

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. IPR2023-00573
U.S. Patent No. 8,955,038

DECLARATION OF JOHN R. BLACK, JR., PH.D.

TABLE OF CONTENTS

	Page
I. Introduction	1
II. Background and Qualification	2
III. Legal Standards Used in My Analysis	5
A. Prior Art	5
B. Person of Ordinary Skill in the Art.....	6
C. Obviousness	8
IV. The '038 Patent	10
A. Overview of the Challenged '038 Patent.....	10
B. Claims	11
C. Relevant Prosecution History	13
V. Claim Construction	14
VI. Summary of Cited Prior Art Reference.....	15
A. Cheng (Ex. 1004)	15
VII. Opinions Regarding Unpatentability.....	20
A. Ground 1: Claims 1-33 Would Have Been Obvious Over Cheng (Ex. 1004) in View of the Knowledge of a POSITA.....	21
1. Independent Claims 1 and 12	21
a. Claim 1	21
b. Claim 12	34
2. Dependent Claims 2-11 and 13-22	37
a. Claims 2 and 13.....	37
b. Claims 3 and 14.....	38
c. Claims 4 and 15.....	39
d. Claims 5 and 16.....	41
e. Claims 6 and 17.....	42
f. Claims 7 and 18.....	43
g. Claims 8 and 19.....	44
h. Claims 9 and 20.....	47

i.	Claims 10 and 21.....	48
j.	Claims 11 and 22.....	48
3.	Independent Claim 23.....	50
a.	Claim 23	50
4.	Dependent Claims 24-33	56
a.	Claim 24	57
b.	Claim 25	57
c.	Claim 26	58
d.	Claim 27	58
e.	Claim 28	59
f.	Claim 29	59
g.	Claim 30	60
h.	Claim 31	60
i.	Claim 32	61
j.	Claim 33	61
B.	No Secondary Considerations Exist	62
VIII.	Conclusion	62

CITED EXHIBITS

Ex. No.	Brief Description
1001	U.S. Patent No. 8,955,038
1002	U.S. Patent No. 8,955,038 File History
1004	U.S. Patent No. 8,065,712 to Cheng et al. (“Cheng”)
1005	U.S. Patent No. 7,197,561 to Lovy et al.
1006	U.S. Patent No. 8,281,114 to Linetsky

I, John R. Black, Jr., declare as follows:

I. Introduction

1. I have been retained by Palo Alto Networks, Inc. (“Petitioner”) in connection with its request for *inter partes* review of U.S. Patent No. 8,955,038 (the “’038 patent”). A copy of the ’038 patent has been marked Ex. 1001. I have reviewed and am familiar with the ’038 patent, which generally relates to controlling access of endpoints to networked computing resources.

2. I have been asked to provide my opinions regarding the patentability of claims 1-33 of the ’038 patent (the “challenged claims”). This declaration discusses my background and qualifications, the legal standards used in my analysis, an overview of the ’038 patent from the perspective of a person of ordinary skill in the art as of the patent’s alleged priority date (a “POSITA”), and my opinions regarding the patentability of the challenged claims.

3. My work in this proceeding is being charged to Petitioner at a standard rate of \$735 per hour. My compensation is in no way contingent on the substance of my opinions or the outcome of this proceeding.

4. As set forth more fully below, it is my opinion that the challenged claims of the ’038 patent are unpatentable as obvious based on the following ground below:

Ground	Claims	Basis	References
1	1-33	103	Cheng in view of the knowledge of a POSITA

II. Background and Qualification

5. A current copy of my CV is attached as Appendix A.

6. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now “California State University, East Bay”) in 1988. I received an M.S. in Computer Science in 1997 and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

7. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers for over 40 years in both commercial and academic capacities.

8. My earliest interest was in networks and security. My first memories in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available, and I spent most of my free time studying, programming, and modifying

them. I worked extensively with various networking products throughout the 1980s and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

9. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp. as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

10. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security, and my research involved encryption, authentication, hash functions, and network security.

11. After graduation, I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, IP, UDP, TCP, HTTP, SMTP, and other protocols. In 2001, a graduate student and I looked at the security of ARP and invented a new protocol “AuthARP” to add security to the protocol.

12. In 2002, I moved to the University of Colorado at Boulder, where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new

course called “Foundations of Computer and Network Security,” which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services, including the world-wide web. I have taught this class seven more times since then and have included modern topics such as wireless networking, the Internet of Things, and so forth. In particular, Network Intrusion Detection Systems (or “NIDS”) are taught in this class; these systems are similar to the embodiments in the patent-at-issue here.

13. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several Ph.D. students in these areas.

14. I also have worked for a consulting company at times, writing software on a contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

15. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App,

worked on 802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop.

16. In 2016, I took a leave of absence from the University of Colorado to start a company named “SecureSet” in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. I designed the curriculum used at SecureSet, including system and network security much like the technology described in the patent-at-issue here. SecureSet was sold to WeWork in 2019 and continues to offer computer security classes today.

III. Legal Standards Used in My Analysis

17. 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

18. 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 I discuss in this Declaration is prior art at least because it would have been available to members of

the public as of December 21, 2005, and it is relevant to the subject matter of the '038 patent.

19. The reference I discuss 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

20. I understand that the '038 patent issued from Application No. 13/587,505 (the "'505 Application"), filed August 16, 2012. I understand that the '038 patent alleges priority to Provisional Application No. 60/752,424, filed December 21, 2005. For the purposes of my analysis in this Declaration, I have assumed that the challenged claims are entitled to a priority date no earlier than December 21, 2005.

21. I understand that the assessment of the patentability of the challenged claims of the '038 patent must be undertaken from the perspective of a hypothetical POSITA as of the priority date of the '038 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.

22. 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.

23. Based on these factors, my knowledge and expertise, and the prior art to the '038 patent, it is my opinion that a POSITA at the time of the relevant priority date 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.

24. I meet this definition of a POSITA today and met this definition by December 21, 2005.

C. Obviousness

25. 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.

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

27. 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.

28. 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.

29. 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 '038 Patent

A. Overview of the Challenged '038 Patent

30. The '038 patent, titled “Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities,” relates to “fine tuning access control by remote, endpoint systems to host systems.” Ex. 1001, cover, abstract. The '038 patent purports to address security concerns for electronic networks that allow, e.g., employees at work or away from work to access “office files, design documents, employee work products, company information, and most other important business information [] being created and stored electronically on desktop computers, laptop computers, handheld computing devices (collectively ‘personal computing device’ or ‘computing device’) and company networks.” *Id.*, 1:30-47. The '038 patent aims to prevent “[i]nappropriate and/or unauthorized access to such electronic networks, and the computing resources accessible there through,” by employing flexible endpoint access control. *Id.*, 1:47-55.

31. The '038 patent admits that the field of endpoint access control has followed an evolutionary path in the prior art, starting with “operating system services that controlled user access to one or more system resources” and “permitted or denied access to these resources based on a variety of factors, such as their login ID (which was authenticated using a secret) and a secured profile of policy settings identifying permissions and/or restrictions.” *Id.*, 1:63-2:3. This was followed by “point solutions,” such as personal firewalls, antivirus agents, software update agents, restricting access to specific resources, etc., and then by “context awareness,” such as restricting access if a named application is not running or is not of a specified minimum version or if a user is in a certain location, etc. *Id.*, 2:9-30, 2:42-61.

B. Claims

32. The '038 patent has three independent claims. Claim 1 recites:

1. A method for controlling the operation of an endpoint,
comprising:
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 monitor;

configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;
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 agents;
determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and
initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

The other two independent claims restate the same steps in the context of a “non-transitory computer readable medium” (claim 12) or “system” (claim 23).

33. Dependent claims 2, 13, and 24 further add the concept of “controlling access of the endpoint to computing resources” based on the determined compliance state. The remaining dependent claims recite either additional components of conventional networks—i.e., a “web page” (claims 3, 14, 25), “mobile device” (claims 5, 16, 27), “servers” (claims 10, 21, 32), and “software agents” provided by either the operating system (claims 6, 17, 28) or endpoint applications (claims 7, 18, 29)—or variations on determining compliance with a policy—i.e., requesting “status information on a periodic basis” (claims 4, 15, 26), monitoring a “hardware condition” (claims 8, 19, 30) or “software

condition” (claims 9, 20, 31), and having “at least one policy” that includes a rule identifying an action (claims 11, 22, 33).

