

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-2023-00706
U.S. Patent No. 9,092,616

~~PETITION FOR INTER PARTES REVIEW~~
~~OF U.S. PATENT NO. 9,092,616~~

Palo Alto Networks - Exhibit 1003
Palo Alto Networks v. Taasera - IPR2023-00706
Page 1 of 107

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.....	6
C. Obviousness.....	8
IV. The '616 Patent.....	10
A. Overview of the Challenged '616 Patent.....	10
B. Relevant Prosecution History	12
V. Claim Construction.....	13
VI. Summary of Cited Prior Art Reference	14
A. Das (Ex. 1006).....	14
VII. Opinions Regarding Unpatentability.	17
A. Ground 1: Claims 1-7 Would Have Been Obvious Over Das	17
1. Claim 1.....	17
a. “A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising:”.....	17
b. “sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime;”	20
c. “receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime;”	25
d. “analyzing, by the trust orchestration server, the received endpoint events;”	27
e. “receiving, by the trust orchestration server, third party network endpoint assessments;”	29
I.—Introduction.....	1
II.—Requirements for <i>Inter Partes</i> Review	2



Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

A. Certification	2
B. Identification of Challenges	2
III. The '616 Patent	2
A. Effective Filing Date	2
B. Level of Ordinary Skill in the Art	3
C. Overview	3
D. Relevant Prosecution History	5
IV. Claim Construction	6
V. Detailed Discussion of the Grounds for Unpatentability	6
A. Overview of the Prior Art	6
1. Das (Ex. 1006)	6
B. Ground 1: Claims 1-7 Would Have Been Obvious Over Das	9
1. Claim 1	9
a. "A method of providing an attestation service for providing runtime- operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration- server, the method comprising;"	9
b. "sending, by the endpoint trust agent on a monitored device, a dynamic- context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime;"	12
c. "receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime;"	17
d. "analyzing, by the trust orchestration server, the received endpoint- events;"	19
e. "receiving, by the trust orchestration server, third party network- endpoint assessments;"	21
a.f. "generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments;" .2230	230
f. "correlating, by the trust orchestration server, the received endpoint- events and the generated temporal events; and"	25
g. "generating, by the trust orchestration server, an integrity profile for the system."	27

iv

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

2. Claim 2.....	29
3. Claim 3.....	30
4. Claim 4.....	33
5. Claim 5.....	34
6. Claim 6.....	37
a. “The method of claim 1, wherein the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents, and”	37
g. “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and”	33
h. “generating, by the trust orchestration server, an integrity profile for the system.”	35
2. Claim 2.....	37
3. Claim 3.....	37
4. Claim 4.....	40
5. Claim 5.....	42
6. Claim 6.....	44
a. “The method of claim 1, wherein the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents, and”	45
b. “The method of claim 1, wherein the temporal events are generated by a trust broker of the trust orchestration server and are received by the system event correlator from the trust broker.”	38
46	
7. Claim 7.....	40
Claim 7.....	47
C. No Secondary Considerations Exist.....	41
VI. Discretionary Factors.....	41
VII. Mandatory Notices.....	42
A. Real Parties in Interest.....	42
B. Related Proceedings	42
C. Lead and Backup Counsel.....	43

~~Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616~~

~~D. Electronic Service.....44~~

~~VIII. Fees.....44~~

~~7. Conclusion.....44~~

~~B. No Secondary Considerations Exist.....49~~

~~H. VIII. Conclusion.....49~~

CITED EXHIBITS

TABLE OF AUTHORITIES

	Page(s)
Statutes	
35 U.S.C. § 102	5
35 U.S.C. § 103	2, 5
35 U.S.C. § 112	5
35 U.S.C. § 314(a)	41, 42
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

PETITIONER'S EXHIBIT LIST

Ex. No.	Brief Description
1001	U.S. Patent No. 9,092,616
1002	File History of U.S. Patent No. 9,092,616
~~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.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

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 1-7 (“Challenged Claims”) of U.S. Patent No. 9,092,616 (“the ‘616 Patent”). The Challenged Claims recite a method of providing
A copy of the ‘616 Patent has been marked Ex. 1001. I have reviewed and am familiar with the ‘616 Patent, which generally relates to systems and methods for threat identification and remediation.

2. I have been asked to provide my opinions regarding the patentability of claims 1-7 of the ‘616 Patent (the “challenged claims”). This declaration discusses my background and qualifications, the legal standards used in my analysis, an attestation service for providing runtime operational integrity of a system. See, e.g., Ex. 1001, claim 1. As shown below, all Challenged Claims would have been obvious to overview of the ‘616 Patent from the perspective of a person of ordinary skill in the art (“POSITA”), as of the patent’s alleged priority date of the ‘616 Patent (a “POSITA”), and my opinions regarding the patentability of the challenged claims.

3. The only ground in this Petition relies on 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.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

~~As set forth more fully below, itDas (Ex. 1006), which was not before the examiner during prosecution of the '616 Patent. As shown in this Petition, Das renders obvious all Challenged Claims. And as confirmed by Petitioner's expert declarant, 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 '616 Patent's priority date, as evidenced by the disclosure of Das.~~

~~As explained in this Petition, the Challenged Claims would not have been allowed if Das had been substantively evaluated by the examiner during prosecution of the '616 Patent. Das discloses a substantially similar computer network and application security system. Therefore, the Challenged Claims should be found unpatentable given the strength of the prior art as shown herein.~~

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

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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 '616 Patent is available for IPR and Petitioner is not barred or estopped from requesting an IPR challenging themy opinion that the challenged 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 '616 Patent and cancel those claims as are unpatentable as obvious based on the following ground below:~~

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

Ground	Claims	Basis for Unpa tenta bility	<u>References</u>
1	1-7	~~Obvious under~~ 35 U.S.C. § 103 ~~over Das (Ex. 1006)~~ (Obviousness)	<u>Das (Ex. 1006)</u>

Inserted Cells

H. The '616 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

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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, distributed systems, real-time systems, operating systems, multimedia networking,

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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.

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

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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 Systems*. I have also been an active participant in the Association for Computing Machinery (“ACM”) and the Institute of Electrical and Electronics Engineers

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

(“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.

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 reference discussed in this Declaration is prior art at least because it would have been available to members of the public as of May 1, 2012, and it is relevant to the subject matter of the '616 Patent.

18. The reference discussed in this Declaration is from the same field of endeavor as the claimed invention (even if it addresses a different problem) and/or is reasonably pertinent to the problem faced by the named inventors (even if it is not in the same field of endeavor as the claimed invention).

B. Person of Ordinary Skill in the Art

5-19. I understand that the '616 Patent ~~resulted~~ issued from Application No. 13/559,766, (the "'766 Application"), filed July 27, 2012. ~~The~~ I also understand that the '616 Patent alleges priority to Provisional Application No. 61/641,007, filed

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

May ~~1, 2012. Without conceding entitlement to this~~

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

1, 2012. 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~~ no earlier than May 1,
2012.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

purposes of this Petition only, Petitioner has used May 1, 2012 as the priority date for the Challenged Claims.

B. Level of Ordinary Skill in the Art

20. As of May 1, 2012, a person of ordinary skill in the art ("POSITA") in the '616 Patent's technical field would have been a person with
I understand that the assessment of the patentability of the challenged claims of the '616 Patent must be undertaken from the perspective of a hypothetical POSITA as of the priority date of the '616 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.

21. 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 understand that a POSITA is also a person of ordinary creativity, not an automaton. Further, I understand that the hypothetical POSITA may comprise a team.

22. Based on these factors, my knowledge and expertise, and the prior art

7

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

to the '616 Patent, it is my opinion that a POSITA at the time of the relevant

1

Palo Alto Networks - Exhibit 1003
Palo Alto Networks v. Taasera - IPR2023-00706
Page 11 of 55

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

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 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.

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:

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

(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.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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.

