[0079], [0229]–[0230], FIGS. ~~4-6 and 8-9; Ex. 1003, ¶ 66-6 and 8-9.~~ For example, Overcash explains that “[t]he event viewer display 602 includes an event detection window 604 with a list of events detected by the Web application security system.” Ex. 1007, [0077]; ~~Ex. 1003, ¶ 66.~~ At least based on

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

the foregoing disclosure from Overcash, a POSITA would have ~~readily~~ understood that Overcash discloses and/or renders obvious “*displaying, in a plurality of runtime dashboards*”

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

of an administrative console of the computing environment, real-time status indications for operational integrity of the application.” ~~Ex. 1003, ¶ 66.~~

67. As to the combination, Das and Overcash are analogous art to the '948 Patent because each is from the field of computer network security and computer network application security. Ex. 1001, 1:15-19; Ex. 1006, [0001]-[0002]; Ex. 1007, [0008], [0020].

~~38-68.~~ As of the priority date of the '948 Patent, it would have been obvious to a POSITA to include Overcash's "management console" and associated displays/windows in the computer network/application security system of Das because to do so would have been merely an arrangement of old elements (Das's computer network/application security system and Overcash's management console and associated displays/windows), each performing the same function it had been known to perform (Overcash's management console and associated displays/windows "generat[ing] displays of information to a network administrator" and Das's computer network/application security system performing "evaluation[s] of applications to determine their respective trust status"), in a way that yields no more than a POSITA would expect from such an arrangement (Overcash's management console and associated displays/windows being used to display computer network/application security information resulting from Das's computer network/application security system's "evaluation of

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~As to the combination, Das and Overcash are analogous art to the '948 Patent because each is from the field of computer network security and computer network application security. Ex. 1001, 1:15-19; Ex. 1006, [0001]-[0002]; Ex. 1007, [0008], [0020]; Ex. 1003, ¶ 67.~~

~~As of the priority date of the '948 Patent, it would have been obvious to a POSITA to include Overcash's "management console" and associated displays/windows in the computer network/application security system of Das because to do so would have been merely an arrangement of old elements (Das's computer network/application security system and Overcash's management console and associated displays/windows), each performing the same function it had been known to perform (Overcash's management console and associated displays/windows "generat[ing] displays of information to a network administrator" and Das's computer network/application security system performing "evaluation[s] of applications to determine their respective trust status"), in a way that yields no~~

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~more than a POSITA would expect from such an arrangement (Overcash's management console and associated displays/windows being used to display computer network/application security information resulting from Das's computer network/application security system's "evaluation of applications to determine their respective trust status"). Ex. 1006, [0048]; Ex. 1007, [0068]; Ex. 1003, ¶ 68.]~~ For example, as combined, Das's computer network/application security system would use Overcash's management console and associated displays/windows to display, to a network administrator, computer network/application security information resulting from Das's computer network/application security system's "evaluation of applications to determine their respective trust status." Ex. 1006, [0048]; Ex. 1007, [0068]; ~~Ex. 1003, ¶ 68.]~~ As shown here, such a combination and/or modification would have been obvious. ~~Ex. 1003, ¶ 68.~~

~~39-69.~~ A POSITA would also have been motivated to make such a combination and would have had a reasonable expectation that the combination would be successful. ~~Ex. 1003, ¶ 69.~~ For example, Das discloses that "innovative tools are needed to assist IT administrators in the effective control and management of applications on mobile devices within computer and communication network environments," and that "continuous efforts (both electronic and manual) are usually necessary to protect against unknown and/or malicious software." Ex.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

1006, [0002], [0027]. The “innovative tools” that a POSITA would have been motivated to include in Das’s computer network/application security system would have included Overcash’s “management console” that includes a plurality of real-time displays/windows because including Overcash’s “management console” that includes a plurality of real-time displays/windows in Das’s computer network/application security system

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

would allow Das's computer network/application security system to display various real-time "information" obtained from the "continuous monitoring [of applications]," thereby allowing for "continuous efforts" in the "management of applications," which are goals of both Das and Overcash. Ex. 1006, [0002], [0027], [0029]; Ex. 1007, [0020], [0062], [0068]-[0079], [0229]-[0230], FIGS. 4-6 and 8-9;

~~Ex. 1003, ¶ 69.9.~~ A POSITA would have had a reasonable expectation that Das and Overcash would successfully operate together as described because both Das and Overcash disclose the use of a "management console," with Das disclosing that the "management console . . . may aggregate and store application reputations," and Overcash disclosing that the "management console" "generate[s] displays of information," such as displays of various real-time "information" obtained from the "continuous monitoring [of applications] for defects as they are exposed through usage." Ex. 1006, [0029]; Ex. 1007, [0020], [0062], [0068]-[0079], ~~[0229]-[0230],~~ ~~[0229]-[0230]~~, FIGS. 4-6 and 8-9; ~~Ex. 1003, ¶ 69.~~ In other words, both Das and Overcash disclose the use of a "management console," with each elaborating on different features for which the management console can be used. ~~Ex. 1003, ¶ 69.~~ As shown here, such a combination and/or modification would have been obvious. ~~Ex. 1003, ¶ 69.~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~40-70.~~ In light of the foregoing, claim 1 is ~~unpatentable as obvious over~~in
light of Das and Overcash. ~~Ex. 1003, ¶ 70.~~

2. Claim 2

~~41-71.~~ Claim 2 depends on claim 1 and recites “*wherein the real-time operations of applications are monitored continuously.*”

~~42-72.~~ Das does not explicitly disclose that “*the real-time operations of applications are monitored continuously,*” but it would have been obvious, in light of Overcash, to include those features in the system of Das. ~~Ex. 1003, ¶ 72.~~

~~43-73.~~ In particular, the features of claim 2 were well-known in the art by the ‘948 Patent’s priority date. ~~Id., ¶ 73.~~ For example, Overcash discloses that “application defect detection” “occur[s] in real-time” through “continuous monitoring [of application operations] for defects as they are exposed through usage” (“*the real-time operations of applications are monitored continuously*”). Ex. 1007, [0020]; ~~Ex. 1003, ¶ 73.~~

74. As to the combination, Das and Overcash are analogous art to the ‘948 Patent because each is from the field of computer network security and computer network application security. Ex. 1001, 1:15-19; Ex. 1006, [0001]-[0002]; Ex. 1007, [0008], [0020].