C. Relevant Prosecution History

34. I have reviewed and considered the prosecution history of the ’038 patent, which is marked Ex. 1002. I provide a brief summary of certain key events during the prosecution of the ’038 patent below.

35. The Examiner initially rejected the pending claims of the ’038 patent as anticipated or obvious based on U.S. Patent Publication No. 2005/0086511 to Balacheff et al. (“Balacheff”), Balacheff in view of U.S. Patent No. 7,805,752 to Newstadt et al. (“Newstadt”), and Balencheff in view of U.S. Patent Publication No. 2007/0124803 to Taraz (“Taraz”). Ex. 1002, 205-219.

36. In response, the applicants amended the claims, including the three pending independent claims, to recite that the claimed steps are performed by “software agents” and that the resulting actions are “carried out by a processor on the endpoint.” *Id.*, 239-44. The applicants argued that the Examiner’s primary reference, Balacheff, lacked these limitations because it instead discloses “a specific hardware device” (not “software agents”) to test compliance with a policy and takes resulting actions “at the host” (not “on the endpoint”). *Id.*, 245.

37. The Examiner then received authorization in a telephonic interview with the applicants to further amend the pending independent claims to clarify that

the “conditions” of the endpoint to be monitored are “operating conditions” and that the recited “processors” are “hardware processors.” *Id.*, 256-58. The Examiner issued a Notice of Allowance in view of the Examiner’s amendment and for the reasons argued by the applicants in the applicants’ remarks in response to the non-final office action. *Id.*, 256-259.

38. The prior art, Cheng, cited in this Declaration was not considered during prosecution. Nor is it cumulative of anything cited during prosecution. As discussed below, it is my opinion that Cheng teaches all limitations of the ’038 patent’s claims—including the limitations added to distinguish Balacheff.

V. Claim Construction

39. Counsel for Petitioner has informed me that language in a patent claim should be construed in accordance with the ordinary and customary meaning of such claim as understood by a POSITA in light of the specification and prosecution history of the patent.

40. 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.

41. For purposes of my opinions of unpatentability in this Declaration, no claim construction is necessary because, in my opinion, the challenged claims

would have been rendered obvious over the cited reference under any reasonable construction and based on their plain and ordinary meaning to a POSITA.

VI. Summary of Cited Prior Art Reference

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

A. Cheng (Ex. 1004)

43. I understand that Cheng is prior art to the '038 patent at least because it issued from an application filed on May 25, 2005. Ex. 1004.

44. Cheng, titled “Methods and Devices for Qualifying a Client Machine to Access a Network,” states that it is directed to “[m]ethods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates.” *Id.*, cover, abstract. Cheng teaches an approach for protecting a network that “extend[s] network security to every node and entry point on a network. Users are recognized through authentication and authorization, and vulnerabilities of user devices are assessed according to configured security policies. Significantly, devices are assessed before the user gains access to network resources.” *Id.*, 3:16-21.

45. Cheng's Figure 1 below shows an exemplary system for qualifying a client to access a network.

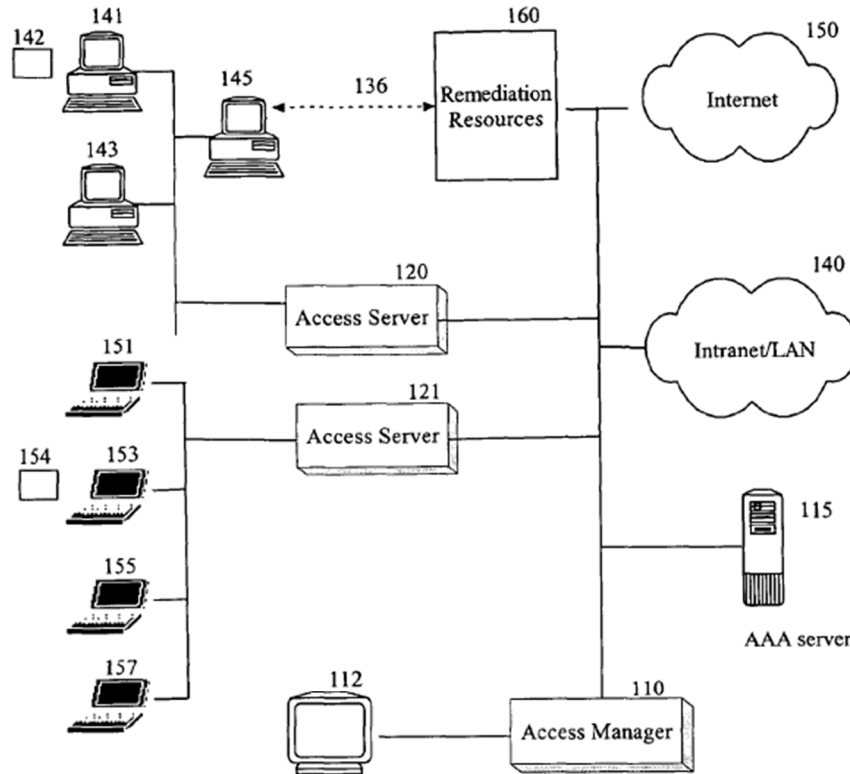


FIG. 1

Id., Fig. 1. “Multiple client machines 141, 143, 145, 151, 153, 155, 157 are depicted” in Figure 1. Client machines “broadly include any IP-enabled end station device that can access a network, such as a PC, workstation, laptop, PDA,¹

¹ Cheng defines “PDAs” as “Personal Data Assistants.” Ex. 1004, 1:45.

printer, etc.” *Id.*, 5:59-64. A client machine, such as “client machine 141, 153[,] may include optional client agent software 142, 154 resident on the client machine. ... In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation,” where “it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.” *Id.*, 5:65-6:9.

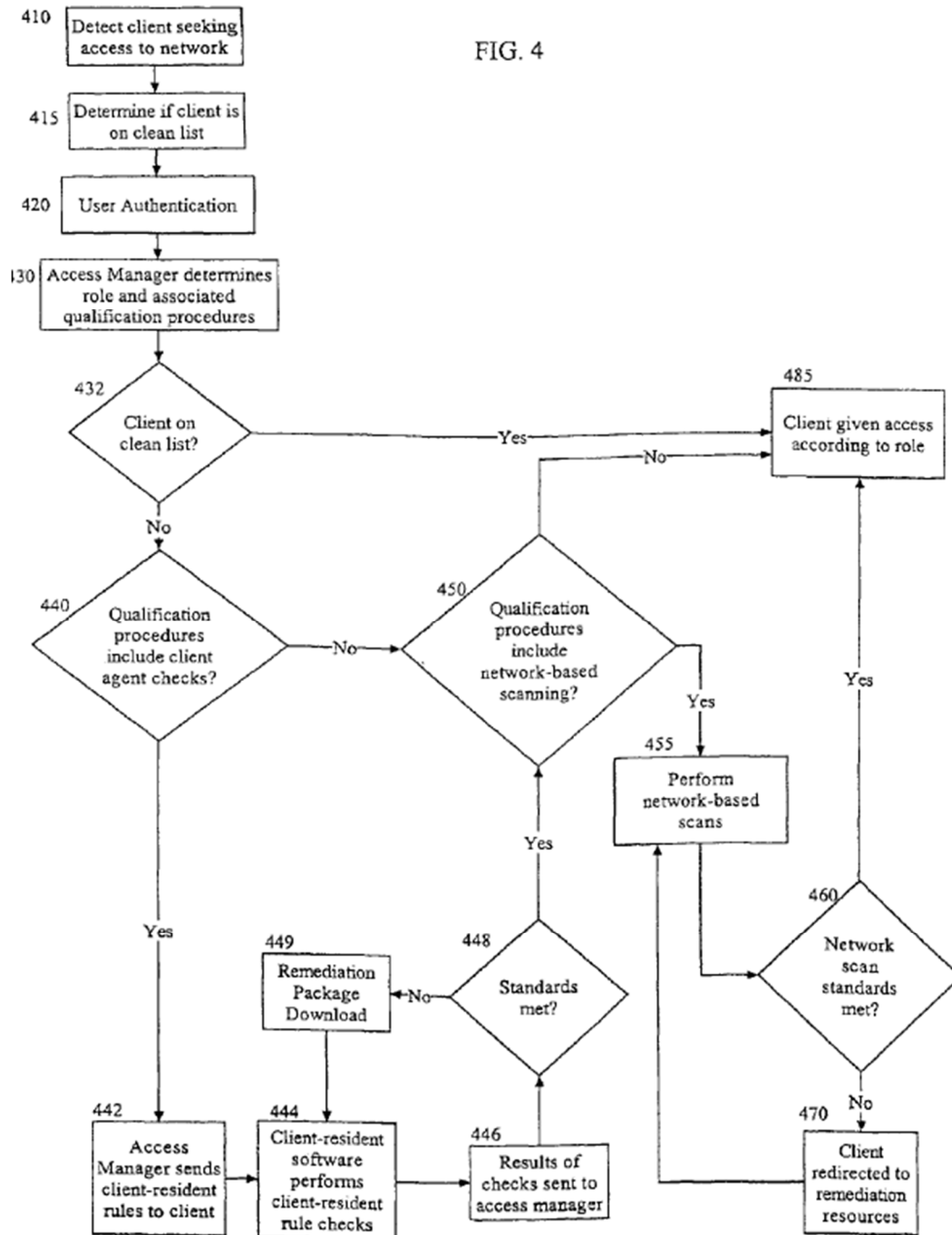
46. Cheng’s qualification system includes “[a]ccess manager 110 [that] acts as a qualification authority. ... [A]ccess manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” *Id.*, 6:55-62. As part of the qualification system, “a policy repository stores ‘policy rules’ specified as combinations of conditions.” *Id.*, 5:11-12. Cheng teaches that “[a] system administrator interacts with an access manager to establish user roles and select a set of policy rules and remediation procedures retrieved from the policy repository to be associated with the user roles. The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.” *Id.*, 5:26-32.