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.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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

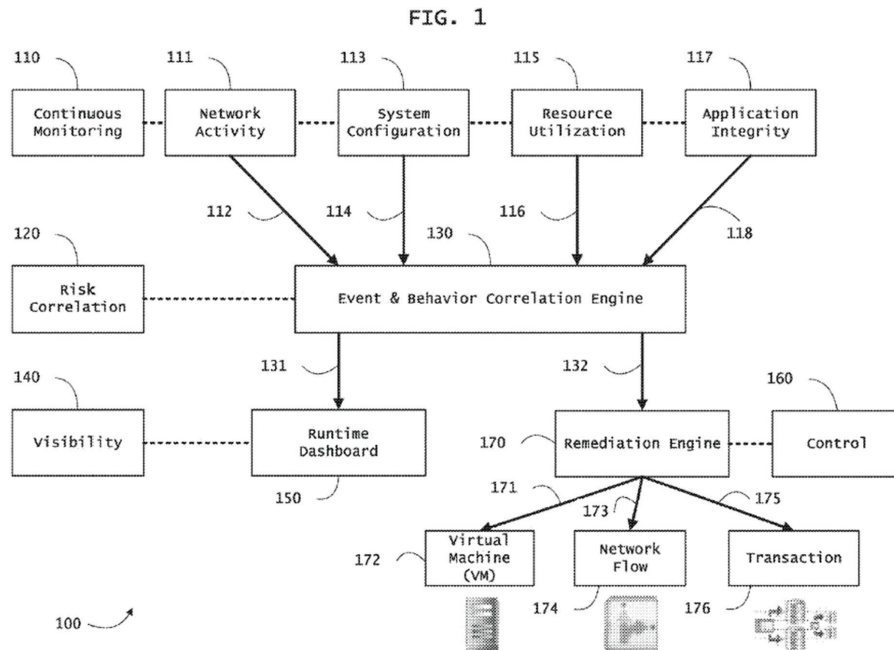
- combining prior art elements according to known methods to yield predictable results;
- substituting known elements for other known elements to obtain predictable results;
- using a known technique to improve similar devices, methods, or products in the same way;
- choosing from a finite number of 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.

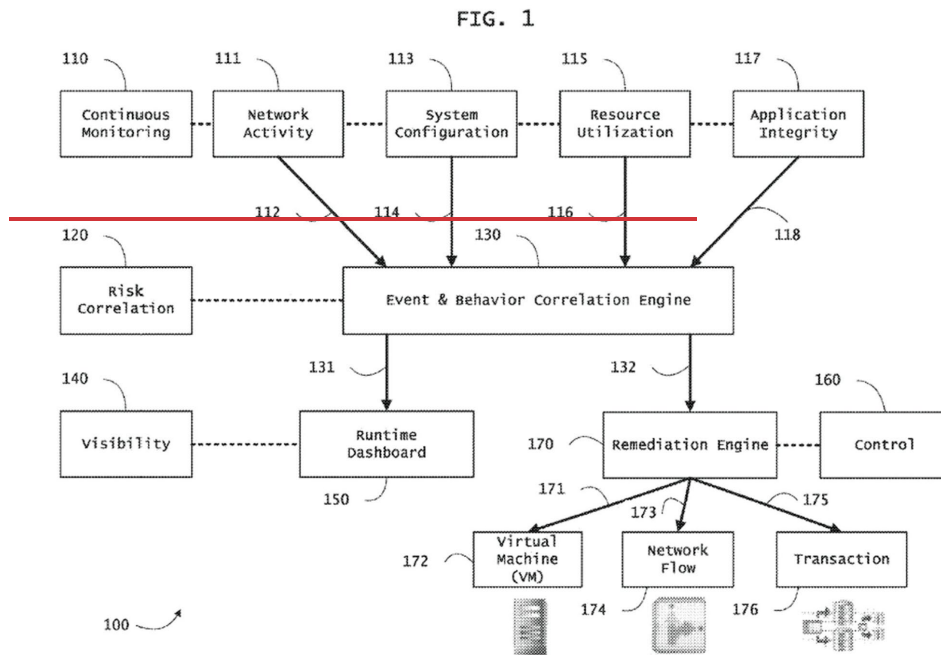
IV. The '616 Patent

A. Overview of the Challenged '616 Patent

29. The '616 Patent describes systems and methods for threat identification and remediation. Ex. 1001, Title. The '616 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 on an instrumented target platform at runtime using or based on a plurality of assertions (or statements).” *Id.*, 4:28-32.

6.30. The security system can further include an “administration console interface comprising various dashboards for displaying data related to operational

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

integrity, resource utilization, application integrity, and network activity, in accordance with embodiments of the invention.” *Id.*, 26:52-56.

B. Relevant Prosecution History

31. I have reviewed and considered the prosecution history of the '616 Patent, which is marked Ex. 1002. Below, I provide a brief summary of certain key events during the prosecution of the '616 Patent.

~~7-32.~~ During prosecution, in the first substantive action, the examiner rejected claims 1-7 (the claims relevant ~~to this proceeding~~ here) under 35 U.S.C. § 102, relying on U.S. Pat. App. Pub. No. 2009/0328222 (Helman) for the § 102 rejections. Ex. 1002, 250-280. Those claims were also rejected under 35 U.S.C. § 112 as being indefinite. *Id.*

~~8-33.~~ In response, Applicant amended independent claim 1 “to recite that steps central to the respective method claim are performed by a specific device.” *Id.*, 175-~~206.~~ The dependent claims were similarly amended. *Id.*

~~9-34.~~ ~~206. The dependent claims were similarly amended. *Id.*~~ In the second substantive action, the examiner rejected claims 1-7 under 35 U.S.C. § 103, relying on Helman, U.S. Pat. App. Pub. No. 2008/0244748 (Neystadt), and U.S. Pat. App. Pub. No. 2012/0110174 (Wootton) for the obviousness rejections. *Id.*, 109-146.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

~~10-35~~. In response, Applicant amended independent claim 1 to recite the “sending” element of now-issued claim 1 and to amend the “receiving” element of

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

now-issued claim 1. *Id.*, 64-80. Applicant also added a new claim, which issued as current claim 7 of the '616 Patent. *Id.*, 73. The other dependent claims of the Challenged Claims were not amended. *Id.*, 64-80. The examiner subsequently issued a Notice of Allowance. *Id.*, 7-14.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~11.36.~~ Das As discussed below, the challenged claims that were allowed to issue in the '616 Patent are taught by the Das prior art reference. Das, cited in this Declaration, was not cited, nor considered during prosecution and is not cumulative of anything cited, during prosecution. As discussed below, it is my opinion that Das teaches all limitations of the '616 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 submit~~has informed me that for the purposes of this Petition, the 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.[†]

~~12.37. 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

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

construction and based on their plain and ordinary meaning to a POSITA as of the '616 Patent's alleged priority date.

III.VI. Summary of Cited Prior Art Reference

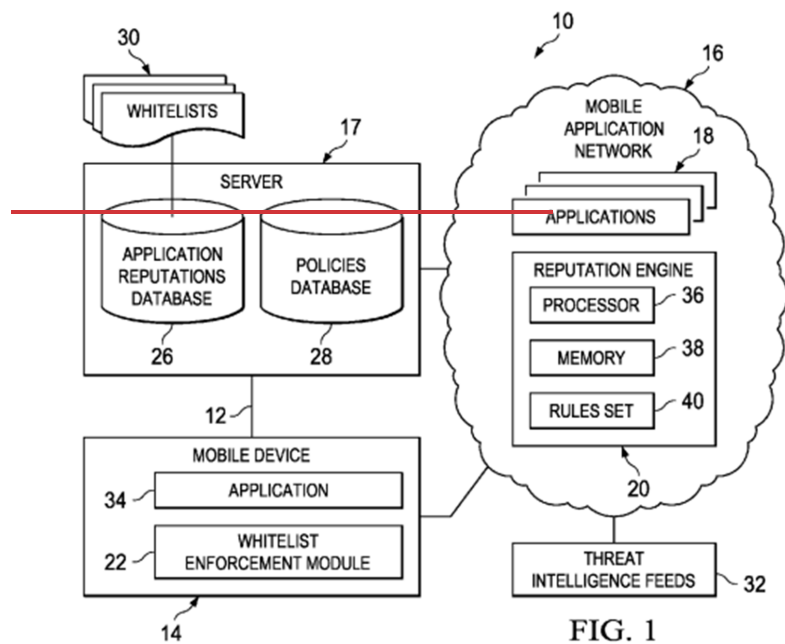
40. The prior art reference Das that is relevant to my analysis is briefly summarized below. I discuss additional elements of Das in my analysis of how Das invalidates the challenged claims.

