UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,

Petitioner,

v.

TAASERA LICENSING LLC,

Patent Owner.

Patent No. 9,923,918
Filing Date: March 27, 2017
Issue Date: March 20, 2018

Inventors: Blair Nicodemus and Billy Edison Stephens
Title: METHODS AND SYSTEMS FOR CONTROLLING ACCESS TO COMPUTING RESOURCES BASED ON KNOWN SECURITY VULNERABILITIES

DECLARATION OF DR. ERIC COLE

Case No. IPR2023-00574

Taasera's Exhibit No. 2004, IPR2023-00574
Page 001

I, Eric Cole, Ph.D., declare as follows:

I. BACKGROUND AND QUALIFICATIONS

1. The details of my education, work experience, and research are summarized in my curriculum vitae ("CV") which is attached to this Report as **Exhibit A**. I have summarized some of the relevant information about my experience and qualifications below.

2. I hold a master's degree in Computer Science and a doctorate in Information Security and have worked in the cyber and technical information security industry for over 25 years. During this time, I have actively been involved with the design and development of a wide range of software products. I am fully aware of both the process of developing software and the importance and criticality of keeping software up-to-date and current based on changing market conditions.

3. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

4. I am the founder of Secure Anchor Consulting where I provide cyber security consulting services and lead research and development initiatives to advance information systems security. I was a Fellow and instructor with The SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world.

Taasera's Exhibit No. 2004, IPR2023-00574
Page 002

5. I am an author of several security courses, such as SEC401-Security Essentials and SEC501-Enterprise Defender.

6. In addition, I have also been the curriculum lead for cyber defense for SANS, which involves overseeing the management and creation of new courses in addition to all of the existing courses.

7. I have worked for the government for 8 years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have held various top-secret security clearances with the Department of Defense (DOD), Central Intelligence Agency (CIA), and the Nuclear Regulatory Commission (NRC). I have worked for a wide range of government organizations including the Federal Bureau of Investigation (FBI), National Security Agency, CIA, Department of Energy, DOD, the Treasury, Secret Service and the NRC.

8. While serving as a Senior Officer for the CIA as Program Manager and Technical Director for the Internet Program Team with the Office of Technical Services, I implemented the Internet Program Team that designs, develops, tests, and deploys Internet security products in 3- to 6-month intervals. In this role, I received a letter of appreciation from the Director of Central Intelligence (DCI) and six Exceptional Performance Awards.

9. As a member of the Information Security Assessment Team with the

Office of Security, I also evaluated and performed security assessment of network operating systems to identify potential vulnerabilities and solutions. I also designed a large scale auditing system with automated review capability and worked on several virus investigations for the Office of Security.

10. In my role as Chief Information Officer for the American Institutes for Research, I have repaired and developed IT infrastructures for various organizations and provided technical support for the Defense Advanced Research Projects Agency (DARPA), an agency of the DOD responsible for the development of new technologies for use by the military.

11. As Chief Scientist and Senior Fellow for Lockheed Martin ("Lockheed"), I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as technical advisor in high-profile security projects for government clients including the DOD, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

12. At Lockheed I was actively involved in negotiating licensing agreements for technology both created by Lockheed and owned by other entities.

Taasera's Exhibit No. 2004, IPR2023-00574
Page 004

In the course of negotiating the contracts, I would need to determine the value of the technology that would be licensed so a dollar value could be attributed to the technology. The methodology of apportionment I used in this Report is the same method that I utilized at Lockheed. Based on my decades-long experience in negotiating contracts, this process is not purely mathematical in nature because this is not a math problem and cannot be solved with straight math. Instead, it is a quantitative estimate based on experience and the documents and evidence available to perform the analysis. The process used at Lockheed involved taking the totality of a system and breaking the system in relative pieces of technology and assigning a percent value to each of those components so that we could evaluate the product during our negotiations. This allows for one to be able to determine the percentage of value or apportionment that a certain technology contributes to the overall product. The methodology that has been well accepted at Lockheed and in other cases I have worked is the same methodology that I have used in this case.

13. As Chief Technical Officer for McAfee, I executed the technology strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. I was responsible for the development of new products, and the ongoing challenge of keeping existing products up-to-date and relevant in the market. In this capacity, I worked closely with groups tasked with the development of intellectual property.

Taasera's Exhibit No. 2004, IPR2023-00574
Page 005

14. At McAfee, I was frequently involved in evaluating gaps in our technology and performing a buy or build analysis. This involved determining whether we should try to build the technology in house or buy the technology from a third party. Since it is often quicker to buy a technology, I was actively involved in evaluating the value of a given technology, including assigning a quantitative value to the technology. During the buy analysis, we would often find patented technology we wished to license and, in order to determine how much we were willing to pay, I had to determine how much value would the technology contribute to the overall product and use those apportionment values to determine how much profit we would make by adding this technology to the product. This process cannot be broken into a simple math problem because this cannot be solved with straight math. It instead is a quantitative estimate based on experience and the documents and evidence available to perform the analysis.