~~As to the combination, Das and Overcash are analogous art to the ‘948 Patent because each is from the field of computer network security and computer network application security. Ex. 1001, 1:15-19; Ex. 1006, [0001]-[0002]; Ex. 1007, [0008], [0020]; Ex. 1003, ¶ 74.~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~44-75.~~ As of the priority date of the '948 Patent, it would have been obvious to a POSITA to include Overcash's continuous monitoring functionality in the computer network/application security system of Das because to do so would have been merely an arrangement of old elements (Das's computer network/application security system and Overcash's system that includes continuous monitoring of

applications for detecting security defects), each performing the same function it had been known to perform (Overcash's functionality of continuous monitoring of applications for detecting security defects and Das's computer network/application security system performing "evaluation[s] of applications to determine their respective trust status"), in a way that yields no more than a POSITA would expect from such an arrangement (Overcash's continuous application monitoring functionality being used in Das's computer network/application security system to continuously monitor applications as part of Das's computer network/application security system's "evaluation of applications to determine their respective trust status"). Ex. 1006, [0048]; Ex. 1007, [0020], [0068]; ~~Ex. 1003, ¶ 75.~~ For example, as combined, Das's computer network/application security system would use Overcash's continuous application monitoring functionality as part of its "evaluation of applications to determine their respective trust status." Ex. 1006, [0048]; Ex. 1007, [0020], [0068]; ~~Ex. 1003, ¶ 75.~~ As shown here, such a combination and/or modification would have been obvious. ~~Ex. 1003, ¶ 75.~~

~~45-76.~~ A POSITA would also have been motivated to make such a combination and would have had a reasonable expectation that the combination would be successful. ~~Ex. 1003, ¶ 76.~~ For example, Das discloses that "continuous efforts (both electronic and manual) are usually necessary to protect against unknown and/or malicious software." Ex. 1006, [0002], [0027]. The

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

“continuous efforts” that a

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

POSITA would have been motivated to include in Das's computer network/application security system would have included Overcash's "continuous monitoring [of application operations] for defects as they are exposed through usage" because including Overcash's "continuous monitoring" in Das's computer network/application security system would allow for "continuous efforts" in the "management of applications," which are goals of both Das and Overcash. Ex. ~~1006, [0002], [0027], [0029]; Ex. 1007, [0020], [0062], [0068] [0079], [0229] [0230], FIGS. 4-6 and 8-9;~~
~~1006, [0002], [0027], [0029]; Ex. Ex. 1003, ¶ 76, 1007, [0020], [0062], [0068]-[0079], [0229]-[0230], FIGS. 4-6 and 8-9.~~ A POSITA would have had a reasonable expectation that Das and Overcash would successfully operate together as described because Das already discloses that "continuous efforts (both electronic and manual) are usually necessary to protect against unknown and/or malicious software," and Overcash merely elaborates on how to implement such "continuous efforts," such as by "continuous[ly] monitoring [applications] for defects as they are exposed through usage." Ex. 1006, [0002], [0027]; Ex. 1007, [0020], [0062], [0068]-[0079],-
~~[0229]-~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~{[0229]-[0230]~~, FIGS. 4-6 and 8-9; ~~Ex. 1003, ¶ 76.~~ As shown here, such a combination and/or modification would have been obvious. ~~Ex. 1003, ¶ 76.~~

77. Therefore, Das and Overcash ~~discloses~~disclose and/or ~~renders~~render obvious ~~all elements of claim 2, and claim 2 is unpatentable as obvious over Das and Overcash. Ex. 1003, ¶ 77.~~

3. Claim 3

~~46-78.~~ The combination of Das and Overcash discloses and/or renders obvious all elements of claim 3.

- a. **“The method of claim 1, wherein the event and behavior correlation engine receives one or more of: . . .”**

~~47-79. This claim element is taught by Das.~~ Das discloses that “reputation engine 20” (“*the event and behavior correlation engine*”) receives (“*receives one or more of . . .*”) information “from a plurality of sources such as mobile device 14 [e.g., via whitelist enforcement module 22], application software distribution platforms, threat intelligence feeds 32, etc.” Ex. 1006, [0021], [0023]-[0024], [0031], [0035], [0053], [0055]. Das
~~[0055]; Ex. 1003, ¶ 79. Das~~ discloses that the information “encompasses one or more characteristics of the application . . . and/or the application’s behavior . . . that uniquely identifies the application,” including “behavior and activities of any one or more applications” monitored by “whitelist enforcement module 22.” Ex. 1006, [0021], [0052]; ~~Ex. 1003, ¶ 79.].~~

~~48-80.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 80.~~

- b. **“system events and infection profiles from a network activity sensor;”**

~~49-81. This claim element is taught by Das.~~ Das discloses that the information received by reputation engine 20 includes “security events” (“*system events*”) provided from the aspects of the whitelist enforcement module 22 that sense (i.e., monitor, detect, and/or report (e.g., to reputation engine 20)) characteristics, behavior (e.g., network activity), activity, and/or security events associated with

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

applications (“system events . . . from a network activity sensor”). Ex. 1006, [0021], [0052], [0055]~~], Ex. 1003, ¶ 81].~~ A POSITA would ~~readily~~ understand that whitelist enforcement module 22 functions as, and therefore

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

discloses and/or renders obvious, “a network activity sensor” based at least on the fact that whitelist enforcement module 22 includes functionality to sense (i.e., monitor, detect, and/or report (e.g., to reputation engine 20)) characteristics, behavior (e.g., network activity), activity, and/or security events associated with applications. ~~Ex. 1003, ¶ 81.~~ Das further discloses that aspects of the whitelist enforcement module 22 that sense characteristics, behavior (e.g., network activity), activity, and/or security events associated with applications (“network activity sensor”) also provide to reputation engine 20 information that includes: (i) endpoint address information, e.g., information contained in an application manifest associated with an application and that “uniquely identif[ies] an application,” of a victim application, such as an “application[] evaluated and determined to be untrustworthy (e.g., containing malicious code such as viruses, worms, and the like, etc.)”; (ii) “a statistical confidence level of the reputation score”; (iii) information about the source of an attacker, such as “attack history,” the “location” of where the attack originated, and whether the source was “malware,” “spyware,” or “viruses, worms, and the like, etc.”; and (iv) a time range for an infection, such as “a short span of time.” Ex. 1006, [0021]-[0022], [0028]-[0029], [0046], [0055] ~~[0056]; Ex. 1003, ¶ 81. A POSITA]~~ [0056]. A POSITA would have ~~readily~~ understood some or all the foregoing information (i)-(iv) to disclose and/or render obvious “infection profiles,” which

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

the specification of the '948 Patent suggests “comprises at least the victim endpoint

address and one or more of a forensic confidence of the declared infection, the attacker source, the command and control source, the full evidence chain, and the infection time range (onset, duration).” Ex. 1001, 18:48-52. As such, Das discloses and/or renders obvious that “*the event and behavior correlation engine receives one or more of: system events and infection profiles from a network activity sensor.*” ~~Ex. 1003, ¶ 81.~~

~~50-82.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 82.~~

c. “integrity measurement and verification reports of scans from a system configuration sensor;”