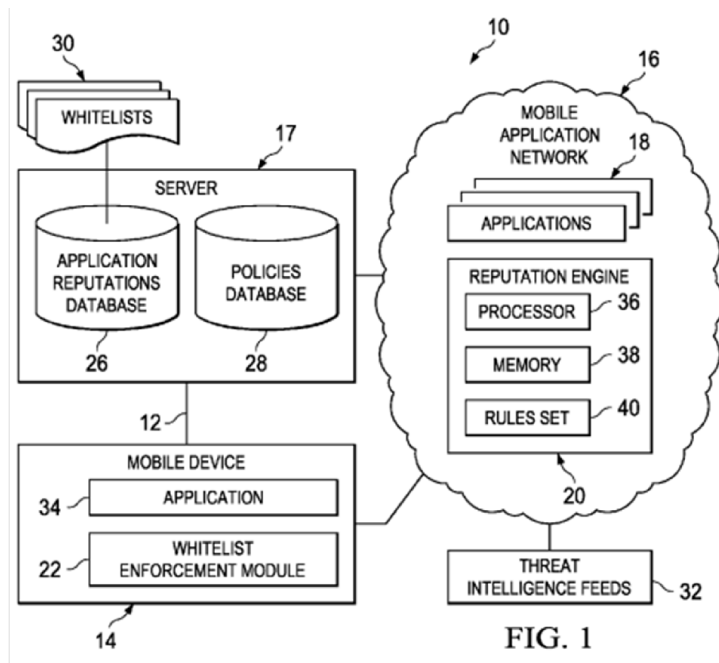
A. Das (Ex. 1006)

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.

13.42. 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 relatesdisclosures 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.

⁺~~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. 1.~~

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

1003, ¶ 43.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~15-44.~~ 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. 9,092,616

~~16.45.~~ 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.~~

~~17.46.~~ 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.~~

VII. Opinions Regarding Unpatentability

47. In my opinion, the challenged claims are unpatentable based upon one ground. Claims 1-7 are obvious over Das.

A. Ground 1: Claims 1-7 Would Have Been Obvious Over Das

1. Claim 1

~~18.48.~~ As set forth below, it is my opinion that Das discloses ~~and/or~~ renders obvious all ~~elements~~ limitations of claim 1 of the '616 Patent.

- a. “A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising:”**

~~19.49.~~ To the extent the Board considers the preamble a limitation, this ~~limitation~~ is taught by Das. Ex. 1003, ¶ 49.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

limitation is taught by Das.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~20-50.~~ Das discloses that “system 10 may be implemented as a remote automated service” and includes components and functionality to perform “evaluation of applications to determine their respective trust status . . . in real-time for applications associated with an execution attempt in mobile device 14” (*“providing an attestation service for providing runtime operational integrity of a system”*). Ex. 1006, [0081], [0048], [0030]; ~~Ex. 1003, ¶ 50.~~ A POSITA would have ~~readily~~ further understood that Das’s automated service is an attestation service at least because it determines a trust status (i.e., certifies that something is true). A POSITA would have further understood that the term “runtime” is interchangeable with the term “real-time.” ~~Ex. 1003, ¶ 50.~~ For example, the ’616 Patent suggests that the term “runtime” is interchangeable or synonymous with the term “real-time.” See, e.g., Ex. 1001, Abstract, 8:17-22, 9:43-48, 28:27-31, 35:61-63; ~~Ex. 1003, ¶ 50.~~ A POSITA would also have ~~readily~~ understood that real-time trust statuses are for the “operational integrity of a system” based, at least in part, on Das’s disclosure regarding “whitelists” (*i.e., that the status of an application is untrusted if the application does not appear on a whitelist*) and 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, [0030], [0048]; ~~Ex. 1003, ¶ 50.~~ For example, Das discloses that trust statuses

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

(also referred to as “reputation scores” or

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

“trust scores” in Das) “can be used to build whitelists” and that “a particular whitelist” may be associated with a “mobile device, its user, network, etc.” (“*of a system*”). Ex. 1006, [0019], [0046], [0033]; ~~Ex. 1003, ¶ 50.~~ Similarly, Das discloses that a “whitelist[]” can be for “a plurality of different mobile devices, mobile operating systems, mobile device manufacturers, network service providers, enterprises, and other entities and groupings” (“*of a system*”) Ex. 1006, [0046]; ~~Ex. 1003, ¶ 50.~~ Das also discloses that the “network” (“*system*”) may include “system 10” that includes “a network 12 connecting one or more mobile devices 14 with mobile application network

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~connecting one or more mobile devices 14 with mobile application network 16.~~ Ex. 1006, [0046]; ~~Ex. 1003, ¶ 50.~~

~~21-51.~~ Das also discloses “whitelist enforcement modules 22” (“*endpoint trust agent[s]*”) “on mobile devices (e.g., mobile device 14),” a “*trust orchestration server*” in the form of a “[r]eputation engine 20” that is “included in a server,” “*network trust agent[s]*” in the form of “server 17” that includes “whitelists” that can be associated with a “network,” and “*network trust agent[s]*” in the form of “[t]hreat intelligence feeds 32” that can include “network threat information.” Ex. 1006, [0029], [0023], [0033]; ~~Ex. 1003, ¶ 51.~~ As such, a POSITA would have ~~readily~~ understood that Das’s “system 10” that “may be implemented in hardware or software” and that includes “whitelist enforcement modules 22,” a “*trust orchestration server*” in the form of a “[r]eputation engine 20” that is “included in a server,” “*network trust agent[s]*” in the form of “server 17” that includes

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

“whitelists” that can be associated with a “network,” and “*network trust agent[s]*” in the form of “[t]hreat intelligence feeds 32” that can include “network threat information” discloses and/or renders obvious “*using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising.*” Ex. 1006, [0081], [0029]-[0030],- [0023], [0033]; Ex. 1003, ¶ 51. [0023], [0033].

22.52. Das further discloses “trust evaluation techniques” for determining the foregoing “real-time” “trust status[es]” (“*[a] method of providing an attestation service for providing runtime operational integrity of a system*”). Ex. 1006, [0048].

~~service for providing runtime operational integrity of a system”). Ex. 1006, [0048];
Ex. 1003, ¶ 52.~~

~~23-53.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 53.~~

- b. “sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime;”**

~~24-54.~~ This claim element is taught by Das. Das discloses “whitelist enforcement modules 22” (“*endpoint trust agent*”) “on mobile devices (e.g., mobile device 14)” (“*on a monitored device*”), where any one of the “whitelist enforcement modules 22” can be the “*endpoint trust agent*,” and any one of the “mobile devices” can be the “*monitored device*.” Ex. 1006, [0029]; ~~Ex. 1003, ¶ 54.].~~

~~25-55.~~ Das discloses that the “whitelist enforcement module 22” (“*endpoint trust agent on a monitored device*”) “monitor[s] behavior and activities of any one or more applications already installed on mobile device 14” to “collect and

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

aggregate” “applications fingerprints” (“*dynamic context*”), where each “application fingerprint” (“*dynamic context*”) “encompasses [(“*includ[es]*”)] one or more characteristics of the application (e.g., obtained from the application’s manifest, application code, etc.) [(“*endpoint events . . . of the monitored device and applications*”)] and/or the application’s behavior (e.g., application requests or actions, network activity, etc.) [(“*actions . . . of the monitored device and applications*”)] that uniquely identifies the application.” Ex. 1006, [0052], [0021]¹⁵

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~Ex. 1003, ¶ 55.~~ Das discloses that the “characteristics” and “behavior” (“*endpoint events and actions*”) can relate to applications, mobile devices, or both mobile devices and applications. Ex. 1006, [0021]; ~~Ex. 1003, ¶ 55.~~ For example, just a few of the monitored “characteristics” and “behavior” (“*endpoint events and actions*”) that Das explicitly discloses include a “unique application identification (ID),” an “application certificate,” an “application name,” “application capabilities [on the mobile device] such as camera activation, network connectivity, phone activation, geolocation, etc.,” “ports and protocols usable by the application” on the mobile device, an “application life span,” “a geographical origination of the application,” “a day and/or time of a first and/or latest appearance of the application on a mobile device,” “files and file hashes associated with the application,” “country/region where the mobile device is currently located,” “geographical locations of subsequent appearances of the application,” “ports and protocols actually used by

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

the application” and mobile device, “application requests for resources” of the mobile device, “application actions,” “installations [of applications] on . . . mobile devices,” “attempt[s] to access resources (e.g., processor, memory, camera, microphone, etc.) in the mobile device,” “execution of one or more applications” on a mobile device, and any other “application action [] involving the mobile device, for instance, in connection with an attempt to perform the action using the mobile device.” Ex. ~~1006~~, 1006, [0021], [0022], [0056], [0048], [0052], [0076]; *see also*

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~[0021], [0022], [0056], [0048], [0052], [0076]; see also Ex. 1006, [0055]; Ex. 1003, ¶ 55.~~

~~26-56.~~ Das discloses that the “monitor[ed]” applications, e.g., applications for which “applications fingerprints” that include “characteristics” and “behavior” information regarding the applications (“*dynamic context including endpoint events and actions*”) are evaluated, can be “applications already installed on mobile device 14” and “associated with an execution attempt in mobile device 14” (“*applications executing on the monitored device at runtime*”) so that the “evaluation of applications to determine their respective trust status is performed in real-time.” Ex. 1006, [0052], [0021], [0048]; *see also* Ex. 1006, [0037], [0055]; ~~Ex. 1003, ¶ 56.~~

Indeed, Das discloses that the “real-time” evaluations of “whether the particular action of the particular application 34 is approved” can be initiated “in response to . . . an attempt to perform a particular action by a particular application 34 installed on mobile device 14” (“*applications executing on the monitored device at runtime*”). ~~Ex. 1006, [0048], [0037]; see also Ex. 1006, [0052], [0055]; Ex. 1003, ¶ 56.~~

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

runtime”). Ex. 1006, [0048], [0037]; see also Ex. 1006, [0052], [0055].