15. I have prepared this Declaration as an expert witness retained by Taasera Licensing LLC. In this Declaration, I provide my opinions as to whether the Challenged Claims of U.S. Patent No. 9,923,918 (the "'918 Patent") are valid. I provide technical bases for these opinions as appropriate.

16. This Declaration contains statements of my opinions formed to date and the bases and reasons for those opinions. I may offer additional opinions based on further review of the materials in this proceeding, including opinions and/or

testimony of other expert witnesses.

17. My time in this matter is being compensated at a customary rate of $700 per hour. My compensation is not dependent upon the substance of the opinions I offer herein, the outcome of this proceeding, or any issues involved in or related the '918 patent. I have no financial interest in, or affiliation with, any of the real parties in interest or the patent owner.

II. MATERIALS CONSIDERED

18. The materials I considered include the '918 patent and the prosecution history for the '918 Patent. I also considered the materials that I refer to and that I cite in this declaration.

19. I also considered all papers and exhibits filed in IPR2023-00574 including the petition ("Pet.") and the declaration of Dr. John Black.

20. I have also considered the Board's Decision on Institution (IPR2023-00574, Paper 7) ("Inst.") in this proceeding.

21. I have also considered any exhibits attached to the Patent Owner's Response in this proceeding, including the deposition transcript of Dr. John Black.

22. In addition, I have drawn on my experience and knowledge, as discussed above and described more fully in my CV.

III. LEGAL PRINCIPLES

23. I understand that a patent claim is unpatentable as "obvious" if the

subject matter of the claim as a whole would have been obvious to a person of ordinary skill in the art as of the time of the invention at issue.

24. I understand that the use of the "person of ordinary skill" rubric is to prevent one from improperly, in the present day, using hindsight to decide whether a claim is obvious.

25. I understand that the following factors must be evaluated to determine whether the claimed subject matter is obvious: (1) the scope and content of the prior art; (2) the difference or differences, if any, between the scope of the patent claim and the scope of the prior art; and (3) the level of ordinary skill in the art at the time of the invention.

26. I understand that, unlike anticipation, which allows consideration of only one item of prior art, obviousness may be shown by considering more than one item of prior art. I understand that, when considering a combination of prior art references as part of an obviousness analysis, it can be important to ascertain if the references are from the same field of endeavor and also to ascertain whether there is any reason that would have prompted a person of ordinary skill in the relevant art to combine the elements in the way the claim does. In other words, a claim generally cannot be rendered obvious by combining (i) art from across different fields, including outside the field of the claimed invention, or (ii) art that itself teaches away from combination with other art that would otherwise provide its missing limitations,

or (iii) art for which there is not at least an articulable, common sense reason to bridge the gap between its disclosure and the claim at issue.

27. Moreover, I understand that so-called "objective indicia of nonobviousness," also known as "secondary considerations," are also to be considered when assessing obviousness. I understand that this objective evidence includes at least: the commercial success of the invention; the long felt but unresolved need to develop the invention; any praise of the invention in the market; and copying by others. I also understand that evidence of objective indicia of non-obviousness must be commensurate in scope with the claimed subject matter; *i.e.*, that there must be a nexus or connection between the criteria and the claim itself.

28. I understand that the disclosure of an asserted prior art reference must provide an enabling disclosure of the desired subject matter and that mere naming or description of the subject matter is insufficient; to be enabling, I understand that it must be able to be produced without undue experimentation.

29. I understand that I must construe a claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and consistent with the prosecution history pertaining to the patent.

IV. LEVEL OF ORDINARY SKILL IN THE ART

26. I understand that I should perform my analysis from the viewpoint of a person of ordinary skill in the art. I understand that this hypothetical person of

Taasera's Exhibit No. 2004, IPR2023-00574
Page 009

ordinary skill in the art is considered to have the normal skills of a person in a certain technical field. I understand that factors that may be considered in determining the level of ordinary skill in the art include: (1) the education level of the inventor; (2) the types of problems encountered in the art; (3) the prior art solutions to those problems; (4) rapidity with which innovations are made; (5) the sophistication of the technology; and (6) the education level of active workers in the field.

27. In my opinion, a person of ordinary skill in the art would have had a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cyber security, or a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields. 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. This aligns with Petitioner's proposed level of skill in the art. Pet. at 3.