~~51-83.~~ ~~This claim element is taught by Das.~~ Das discloses that reputation scores and associated trust statuses are determined and/or updated based on security/risk assessments (“*scans*”) by reputation engine 20 and/or threat intelligence feeds 32, Ex. 1006, [0019]-[0020], ~~Ex. 1006, [0019]-[0020]~~, [0031], [0048], [0057]; *see also* Ex. 1006, [0023] (“Threat intelligence feeds 32 may be provided to update reputation scores . . .”); ~~Ex. 1003, ¶ 83-.~~ Das discloses that the trust statuses of applications (“*integrity measurement and verification reports*”) that are determined based on the security/risk assessments (“*of scans*”) are stored at server 17, e.g., at application reputations database 26 and/or whitelists 30. ~~Ex. 1006, [0020]; Ex. 1003, ¶ 83-.~~ Das further discloses that those trust statuses of applications stored at server 17, e.g., at application reputations database 26 and/or whitelists 30, are accessed by whitelist

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

enforcement module 22. Ex. 1006, [0033], [0049], [0050]-

[0033], [0049], [0050] [0051]; Ex. 1003, ¶ 83.] A POSITA would have readily

understood that whitelist enforcement module 22

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

also functions as, and therefore discloses and/or renders obvious, “a system configuration sensor” based at least on the fact that whitelist enforcement module 22 includes functionality to sense (i.e., monitor, detect, and/or report (e.g., to reputation engine 20)) system configurations, such as “ports and protocols actually used by the application,” “network connectivity,” and “association with other known Internet Protocol (IP) addresses.” Ex. 1006, [0022]; ~~Ex. 1003, ¶ 83.~~ Das further discloses that whitelist enforcement module 22 (“a system configuration sensor”) provides the trust statuses determined based on security/risk assessments (“integrity measurement and verification reports”), e.g., the trust statuses accessed by whitelist enforcement module from server 17, to reputation engine 20 (“the event and behavior correlation engine”). See Ex. 1006, [0053] (“Whitelist enforcement module 22 may provide application status to reputation engine 20 . . .”). ~~to reputation engine 20 . . .~~); ~~Ex. 1003, ¶ 83.~~ Accordingly, Das discloses that reputation engine 20 receives applications’ trust statuses determined based on security/risk assessments from the whitelist enforcement module 22, thereby disclosing and/or rendering obvious that “the event and behavior correlation engine receives one or more of: . . . integrity measurement and verification reports of scans from a system configuration sensor.” Ex. 1006, [0019]-[0023], [0031], [0033], ~~[0048]-[0049],~~ ~~[0050]-[0051],~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

~~[0048] [0049], [0050] [0051], [0053], and [0057]; Ex. 1003, ¶ 83.].~~

~~52-84.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 84.~~

- d. “system events pertaining to processor, network, memory, and storage resource consumption from a resource utilization sensor; and”

~~53-85. This claim element is taught by Das.~~ Das discloses that whitelist enforcement module 22 “include[s] event detection capabilities” to “detect security events [(“system events”)] relating to [(“pertaining to”)] particular applications and application activities,” including “behavior and activities of any one or more applications,” such as applications’ “requests for,” “access [to],” and “use of,” “resources” (“resource consumption”). Ex. 1006, [0022], [0028], [0048], [0052]-~~[0053], [0055], [0073]. Das discloses that~~ ~~[0053], [0055], [0073]; Ex. 1003, ¶ 85. Das discloses that~~ the resources, e.g., the resources to which the security events may relate, include “the mobile device’s processor and memory” (“processor . . . [and] . . . memory . . . ~~resource consumption~~”). ~~Ex. 1006, [0019], [0048]; Ex. 1003, ¶ 85. Das discloses that the~~ resource consumption”). Ex. 1006, [0019], [0048]. Das discloses that the resources also include an application’s “network connectivity” and/or “network activity” usage (“network . . . resource consumption”). Ex. 1006, [0021]-~~[0022]; Ex. 1003, ¶ 85.]~~. Das further discloses that the resources include “storage device[s] in communication with reputation engine 20,” such as “server 17,” which may be used to “store [applications]” (“storage resource consumption”). Ex. 1006, [0021]; *see also* Ex. 1006, [0038], [0086]; ~~Ex. 1003, ¶ 85.]~~. Thus, Das discloses that the

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

security events relate to resource consumption associated with at least the foregoing listed resources, thereby disclosing and/or rendering obvious “*system events pertaining to processor, network, memory, and storage resource consumption.*” Ex. ~~1006~~, 1006, ~~[0019], [0021], [0022], [0028], [0038], [0048], [0052], [0053], [0055], [0072], [0086];~~ Ex.

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

[0019], [0021]-[0022], [0028], [0038], [0048], [0052]-[0053], [0055], [0073], 1003, ¶ 85.

[0086].

54-86. A POSITA would have ~~readily~~ understood that whitelist enforcement module 22 also functions as, and therefore discloses and/or renders obvious, “a resource utilization sensor” based at least on the fact that whitelist enforcement module 22 includes functionality to sense (i.e., monitor, detect, and/or report (e.g., to reputation engine 20)) “behavior and activities of any one or more applications,” such as applications’ “requests for,” “access [to],” and “use of,” “resources,” i.e., resource utilization. Ex. 1006, [0022], [0028], [0048], [0052]-[0053], [0055], ~~[0073]; Ex. 1003, ¶ 86.~~

~~1003, ¶ 86.~~ [0073]. Das discloses that whitelist enforcement module 22 (“a resource utilization sensor”) “report[s] such events [(“system events pertaining to processor, network, memory, and storage resource consumption”)] to reputation engine 20 or other modules for use in determining the trustworthiness of such applications and application activities.” Ex. 1006, [0055]; ~~Ex. 1003, ¶ 86.~~

Accordingly, Das discloses that reputation engine 20 receives security events relating to resource consumption associated with at least the foregoing listed resources from the whitelist enforcement module 22, thereby disclosing and/or rendering obvious that “the event and behavior correlation engine receives one or

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

more of: . . . system events pertaining to processor, network, memory, and storage resource consumption from a resource utilization sensor.” ~~Ex. 1003, ¶ 86.~~

~~55-87.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 87.~~

- e. **“system events pertaining to image profiles and local execution context from an application integrity sensor.”**

~~56-88.~~ ~~This claim element is taught by Das.~~ Das discloses that whitelist enforcement module 22 “include[s] event detection capabilities” to “detect security events [(“*system events*”)] relating to [(“*pertaining to*”)] particular applications and application activities,” including “behavior and activities of any one or more applications.” Ex. 1006, [0052]-[0053], [0055]; ~~Ex. 1003, ¶ 88.~~ More specifically, the “monitor[ed] behavior and activities of any one or more applications” include the presence of “[m]alicious software (malware)[,] includ[ing] hostile, intrusive, or annoying programming (e.g., code, script [(“*image profiles*”)], active content, etc.) that can disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and exhibit other abusive behavior.” Ex. 1006, [0028], [0052]; ~~Ex. 1003, ¶ 88.~~ The ’948 Patent discloses that “image profiles are generated for executable images such as, but not limited to, binary images, intermediate images, or *scripts*” Ex. 1001, 12:63-65 (emphasis added). Thus, a POSITA would have ~~readily~~ understood that Das’s foregoing disclosure regarding security events that relate to the presence of malicious software scripts discloses and/or renders obvious “*system events pertaining to image profiles.*” ~~Ex. 1003, ¶ 88.~~ The “behavior and activities of any one