Additionally, a POSITA would have readily understood that the term “runtime” is interchangeable with the term “real-time.” ~~Ex. 1003, ¶ 56.~~ For example, the ’616 Patent suggests that the term “runtime” is interchangeable or synonymous with the term “real- time.” See, e.g., Ex. 1001, Abstract, 8:17-22, 9:43-48, 28:27-31, 35:61-

63.

~~63; Ex. 1003, ¶ 56.~~

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~27-57.~~ Das further discloses “report[ing] or otherwise ma[king] available to reputation engine 20” (“*sending*”) “information about an application or actions of applications” and mobile devices, including “aggregated application fingerprints” (“*dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime*”), to “be evaluated to determine a reputation score of the application.” Ex. 1006, [0055~~;~~ ~~Ex. 1003, ¶ 57.~~]. Das confirms that the foregoing reporting (“*sending*”) is performed by the “whitelist enforcement module 22” (“*by the endpoint trust agent on a monitored device*”) by disclosing that “whitelist enforcement modules 22 operating mobile devices 14 [(“*endpoint trust agent on a monitored device*”)] in a system can detect security events relating to particular applications and application activities[, such as those part of ‘application fingerprints’ (“*dynamic context . . .*”),] and report [(“*send[]*”)] such events [(“*dynamic context . . .*”)] to reputation engine 20 or other modules for use in determining the trustworthiness of such applications and application activities.” Ex. 1006, [0053], [0055~~;~~ ~~Ex. 1003, ¶ 57.~~]. Indeed, as further confirmation, Das discloses that

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

“reputation engine 20 may [receive] applications fingerprints from a plurality of sources such as mobile device 14 [(e.g., through whitelist enforcement module 22)].” Ex. 1006, [0021], [0038]; ~~Ex. 1003, ¶ 57.~~ And a POSITA would have readily-understood that the foregoing “report[ing]” (“*sending . . .*”) would had to have been performed in-~~“real-time” (“at runtime”) “for applications associated with~~ “real-time” (“at runtime”) “for applications associated with an execution attempt in mobile device 14” (“*applications executing on the monitored device at runtime*”) so that the “evaluation of [those] applications to determine their respective trust status is performed in real-time” “using one or more trust evaluation techniques in real-time (e.g., using reputation engine 20 and other components).” Ex. 1006, [0055], [0048]; ~~Ex. 1003, ¶ 57.~~ For example, Das discloses that such reporting (“*sending . . .*”) could be performed “in response to . . . an attempt to perform a particular action by a particular application 34 installed on mobile device 14” (“*at runtime*”). See Ex. ~~1006, [0037], [0055]; Ex. 1003, ¶ 57. Additionally, as discussed above, a POSITA would have understood that the term “runtime” is interchangeable with the term “real-time,” which is confirmed by disclosure of the~~ 1006, [0037], [0055]. Additionally, as discussed above, a POSITA would have understood that the term “runtime” is interchangeable with the term “real-time,” which is confirmed by disclosures in the ‘616 Patent. Ex. 1003, ¶ 57.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~28-58.~~ At least based on the foregoing ~~disclosure~~disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime.*” ~~Ex. 1003, ¶ 58.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 58.~~

- c. “receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime;”

29-59. This claim element is taught by Das. Das discloses a “*trust orchestration server*” in the form of a “[r]eputation engine 20” that is “included in a server in mobile application network 16.” Ex. 1006, [0029]; ~~Ex. 1003, ¶ 59.~~ In other words, the “*trust orchestration server*” ~~can be~~ is found in Das in the form of “a server in mobile application network 16” that includes “reputation engine 20.” Ex. 1006, [0029]; ~~Ex. 1003, ¶ 59.~~

30-60. As discussed above in Section ~~V.B.VII.A.~~ 1.b., Das discloses and/or renders obvious “*the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime.*” ~~Ex. 1003, ¶ 60.~~

31-61. Das further discloses “report[ing] or otherwise ma[king] available to reputation engine 20” that is “included in a server” (“*receiving[] at the trust orchestration server*”) “information about an application or actions of applications” and mobile devices, including “aggregated application fingerprints” (“*dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime*”), to “be evaluated to determine a reputation score of the application.” Ex. 1006, [0055], [0029]; ~~Ex. 1003.~~ Das confirms that the foregoing reported information is received by the

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

“reputation

~~¶ 61. Das confirms that the foregoing reported information is received by the “reputation engine 20”~~
that is “included in a server” (“*receiving[] at the trust orchestration*”

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

server”) by disclosing that “whitelist enforcement modules 22 operating mobile devices 14 in a system can detect security events relating to particular applications and application activities[, such as those part of ‘application fingerprints’ (*“dynamic context . . .”*),] and report such events [(*“dynamic context . . .”*)] to reputation engine 20” that is “included in a server” (*“receiving[] at the trust orchestration server”*) “or other modules for use in determining the trustworthiness of such applications and application activities.” Ex. 1006, [0029], [0053], [0055]~~]; Ex. 1003, ¶ 61.~~

Indeed, as further confirmation, Das discloses that “reputation engine 20 may [receive] applications fingerprints from a plurality of sources such as mobile device 14 [(e.g., through whitelist enforcement module 22)].” Ex. 1006, [0021], [0038]~~]; Ex. 1003, ¶ 61.~~ And a POSITA would have ~~readily~~ understood that the foregoing “receiving” of information by the reputation engine 20 included in a server would had to have been performed in “real-time” (*“at runtime”*) “for applications associated with an execution attempt in mobile device 14” (*“applications executing on the monitored device at runtime”*) so that the “evaluation of [those] applications to determine their respective trust status is performed in real-time” “using one or more trust evaluation techniques in real-time (e.g., using reputation engine 20 and other components).” Ex. 1006, [0055], [0048]~~]; Ex. 1003, ¶ 61.~~ For example, Das discloses that such “receiving” could

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

be performed “in response to . . . an attempt to perform a particular action by a particular application 34 installed on mobile device 14” (“~~*at-runtime*~~”). ~~See Ex. 1006, [0037], [0055]; Ex. 1003, ¶ 61. Additionally, as~~

runtime"). See Ex. 1006, [0037], [0055]. Additionally, as discussed above, a POSITA would have understood that the term "runtime" is interchangeable with the term "real-time," which is confirmed by ~~disclosure of~~disclosures in the '616 Patent. ~~Ex. 1003, ¶ 61.~~

~~32-62.~~ At least based on the foregoing ~~disclosure~~disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious "*receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime.*" ~~Ex. 1003, ¶ 62.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 62.~~

d. "analyzing, by the trust orchestration server, the received endpoint events;"

~~33-63.~~ This claim element is taught by Das. As discussed above in Sections ~~V-B~~VII.A.1.b.-c., Das discloses and/or renders obvious "*the trust orchestration server*" and "*the received endpoint events.*" ~~Ex. 1003, ¶ 63.~~

~~34-64.~~ Das further discloses that "reputation engine 20" that is "included in a server" "evaluat[es]" ("*analyzing[] by the trust orchestration server*") "one or more applications fingerprints of application[s]" ("*dynamic context*"), which include the "security events relating to particular applications and application activities" that the reputation engine 20 receives from whitelist enforcement module 22 ("*the received endpoint events*"). Ex. 1006, [0029], [0031], [0055]; see