28. My qualifications and experience exceed those of a person of ordinary skill in the art. Nonetheless, my analysis and opinions herein regarding the '918 patent are given from the perspective of a person of ordinary skill in the art.

V. CLAIM CONSTRUCTION

29. I have been informed by Counsel that, for purposes of my analysis in this *inter partes* review proceeding, claim terms should be given their ordinary and

Taasera's Exhibit No. 2004, IPR2023-00574
Page 010

customary meaning within the context of the patent in which the terms are used, *i.e.*, the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention in light of what the patent teaches, unless it appears that the inventors were using them to mean something else. Additionally, the specification and prosecution history must be consulted to confirm whether the patentee has acted as his/her own lexicographer (*i.e.*, provided special meaning to any disputed terms), or intentionally disclaimed, disavowed, or surrendered any claim scope).

30. I have further been informed by Counsel that a person of ordinary skill in the art is deemed to read a claim term not only in the context of the particular claim in which the disputed term appears, but also in the context of the entire patent, including the specification and the prosecution history. The prosecution file history provides evidence of how both the Patent Office and the inventors understood the terms of the patent, particularly in light of what was known in the prior art. Further, where the specification describes a claim term broadly, arguments and amendments made during prosecution may require a more narrow interpretation. For these reasons, the words of the claim must be interpreted in view of, and be consistent with, the entire specification. The specification is the primary basis for construing the claims and provides a safeguard such that correct constructions closely align with the specification. Ultimately, the interpretation to be given a term can only be

Taasera's Exhibit No. 2004, IPR2023-00574
Page 011

determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim as set forth in the patent itself.

31. I have further been informed by Counsel that, to determine how a person of ordinary skill would understand a claim term, one should look to those sources available that show what a person of skill in the art would have understood disputed claim language to mean. Such sources include the words of the claims themselves, the remainder of the patent's specification, the prosecution history of the patent (all considered "intrinsic" evidence), and "extrinsic" evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art. I understand that one looks primarily to the intrinsic patent evidence, but extrinsic evidence may also be useful in interpreting patent claims when the intrinsic evidence itself is insufficient. Additionally, the context in which a term is used in the Asserted Claims can be highly instructive. Likewise, other claims of the patent in question, both asserted and not asserted, can inform the meaning of a claim term. For example, because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

32. I have further been informed by Counsel that, while intrinsic evidence is of primary importance, extrinsic evidence, *e.g.*, all evidence external to the patent

Taasera's Exhibit No. 2004, IPR2023-00574
Page 012

and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises, can also be considered. For example, technical dictionaries may help one better understand the underlying technology and the way in which one of skill in the art might use the claim terms. Extrinsic evidence should not be considered, however, divorced from the context of the intrinsic evidence. Evidence beyond the patent specification, prosecution history, and other claims in the patent should not be relied upon unless the claim language is ambiguous in light of these intrinsic sources. Furthermore, while extrinsic evidence can shed useful light on the relevant art, it is less significant than the intrinsic record in determining the legally operative meaning of claim language.

33. I have been asked to provide my opinion on the differences between "operating conditions" and "status information about the plurality of operating conditions," in the context of the '918 Patent specification and claims.

34. In my opinion, a POSITA reading the '918 Patent specification and the claims themselves would consider "operating conditions" to possess a different meaning than "status information about the plurality of operating conditions," as described more fulsomely in Sections VI.A and VI.B below.

Taasera's Exhibit No. 2004, IPR2023-00574
Page 013

VI. CHENG DOES NOT RENDER CLAIMS 1-24 OBVIOUS

A. Cheng Does Not Render Obvious "*providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies*," "*maintaining the plurality of policies in a data store on the computing system*," "*identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate,*" and "*configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions*," as Required by Claim 1

35. In my opinion, Petitioner incorrectly alleges that the claimed "plurality of policies" is disclosed by Cheng's ***rules*** (also called policy rules) that identify operating conditions: "***Rules*** are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date." *See* Pet. at 17-18 (citing to Ex. 1004, 8:30-34). But a POSITA would not consider Cheng's rules to be the claimed "plurality of policies" because the claimed "plurality of policies" identify "operating conditions." In my opinion, Petitioner incorrectly asserts that "Cheng discloses [] a plurality of operating conditions on the endpoint (i.e., ***the assessed posture of the client machine, as determined based on the standards for adequacy for particular protective measures that are met,*** such as a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware on the client machine)." Pet. at 18. But the claimed operating conditions cannot be the assessed posture of the client machine when an assessment of the

Taasera's Exhibit No. 2004, IPR2023-00574
Page 014

endpoint (or the "determining" claim limitation) has not even occurred yet. Claim 1 is clear that the compliance state of the endpoint (*e.g.*, any assessed posture of the endpoint) is "determin[ed], by the computing system, … based on the status information [about the plurality of operating conditions] and a plurality of compliance policies in the data store." Ex. 1001, Claim 1. Put simply, the compliance state or any assessed posture of the client machine is determined based, in part, on the status information about the plurality of operating conditions, and cannot be the operating conditions itself.