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

or more applications” also includes applications’ usage of functions as “determined from

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

the code flow graphs . . . [that] show[] a graphical representation of paths that may be traversed through an application during its execution” (“*local execution context*”). Ex. 1006, [0032], [0052]; ~~Ex. 1003, ¶ 88.~~ Thus, Das also discloses and/or renders obvious “*system events pertaining to . . . local execution context.*” ~~Ex. 1003, ¶ 88.~~

~~57-89.~~ A POSITA would have ~~readily~~ understood that whitelist enforcement module 22 also functions as, and therefore discloses and/or renders obvious, “*an application integrity sensor*” based at least on the fact that whitelist enforcement module 22 includes functionality to sense (i.e., monitor, detect, and/or report (e.g., to reputation engine 20)) “the trust status of application[s]” and/or “attack history” of applications. Ex. 1006, [0051]-[0055], [0022], [0033], [0038], [0057]; ~~Ex. 1003, ¶ 89.~~ Das discloses that whitelist enforcement module 22 (“*an application integrity sensor*”) “report[s] such events [(“*system events pertaining to image profiles and local execution context*”)] to reputation engine 20 or other modules for use in determining the trustworthiness of such applications and application activities.” Ex. 1006, [0055]; ~~Ex. 1003, ¶ 89.~~ Accordingly, Das discloses that reputation engine 20 receives security events relating to software scripts and to usage of functions and/or resources by applications during their execution from the whitelist enforcement module 22, thereby disclosing and/or rendering obvious that “*the*

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

*event and behavior correlation engine receives one or more of: . . . system events
pertaining to image profiles and local execution context from an application
integrity sensor.”* ~~Ex. 1003, ¶ 89.~~

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

58-90. Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 90.~~

~~* * *~~

59-91. In light of the foregoing, Das discloses and/or renders obvious ~~all the~~ elements of claim 3, and thus claim 3 is ~~unpatentable as obvious over~~ in light of Das and Overcash. ~~Ex. 1003, ¶ 91.~~

4. Claim 4

60-92. Claim 4 depends on claim 3 and further recites “*wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly, by a third party collaboration service to score the severity of an application based on the vulnerability, compliance, and patch status to affirm positive presence of a threat.*”

61-93. ~~This claim element is taught by Das.~~ As discussed above in § V.B.3.c, Das discloses and/or renders obvious “*scans*,” such as security/risk assessments. ~~Ex. 1003, ¶ 93.~~ Das further discloses “scan[ning] a targeted mobile device according to a pre-determined schedule, for example, once every 24 hours” (“*wherein the scans are performed as per a schedule, and wherein the schedule is one or more of hourly, daily, weekly, bi-weekly, or monthly*”). Ex. 1006, [0081]; ~~Ex. 1003, ¶ 93.].~~

62-94. Das discloses that the security/risk assessments (“*scans*”), such as the security/risk assessments performed per an hourly or daily schedule, can be

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

performed (“*are performed*”) by “[t]hreat intelligence feeds 32 [that] may be provided by independent third parties” (“*by a third party collaboration service*”) “to update reputation scores” (“*to score the severity of an application*”), e.g., based

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

on “threat information” included in threat intelligence feeds 32, and/or to “provide real-time, dynamic, and up-to-date information on a variety of potential threats.”

Ex. 1006, [0023], [0021], [0055]; ~~Ex. 1003, ¶ 94.~~

~~63-95.~~ Das also discloses that the “threat information” includes “vulnerability information” so that “threat intelligence feeds 32” (“*a third party collaboration service*”) can determine “reputation scores” based on the “vulnerability information” (“*. . . to score the severity of an application based on the vulnerability*”). Ex. 1006, [0023], [0021], [0055], [0039]; ~~Ex. 1003, ¶ 95.~~ Das further discloses that “reputation scores” (also referred to as “trust scores”) (“*score [of] the severity of an application*”) “denote[] a relative level of trustworthiness or security of the application” that is determined based, at least in part, on applications’ “compliance with one or more mobile application policies enforced in a network or system” (“*scor[ing] the severity of an application based on the . . . compliance*”). Ex. 1006, [0019], [0023], [0073], [0076]; ~~Ex. 1003, ¶ 95.~~ Das also discloses that applications’ “reputation scores” (“*score [of] the severity of an application*”) can be determined and/or “modif[ied]” based, at least in part, on whether or not “components of system 10” have “remediate[d] the threat to the host mobile device” (“*patch status*”) (“*scor[ing] the severity of an application based on the . . . patch status*”). Ex. 1006, [0019], [0055], [0079]; ~~Ex. 1003, ¶ 95.~~ As such, a POSITA would have readily understood the foregoing disclosure as

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

disclosing and/or rendering obvious that the “*scans [being]*”

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

performed as per a schedule, [such as] hourly, daily, . . . by a third party collaboration service [] score the severity of an application based on the vulnerability, compliance, and patch status.” ~~Ex. 1003, ¶ 95.~~

~~64-96.~~ Das discloses that “reputation scores” (“*score[s of] the severity of an application*”), such as reputation scores determined based on vulnerability, compliance, or remediation status (“*scor[ing] the severity of an application based on the vulnerability, compliance, and patch status*”), are used to provide an indication of the presence of “an application [that] is malicious software or otherwise poses a threat to mobile devices or networks upon which it is installed” (“*to affirm positive presence of a threat*”). Ex. 1006, [0019], [0036], [0046],-
~~[0049], [0052],~~
~~[0049], [0052], [0072]; Ex. 1003, ¶ 96.]~~

~~65-97.~~ Therefore, Das discloses and/or renders obvious ~~at the~~ elements of claim 4, and thus claim 4 is ~~unpatentable as~~ obvious over in light of Das and Overcash.