47. Cheng further teaches that “[t]he policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has

been installed on a client machine, etc. In one embodiment, the conditions generally include ‘checks,’” which “are used as the qualification procedures.” *Id.*, 5:12-20; *see also id.*, 8:17-20 (“For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.”). The “[a]ccess Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser.” *Id.*, 6:63-66.

48. Furthermore, in Cheng’s qualification system, “[a]n administrator uses the rules manager [of the access manager] to adopt and apply rule sets for a particular organization or department. Preferably, rule sets are selected and associated with roles, so that the roles can be reused and applied to particular users or user groups. The rule sets associated with a role are used to govern qualification of a client to access a network according the user’s role.” *Id.*, 9:35-41. Cheng teaches that “[d]ifferent rule sets can be applied to different users or user groups through roles.” *Id.*, 9:60-61. Cheng’s qualification system provides for controlling access to different resources based on roles. “Role-based access means that different user groups can be subject to various types of qualification procedures and various standards of adequate protection. Role-based access controls network access based on user, device and traffic attributes or characteristics.” *Id.*, 9:50-54.

49. Figure 4 below is a flowchart illustrating an exemplary process for qualifying a device to access a network according to Cheng's qualification system.



Id., Fig. 4.

50. As shown in Figure 4, “[a]t step 410, a client attempts to connect to a network. For example, a user may access an access point on a wireless LAN with his laptop computer,” and “[a]n access server, such as access server 121, detects that a client is attempting to access the network.” *Id.*, 10:64-11:3. Some of the key steps in the qualification process include “[a]t step 444, the client agent applies the checks in the rule sets associated with the user’s determined role, and determines whether conditions defined by elements of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets,” with “[a]ny results from the checks [] forwarded to the access manager via the access server at step 446.” *Id.*, 12:33-40. If the qualification standards are met, and there are no network-based scans to apply, “the process continues to step 485, where the user is given his normal login role, with its associated privileges,” and the client machine is allowed to access network resources. *Id.*, 13:41-42.

VII. Opinions Regarding Unpatentability

51. In my opinion, the challenged claims are unpatentable based upon one ground. Claims 1-33 are obvious over Cheng in view of the knowledge of a POSITA.

A. Ground 1: Claims 1-33 Would Have Been Obvious Over Cheng (Ex. 1004) in View of the Knowledge of a POSITA

1. Independent Claims 1 and 12

52. As set forth below, it is my opinion that Cheng in view of the knowledge of a POSITA meets all limitations of independent claims 1 and 12 of the '038 patent.

a. Claim 1

i. “A method for controlling the operation of an endpoint, comprising:”

53. To the extent the preamble is a limitation, it is my opinion that Cheng discloses, teaches, or suggests it. Cheng discloses that “[m]ethods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates, are disclosed. A client machine must pass various checks to qualify for access.” Ex. 1004, abstract.

54. A POSITA would have understood that a “client machine” in Cheng (*id.*) is an “endpoint” within the meaning of the '038 patent, which includes any computer device or processing system capable of connecting to a network. Ex. 1001, 7:52-64. As Cheng explains, “[t]he term ‘client machine’ as used herein is intended to broadly include any IP-enabled end station device that can access a network, such as a ... laptop, PDA, ... etc.” Ex. 1004, 5:61-64. In my opinion, a POSITA would have understood that qualifying a client machine before allowing it

to access a network is a method for controlling the operation of an endpoint (i.e., a client machine).

55. Thus, Cheng discloses, teaches, or suggests a method for controlling the operation of an endpoint.

ii. “providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;”

56. It is also my opinion that Cheng discloses this limitation of claim 1. As Cheng discloses, an access manager 110 is part of a computing system remote from the end point (i.e., the client machine) and configured to allow configuration of a plurality of policies. Cheng explains:

[T]he access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single rules manager is shown in FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks.

Ex. 1004, 7:23-31. Figure 1 of Cheng below shows the computing system with access manager 110 remote from the end point, e.g., client machines 141, 143, 145, 151, 153, 155, and 157.

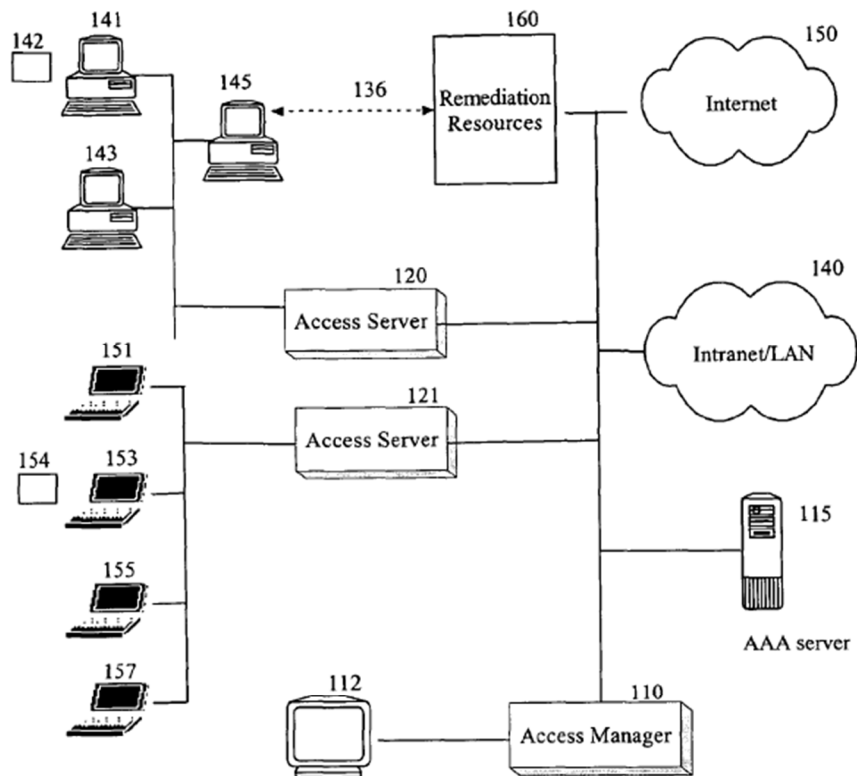


FIG. 1

Id., Fig. 1.