B. Cheng Does Not Render Obvious "*receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint*," as Required by Claim 1

36. In my opinion, since Petitioner fails to show how Cheng discloses, teaches, or suggests "identifying, from the plurality of policies, a plurality of operating conditions," as I described in Section VI.A, it therefore cannot disclose, teach, or suggest "receiving…status information about the plurality of operating conditions."

37. Petitioner also argues that Cheng's "results or sum evaluation of the checks" disclose the claimed "status information about the plurality of operating conditions." Pet. at 21. In my opinion, this position does not make sense in view of Petitioner's previous allegation that "operating conditions" are the "***the assessed***

Taasera's Exhibit No. 2004, IPR2023-00574
Page 015

posture of the client machine" (Pet. at 18) because Cheng's "results or sum evaluation of the checks" ***are*** the "assessed posture of the client machine." Cheng explicitly says that checks ***are*** posture evaluation elements or at the very least are "elements" of the "assessed posture of the client machine."

> Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.

Ex. 1004, 8:39-42. My understanding is that Petitioner's expert confirmed that Petitioner failed to differentiate between the two terms "status information" and "operating conditions" by asserting that "status information is more or less synonymous with operating condition":

> Q. Yeah, I mean, just to clarify that more, you're saying the -- in the example you gave, are you saying that the operation condition, you know, is that [antivirus] version number, for example?
>
> A. All the measurements taken by the client software I would call, you know, operating conditions in this context.
>
> Q. And each of the measurements would be an operating condition -- an operating condition?
>
> A. I think that's fair."
>
> Q. And just to really clarify that, so in the example you gave, the [antivirus] version is the operating condition; The status information is whether that version meets a threshold. Is that right?
> …
> A. No, I would say status information is also more or less

Taasera's Exhibit No. 2004, IPR2023-00574
Page 016

> synonymous with operating condition. The status information includes the measurements taken by the client endpoint.

Ex. 2005, 54:4-22.

38. I agree with Petitioner's expert, who acknowledges that Cheng's client software (*i.e.*, software agents) only takes measurements instead of actively derive status information from operating conditions, as the claim requires. *See* Ex. 2005, 45:25-46:9 ("I wouldn't characterize the client software as determining the compliance state, because, as I said a moment ago, Cheng describes situations where it may be possible to determine the compliance state, but also situations where the client software really is kind of just a dumb service that's saying, I took some measurements, here they are, and it doesn't really try and ascertain what the ultimate determination is going to be based on those measurements."). In my opinion, this "dumb service" of Cheng is exactly what the '918 patent describes as inadequate prior art:

> Today's access control solutions still lack significant functions and capabilities. As one example, they lack the ability to form context-based access control decisions **using as decision inputs state information provided by point solutions that are not context aware**.

Ex. 1001, 3:7-11. Like the prior art discussed in the '918 Patent specification, Cheng's client agents are "point solutions that are not context aware" and do not pull status information about operating conditions, but, at most, only the operation

Taasera's Exhibit No. 2004, IPR2023-00574
Page 017

conditions themselves. In my opinion, this distinction is made even clearer in the '918 Patent specification, which shows that software agents must be context aware because status information is another level of data "subsequent to" the plurality of policies identifying operation conditions:

> Subsequent to identifying the various conditions to be monitored within endpoint system **104** (step **202),** the various 55 agents **104E** and agent managers **104D** and agent monitor(s) **104C** are identified and configured for monitoring those various conditions (step **204).** For example an agent manager **104D** may be configured to query a vendor-specific API exposed by a third party antivirus agent, may be configured to 60 query an operating system service periodically to determine if the endpoint has an active network interface and if so, the IP address of that interface, etc.

Ex. 1001, 14:58-67.

C. Cheng Does Not Disclose "*determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store*" as Required by Claim 1

39. In my opinion, since Petitioner fails to show how Cheng discloses, teaches, or suggests a "plurality of policies," as I described in Section VI.A, it therefore cannot disclose, teach, or suggest "determining, by the computing system, a compliance state of the endpoint based on … a plurality of compliance policies in the data store."

40. In my opinion, since Petitioner fails to show how Cheng discloses, teaches, or suggests "receiving, across a network, at the computing system, status

Taasera's Exhibit No. 2004, IPR2023-00574
Page 018

information about the plurality of operating conditions on the endpoint gathered by the one or more software services," as I described in Section VI.B, it therefore cannot disclose, teach, or suggest "determining, by the computing system, a compliance state of the endpoint based on the status information."