5. Claim 5

~~66-98.~~ Claim 5 depends on claim 1 and recites “*wherein the plurality of runtime dashboards are a plurality of application runtime reputation score dashboards that comprise one or more of: a global view dashboard; a system configuration dashboard; a resource utilization dashboard; an application integrity dashboard; and a network activity dashboard.*”

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~67-99.~~ Das does not explicitly disclose ~~these features, that~~ “the plurality of runtime dashboards are a plurality of application runtime reputation score dashboards that comprise one or more of: a global view dashboard; a system configuration dashboard; a resource utilization dashboard; an application integrity dashboard; and a network activity dashboard,” but it would have been obvious, in light of Overcash, to include those features in ~~Das’s~~the system. ~~Ex. 1003, ¶ 99 of Das.~~

~~68-100.~~ In particular, the ~~features of claim 5 were well-~~use of dashboards in monitoring systems generally, and computer and network monitoring systems specifically, was well-known in the art by the ’948 Patent’s priority date. ~~Id., ¶ 100.~~
~~100.~~Thus, the features of claim 5 were well- known in the art by the ’948 Patent’s priority date. For example, as discussed above in § V.B.1.e, Overcash discloses and/or renders obvious “the plurality of runtime dashboards.” ~~Ex. 1003, ¶ 100.~~ Similarly, as discussed above in § V.B.1.e, Overcash discloses and/or renders obvious that the plurality of real-time displays/windows (“the plurality of runtime dashboards”) are a plurality of displays/windows for displaying “real-time” “application defect detection” “information” obtained from the “continuous monitoring [of applications] for defects as they are exposed through usage” (“a plurality of application runtime reputation score dashboards”). Ex. 1007, [0020], [0062], [0068]-[0079], [0229]-[0230], FIGS. 4-6 and 8-9; ~~Ex. 1003, ¶ 100.~~

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

69-101. Overcash discloses that those windows for displaying “real-time” “application defect detection” “information” from “vulnerability assessments” (the

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

“plurality of application runtime reputation score dashboards”) include
“comprise one or more of”) a “System Configuration” window (*“a system
configuration dashboard”*). Overcash, FIG. 8; ~~Ex. 1003, ¶ 101~~. Specifically, figure 8
of Overcash (shown below) shows that the management console includes a
“System Configuration” tab that can be selected to display the “System
Configuration” window. Overcash, FIG. 8; ~~Ex. 1003, ¶ 101~~8.

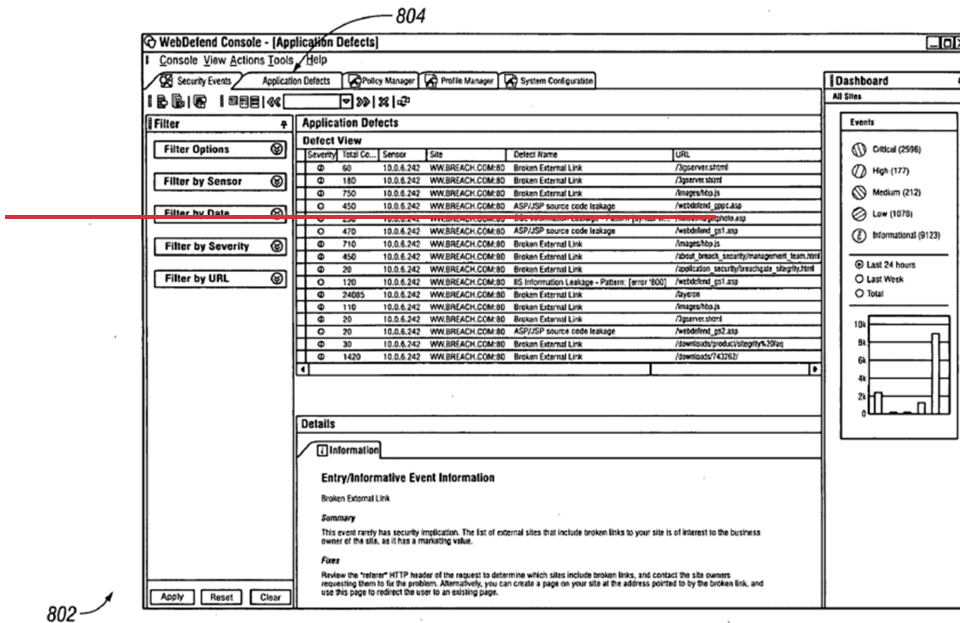


FIG. 8

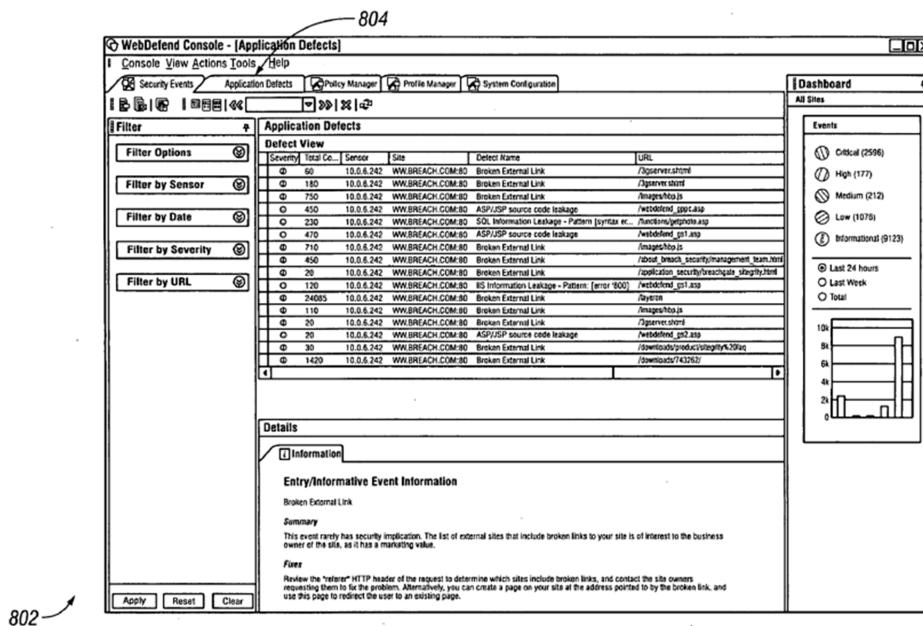


FIG. 8

Overcash, FIG. 8.

70-102. Overcash further discloses in figure 8 (shown above) that the windows (“dashboards”) also include (“comprise one or more of”) an “Application Defects”

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

window that functions as, and therefore discloses and/or renders obvious, “a *resource utilization dashboard*” based on the “Application Defects” window’s inclusion of resource utilization information associated with applications, such as information about a Uniform Resource Locator (URL) and/or a site (“*resource[s]*”) utilized by an application. Overcash, FIG. ~~8; Ex. 1003, ¶ 1028~~.

~~71.103.~~ Overcash discloses in figure 6 (shown below) that the windows (“*dashboards*”) also include (“*comprise one or more of*”) a “Security events” window that functions as, and therefore discloses and/or renders obvious, “an *application integrity dashboard*” based on the “Security events” window’s inclusion of security and vulnerability information associated with applications, such as the “[s]everity” of a security event associated with an application and/or the “[a]ttack [e]vent [i]nformation” associated with an application that provides details on whether (or how) a security event impacts the integrity of an application. Overcash, FIG. ~~6; Ex. 1003, ¶ 1036~~.