57. Furthermore, Cheng discloses an administrator console 112 as a user interface for allowing configuration of a plurality of policies at access manager 110. “Access Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser.” *Id.*, 6:63-66. Moreover, “an administrator may interact with the rules manager via a command line or graphic user interface

through administrator console 112 to select specific rule sets for each role. ... The administrator can use the rules manager to create roles, associate rule sets with roles, and assign prospective clients or users to roles” (*id.*, 9:42-49), where “a policy rule set is a collection of policy rules” (*id.*, 8:27-28). Therefore, Cheng discloses a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies (i.e., Cheng’s policy rule sets).

58. Thus, Cheng discloses providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies.

iii. “maintaining the plurality of policies in a data store on the computing system;”

59. It is also my opinion that Cheng discloses this limitation of claim 1. Cheng discloses a policy repository for storing policy rules. “In one embodiment, a policy repository stores ‘policy rules’ specified as combinations of conditions. The policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc.” Ex. 1004, 5:11-15; *see also id.*, abstract (“A policy repository is updated regularly by vendors of protective measures.”). Cheng further discloses that “[a] system administrator interacts with an access manager to establish user roles and select a set of policy rules and remediation procedures retrieved from the policy repository

to be associated with the user roles.” *Id.*, 5:26-29. Therefore, Cheng discloses that the plurality of policies is maintained in a data store (i.e., policy repository) on the computer system, as selected and retrieved by the access manager.

60. Thus, Cheng discloses maintaining the plurality of policies in a data store on the computing system.

iv. “identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;”

61. It is also my opinion that Cheng discloses this limitation of claim 1. As Cheng discloses, the “access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” Ex. 1004, 6:59-62. The policy rule set “defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. Policy rule sets further set standards for adequacy for the particular protective measures. For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.” *Id.*, 8:14-20. In other words, “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” is determined. *Id.*, 8:30-34. Therefore, Cheng discloses that 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) is identified from the plurality of policies (i.e., policy rule sets) and monitored on the endpoint (i.e., determined by the client agent software on the client machine).

62. Thus, Cheng discloses identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor.

v. “configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;”

63. It is also my opinion that Cheng discloses this limitation of claim 1. As Cheng discloses, “[t]he client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.” Ex. 1004, 5:37-40. The “access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” *Id.*, 6:59-62.

64. With the client agent software installed on the client machine, Cheng discloses that “the client agent applies the checks in the rule sets associated with the user’s determined role, and determines whether conditions defined by elements

of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets.” *Id.*, 12:33-38. Therefore, Cheng discloses that one or more software agents (i.e., client agent software) are configured on the endpoint (i.e., client machine) to monitor the plurality of operating conditions (i.e., determine whether conditions defined by elements of the rule sets are true or false, thus determining the posture of the client machine).

65. Accordingly, Cheng discloses configuring one or more software agents on the endpoint to monitor the plurality of operating conditions.

vi. “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 agents;”

66. It is also my opinion that Cheng discloses this limitation of claim 1. As I discussed above in §VII.A.1.a.v, Cheng discloses the client agent as a software agent on a client machine that gathers status information about the plurality of operating conditions on the client machine, as defined by elements of rule sets. Cheng further discloses that the status information about the plurality of operating conditions is then reported back to the computing system, at the access manager. As Cheng discloses, “the client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.” Ex. 1004, 5:37-40;

see also id., 6:5-9 (“Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.”).

67. Furthermore, Cheng discloses that the status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents is received, across a network, at the computing system. As Cheng discloses:

Any results from the checks are forwarded to the access manager via the access server at step 446. ... Reporting the results of the checks may simply include reporting a set of true and false indications. Alternatively, rule sets could fully describe conditions necessary for qualification and the resident client agent software could report the sum evaluation of the checks. These results are evaluated by the access manager to determine whether the checks meet the standards of adequacy set by the rule sets.

Id., 12:39-49. Therefore, Cheng discloses that the gathered status information (i.e., results or sum evaluation of the checks by the client agent) are received at the computing system (i.e., reported to and evaluated by the access manager).

Moreover, Fig. 1 below shows that the gathered status information is received by the access manager across a network, e.g., intranet or LAN 140, the Internet 150.

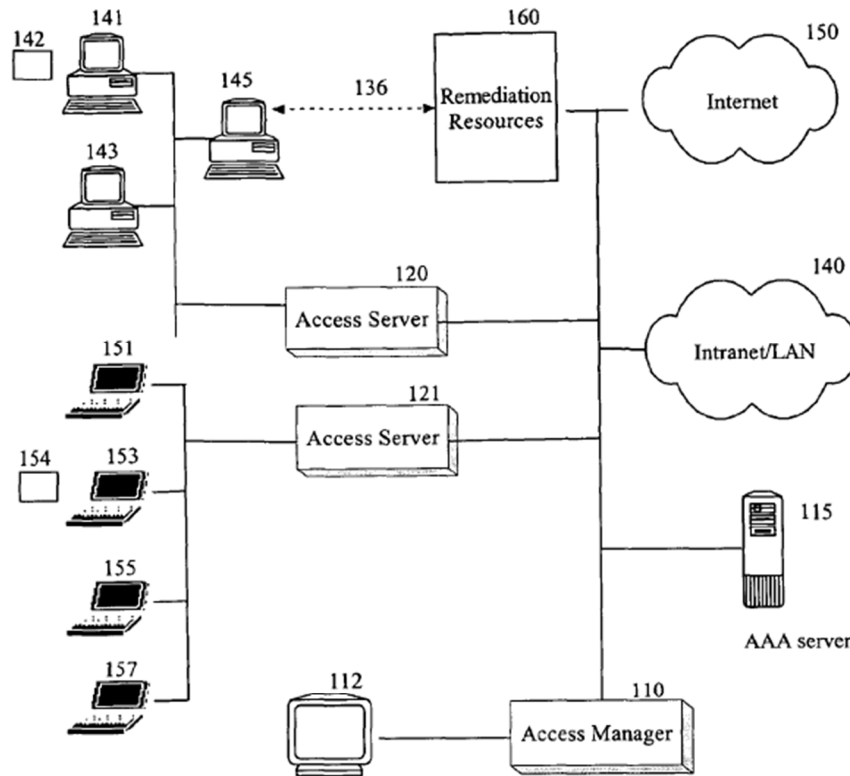


FIG. 1

Id., Fig. 1; *see also id.*, 6:22-28 (“In order to access an internal intranet or LAN 140, the Internet 150, or any other resources available on the network, client machines must first go through access servers 120, 121. Access servers can be deployed at the edge of a network, as shown in FIG. 1, or they may be deployed centrally.”).

68. Thus, Cheng discloses 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 agents.

vii. “determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and”

69. It is also my opinion that Cheng discloses, teaches, or suggests this limitation of claim 1. Cheng discloses that as the acting “qualification authority,” access manager 110 determines the compliance state of the endpoint, i.e., “determines whether the client machine meets the standards of adequate protection.” Ex. 1004, 6:55-62, 13:44-46; *see also id.*, 5:29-32 (“The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.”). As I discussed above in § VII.A.1.a.vi, the client agent on the client machine in Cheng gathers the status information about the plurality of operating conditions on the client machine by carrying out checks based on rule sets from the access manager, which it then sends to the access manager. *See* Ex. 1004, 5:37-40 (“The client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.”). Based on the results or sum evaluation of the

checks, the access manager determines whether the client machine meets the standards of adequate protection.

70. Cheng further discloses, teaches, or suggests that the compliance state of the endpoint is also based on a plurality of additional compliance policies in the data store, such as identifying attributes of the client machine and/or user and using this information to determine network access. For example, “[a] user may enter user identification information as part of the request for access. For example, a user may enter a user identifier and a password, or use a biometric appliance.” Ex. 1004, 11:4-6. Moreover, as Cheng discloses, “[r]ole-based access controls network access based on user, device and traffic attributes or characteristics.” *Id.*, 9:52-54; *see also id.*, 9:50-52 (“Role-based access means that different user groups can be subject to various types of qualification procedures and various standards of adequate protection”). A “role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role.” *Id.*, 11:39-43.