D. Cheng Does Not Disclose "*requesting, at the computing system, the status information on a periodic basis*" as Required by Claim 3

41. In my opinion, since Petitioner fails to show how Cheng discloses, teaches, or suggests "receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint," as I describe in Section VI.B, it therefore cannot disclose, teach, or suggest "requesting, at the computing system, the status information on a periodic basis."

42. In my opinion, Cheng does not show receiving status information on a periodic basis. I note that Petitioner's only cited portion of Cheng relates to receiving periodic information that has nothing to do with the claimed status information. For example, that portion of Cheng describes that "[m]ost or all the ***information needed regarding protective measures*** can be automatically retrieved by the policy server ***from the outside sources***. The policy server regularly receives up-to-date information from outside sources. The policy server may pull the information on a periodic or event-driven basis." Ex. 1004, 7:58-8:3. I agree with Petitioner's expert,

Taasera's Exhibit No. 2004, IPR2023-00574
Page 019

who confirms that the pulled information from Petitioner's citation refers only to protective measures that are received from outside sources:

> Q. Thank you. So what you just read refers to information from outside sources; is that correct?
> . . .
> A. This -- yeah, information needed regarding protective measures, it says can be retrieved from the outside resources 240.
>
> Q. Okay. And as you just mentioned, it's fair -- is it fair to say that this information from outside sources is in regards to protective measures?
>
> A. Information needed regarding protective measures is exactly what Cheng says in that passage, yes.

Ex. 2005, 70:24-72:4. Protective measures from outside sources is not relevant to the claimed "status information on a periodic basis."

43. In my opinion, Petitioner's motivation to combine Cheng with the knowledge of a POSITA at the time of invention is not persuasive because Petitioner simplistically suggests that the inquiry is whether "[r]equesting status information on a periodic basis was well-known as of the priority date of the '918 patent." Pet. at 31. In my opinion, Petitioner is not correct because it strips the claimed term, "status information" of its meaning within the claim as status information about the plurality of operating conditions. Without that meaning, it seems to me that Petitioner merely suggests that because a POSITA would have known to send any information periodically, there is motivation combine. Pet. at 31-32. However, as

Taasera's Exhibit No. 2004, IPR2023-00574
Page 020

described above in Section VI.B, the '918 Patent describes prior art systems where "status information" is not context aware. Based on my experience and as I describe in Section VI.B with respect to Ex. 1001, 3:7-11, these are the only systems a POSITA would have been aware of at the time of the '918 Patent's invention.

E. Cheng Does Not Disclose "*configuring one or more applications running on the endpoint on the endpoint to monitor at least a subset of the plurality of operating conditions,*" as Required by Claim 5

44. In my opinion, since Petitioner fails to show how Cheng discloses, teaches, or suggests "configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions" or "operating conditions" generally, as I describe in Sections VI.A and VI.B, it therefore cannot disclose, teach, or suggest "configuring one or more applications running on the endpoint on the endpoint to monitor at least a subset of the plurality of operating conditions."

F. Cheng Does Not Disclose "*wherein the conditions comprise at least one hardware condition*," as Required by Claim 6 or "*wherein the conditions comprise at least one software condition*" as Required by Claim 7

45. In my opinion, since Petitioner fails to show how Cheng discloses, teaches, or suggests "operating conditions," as I describe in Sections VI.A and VI.B, it therefore cannot disclose, teach, or suggest "at least one hardware condition" or "at least one software condition."

Taasera's Exhibit No. 2004, IPR2023-00574
Page 021

G. Cheng Does Not Render Claims 2, 4, and 8 Obvious

46. I note that Claims 2, 4, and 8 are dependent upon Claim 1, and are therefore, in my opinion, not obvious over Cheng for at least the same reasons as Claim 1.

H. Cheng Does Not Render Claims 9-24 Obvious

47. I note that Claims 9-16 and 17-24 are respectively "non-transitory computer readable medium containing computer instructions" and "system" analogues to the method claims of Claims 1-8. Therefore, in my opinion, Claims 9-16 and Claims 17-24 are each, respectively, not obvious over Cheng for at least the same reasons as Claims 1-8.

VII. SUMMARY OF OPINIONS

48. It is my opinion that the Board should confirm the validity of the challenged claims. I reserve the right to supplement my opinions in response to any additional contentions by Petitioner or opinions by Dr. John Black, and as the Board permits.

49. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and 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.

Executed on November 9th, 2023 in Dallas, TX.



Eric Cole, Ph.D.

Taasera's Exhibit No. 2004, IPR2023-00574
Page 023

EXHIBIT A

Dr. Eric Cole, Ph.D.