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

also Ex. 1006, [0048; ~~Ex. 1003, ¶ 64.~~]. In other words, Das teaches that the

“reputation engine 20” ~~“evaluat[es]”~~

~~“evaluat[es]”~~ the “security events relating to particular applications [~~‘endpoints’~~]

and application activities” that are reported to it (“*analyzing, by the trust orchestration server, the received endpoint events*”), e.g., to “determin[e] the trustworthiness of such applications and application activities.” Ex. 1006, [0029], [0031], [0055]; *see also* Ex. 1006, [0048]; ~~Ex. 1003, ¶ 64.~~ Indeed, Das expressly discloses that “reputation engine 20 may determine a reputation score of application 18 by aggregating and evaluating one or more applications fingerprints of application 18 uploaded to reputation engine 20 by one or more sources,” and that “trust status[es] may be determined using one of the trusted software inventories (e.g., whitelists 30) or may be determined using one or more trust evaluation techniques in real- time (e.g., using reputation engine 20 and other components).” Ex. 1006, [0031], [0048]. Das goes on to explicitly disclose that “aggregated application fingerprints may include aggregated behaviors of the application that may also be evaluated to determine a reputation score of the application,” such as when “whitelist enforcement modules 22 operating mobile devices 14 in a system [] detect[s] security events relating to particular applications and application activities and report[s] such events to reputation engine 20 or other modules for use in determining the trustworthiness of such applications and application activities.” Ex. 1006, [0055]. At least based on the foregoing disclosure from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*analyzing, by the trust orchestration server, the*

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

received endpoint events.” ~~Ex. 1003, ¶ 64.~~

~~35-65~~. Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 64~~.

e. “receiving, by the trust orchestration server, third party network endpoint assessments;”

This claim element is taught by Das. As discussed above in Section

~~V.B.VII.A~~. 1.c., Das discloses and/or renders obvious “*the trust orchestration server*.”

~~Ex. 1003, ¶~~

~~36-66~~. 66. Das further discloses that “reputation engine 20” that is “included in a server” receives (“*receiving, by the trust orchestration server*”) information “from a plurality of sources such as mobile device 14, application software distribution platforms, threat intelligence feeds 32, etc.” Ex. 1006, [0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]; ~~Ex. 1003, ¶ 66~~. Das discloses that the information that “reputation engine 20” (“*the trust orchestration server*”) receives from the “[t]hreat intelligence feeds 32 include[s] threat information,” including “network threat information” (“*network endpoint assessments*”). Ex. 1006, [0023]; ~~Ex. 1003, ¶ 66~~. Das also discloses that the “[t]hreat intelligence feeds 32” that provide the “threat information” to “reputation engine 20” “may be provided by independent third parties” (“*third party*”), thereby making the “network threat information” (“*network endpoint assessments*”) received by the “reputation engine 20” via “[t]hreat intelligence feeds 32” “*third party network endpoint assessments*.” Ex. ~~1006, [0023]; Ex. 1003, ¶ 66~~. At least based on the foregoing

29

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

~~disclosure from Das, a POSITA would have readily understood that Das
discloses and/or renders~~

1006, [0023]. At least based on the foregoing disclosure from Das, a POSITA

would have understood that Das discloses and/or renders obvious “receiving, by

the trust orchestration server, third party network endpoint assessments.” ~~Ex. 1003,
¶ 66.~~

~~37-67.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 67.~~

- f. **“generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments;”**

~~68.~~ This claim element is taught by Das. As discussed above in Sections ~~V.B~~

~~VII.A.1.c.~~ and ~~V.B.VII.A.1.e.~~, Das discloses and/or renders obvious “*the trust orchestration server*” and “*the third party network endpoint assessments.*” ~~Ex. 1003, ¶ 68.~~

~~38-69.~~ Regarding “*temporal events*,” the ’616 Patent discloses that “temporal events 409 [] annotate the state of the endpoints (devices) at scan time,” i.e., at the time of threat evaluation, and that “temporal events 409 can . . . include trust and severity scores.” Ex. 1001, 11:47-48, 11:59-62; ~~Ex. 1003, ¶ 69.~~ As shown here next, Das teaches these same “*temporal events.*” ~~Ex. 1003, ¶ 69.~~

~~39-70.~~ In particular, Das discloses that “reputation engine 20” that is “included in a server” “may calculate reputation scores” (“*generating, by the trust orchestration server, temporal events*”), where the “reputation scores” of Das are the “*temporal events*” recited in this claim element. Ex. 1006, [0020], [0029]; ~~Ex. 1003, ¶ 70.~~ Indeed, Das discloses that “a reputation score . . . may be generated,” and a POSITA would have ~~readily~~ understood from the context of that disclosure in paragraph [0056] of Das that Das discloses that it is “[r]eputation engine 20” that generates that reputation score (“*generating, by the trust orchestration*

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

server, temporal events”). Ex. 1006, [0056]; ~~Ex. 1003, ¶ 70.~~ Das discloses that
“reputation scores” (also referred to

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

as “trust scores”) (“*temporal events*”) “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,” and that “reputation scores” 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,” i.e., when the application was actually evaluated. Ex. 1006, [0019], [0023], [0036], [0046], [0049], [0052], [0072]-[0073], [0076]; ~~Ex. 1003, ¶ 70.~~ As such, the “reputation scores” (“*temporal events*”) stored in “whitelists 30” can “indicate applications and/or application actions determined [at the time of threat evaluation] to be in compliance with a corresponding entity’s policies.” Ex. 1006, [0020]; ~~Ex. 1003, ¶ 70.~~

~~40-71.~~ The fact that Das’s “reputation scores” are indeed “*temporal events*” is confirmed by Das’s explicit ~~disclosure. Ex. 1003, ¶ 71.~~ disclosures. For example, Das discloses that “any threat or vulnerability [associated with a reputation score] may be temporal in nature (e.g., if an application is interacting with an IP address that is temporarily compromised), and components of system 10 may modify the application’s reputation score appropriately in real time to remediate the threat to the host mobile device. For example, reputation engine 20 may incorporate and adjust reputation scores with each additional data point.” Ex.

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

1006, [0055], ~~Ex. 1003, ¶ 71.~~ More specifically, Das discloses that “reputation engine 20 may calculate reputation

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

scores and store the reputation scores in a suitable location along with other information to identify the application.” Ex. 1006, [0020]; ~~Ex. 1003, ¶ 71.~~ Those stored reputation scores provide an indication of “trustworthiness or compliance with one or more mobile application policies enforced in a network or system,” as determined at the time the “reputation engine 20 [] calculate[s the] reputation scores and store[s] the reputation scores.” Ex. 1006, [0073], [0020]; ~~Ex. 1003, ¶ 71.~~ Das discloses that later, “reputation engine 20 may calculate an updated reputation score . . . [that] may be distributed to all other mobile devices on which the application is installed.” Ex. 1006, [0057]; ~~Ex. 1003, ¶ 71.~~ At least based on the foregoing disclosure from Das, a POSITA would have ~~readily~~ understood that Das’s “reputation scores” disclose and/or render obvious “*temporal events*.” ~~Ex. 1003, ¶ 71.~~

Das further discloses that reputation engine 20 that is included in a server, calculates and updates reputation scores (“*generating, by the trust orchestration server, temporal events*”) based on analysis of (“*based at least in part on analyzing*”) “[t]hreat intelligence feeds 32” that are “provided by independent third parties” and include “network threat information” (“*the third party network endpoint assessments*”). Ex. 1006, [0023], [0020], [0057], [0029]; ~~Ex. 1003, ¶ 72.~~

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

44.72.1. Specifically, Das discloses that “[t]hreat intelligence feeds 32 may be provided to update reputation scores, and/or facilitate analysis of applications by reputation engine 20,” where the “[t]hreat intelligence feeds 32 may be provided by

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

independent third parties” and “include . . . network threat information.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 72.~~ And, as already described above, Das discloses that “reputation engine 20 may calculate reputation scores” and “may calculate an updated reputation score.” Ex. 1006, [0020], [0057]; ~~Ex. 1003, ¶ 72.~~

~~42-73.~~ At least based on the foregoing ~~disclosure~~disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments.*” ~~Ex. 1003, ¶ 73.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 73.~~

g. “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and”

This claim element is taught by Das. As discussed above in Sections ~~V.BVII.A.~~ 1.c.-

~~43-74.~~ ~~V.BVII.A.~~ 1.d. and ~~V.BVII.A.~~ 1.f., Das discloses and/or renders obvious “*the trust orchestration server,*” “*the received endpoint events,*” and “*the generated temporal events.*” ~~Ex. 1003, ¶ 74.~~

~~44-75.~~ Das discloses that “information about an application or actions of applications [(“*received endpoint events*”)] are reported or otherwise made available to reputation engine 20” that is “included in a server” (“*trust orchestration server*”) so that “reputation engine 20 [(“*trust orchestration server*”)] may incorporate and adjust [(“*correlating*”)] reputation scores [(“*the generated*”)]