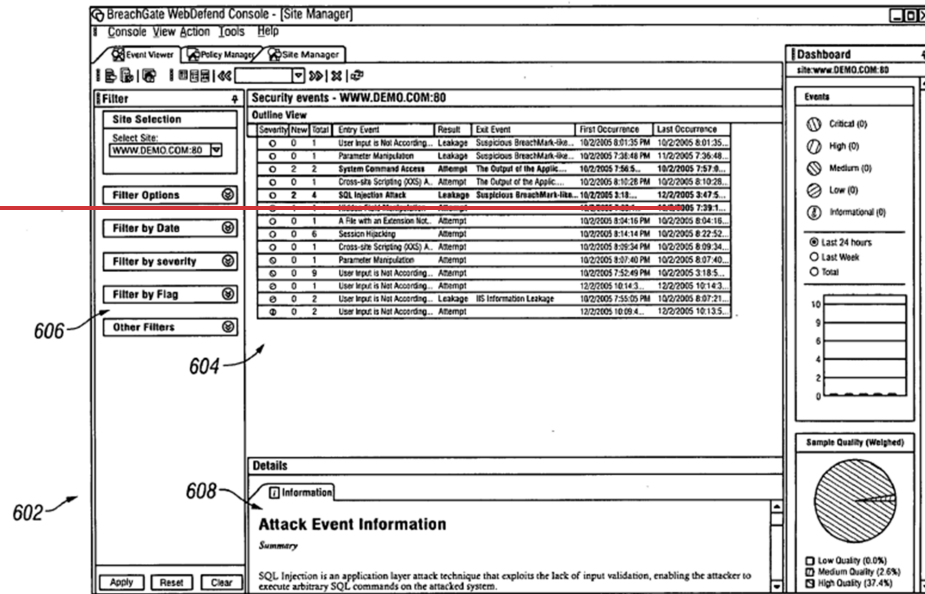


FIG. 6

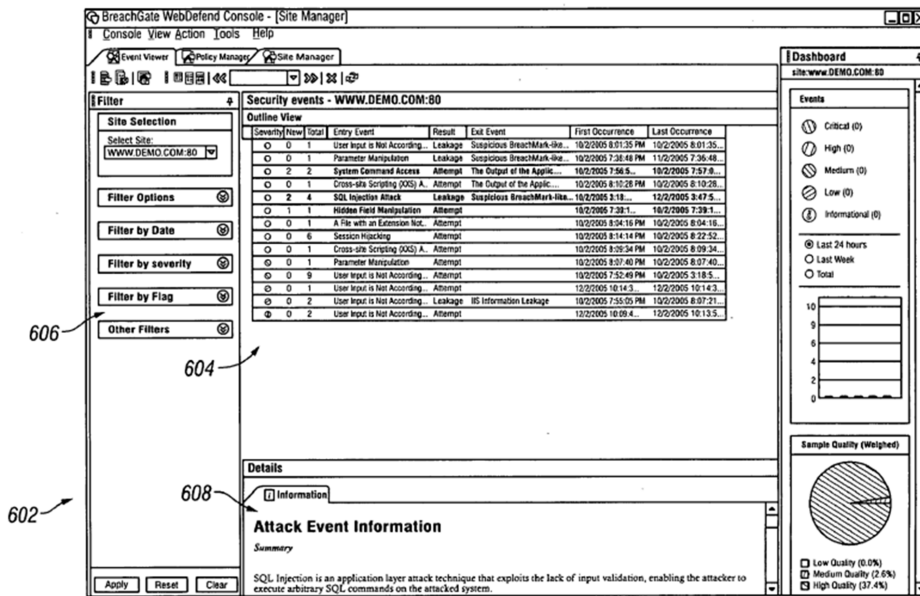


FIG. 6

Overcash, FIG. 6.

72-104. Overcash further discloses in figure 9 (shown below) that the windows (“dashboards”) also include (“comprise one or more of”) a “vulnerability” “drill-down” window 902 that functions as, and therefore discloses and/or renders obvious, “a network activity dashboard” based on the “drill-down” window’s inclusion of network activity information association with applications, such as a site associated with an application, a source IP address associated with an application, and/or a date/time associated with the application’s network activity.

Ex. 1007, [0230], FIG. 9; Ex. 1003, ¶ 1049.