Cybersecurity Expert Witness

44651 Provincetown Drive,
Ashburn, VA 20147
(703) 909-2998
ecole@secure-anchor.com
www.secure-anchor.com/expert-witness/



EXPERT OVERVIEW

Cybersecurity and technology expert witness with over 30 years of practical, hands-on experience. Works on a wide range of cases, including IP litigation, apportionment, trade secrets, and cybersecurity breaches. Extensive experience with report writing, depositions, and testifying at trial. Actively worked in the industry and have extensive experience implementing and working with a variety of technologies across, cybersecurity, networking, and operating systems. Former adjunct professor at Georgetown University, NY Institute of Technology, and a guest lecturer at Purdue, MIT, Harvard, and Berkeley. Served as a member of the Presidential Commission on Cybersecurity and member of several advisory boards. Author of several textbooks and books and inducted into the InfoSec European Hall of Fame in 2014.

PROFESSIONAL EXPERIENCE

Secure Anchor Consulting Services: 2005-Present
Founder and CEO
Provides consulting services to Fortune 500, Fortune 50, financial institutions, international organizations and the federal government. Employs cutting edge technology and technical components (network security, network architecture, and incident response, NOC/SOC design) to provide security solutions.

SANS (SysAdmin Audit Network Security): 1999-2019
Director of the Cyber Defense Initiative
Lead instructor and course developer for several security courses, including the top selling courses. Executed and contributed to the development of several of the GIAC certifications including GIAC Certified Security Essentials (GSEC).

McAfee: 2009-2010
SVP, CTO of the Americas
Responsible for influencing the company's strategic and technical direction, development, and growth as the global leader in digital security solutions. Worked closely with CEO, EVP of Product Operations, and other stakeholders to establish a product vision and road map to achieve McAfee's goals.

Lockheed Martin: 2005-2009
IS&GS Chief Scientist
LM Senior Fellow
The Sytex Group, Inc. (TSGI) was acquired by Lockheed Martin with a key component being the intellectual property created under the CTO leadership. As Lockheed Martin Chief Scientist, performed research and development to advance the state-of-the art in information systems security.

Taasera's Exhibit No. 2004, IPR2023-00574
Dr. Eric Cole, Ph.D.
Page 025

The Sytex Group, Inc. (TSGI): 2001-2005
Chief Technology Officer (CTO)
Created an intellectual property portfolio that included patents, journals, books, and white papers, resulting in an overall increase in market value and customer engagement. Yearly patents were in line with the top 1000 producing patent companies in the United States.

GraceIC: 2000-2001
Chief Security Officer (CSO)
Designed and executed strategy for establishing GraceIC as a leader in the network security arena.

American Institutes for Research: 1999-2000
Chief Information Officer (CIO)
Re-worked the IT infrastructure based on the organization having experienced several security breaches, virus outbreaks and unreliable performance on the network. Provided technical support for DARPA-sponsored research projects.

Vista Information Technologies: 1998-1999
VP of Enterprise Security Services
Developed the Enterprise Security Services Group and was responsible for all internal and external security issues.

Teligent: 1996-1998
Director of Security
Created and managed IT Corporate Security Department. Evaluated strategic plans and operational activities by performing risk assessment and determining how it might impact corporate security.

Central Intelligence Agency: 1991-1996
Program Manager / Technical Director for the Internet Program Team with Office of Technical Services
A Senior Officer of the agency that implemented the Internet Program Team The team designed, developed, tested, and deployed products over three to six-month intervals. Received letter of appreciation from the DCI (Director of Central Intelligence) and six Exceptional Performance Awards. Evaluated and performed security assessment of network operating systems.

EDUCATION

Doctorate degree in Network Security, Pace University 2004
Master of Science in Computer Science, New York Institute of Technology (Honors)1994
Bachelor of Science in Computer Science, New York Institute of Technology (Honors) 1993

CERTIFICATIONS

CISSP (Certified Information Systems Security Professional)
Created several of the GIAC (Global Information Assurance Certification) programs and exams

Taasera's Exhibit No. 2004, IPR2023-00574

ORGANIZATIONS / MEMBERSHIPS

Association for Computing Machinery (ACM)
Institute of Electrical and Electronics Engineers (IEEE)
Computer Security Institute (CSI)
Information Systems Security Association (ISSA)
International Computer Security Association (ICSA)
International Who's Who in Information Technology
Common Vulnerability and Exposures (CVE) - member of the editorial board (by invitation only)
HoneyNet Project - member (by invitation only)

BOOKS

Eric Cole. *Cyber Crisis.* BenBella Books, 2021.
Eric Cole. *Online Danger: How to Protect Yourself and Your Loved Ones From the Evil Side of the Internet.* Morgan James Publishing, 2018.
Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization.* Syngress, 2012.
Eric Cole. *Network Security Bible.2nd Edition.* Wiley, 2009.
Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollman, and Rachelle Reese. *Wiley Pathways Network Security Fundamentals Project Manual.* Wiley, 2007.
Eric Cole and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft.* Syngress, 2006.
Eric Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication.* Wiley, 2003.
Eric Cole. *Hackers Beware: The Ultimate Guide to Network Security.* New Riders/Sams Publishing, 2001.