71. In my opinion, a POSITA would have understood that using information such as a user identifier, client machine MAC address, or other device identifier for determining the role of a user, and thus determining network access, is a further determination of the compliance state of the endpoint based on a

plurality of compliance policies in the data store, e.g., determining whether the client machine meets the standards of adequate protection based on various identifying attributes of the client machine and/or user.

72. Moreover, as I discussed above in § VII.A.1.a.iii, Cheng discloses that the plurality of compliance policies for which the determination of the compliance state of the endpoint is based on is maintained in the data store, i.e., policy repository. “[A] set of policy rules and remediation procedures [are] retrieved from the policy repository to be associated with the user roles. The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.” *Id.*, 5:27-32. Therefore, the access manager determines a compliance state of the endpoint (i.e., determines whether the client machine meets the standards of adequate protection) based on the status information (i.e., results or sum evaluation of the checks by the client agent) and a plurality of compliance policies (i.e., different role-based standards of adequate protection) in the data store (i.e., policy repository).

73. Thus, Cheng discloses, teaches, or suggests determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store.

viii. “initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.”

74. It is also my opinion that Cheng discloses, teaches, or suggests this limitation of claim 1. As Cheng discloses, “when a client machine attempts to connect to a network, it must meet standards of adequate protection by applying various qualification procedures, such as checks performed by client agent software resident on a client machine.” Ex. 1004, 5:48-52. The standards of adequate protection are set by the policy rule sets. *Id.*, 8:16-17.

75. Cheng further discloses that a policy rule set that defines the tests for determining whether a client seeking access to the network has implemented particular protective measures may, for example, “set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware” (Ex. 1004, 8:14-20), and “the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc.” (*id.*, 5:13-15). As Cheng discloses, teaches, or suggests, if the client machine does not have the latest antivirus version installed, “[t]he user can use the [remediation] resources to fix detected problems on the client machine in order to meet the required standards of adequate protection. For example, the remediation resources may locally provide one or more up-to-date virus checking options

(engine and definitions).” *Id.*, 7:4-9. Therefore, Cheng discloses, teaches, or suggests that based on the compliance state (i.e., whether the client machine meets the standards of adequate protection, such as for anti-virus protection), an action (i.e., implement up-to-date virus checking options (engine and definitions)) identified in at least one rule (i.e., check that the latest antivirus version has been installed on a client machine) is initiated.

76. Moreover, in my opinion, a POSITA would have understood that the action of implementing the up-to-date virus checking options (engine and definitions) on the client machine (i.e., the endpoint) is an action that is carried out by a processor on the endpoint because the processor on the endpoint needs to invoke operating system functions for the antivirus software installed on the endpoint to be updated with the up-to-date virus checking options (engine and definitions).

77. Thus, Cheng discloses, teaches, or suggests initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, and meets all limitations of claim 1.

b. Claim 12

78. Claim 12 recites:

12. A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising:

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 monitor;

configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;

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 agents;

determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and

initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

79. In my opinion, Cheng in view of the knowledge of a POSITA would have rendered claim 12 obvious for substantially the same reasons I discussed above for claim 1. The only difference between claims 1 and 12 is that claim 12

recites “[a] non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint.” In my opinion, Cheng discloses, teaches, or suggests this difference.

80. To the extent the Board considers the preamble a limitation, Cheng discloses, teaches, or suggests this limitation. As Cheng discloses:

The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306. Such instructions may be read into main memory 306 from another computer-readable medium, such as storage device 310. Execution of the sequences of instructions contained in main memory 306 causes processor 304 to perform the process steps described herein.

Ex. 1004, 14:43-53. Therefore, Cheng discloses, teaches, or suggests a non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint.

81. Cheng discloses, teaches, or suggests all the remaining limitations in claim 12 for the same reasons I discussed above for the corresponding limitations in claim 1. *See supra* § VII.A.1.a. Thus, Cheng in view of the knowledge of a POSITA would have rendered claim 12 obvious.

2. Dependent Claims 2-11 and 13-22

82. It is also my opinion that Cheng in view of the knowledge of a POSITA would have rendered each of the following dependent claims obvious.

a. Claims 2 and 13

83. Claims 2 and 13 depend from claims 1 and 12, respectively, and further recite: “*wherein the action comprises controlling access of the endpoint to computing resources.*”

84. In my opinion, Cheng discloses, teaches, or suggests this limitation. As Cheng discloses, “[a] client machine must pass various checks to qualify for access. ... The policy rule sets govern qualification of client machines for access to the network in accordance with the roles of the users of the machines.” Ex. 1004, abstract. This “[r]ole-based policy enforcement allows access to be restricted to only applications and resources determined to be necessary to the role of the user.” *Id.*, 3:34-36.

85. Therefore, Cheng discloses, teaches, or suggests that access of the client machine to specific applications and resources is controlled and only accessible by users with certain roles. “For example, roles may be established such that only users with sufficient ‘executive’ privileges, such as a Chief Financial Officer, or other executives, are allowed to access confidential financial databases. As another example, a ‘guest’ role may be established that allows a contractor or

other guest access to only public information.” *Id.*, 3:39-45. In my opinion, a POSITA would have understood that allowing only users with sufficient “executive” privileges access to confidential financial databases is controlling access of the endpoint to computing resources, such as confidential financial databases.

86. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 2 and 13 obvious.

b. Claims 3 and 14

87. Claims 3 and 14 depend from claims 1 and 12, respectively, and further recite: “*wherein the user interface comprises a web page.*”

88. In my opinion, Cheng discloses this limitation. As Cheng discloses, “[a]ccess Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser. For example, the administrator console may be a Secure Sockets Layer (SSL)-enabled browser application.” Ex. 1004, 6:63-67; *see also id.*, 3:36-39 (“A web-based administrator console is used to define role-based security policies for various classes of users.”). Therefore, Cheng discloses that the user interface (i.e., administrator console 112) comprises a web page (i.e., it is a web-based application, accessible through any browser).

89. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 3 and 14 obvious.

c. Claims 4 and 15

90. Claims 4 and 15 depend from claims 1 and 12, respectively, and further recite: “*further comprising requesting, at the computing system, the status information on a periodic basis.*”

91. In my opinion, Cheng discloses, teaches, or suggests this limitation. As Cheng discloses, “the access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230.” Ex. 1004, 7:23-26. Cheng further discloses that the policy server 220 of the access manager “regularly receives up-to-date information from outside sources 240. The policy server may pull the information on a periodic or event driven basis. Optionally, outside sources could notify a policy server of available updates.” *Id.*, 7:62-66. Therefore, Cheng discloses, teaches, or suggests that the access manager of the computing system requests and regularly, on a periodic basis, receives up-to-date information about policies, such as, for example, currently available versions of antivirus software. In my opinion, a POSITA would have found it obvious to then also request the status information from Cheng’s client machines on a corresponding periodic basis to ensure up-to-date determinations of the endpoint’s compliance

state based on these updated policies. A POSITA would have further understood that continued monitoring of the operating conditions on the endpoint is also necessary to account for any potential changes in such status information, which could affect the ultimate determination of the endpoint's compliance state.

92. In addition, Cheng in view of the knowledge of POSITA would have rendered this limitation obvious because by the priority date of the '038 patent, requesting status information on a periodic basis was well-known. In my opinion, by the priority date, a POSITA would have known that there are only a finite number of methods for requesting status information of an endpoint—event-driven, continuously, and on a periodic basis. A POSITA would have been motivated to use either event-driven or periodic requesting as a more cost effective, and less resource-intensive, approach in comparison to continuous real-time requesting. Therefore, it would have been obvious for a POSITA to try the claimed periodic approach with a reasonable expectation of success. Indeed, the '038 patent confirms the event-driven and periodic approaches were well-known and predictable to a POSITA by describing them in a manner as interchangeable and without providing any detail as to technological implementation. *See, e.g.*, Ex. 1001, 27:14-22 (“Capabilities of the analysis engine also include the ability to query ... on a fixed periodic basis or be based on a specified system event, for example system startup ...”); *see also, e.g.*, Ex. 1005, abstract (“A network

appliance for monitoring, diagnosing and documenting problems among a plurality of devices and processes (objects) coupled to a computer network utilizes periodic polling and collection of object-generated trap data to monitor the status of objects on the computer network”). In my opinion, implementing a system to request status information periodically as claimed is a predictable use that was well within the ability of a POSITA and would have resulted in a predictable result with a reasonable expectation of success.

93. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 4 and 15 obvious.

d. Claims 5 and 16

94. Claims 5 and 16 depend from claims 1 and 12, respectively, and further recite: “*wherein the endpoint comprises a mobile device.*”

95. In my opinion, Cheng discloses, teaches, or suggests this limitation. As Cheng discloses, “[t]he present invention relates to methods and devices for qualifying a client machine to access a network, based on policies defined by an administrator” (Ex. 1004, 5:46-48), and “[t]he term ‘client machine’ as used herein is intended to broadly include any IP-enabled end station device that can access a network, such as a ... laptop, PDA, ... etc.” (*id.*, 5:61-64). Moreover, the stated purpose of Cheng’s method and system includes addressing the specific security risks posed by mobile devices, including that “[m]obile devices attach to networks

over which IT has no control,” and “[a] mobile device that joins the network will have free access to core network resources without necessarily invoking [a] firewall’s checking mechanism.” *Id.*, 1:56-57, 2:7-10. Therefore, in my opinion, a POSITA would have understood that Cheng discloses, teaches, or suggests that the endpoint (i.e., client machine) comprises a mobile device, such as, e.g., a laptop or PDA.

96. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 5 and 16 obvious.

e. Claims 6 and 17

97. Claims 6 and 17 depend from claims 1 and 12, respectively, and further recite: “*wherein the one or more software agents comprise at least one service provided by the operating system of the endpoint.*”

98. In my opinion, Cheng discloses, teaches, or suggests this limitation. As I discussed above, Cheng discloses one or more software agents as client agent software. *See supra* § VII.A.1.a.v. As Cheng discloses, “[o]nce the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.” Ex. 1004, 6:5-9.

99. In my opinion, a POSITA would have understood that registry, process, application and service checks on the client machine are services provided by the operating system of the endpoint. This is confirmed by Cheng. “The client agent rules are those that include checks that need to be performed by the software resident on the client machine due to security measures typically implemented by clients or operating systems. The client agent software on the client machine is invoked to perform the checks. In this sense, invoking may mean communicating with, as the resident software may be running as a service and may have identified the client seeking access.” *Id.*, 12:5-12; *see also id.*, 8:39-42 (“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.”). Therefore, Cheng teaches that the one or more software agents comprise at least one service provided by the operating system of the endpoint.

100. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 6 and 17 obvious.

f. Claims 7 and 18

101. Claims 7 and 18 depend from claims 1 and 12, respectively, and further recite: “*wherein the one or more software agents comprise at least one application running on the endpoint.*”

102. In my opinion, Cheng discloses, teaches, or suggests this limitation.

As Cheng discloses:

In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation. Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.

Ex. 1004, 6:3-9.

103. In my opinion, a POSITA would have understood that the client agent is an application running on the client machine because the client agent is installed on a client machine and can perform registry, process, application and service checks on the client machine, and an application must be run by the processor of the client machine to be able to perform those functions. Therefore, Cheng teaches that the one or more software agents comprise at least one application running on the endpoint.

104. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 7 and 18 obvious.

g. Claims 8 and 19

105. Claims 8 and 19 depend from claims 1 and 12, respectively, and further recite: “*wherein the conditions comprise at least one hardware condition.*”

106. In my opinion, Cheng discloses, teaches, or suggests this limitation. As Cheng discloses, a “role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role.” Ex. 1004, 11:39-43. A POSITA would have understood that determining a role for a user based on the MAC address of the user’s client machine is determining network access for the client machine by monitoring the hardware condition of whether the client machine has an approved MAC address for a specific role that allows for corresponding network access.

107. In my opinion, a POSITA would have understood that a MAC address—i.e., the Media Access Control address—of a client machine or other device identifier is a hardware condition as disclosed in the ’038 patent. *See* Ex. 1001, 10:45-53 (“Endpoint hardware Information includes: Hardware configuration and state, such as: CPU type Total system memory Free memory Etc.”). As disclosed in the ’038 patent, “Endpoint Hardware Configuration Policies” include monitoring for a “Required device serial number.” *Id.*, 17:7, 17:12. A POSITA would have understood that a MAC address functions essentially as a device serial number for the network card of an endpoint and thus is part of the endpoint hardware configuration. Therefore, monitoring the MAC address to see if it is a required MAC address for determining a role for the user

satisfies a hardware condition as required by this limitation in the same manner as disclosed in an embodiment of monitoring a hardware condition in the '038 patent.

108. In addition, Cheng in view of the knowledge of a POSITA would have rendered this limitation obvious because by the priority date of the '038 patent, monitoring a plurality of operating conditions wherein the conditions comprise at least a hardware condition was well-known. The '038 patent admits as much. For example, the '038 patent discloses that “[a] typical method for monitoring hardware information is through the use of hardware device drivers and other similar operating system services.” Ex. 1001, 15:5-8; *see also, e.g.*, Ex. 1006, 8:14-18 (“a software agent works in conjunction with a computer's underlying operating system to detect the attachment or the detachment/reattachment of any security-sensitive peripheral device”). In my opinion, implementing a prior art hardware device driver or operating system service to monitor either hardware or software conditions on an endpoint is a predictable use that was well within the knowledge of a POSITA, would have resulted in a predictable result as claimed, and would have been obvious to try with a reasonable expectation of success.

109. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 8 and 19 obvious.

h. Claims 9 and 20

110. Claims 9 and 20 depend from claims 1 and 12, respectively, and further recite: “*wherein the conditions comprise at least one software condition.*”

111. In my opinion, Cheng discloses, teaches, or suggests this limitation. As Cheng discloses, “[d]evice-based interrogation tests [executed by a client agent] used to qualify a client machine may perform checks not possible with network-based scanning, such as detecting spyware, anti-virus software version, dates and/or versions of virus definition files, operating system update version information, etc., on the client machine.” Ex. 1004, 4:5-10; *see also id.*, 8:13-20 (“A policy rule set defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. ... For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.”). In my opinion, a POSITA would have understood that detecting spyware, anti-virus software version, versions of virus definition files, and operating system update version information are all detecting software conditions.

112. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 9 and 20 obvious.

i. Claims 10 and 21

113. Claims 10 and 21 depend from claims 1 and 12, respectively, and further recite: “*wherein the computing system comprises a plurality of servers.*”

114. In my opinion, Cheng discloses this limitation. As Cheng discloses, its computing system with the access manager can be comprised of a plurality of servers:

In one embodiment, the access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single rules manager is shown in FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks.

Ex. 1004, 7:23-31. Accordingly, Chen discloses that the computing system comprises a plurality of servers.

115. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 10 and 21 obvious.

j. Claims 11 and 22

116. Claims 11 and 22 depend from claims 1 and 12, respectively, and further recite: “*wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.*”

117. In my opinion, Cheng discloses this limitation. As Cheng discloses, a policy rule set that defines the tests for determining whether a client seeking access to the network has implemented particular protective measures may, for example, “set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.” Ex. 1004, 8:14-20. Cheng further discloses that “the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc.” *Id.*, 5:13-15; *see also id.*, 6:7-9 (“The results of these checks can be used to detect antivirus software installation, status and virus definition states.”). If the client machine does not have the latest antivirus version installed, Cheng discloses that “[t]he user can use the [remediation] resources to fix detected problems on the client machine in order to meet the required standards of adequate protection. For example, the remediation resources may locally provide one or more up-to-date virus checking options (engine and definitions).” *Id.*, 7:4-9. Therefore, Cheng discloses that at least one of the policies (i.e., adequate protection for anti-virus protection) includes the rule (i.e., check that the latest antivirus version has been installed on a client machine) that identifies the action (i.e., implement up-to-date virus checking options (engine and definitions)).