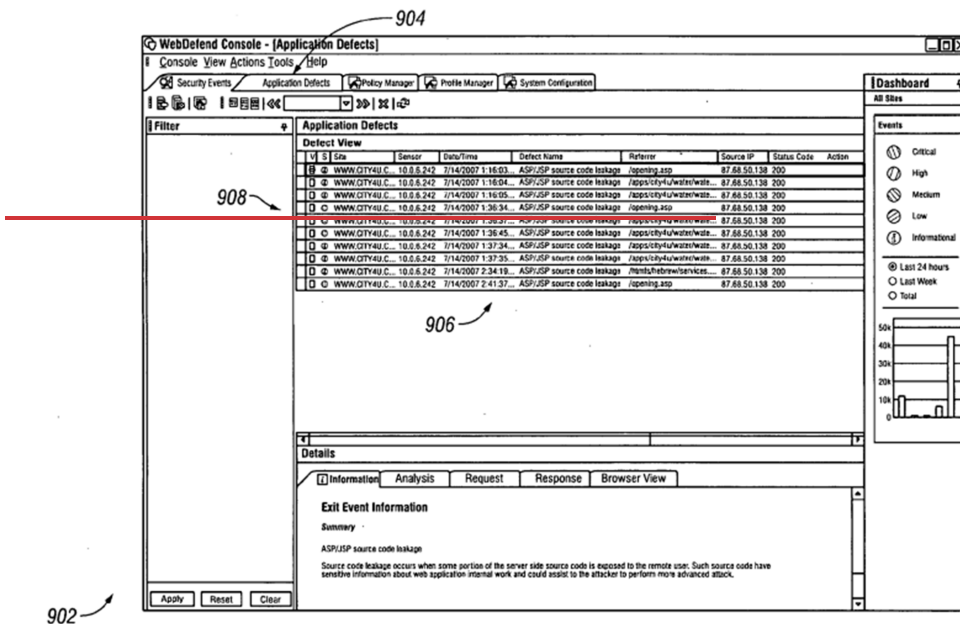


FIG. 9

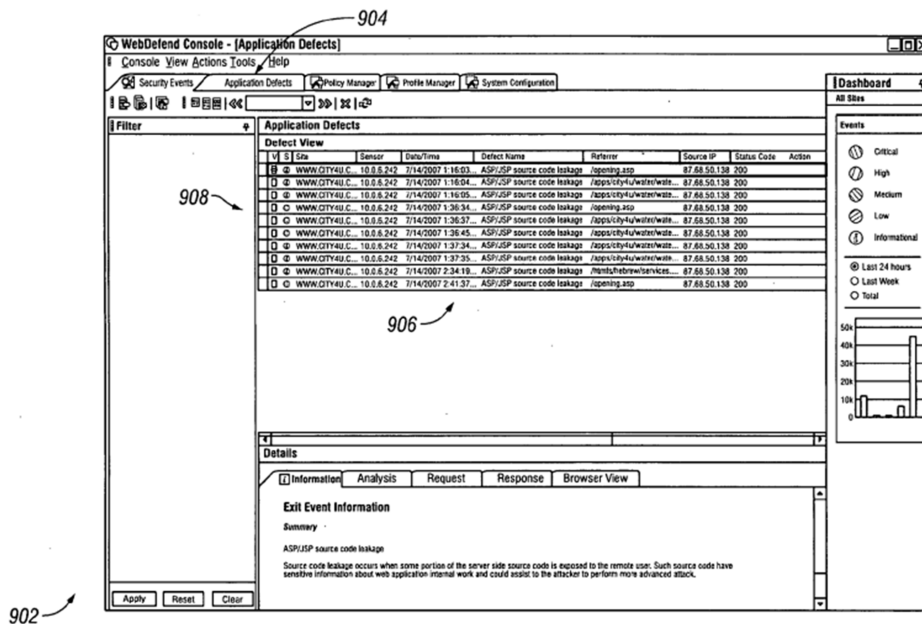


FIG. 9

Overcash, FIG. 9.

73-105. As to the combination, Das and Overcash are analogous art to the '948 Patent because each is from the field of computer network security and computer network application security. Ex. 1001, 1:15-19; Ex. 1006, [0001]-[0002]; Ex. 1007, [0008]; [00200002]; Ex. 1003, ¶ 105, 1007, [0008], [0020].

106. As of the priority date of the '948 Patent, it would have been obvious to a POSITA to include Overcash's "management console" and associated displays/windows in the computer network/application security system of Das because to do so would have been merely an arrangement of old elements (Das's

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~computer network/application security system and Overcash's management console and associated displays/windows), each performing the same function it had been known to perform (Overcash's management console and associated displays/windows "generat[ing] displays of information to a network administrator" and Das's computer network/application security system performing "evaluation[s] of applications to determine their respective trust status"), in a way that yields no more than a POSITA would expect from such an arrangement (Overcash's management console and associated displays/windows being used to display computer network/application security information resulting from Das's computer network/application security system's "evaluation of As of~~
the priority date of the '948 Patent, it would have been obvious to a POSITA to include Overcash's "management console" and associated displays/windows in the computer network/application security system of Das because to do so would have been merely an arrangement of old elements (Das's computer network/application security system and Overcash's management

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

console and associated displays/windows), each performing the same function it had been known to perform (Overcash's management console and associated displays/windows "generat[ing] displays of information to a network administrator" and Das's computer network/application security system performing "evaluation[s] of applications to determine their respective trust status").), in a way that yields no more than a POSITA would expect from such an arrangement (Overcash's management console and associated displays/windows being used to display computer network/application security information resulting from Das's computer network/application security system's "evaluation of applications to determine their respective trust status"). Ex. 1006, [0048]; Ex.

1007, [0068]; ~~Ex. 1003, ¶ 106.~~ For example, as combined, Das's computer network/application security system would use Overcash's management console and associated displays/windows to display, to a network administrator, computer network/application security information resulting from Das's computer network/application security system's "evaluation of applications to determine their respective trust status." Ex. 1006, [0048]; Ex. 1007, [0068]; ~~Ex. 1003, ¶ 106.~~ As shown here, such a combination and/or modification would have been obvious. ~~Ex. 1003, ¶ 106.~~

74-107. A POSITA would also have been motivated to make such a

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

combination and would have had a reasonable expectation that the combination would be successful. ~~Ex. 1003, ¶ 107.~~ For example, Das discloses that “innovative tools are needed

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

to assist IT administrators in the effective control and management of applications on mobile devices within computer and communication network environments,” and that “continuous efforts (both electronic and manual) are usually necessary to protect against unknown and/or malicious software.” Ex. 1006, [0002], [0027]. The “innovative tools” that a POSITA would have been motivated to include in Das’s computer network/application security system would have included Overcash’s “management console” that includes a plurality of real-time displays/windows because including Overcash’s “management console” that includes a plurality of real-time displays/windows in Das’s computer network/application security system would allow Das’s computer network/application security system to display various real-time “information” obtained from the “continuous monitoring [of applications],” thereby allowing for “continuous efforts” in the “management of applications,” which are goals of both Das and Overcash. Ex. 1006, [0002], [0027], [0029]; Ex. 1007, [0020], [0062], [0068]-[0079], [0229]-[0230], FIGS. 4-6 and 8-9;

~~Ex. 1003, ¶ 107.9.~~ A POSITA would have had a reasonable expectation that Das and Overcash would successfully operate together as described because both Das and Overcash disclose the use of a “management console,” with Das disclosing that the “management console . . . may aggregate and store application reputations,” and Overcash disclosing that the “management console” “generate[s]

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

displays of information,” such as displays of various real-time “information”
obtained from

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

the “continuous monitoring [of applications] for defects as they are exposed through usage.” Ex. 1006, [0029]; Ex. 1007, [0020], [0062], [0068]-[0079],-
[0229]-[0230],
[0229]-[0230], FIGS. 4-6 and 8-9; ~~Ex. 1003, ¶ 107.~~ In other words, both Das and Overcash disclose the use of a “management console,” with each elaborating on different features for which the management console can be used. ~~Ex. 1003, ¶ 107.~~ As shown here, such a combination and/or modification would have been obvious.-
~~Ex. 1003, ¶ 107.~~

~~75-108.~~ Therefore, Overcash discloses and/or renders obvious ~~at~~the elements of claim 5, and thus claim 5 is ~~unpatentable as~~ obvious overin light of Das and Overcash. ~~Ex. 1003, ¶ 108.~~

B. No Secondary Considerations Exist

~~No I am unaware of any secondary indicia of non-obviousness exist. Petitioner reserves considerations of nonobviousness, and I understand no such considerations were alleged during prosecution. I reserve the right to respond to rebut any assertion of alleged secondary indicia of non-obviousness advanced by Taasera.~~

III.—Discretionary Factors

~~Under the Director’s interim procedure for evaluating requests for discretionary denial under 35 U.S.C. §314(a), regardless of any factors considerations that otherwise apply, “the PTAB will not discretionarily deny institution of an IPR Patent Owner or PGR in view of parallel district court litigation~~
50

Palo Alto Networks - Exhibit 1003
Palo Alto Networks v. Taasera - IPR2023-00705
Page 54 of 57

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~where a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or Patent Owner's expert declarant may assert during any grounds that could have reasonably been raised in the petition." Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation, 7 (USPTO Dir. June 21, 2022).~~

~~76.109. Petitioner stipulates that, should the Board institute instituted inter partes review, Petitioner will not pursue in parallel district court proceedings the same grounds as in the Petition or any grounds that could have reasonably been raised in the petition. Thus, the Board should not exercise discretion to deny institution under §314(a).~~

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

IV. — Mandatory Notices

A. — Real Parties in Interest

Petitioner is the real party in interest. No other party had access to or control over the present Petition, and no other party funded or participated in preparation of the present Petition.