33

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

temporal events”)] with each additional data point” (“received endpoint events”), e.g., to improve “a statistical confidence level of the reputation score[s].” Ex. 1006, [0055], [0029]; ~~Ex. 1003, ¶ 75-1~~

~~75-1~~. For example, Das explicitly discloses that “knowledge gained from monitoring application activity on any one mobile device [(“received endpoint events”)] may be aggregated and analyzed . . . and correlated [by reputation engine 20 (“correlating, by the trust orchestration server”)] with data from other vectors,” which a POSITA would have readily understood would include the previously determined “reputation scores” associated with “applications and application activities” (“generated temporal events”) so that “reputation engine 20” can “adjust,” “modify,” and/or “update[]” (“correlating, by the trust orchestration server”) those previously determined “reputation scores” (“generated temporal events”) based on “each additional data point” (“received endpoint events”) to improve “a statistical confidence level of the reputation score[s].” Ex. 1006, [0055]-[0057]; ~~Ex. 1003, ¶ 75-1~~

~~75-1~~. Indeed, Das discloses “[c]ollection and analysis of reputation information” by “reputation engine 20,” as well as that an “application’s reputation score” may need to be modified appropriately over time to account for the temporal nature of the threat because “any threat or vulnerability may be temporal in nature (e.g., if an application is interacting with an IP address that is temporarily compromised).”

See Ex. 1006, [0029], [0055]; ~~Ex. 1003, ¶ 75-1~~. For example, Das discloses that “the identification of undesirable functionality within an application can serve as the basis for a lower

overall reputation score for the application or the identified application functions.”

Ex. 1006, [0061]; ~~Ex. 1003, ¶ 75.~~ Das discloses numerous examples of the correlation described in this paragraph. *See, e.g.,* Ex. 1006, [0019], [0044]-[0045], [0055]-[0057], [0061]; ~~Ex. 1003, ¶ 75.~~

~~45-76.~~ At least based on the foregoing ~~disclosure~~disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.*” ~~Ex. 1003, ¶ 76.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 76.~~

h. “generating, by the trust orchestration server, an integrity profile for the system.”

~~46-77.~~ This claim element is taught by Das. As discussed above in Section ~~V.B.VII.A.1.c.~~, Das discloses and/or renders obvious “*the trust orchestration server.*” ~~Ex. 1003, ¶ 77.~~

~~47-78.~~ Das discloses that “[r]eputation engine 20” that is “included in a server” (“*trust orchestration server*”) “generate[s]” “reputation score[s].” Ex. 1006, [0029], [0056]; ~~Ex. 1003, ¶ 78.~~ Indeed, Das discloses that “reputation engine 20 may calculate reputation scores.” Ex. 1006, [0020]; ~~Ex. 1003, ¶ 78.~~ Das further discloses that those “[r]eputation scores can be used to build whitelists,” where a whitelist may be an “*integrity profile.*” Ex. 1006, [0046]; ~~Ex. 1003, ¶ 78.~~ In other words, Das discloses that “[r]eputation engine 20” “generate[s]”

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

“reputation score[s]” that are used to “build [(“*generat[e]*”)] whitelists”

(“*generating, by the trust orchestration server, an integrity profile*”). Ex. 1006,

[0029], [0056], [0046]; ~~Ex. 1003, ¶ 78.~~ A POSITA would have

~~readily~~ understood that at least the foregoing disclosure from Das discloses and/or renders

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

obvious “*generating, by the trust orchestration server, an integrity profile.*” ~~Ex. 1003, ¶ 78.~~ Indeed, Das expressly discloses that “whitelists [are] generated” from “reputations,” and a POSITA would have readily understood from the context of that disclosure in paragraph [0031] of Das that Das discloses that it is “reputation engine 20” that generates the whitelists (“*generating, by the trust orchestration server, an integrity profile*”). Ex. 1006, [0031]; ~~Ex. 1003, ¶ 78.~~

~~48-79.~~ Das further discloses that “a particular whitelist” (“*integrity profile*”) may be for a “mobile device, its user, network, etc.” (“*for the system*”). Ex. 1006, [0033]; ~~Ex. 1003, ¶ 79.~~ Similarly, Das discloses that a “whitelist[]” (“*integrity profile*”) can be for “a plurality of different mobile devices, mobile operating systems, mobile device manufacturers, network service providers, enterprises, and other entities and groupings” (“*for the system*”) Ex. 1006, [0046]; ~~Ex. 1003, ¶ 79.~~ Das also discloses that the “network” may include “system 10” that includes “a network 12 connecting one or more mobile devices 14 with mobile application network 16.” Ex. 1006, [0046]; ~~Ex. 1003, ¶ 79.~~

~~49-80.~~ At least based on the foregoing disclosure from Das, a POSITA would have readily understood that Das discloses and/or renders obvious “*generating, by the trust orchestration server, an integrity profile for the system.*” ~~Ex. 1003, ¶ 80.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 80.~~

~~50-81.~~ In light of the foregoing, claim 1 is ~~unpatentable as~~ obvious over in light of Das. ~~Ex.~~

~~1003, ¶ 81.~~

2. Claim 2

~~51-82.~~ Claim 2 depends on claim 1 and further recites “*wherein the third party network endpoint assessments are received from an endpoint assessment service.*” Das discloses and/or renders obvious all elements of claim 2.

~~52-83.~~ As discussed above in Section ~~V-BVII.A.~~, i.e., Das teaches “*receiving, by the trust orchestration server, third party network endpoint assessments.*” ~~Ex. 1003, ¶ 83.~~ Das further discloses that the “[t]hreat intelligence feeds 32” that include “network threat information” (“*the third party network endpoint assessments*”) “may be provided by [(“*are received from*”)] . . . security service providers, or by the enterprise’s (or the network’s) security services” (“*an endpoint assessment service*”). Ex. 1006, [0023]; ~~Ex. 1003, ¶ 83.~~ At least based on the foregoing disclosure from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*wherein the third party network endpoint assessments are received from an endpoint assessment service.*” ~~Ex. 1003, ¶ 83.~~

~~53-84.~~ Therefore, Das discloses and/or renders obvious all elements of claim 2, and claim 2 is ~~unpatentable as~~ obvious over in light of Das. ~~Ex. 1003, ¶ 84.~~

3. Claim 3

~~54-85.~~ Claim 3 depends on claim 2 and recites that the method further

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

comprises “receiving, by the trust orchestration server, integrity measurement and

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

verification reports from the endpoint assessment service.” Das discloses and/or renders obvious all elements of claim 3.

55-86. As discussed above in Section ~~V.B~~ VII.A.2., Das discloses “the endpoint assessment service” in the form of “security service providers” or an “enterprise’s (or the network’s) security services” that provide the “[t]hreat intelligence feeds 32” that include “network threat information.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 86.~~

56-87. Das further discloses that reputation scores and associated trust statuses are determined and/or updated based on security/risk assessments performed by reputation engine 20 and/or threat intelligence feeds 32. Ex. 1006, [0019]-[0020], [0031], [0048], [0057]; see also Ex. 1006, [0023] (“Threat ~~[0031], [0048], [0057]; see also Ex. 1006, [0023]~~ (“Threat intelligence feeds 32 may be provided to update reputation scores . . .”); ~~Ex. 1003, ¶ 87.~~”). Das discloses that the trust statuses of applications (“integrity measurement and verification reports”) that are determined based on the security/risk assessments can be provided to “reputation engine 20” that is “included in a server” (“receiving, by the trust orchestration server”) via the “[t]hreat intelligence feeds ~~32.” Ex. 1006, [0020] [0021], [0023]~~ 32.” Ex.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~{1006, [0020]-[0021], [0023]-[0024], [0029], [0031], [0035], [0053],~~

~~[0055]; Ex. 1003, ¶ 87.].~~ For example, Das discloses that “reputation engine 20”

that is “included in a server” receives (“*receiving, by the trust orchestration*

server”) information “from a plurality of sources such as . . . threat intelligence

feeds 32, etc.” Ex. 1006, [0021], [0023]~~]-[0024], [0029], [0031], [0035], [0053],~~