118. Thus, Cheng in view of the knowledge of a POSITA would have rendered claims 11 and 22 obvious.

3. Independent Claim 23

119. As shown below, it is my opinion that Cheng in view of the knowledge of a POSITA meets all limitations of independent claim 23 of the '038 patent.

a. Claim 23

i. “A system for controlling the operation of an endpoint, comprising:”

120. To the extent the preamble is a limitation, it is my opinion that Cheng discloses, teaches, or suggests it. Cheng discloses in Fig. 1 “a high level diagram of one embodiment of a system for qualifying a client to access a network.” Ex. 1004, 2:46-47. To qualify a client to access a network, “[t]he access manager 110 directs the qualification of a client machine through policies configured by an administrator.” *Id.*, 7:18-19. Therefore, Cheng discloses, teaches, or suggests a system with an access manager for controlling the operation (i.e., qualifying for access to a network) of an endpoint (i.e., a client machine).

121. Cheng further discloses, teaches, or suggests the remaining elements of the preamble of claim 23 for the same reasons I discussed above for the preamble of claim 1. *See supra* § VII.A.1.a.i.

122. Thus, Cheng discloses a system for controlling the operation of an endpoint.

ii. “a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;”

123. It is also my opinion that Cheng discloses this limitation of claim 23 for the same reasons I discussed above for the similar limitation of claim 1. *See supra* § VII.A.1.a.ii.

124. Thus, Cheng discloses a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies.

iii. “a data store, at the computing system, that contains the plurality of policies;”

125. It is also my opinion that Cheng discloses this limitation of claim 23 for the same reasons I discussed above for the similar limitation of claim 1. *See supra* § VII.A.1.a.iii.

126. Thus, Cheng discloses a data store, at the computing system, that contains the plurality of policies.

iv. “one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and”

127. It is also my opinion that Cheng discloses this limitation of claim 23. As Cheng discloses, the “access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” Ex. 1004, 6:59-62. The policy rule set “defines

the tests that determine whether a client seeking access to the network has implemented particular protective measures. Policy rule sets further set standards for adequacy for the particular protective measures. For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.” *Id.*, 8:14-20. In other words, “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” is determined. *Id.*, 8:30-34. Therefore, Cheng discloses that 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) is identified in the plurality of policies (i.e., policy rule sets) and monitored on the endpoint (i.e., determined by the client agent software on the client machine).

128. Cheng further discloses that one or more software agents on the endpoint are configured to monitor the plurality of operating conditions for the same reasons I discussed above for the similar limitation of claim 1. *See supra* § VII.A.1.a.v.

129. Thus, Cheng discloses one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies.

v. “one or more hardware processors at the computing system configured to:”

130. It is also my opinion that Cheng teaches this limitation of claim 23.

As Cheng discloses:

The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306. Such instructions may be read into main memory 306 from another computer-readable medium, such as storage device 310. Execution of the sequences of instructions contained in main memory 306 causes processor 304 to perform the process steps described herein.

Ex. 1004, 14:43-53. Therefore, in my opinion, a POSITA would have understood that Cheng teaches a processor in a computer system that is configured to perform the process steps for qualifying a client to access a network.

131. To the extent that Cheng’s “processor 304 executing one or more sequences of one or more instructions contained in main memory 306 and such instructions read into main memory 306 from another computer-readable medium,

such as storage device 310” are found not to be “hardware processors,” in my opinion, Cheng in view of a knowledge of a POSITA would have rendered obvious the use of hardware processors in place of the disclosed processors in Cheng’s system for qualifying a client to access a network. As Cheng discloses, “[i]n alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.” *Id.*, 14:53-57. Accordingly, in my opinion, a POSITA would have understood that Cheng’s system for qualifying a client to access a network could also be implemented by using hardware processors, such as hard-wired circuitry or a combination of hard-wired circuitry and software instructions. Moreover, a POSITA would have been motivated to implement hardware processors in place of software instructions run by processors to simplify the design and increase the speed of the computer system, as hardware processors have instructions hardcoded into them such that they do not have to read instructions from a separate memory.

132. Thus, Cheng discloses one or more hardware processors at the computing system.

vi. “receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,”

133. It is also my opinion that Cheng discloses, teaches, or suggests this limitation of claim 23 for the same reasons I discussed above for the similar limitation of claim 1. *See supra* § VII.A.1.a.vi. Moreover, in my opinion, a POSITA would have understood that this limitation can be performed by the one or more hardware processors at the computing system for the same reasons I discussed above in § VII.A.3.a.v.

134. Thus, Cheng discloses, teaches, or suggests one or more hardware processors at the computing system configured to receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents.

vii. “determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and”

135. It is also my opinion that Cheng discloses, teaches, or suggests this limitation of claim 23 for the same reasons I discussed above for the similar limitation of claim 1. *See supra* § VII.A.1.a.vii. Moreover, in my opinion, a POSITA would have understood that this limitation can be performed by the one or more hardware processors at the computing system for the same reasons I discussed above in § VII.A.3.a.v.

136. Thus, Cheng discloses, teaches, or suggests one or more hardware processors at the computing system configured to determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store.

viii. “initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.”

137. It is also my opinion that Cheng discloses, teaches, or suggests this limitation of claim 23 for the same reasons I discussed above for the similar limitation of claim 1. *See supra* § VII.A.1.a.viii. Moreover, in my opinion, a POSITA would have understood that the action can be initiated and carried out by the hardware processor on the endpoint for the same reasons I discussed above in § VII.A.3.a.v.

138. Thus, Cheng discloses, teaches, or suggests one or more hardware processors at the computing system configured to initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint. Accordingly, Cheng meets all limitations of claim 23.

4. Dependent Claims 24-33

139. It is also my opinion that Cheng in view of the knowledge of a POSITA would have rendered each of the following dependent claims obvious.

a. Claim 24

140. Claim 24 depends from claim 23 and further recites: “*wherein the action comprises controlling access of the endpoint to computing resources.*”

141. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 2 and 13. *See supra* § VII.A.2.a.

142. Thus, in my opinion, claim 24 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

b. Claim 25

143. Claim 25 depends from claim 23 and further recites: “*wherein the user interface comprises a web page.*”

144. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 3 and 14. *See supra* § VII.A.2.b.

145. Thus, in my opinion, claim 25 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

c. Claim 26

146. Claim 26 depends from claim 23 and further recites: “*wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis.*”

147. As I discussed above in § VII.A.3.a.v, Cheng teaches that its computer system for qualifying a client to access a network comprises one or more hardware processors. Furthermore, other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 4 and 15. *See supra* § VII.A.2.c.

148. Thus, in my opinion, claim 26 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

d. Claim 27

149. Claim 27 depends from claim 23 and further recites: “*wherein the endpoint comprises a mobile device.*”

150. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 5 and 16. *See supra* § VII.A.2.d.

151. Thus, in my opinion, claim 27 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

e. Claim 28

152. Claim 28 depends from claim 23 and further recites: “*wherein the one or more software agents comprise at least one service provided by the operating system of the endpoint.*”

153. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 6 and 17. *See supra* § VII.A.2.e.

154. Thus, in my opinion, claim 28 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

f. Claim 29

155. Claim 29 depends from claim 23 and further recites: “*wherein the one or more software agents comprise at least one application running on the endpoint.*”

156. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 7 and 18. *See supra* § VII.A.2.f.

157. Thus, in my opinion, claim 29 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

g. Claim 30

158. Claim 30 depends from claim 23 and further recites: “*wherein the conditions comprise at least one hardware condition.*”

159. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 8 and 19. *See supra* § VII.A.2.g.

160. Thus, in my opinion, claim 30 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

h. Claim 31

161. Claim 31 depends from claim 23 and further recites: “*wherein the conditions comprise at least one software condition.*”

162. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 9 and 20. *See supra* § VII.A.2.h.

163. Thus, in my opinion, claim 31 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

i. Claim 32

164. Claim 32 depends from claim 23 and further recites: “*wherein the computing system comprises a plurality of servers.*”

165. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 10 and 21. *See supra* § VII.A.2.i.