B. — Related Proceedings

No previous IPR or post-granting proceeding has been filed challenging the '948 patent. The '948 patent is or was at issue in the following Eastern District of Texas district court litigations: *Taasera Licensing LLC v. Trend Micro Incorporated*, Case No. 2:21-ev-00441; *Taasera Licensing LLC v. Check Point Software Technologies Ltd.*, Case No. 2:22-ev-00063; *Taasera Licensing LLC v. Palo Alto Networks, Inc.*, Case No. 2:22-ev-00062; *In re: Taasera Licensing LLC, Patent Litigation*, Case No. 2:22-md-03042; *Trend Micro Inc. v. Taasera Licensing LLC*, Case No. 2:22-ev-00303; *Palo Alto Networks, Inc. v. Taasera Licensing LLC et al.*, Case No. 2:22-ev-00314; *Taasera Licensing LLC v. Fortinet, Inc.*, Case No. 2:22-ev-00415; *Taasera Licensing LLC v. Musarubra US, LLC*, Case No. 2:22-ev-00427; *Taasera Licensing LLC v. CrowdStrike, Inc. et al.*, Case No. 2:22-ev-00468. The '948 patent is or was at issue in the following additional district court litigations: *Trend Micro Incorporated et al. v. Taasera Licensing LLC*, Northern District of Texas Case No. 3:22-ev-00477; *Trend Micro, Inc. v. Taasera Licensing LLC*, Northern District of Texas Case No. 3:22-ev-005181; *Palo Alto Networks, Inc. v.*

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

~~Taasera Licensing LLC et al.~~, Southern District of New York Case No. 1:22-cv-02306; and ~~Taasera Licensing LLC v. CrowdStrike, Inc. et al.~~, Western District of Texas Case No. 6:22-cv-01094.

C. — Lead and Backup Counsel

Petitioner's lead and backup counsel are:

Lead Counsel for Petitioner	Backup Counsel for Petitioner
Juan C. Yaquian WINSTON & STRAWN LLP 800 Capital Street, Suite 2400 Houston, TX 77002 JYaquian@winston.com T: 713.651.2600, F: 713.651.2700 USPTO Reg. No. 70,755	Michael Rueckheim WINSTON & STRAWN LLP 255 Shoreline Drive, Suite 520 Redwood City, CA 94065 mrueckheim@winston.com T: 650.858.6500, F: 650.858.6550 (pro hac vice to be filed) James C. Lin Winston & Strawn LLP 255 Shoreline Drive, Suite 520 Redwood City, CA 94065 jalin@winston.com T: 650.858.6500, F: 650.858.6550 (pro hac vice to be filed)

D. — Electronic Service

Petitioner consents to electronic service at:

EMAIL ADDRESS: ~~Winston-PAN-Taasera@winston.com.~~

V. — Fees

All fees may be charged to Deposit Account No. ~~50-1814.~~

IV.VIII. Conclusion

~~Petitioner respectfully requests~~In sum, for the reasons I have discussed above, it is my opinion that the Board institute IPR and enter a final written decision finding the Challenged Claimsclaims 1-5 of the '948 ~~patent~~Patent are unpatentable.

Dated: March 13, 2023 ————— Respectfully submitted,

~~/ Juan C. Yaquian /~~
Juan C. Yaquian
WINSTON & STRAWN LLP
800 Capital Street, Suite 2400
Houston, TX 77002
JYaquian@winston.com
T: 713.651.2600, F: 713.651.2700
USPTO Reg. No. 70,755

Michael Rueckheim
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
mrueckheim@winston.com
T: 650.858.6500, F: 650.858.6550
(*pro hac vice* to be filed)

James C. Lin
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
jalin@winston.com
T: 650.858.6500, F: 650.858.6550
(*pro hac vice* to be filed)

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

CERTIFICATE OF COMPLIANCE

~~This Petition complies with the word count limits set forth in 37 C.F.R.~~

~~77.110.~~ § 42.24(a)(1)(i) ~~because this Petition contains 9,027 words, excluding the~~
~~parts of the Petition exempted by 37 C.F.R. § 42.24(a)(1), determined using the word count provided~~
~~by Microsoft Word, which was used to prepare this Petition~~they would have been obvious to
a POSITA over the Das and Overcash prior art references cited above.

~~Dated: March 13, 2023~~ _____ ~~Respectfully submitted,~~

~~/Juan C. Yaquian/~~
~~Juan C. Yaquian~~
~~WINSTON & STRAWN LLP~~
~~800 Capital Street, Suite 2400~~
~~Houston, TX 77002~~
~~JYaquian@winston.com~~
~~T: 713.651.2600, F: 713.651.2700~~
~~USPTO Reg. No. 70,755~~

Petition for Inter Partes Review of U.S. Patent No. 8,990,948

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(a), I certify~~understand~~ that ~~on~~
~~March 13, 2023, I caused to be served a true and correct copy of the foregoing~~
~~“PETITION FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,990,948”~~
~~and Exhibits~~
~~1001-1007 by Federal Express on~~this Declaration will be filed as evidence in a
contested case before the Patent Owner at the correspondence address of record for
U.S. Trial and Appeal Board of the United States Patent No. 8,990,948:

BUCHANAN, INGERSOLL & ROONEY PC
1737 KING STREET
SUITE 500
ALEXANDRIA, VA 22314-2727

78.111. ~~A courtesy copy of this Petition and supporting material was~~ and Trademark
Office. I also ~~served on litigation counsel for Patent Owner via email:~~ understand that I may be
subject to cross-

Alfred Ross Fabricant
Fabricant LLP—NY
230 Park Avenue, 3rd Floor W.
New York, NY 10169
Email: ffabricant@fabricantllp.com

~~/Juan C. Yaquian/~~
Juan C. Yaquian
WINSTON & STRAWN LLP
800 Capital Street, Suite 2400
Houston, TX 77002
JYaquian@winston.com
T: 713.651.2600, F: 713.651.2700

USPTO Reg. No. 70,755

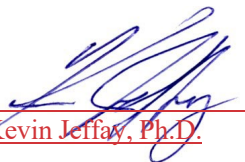
Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

examination concerning this Declaration, and I will appear for cross-examination,
if required of me, during the time allotted for cross-examination.

Petition for *Inter Partes* Review of U.S. Patent No. 8,990,948

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

Date: March 13, 2023


Kevin Jeffay, Ph.D.

Palo Alto Networks - Exhibit 1003
Palo Alto Networks v. Taasera - IPR2023-00705
Page 57 of 57