~~[0055]; Ex. 1003, ¶ 87.].~~ The information~~that~~

that “reputation engine 20” (“*the trust orchestration server*”) receives from the “[t]hreat intelligence feeds 32” includes the trust statuses of applications (“*integrity measurement and verification reports*”) that are determined based on the security/risk assessments and that are used “to update reputation scores” and/or to “facilitate analysis of applications by reputation engine 20.” Ex. 1006, [0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]; ~~Ex. 1003, ¶ 87.~~ A POSITA would have ~~would have readily~~ understood that the information included as part of the trust status information of applications (“*integrity measurement and verification reports*”) that are received by the “reputation engine 20” via the “[t]hreat intelligence feeds 32” would include numerous information, including general “threat information,” “network threat information, . . . vulnerability information, . . . real-time, dynamic, and up-to-date information on a variety of potential threats.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 87.~~

~~57-88.~~ As described above, the “security service providers” or an “enterprise’s (or the network’s) security services” (“*the endpoint assessment service[s]*”) can provide the “[t]hreat intelligence feeds 32” that provide the trust statuses of applications (“*integrity measurement and verification reports*”) to the “reputation engine 20” that is “included in a server” (“*receiving, by the trust orchestration server*”), so a POSITA would have ~~readily~~ understood that the

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

“security service providers” or an “enterprise’s (or the network’s) security services” (“*the endpoint assessment service[s]*”) provide the trust statuses of applications

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

(“integrity measurement and verification reports”) to the “reputation engine 20” that is “included in a server” (“receiving, by the trust orchestration server”). Ex. 1006, [0020]-[0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]; Ex. 1003, ¶ 88. In other words, a POSITA would have readily understood, based at least in part on the disclosed disclosures from Das cited for this limitation, that “reputation engine 20” that is “included in a server” can receive (“receiving, by the trust orchestration server”) the trust statuses of applications (“integrity measurement and verification reports”) from the “security service providers” or an “enterprise’s (or the network’s) security services” (“from the endpoint assessment service[s]”). Ex. 1006, [0020]-[0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]. [0029], [0031], [0035], [0053], [0055]; Ex. 1003, ¶ 88.

58-89. At least based on the foregoing disclosed disclosures from Das, a POSITA would have readily understood that Das discloses and/or renders obvious “receiving, by the trust orchestration server, integrity measurement and verification reports from the endpoint assessment service.” Ex. 1003, ¶ 89.

59-90. Therefore, Das discloses and/or renders obvious all elements of claim 3, and claim 3 is unpatentable as obvious over in light of Das. Ex. 1003, ¶ 90.

4. Claim 4

60-91. Claim 4 depends on claim 1 and further recites “wherein the third

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

party network endpoint assessments are received from one or more collaboration services.” Das discloses and/or renders obvious all elements of claim 4.

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

As discussed above in Section ~~V.B.VII.A.~~ i.e., Das teaches “receiving, by the trust orchestration server, third party network endpoint assessments.” ~~Ex. 1003, ¶ 92.~~ Das further discloses that the “[t]hreat intelligence feeds 32” that include “network threat information” (“the third party network endpoint assessments”) “may be provided by [(“are received from”)] independent third parties” (“one or more collaboration services”). Ex. 1006, [0023]; ~~Ex. 1003, ¶ 92.~~ Das discloses that the “independent third parties” that collaborate to provide the “[t]hreat intelligence feeds 32” may be “one or more sources internal or external to network 12.” Ex. 1006, [0023]; ~~Ex. 1003,~~

~~61.92.¶92.]~~ Das discloses that the collaborative services provided by the “independent third parties” (“one or more collaboration services”) that collaborate via the “[t]hreat intelligence feeds 32” include “web reputation engines, file reputation engines, network threat information, internet protocol (IP) and sender reputation engine, vulnerability information, etc.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 92.]~~. At least based on the foregoing ~~disclosure~~ disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “wherein the third party network endpoint assessments are received from one or more collaboration services.” ~~Ex. 1003, ¶ 92.~~

~~62.93.~~ Therefore, Das discloses and/or renders obvious all elements of claim 4, and claim 4 is ~~unpatentable as~~ obvious over in light of Das. ~~Ex. 1003, ¶ 93.~~

5. Claim 5

~~63-94.~~ Claim 5 depends on claim 4 and recites that the method further comprises “receiving, by the trust orchestration server, integrity measurement and verification reports from the one or more collaboration services.” Das discloses and/or renders obvious all elements of claim 5.

~~64-95.~~ As discussed above in Section ~~v-B VII.A.4.~~, Das discloses “the one or more collaboration services” in the form of “independent third parties” that collaborate to provide the “[t]hreat intelligence feeds 32” that include “network threat information.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 95.~~

~~65-96.~~ Das further discloses that reputation scores and associated trust statuses are determined and/or updated based on security/risk assessments performed by reputation engine 20 and/or threat intelligence feeds 32. Ex. 1006, [0019]-[0020], [0031], [0048], [0057]; *see also* Ex. 1006, [0023] (“Threat ~~[0031], [0048], [0057]; see also Ex. 1006, [0023]~~ (“Threat intelligence feeds 32 may be provided to update reputation scores . . .”); ~~Ex. 1003, ¶ 96.~~”). Das discloses that the trust statuses of applications (“integrity measurement and verification reports”) that are determined based on the security/risk assessments can be provided to “reputation engine 20” that is “included in a server” (“receiving, by the trust orchestration server”) via the “[t]hreat intelligence feeds ~~32.” Ex. 1006, [0020]-[0021], [0023]~~.”

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

32.” Ex. 1006, [0020]-[0021], [0023]-[0024], [0029], [0031], [0035], [0053],

[0055]; Ex. 1003, ¶ 96. For example, Das discloses that “reputation engine 20”
that is “included in

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

a server” receives (“*receiving, by the trust orchestration server*”) information “from a plurality of sources such as . . . threat intelligence feeds 32, etc.” Ex. 1006, [0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]; ~~Ex. 1003, ¶ 96.~~

The information ~~that~~ that “reputation engine 20” (“*the trust orchestration server*”) receives from the “[t]hreat intelligence feeds 32” includes the trust statuses of applications (“*integrity measurement and verification reports*”) that are determined based on the security/risk assessments and that are used “to update reputation scores” and/or to “facilitate analysis of applications by reputation engine 20.” Ex. 1006, [0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]; ~~Ex. 1003, ¶ 96.~~ A POSITA would have ~~would have readily~~ understood that the information included as part of the trust status information of applications (“*integrity measurement and verification reports*”) that are received by the “reputation engine 20” via the “[t]hreat intelligence feeds 32” would include numerous information, including general “threat information,” “network threat information, . . . vulnerability information, . . . real-time, dynamic, and up-to-date information on a variety of potential threats.” Ex. 1006, [0023]; ~~Ex. 1003, ¶ 96.~~

~~66-97.~~ As described above, the collaborative “independent third parties” (“*the one or more collaboration services*”) can provide the “[t]hreat intelligence

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

feeds 32” that provide the trust statuses of applications (“*integrity measurement and verification reports*”) to the “reputation engine 20” that is “included in a server” (“*receiving, by the trust orchestration server*”), so a POSITA would have

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

~~readily~~ understood that the collaborative “independent third parties” (“*the one or more collaboration services*”) provide the trust statuses of applications (“*integrity measurement and verification reports*”) to the “reputation engine 20” that is “included in a server” (“*receiving, by the trust orchestration server*”). Ex. 1006, [0020]-[0021], [0023]-~~[]~~[0024], [0029], [0031], [0035], [0053], [0055]; ~~Ex. 1003, ¶ 97.~~ In other ~~words, a~~ words, a POSITA would have ~~readily~~ understood, based at least in part on the disclosure from Das cited for this limitation, that “reputation engine 20” that is “included in a server” can receive (“*receiving, by the trust orchestration server*”) the trust statuses of applications (“*integrity measurement and verification reports*”) from the collaborative “independent third parties” (“*from the one or more collaboration services*”). Ex. 1006, [0020]-[0021], [0023]-[0024], [0029], [0031], [0035], [0053], [0055]; ~~Ex. 1003, ¶ 97.~~

~~67-98.~~ At least based on the foregoing ~~disclosure~~disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*receiving, by the trust orchestration server, integrity measurement and verification reports from the one or more collaboration services.*” ~~Ex. 1003, ¶ 98.~~

~~68-99.~~ Therefore, Das discloses and/or renders obvious all elements of claim 5, and claim 5 is ~~unpatentable as~~ obvious overin light of Das. ~~Ex. 1003, ¶ 99.~~

6. Claim 6

69-100. Das discloses and/or renders obvious all elements of claim 6.