RECENT EXPERT WITNESS TESIMONY

Sunstone Information Defense v. International Business Machines Corporation, United States District Court Western District of Texas (Waco Division)

Case No. 6:20-cv-01033-ADA
Provided expert reports, depositions, demonstration, and testimony on behalf of plaintiff Sunstone Information Defense (2022)

Trustees of Columbia University in the City of New York v. Nortonlifelock, Inc., United States District Court for the Eastern District of Virginia (Richmond Division)

Case No. 3:13-cv-00808
Provided expert reports, depositions, demonstration, and testimony on behalf of plaintiff Trustees of Columbia University in the City of New York (2022)

Appian Corporation v. Pegasystems Inc. and Youyong Zou, Fairfax County Circuit Court

Case No. 2020-07216
Provided expert reports, depositions, demonstration, and testimony on behalf of plaintiff Appian Corporation (2022)

Taasera's Exhibit No. 2004, IPR2023-00574
Page 027

Shana Doty v. ADT, LLC d/b/a ADT Security Services, United States District Court for the Southern District of Florida (Fort Lauderdale Division)

Case No. 20-cv-60972

Provided expert witness consulting services, expert report, and deposition services on behalf of plaintiff Shana Doty. (2020)

United States of America v. Lucy Xi, United States District Court for the Eastern District of Pennsylvania

Criminal Action: 16-22-5

Provided expert witness consulting services on behalf of defendant Lucy Xi (2021)

Centripetal Networks, Inc. v. Lookingglass Cyber Solutions, Inc., et al., United States District Court for the Eastern District of Virginia (Richmond Division)

Case No. 3:21-cv-000597

Provided expert witness consulting services on behalf of plaintiff Centripetal Networks, Inc. (2022)

Root Insurance Co. v. Genpact (UK) LTD., JAMS Arbitration

REF. No. 1450007525

Provided expert reports, depositions, and arbitration support on behalf of respondent Genpact (UK) LTD. (2022)

Sprint Communications LP v. Charter Communications Inc., et al., United States District Court of Kansas (Kansas City)

Case No. 2:20-cv-02161

Provided expert witness consulting services on behalf of defendant Charter Communications Inc. (2021)

Securities and Exchange Commission v. Zhoubin Hong, et al., United States District Court for Central District of California

Case No. 2:20-cv-04080-MCS

Provided expert report on behalf of plaintiff Securities and Exchange Commission (2021)

Synopsys, Inc. v. Risk Based Security, Inc, United States District Court for the Eastern District of Virginia (Richmond Division)

Case No. 3:21-cv-00252

Provided expert report, deposition, and demonstration on behalf of plaintiff Synopsys, Inc. (2022)

Cox Automotive, Inc., et al. v. The Reynolds and Reynolds Company, American Arbitration Association

AAA Case No. 01-19-0000-4548

Provided expert report on behalf of respondent The Reynolds and Reynolds Company (2021).

Bitglass, Inc. v. Netskope, Inc. et al., United States District Court for the Northern District of California (San Francisco Division)

Case No. 3:20-cv-005216

Provided expert report on behalf of plaintiff Bitglass, Inc. (2020).

Taasera's Exhibit No. 2004, IPR2023-00574
Page 028

F*reshub, Inc. et al. v. Amazon.com, Inc. et al.,* United States District Court of Texas Western District,
Case No. 6:21-cv-00511-ADA
Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Freshub, Inc. et al. (2021).

Finjan, Inc. v. Cisco Systems, Inc., United States District Court of California Northern District,
Case No. 5:17-cv-00072-BLF-SVK
Provided expert report and deposition testimony on behalf of plaintiff Finjan, Inc (2020).

Unified Patents Inc. v. Kioba Processing LLC, US Patent Trial and Appeals Board,
Case No. IPR2020-01695
Provided expert declaration on behalf of plaintiff Unified Patents Inc. (2020).

Mark Voelker v. BNSF Railway Company, United States District court of Montana Missoula Division,
Case No. 9:18-CV-00172-DLC
Provided expert report on behalf of defendant BNSF Railway Company. (2020).