- a. **“The method of claim 1, wherein the endpoint events of the monitored device are received by a system event correlator of the trust orchestration server from endpoint trust agents, and”**

70-101. This claim element is taught by Das. Das discloses that “information about an application or actions of applications” and mobile devices, including the “security events relating to particular applications and application activities” (“*the endpoint events of the monitored device*”), “are reported or otherwise made available to reputation engine 20” that is “included in a server” (“*are received by a system event correlator of the trust orchestration server*”) from “whitelist enforcement modules 22” (“*from endpoint trust agents*”). Ex. 1006, [0055], [0029]; ~~Ex. 1003, ¶ 101.~~ A POSITA would have ~~readily~~ understood that “reputation engine 20” functions as, and therefore discloses and/or renders obvious, “*a system event correlator*” based at least on the fact that “reputation engine 20” includes functionality to “aggregate[,]” “evaluate[,]” “analyze[,]” and “correlate[.]” “information about an application or actions of applications” and mobile devices, including the system “security events relating to particular applications and application activities” (“*the endpoint events of the monitored device*”). Ex. 1006, [0055], [0029]; ~~Ex. 1003, ¶ 101.~~

71-102. At least based on the foregoing ~~disclosure~~disclosures from Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “*wherein the endpoint events of the monitored device are received by a*

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

system event correlator~~of the trust orchestration server from endpoint trust~~
~~agents.”~~ Ex. 1003, ¶ 102. Therefore, this claim element is obvious. Ex. 1003, ¶
102.

of the trust orchestration server from endpoint trust agents.” Therefore, this claim element is obvious.

- b. “The method of claim 1, wherein . . . the temporal events are generated by a trust broker of the trust orchestration server and are received by the system event correlator from the trust broker.”

72-103. This claim element is taught by Das. A POSITA would have ~~readily~~ understood that “reputation engine 20” that is “included in a server” functions as, and therefore discloses and/or renders obvious, “a trust broker of the trust orchestration server” based at least on the fact that “reputation engine 20” includes functionality to receive “threat information” from the “[t]hreat intelligence feeds 32” “to determine a reputation score of the application,” “to update reputation scores, and/or [to] facilitate analysis of applications,” i.e., to broker the trust assessments of applications. Ex. 1006, [0023], [0029], [0055]; ~~Ex. 1003, ¶ 103-1~~. Das discloses that “reputation engine 20” that is “included in a server” “may calculate reputation scores” (“the temporal events are generated by a trust broker of the trust orchestration server”). Ex. 1006, [0020], [0029]; ~~Ex. 1003, ¶ 103-1~~. Indeed, Das discloses that “a reputation score . . . may be generated,” and a POSITA would have ~~readily~~ understood from the context of that disclosure in paragraph [0056] of Das that Das discloses that it is “[r]eputation engine 20” that generates that reputation score (“the temporal events are generated by a trust broker of the trust orchestration server”).

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

Ex. 1006, [0056]; ~~Ex. 1003, ¶ 103.~~ Because the “reputation scores” generated by the “*trust broker*”

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

functionality of the “reputation engine 20” (“*temporal events [] generated by a trust broker of the trust orchestration server*”) are used by the “*system event correlator*” functionality of the “reputation engine 20,” e.g., “to update reputation scores” or to “incorporate and adjust reputation scores with each additional data point,” the internal operations of the “reputation engine 20” inherently include “*the temporal events . . . [being] received by the system event correlator from the trust broker.*” Ex. 1006, [0055], [0023]; ~~Ex. 1003, ¶ 103.~~

~~73.104.~~ At least based on the foregoing ~~disclosure from~~disclosures of Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious that “*the temporal events are generated by a trust broker of the trust orchestration server and are received by the system event correlator from the trust broker.*” ~~Ex. 1003, ¶ 104.~~ Therefore, this claim element is obvious. ~~Ex. 1003, ¶ 104.~~

~~74.105.~~ In light of the foregoing, Das discloses and/or renders obvious all elements of claim 6, and thus claim 6 is ~~unpatentable as~~ obvious ~~over~~in light of Das. ~~Ex. 1003, ¶ 105.~~

7. Claim 7

~~75.106.~~ Claim 7 depends on claim 1 and recites that the method further comprises “*performing, by a malware analyzer, detection of code obfuscation and evasion techniques in reverse engineered code of the applications, the code*

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

obfuscation and evasion techniques including at least one of: multiple packing,

Petition for Inter Partes Review of U.S. Patent No. 9,092,616

anti-debug, anti-trace, anti-memory, and anti-emulation.” Das discloses and/or renders obvious all elements of claim 7.

76-107. Das discloses “malware prevention” performed by a “reputation engine 20” (“*performing, by a malware analyzer*”) based on “reputation scores” “calculat[ed]” by “reputation engine 20.” See Ex. 1006, [0029]; ~~Ex. 1003, ¶ 107.~~ Das discloses that the “malware prevention” techniques that are used to “resolve these [malware] issues” include detection of “hostile, intrusive, or annoying programming (e.g., code, script, 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[, such as when] . . . an application on a mobile phone could be remotely controlled, and configured to turn on the phone’s camera and microphone, permitting spying[, or when] . . . an application may track a user’s location and convey that information to unauthorized persons[, or when] . . . malicious applications may provide a pathway for unauthorized access to critical and proprietary information, inappropriate use of resources, business interruptions, fraud, and security breaches” (“*detection of code obfuscation and evasion techniques in reverse engineered code of the applications, the code obfuscation and evasion techniques including at least one of: multiple packing, anti-debug, anti-trace, anti-memory, and anti-emulation*”). Ex. 1006, [0028]-[0029]; ~~Ex. 1003, ¶ 107.~~

~~77.108.~~ 77.108. At least based on the foregoing ~~disclosure from~~ disclosures of Das, a POSITA would have ~~readily~~ understood that Das discloses and/or renders obvious “performing, by a malware analyzer, detection of code obfuscation and evasion techniques in reverse engineered code of the applications, the code obfuscation and evasion techniques including at least one of: multiple packing, anti-debug, anti-trace, anti-memory, and anti-emulation.” ~~Ex. 1003, ¶ 108.~~

~~78.109.~~ 78.109. Therefore, Das discloses and/or renders obvious all elements of claim 7, and claim 7 is ~~unpatentable as~~ obvious over in light of Das. ~~Ex. 1003, ¶ 109.~~

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 or~~

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

~~PGR in view of parallel district court litigation where a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or 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).~~

Petitioner stipulates that, should the Board institute 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).

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 '616 Patent. The '616 Owner or 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-cv-00441; *Taasera Licensing LLC v. Check Point Software Technologies Ltd.*, Case No. 2:22-cv-00063; *Taasera Licensing LLC v. Palo Alto*~~

~~Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616~~

~~*Networks, Inc.*, Case No. 2:22-cv-00062; *In re: Taasera Licensing LLC, Patent*~~

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

~~Litigation, Case No. 2:22-md-03042; Trend Micro Inc. v. Taasera Licensing LLC, Case No. 2:22-cv-00303; Palo Alto Networks, Inc. v. Taasera Licensing LLC et al., Case No. 2:22-cv-00314; Taasera Licensing LLC v. Fortinet, Inc., Case No. 2:22-cv-00415; Taasera Licensing LLC v. Musarubra US, LLC, Case No. 2:22-cv-00427; Taasera Licensing LLC v. CrowdStrike, Inc. et al., Case No. 2:22-cv-00468. The '616 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-cv-00477; Trend Micro, Inc. v. Taasera Licensing LLC, Northern District of Texas Case No. 3:22-cv-00518; Palo Alto Networks, Inc. v. 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 (<i>pro hac vice</i> to be filed)

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

Lead Counsel for Petitioner	Backup Counsel for Petitioner
	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 (<i>pro hac vice</i> to be filed)

D. — Electronic Service

Petitioner consents to electronic service at:

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

V. — Fees

79.110. All fees Owner's expert declarant may be charged to Deposit Account No. 50-4814 assert during any instituted *inter partes* review.

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 Claims claims 1-7 of the '616 Patent are unpatentable.

Dated: March 13, 2023 _____ Respectfully submitted,

/ Juan C. Yaquian /
Juan C. Yaquian
WINSTON & STRAWN LLP

~~Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616~~

~~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~~

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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. 9,092,616

CERTIFICATE OF COMPLIANCE

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

~~80.111. § 42.24(a)(1)(i) because this Petition contains 9,435 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 prior art reference 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. 9,092,616

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. 9,092,616**” and Exhibits 1001-1006 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. 9,092,616:

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

81.112. ~~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

Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

USPTO Reg. No. 70,755

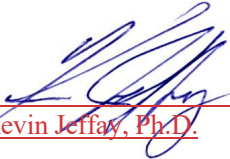
Petition for *Inter Partes* Review of U.S. Patent No. 9,092,616

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. 9,092,616

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.