BrandRep LLC v. Ruskey et al., Court of Chancery of The State of Delaware,
Case No. 2018-0541-SG.
Provided expert report and deposition testimony on behalf of defendant Ruskey et al. (2020).

Association of Owners of Kukui Plaza v. American Savings Bank FSB, Circuit Court of the First Circuit, State of Hawai'i,
Case No. 18-1-0660-05
Provided expert report on behalf of defendant American Savings Bank FSB (2020).

Centripetal Networks, Inc., v. Cisco Systems, Inc., United States District Court of Virginia Eastern District,
Case No. 2:18-cv-00094
Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Centripetal Networks, Inc (2020).

Unified Patents v. TransactionSecure LLC, United States Patent Trial and Appeals Board,
Case No. IPR2020-00321
Provided written declaration on behalf of the petitioner Unified Patents (2019).

Glenn Winder v. Marriott International, Inc., et al., Ontario Court of Superior Justice
Case No. CV-1800611365-00CP
Provided written opinion on behalf of the plaintiff Glenn Winder (2019).

Fortinet, Inc. v. British Telecommunications Public Limited Company, United States Patent Trial and Appeals Board,
Case No. IPR2019-01327 and IPR 2019-01328
Provided written declaration on behalf of the patent owner British Telecommunications (2019).

Taasera's Exhibit No. 2004, IPR2023-00574
Page 029

FFinjan, Inc. v. Juniper Network, Inc., United States District Court of California Northern District
Case No. 3:17cv5659
Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Finjan, Inc (2019).

Vivian Deveroux V. Apple, Inc., Superior Court of the State of California County of Santa Clara
Case No. 1-14-cv-271773
Provided expert report and deposition testimony on behalf of plaintiff Vivian Deveroux (2019).

United States of America v. Shan Shi et al., United States District Court for the District of Columbia
Case No. 1:17-cr-00110-CRC
Provided trial testimony on behalf of defendant Shan Shi et al (2019).

Colortokens, Inc. v. Medovich, United States District Court for the California Northern District
Case No. 3:18-cv-2444
Provided expert opinion on behalf of defendant Medovich (2019).

Avepoint, Inc. v. Onetrust, LLC., Patent Trial and Appeals Board, Post Grant Review
Case No. PGR 2018-00056
Provided expert report on behalf of plaintiff Avepoint, Inc. (2019).

Centripetal Networks, Inc., v. Keysight Technologies, United States District Court of Virginia Eastern District,
Case No. 2:17-cv-3836
Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Centripetal Networks, Inc (2018).

Gubarev et al. v. Buzzfeed, Inc. et al., United States District Court for Florida Southern District,
Case No. 0:17-cv-60426
Provided expert report on behalf of plaintiff Gubarev et al. (2018).

Daniel Bennett. v. Lenovo (Canada) Inc. et al., Ontario Superior Court of Justice,
Court File No. CV-15-00523714-00CP
Provided expert consultation behalf of plaintiff Daniel Bennett. (2018).

Finjan, Inc. v. Blue Coat Systems, Inc., United States District Court of California Northern District
Case Nos. 5:15-cv-3295; 5:13-cv-3999
Provided expert report, deposition testimony, and trial testimony on behalf of plaintiff Finjan, Inc (2018).

Zscaler, Inc., v. Symantec Corporation, United States Patent Trial and Appeals Board,
Case No. IPR2018-00929
Provided written declaration on behalf of the patent owner Symantec Corporation (2018).

Taasera's Exhibit No. 2004, IPR2023-00574
Page 030

YLD Limited v. The Node Firm, LLC et al., United States District Court for the Northern District of California (San Francisco)

Case No. 3:16-cv-399

Provided expert report and deposition testimony on behalf of defendant The Node Firm, LLC et al. (2017).

Phishme, Inc. v. Wombat Security Technologies, Inc., United States District Court of Delaware

Case No. 1:16-cv-403

Provided expert report, deposition testimony, and supplemental expert report on behalf of plaintiff Phishme, Inc (2017).

Smith et al v. Federal Title & Escrow Company et al, United States District Court for the District of Columbia,

Case No. 1:17-cv-1580

Provided expert opinion on behalf of plaintiff Smith et al (2017).

Unified Patents Inc. v. Universal Secure Registry LLC, US Patent Trial and Appeals Board,

Case No. IPR2018-00067

Provided expert declaration, deposition testimony, and supplemental expert declaration on behalf of plaintiff Unified Patents Inc (2017).

BASCOM Global Internet v. AT&T Mobility LLC, United States District Court for the Northern District of Texas,

Case No. 3:14-cv-03942

Provided expert report on behalf of the defendant AT&T Mobility LLC (2017).

---

i Ongoing cases are not included for client confidentiality

Taasera's Exhibit No. 2004, IPR2023-00574