166. Thus, in my opinion, claim 32 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

j. Claim 33

167. Claim 33 depends from claim 23 and further recites: “*wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.*”

168. Other than the differences noted above in my analysis of independent claim 23, it is my opinion that Cheng renders this limitation obvious for the same reasons I discussed above for the same limitation of claims 11 and 22. *See supra* § VII.A.2.j.

169. Thus, in my opinion, claim 33 would have been obvious to a POSITA over Cheng in view of the knowledge of a POSITA.

B. No Secondary Considerations Exist

170. I am unaware of any secondary considerations of nonobviousness, and I understand no such considerations were alleged during prosecution. I reserve the right to rebut any alleged secondary considerations that Patent Owner or Patent Owner's expert declarant may assert during any instituted *inter partes* review.

VIII. Conclusion

171. In sum, for the reasons I have discussed above, it is my opinion that claims 1-33 of the '038 patent are unpatentable because they would have been obvious to a POSITA over the prior art reference cited above.

172. I understand that this Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also understand that I may be subject to cross-examination concerning this Declaration, and I will appear for cross-examination, if required of me, during the time allotted for cross-examination.

173. 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: February 9, 2023



John R. Black, Jr., Ph.D.

APPENDIX A

John R. Black, Jr.

Department of Computer Science
430 UCB
University of Colorado
Boulder, CO 80309-0430 USA

office: +1 303 492-0573
FAX: +1 303 492-2844
secretary: +1 303 492-7514

Email: jrblack@cs.colorado.edu
WWW: <http://www.cs.colorado.edu/~jrblack/>

Position	Assoc. Prof. Computer Science, University of Colorado at Boulder	<i>7/08–present</i>
Research	Cryptography, Network Security, Computer Security.	
Past Employment	SecureSet LLC Vice President of Education	<i>9/15–7/18</i>
	University of Colorado at Boulder Assistant Professor of Computer Science.	<i>7/02–7/08</i>
	University of Nevada, Reno Assistant Professor of Computer Science.	<i>7/00–6/02</i>
	University of California, Davis Research Assistant	<i>7/97–7/00</i>
	University of California, Davis Teaching Assistant	<i>8/95–6/97</i>
	Ingres Corporation Senior Member of Technical Staff	<i>6/88–4/94</i>
Education	University of California, Davis Ph.D. in Computer Science. Thesis: Message Authentication Codes. Advisor: Phillip Rogaway.	<i>9/95–9/00</i>
	California State University at Hayward B.S. in Computer Science and Mathematics, 1988. Honors: Summa Cum Laude	<i>9/84–6/88</i>
Awards	NSF CAREER Award, 2002 Chancellor's Teaching Fellowship, UC Davis, 1998 Outstanding Teaching Assistant, UC Davis, 1998 Outstanding Teaching Assistant, UC Davis, 1997 A Check for \$2.56 from Don Knuth, 1996	

rev January 9, 2023

Journal Publications

1. P. Rogaway, M. Bellare and J. Black, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption.” *ACM Transactions on Information and System Security (TISSEC)*, Volume 6, Issue 3, pp. 365–403, August, 2003.
2. J. Black, and P. Rogaway, “CBC MACs for Arbitrary Length Messages: The Three-Key Constructions.” *Journal of Cryptology*, Volume 18, Number 2, pp. 111–132, Spring, 2005.
3. J. Black, “The Impossibility of Technology-Based DRM and a Modest Suggestion.” *Journal of Telecommunications and High-Technology Law — JTHTL*, Volume 3, Number 2, pp. 387–396, Spring, 2005.
4. J. Black, M. Cochran and R. Gardner, “An Analysis of the Internet Chess Club.” *IEEE Security and Privacy*, Volume 4, Number 1, pp. 46–52, January, 2006.
5. J. Black, M. Cochran and T. Shrimpton, “On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions.” *Journal of Cryptology*, Volume 22, Number 3, pp. 311–329, Fall, 2009.
6. J. Black, P. Rogaway, T. Shrimpton, and M. Stam “An Analysis of the Blockcipher-Based Hash Functions from PGV.” *Journal of Cryptology*, Volume 23, Number 4, pp. 519–545, Fall, 2010.
7. C. Wilks, M. Cline, E. Weiler, M. Diehkans, B. Craft, C. Martin, D. Murphy, H. Pierce, J. Black, D. Nelson, B. Litzinger, T. Hatton, L. Maltbie, M. Ainsworth, P. Allen, L. Rosewood, E. Mitchell, B. Smith, J. Warner, J. Groboske, H. Telc, D. Wilson, B. Sanford, H. Schmidt, D. Haussler, D. Maltbie “The Cancer Genomics Hub (CGHub): overcoming cancer through the power of torrential data.” *Database*, Volume 2014, doi: 10.1093/database/bau093.

Book Chapters

1. J. Black, “Cryptography.” Invited article for the Encyclopedia of Life Support Systems under the auspices of UNESCO. See <http://www.eolss.net>. 14 pages, March, 2004.
2. J. Black, “Authenticated Encryption.” Invited article for the *Encyclopedia of Cryptography and Security*, Springer-Verlag. 12 pages. August, 2005.

**Conference
Publications
(Refereed)**

1. J. Black, C. Martel, and H. Qi, “Graph and Hashing Algorithms for Modern Architectures: Design and Performance.” *Workshop on Algorithm Engineering — WAE ’98*, Saarbrücken, Germany. Second Workshop on Algorithm Engineering, proceedings, pp. 37–48. Full version of this paper available at theory.cs.ucdavis.edu.
2. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, “UMAC: Fast and Secure Message Authentication.” *Advances in Cryptology — CRYPTO ’99*, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 216–233, 1999. Full version and updated version of this paper available at www.cs.ucdavis.edu/~rogaway/umac.
3. J. Black and P. Rogaway, “CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions.” *Advances in Cryptology — CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, Springer-Verlag, pp. 197–215, 2000.
4. P. Rogaway, M. Bellare, J. Black and T. Krovetz, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption.” *Eighth ACM Conference on Computer and Communications Security (CCS-8)*, ACM Press, pp. 196–205, 2001.
5. J. Black and P. Rogaway, “Enciphering Finite Sets of Arbitrary Size.” *RSA Data Security Conference, Cryptographer’s Track (RSA-CT)*, Lecture Notes in Computer Science, Vol. 2271, Springer-Verlag, pp. 114–130, 2002.
6. J. Black and P. Rogaway, “A Block-Cipher Mode of Operation for Parallelizable Message Authentication.” *Advances in Cryptology — EUROCRYPT 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 384–397, 2002.
7. J. Black and H. Urtubia, “Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption.” *USENIX Security Symposium — Security ’02*. 10 pages, 2002.
8. J. Black, P. Rogaway, and T. Shrimpton, “Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV.” *Advances in Cryptology — CRYPTO 2002*, Lecture Notes in Computer Science, Vol. 2442. 16 pages, 2002.
9. J. Black, P. Rogaway, and T. Shrimpton, “Encryption Scheme Security in the Presence of Key-Dependent Messages.” *Selected Areas in Cryptography — SAC 2002*, Lecture Notes in Computer Science, Vol. 2595, 14 pages, 2002.
10. R. Motwani, J. Breidenbach and J. Black, “Collocated Dataglyphs for Large Message Storage and Retrieval.” *Security, Steganography, and Watermarking of Multimedia Contents VI*, Society for Imaging Science and Technology (I&ST) jointly with International Society for Optical Engineering (SPIE), Vol. 5306, 19 pages, 2004.
11. J. Black, M. Cochran and T. Shrimpton, “On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions.” *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science, Vol. 3494, Springer-Verlag, pp. 526–541, 2005.
12. J. Black, M. Cochran and R. Gardner, “Lessons Learned: A Security Analysis of the Internet Chess Club.”, *Annual Computer Security Applications Conference — ACSAC 2005*, Tucson AZ, USA, pp. 220–228, 2005.
13. J. Black and M. Cochran and T. Highland, “A Study of the MD5 Attacks: Insights and Improvements”, *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 262–277, 2006.

**Conference
Publications
(cont.)**

14. J. Black, “The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function.”, *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 328–340, 2006.
15. J. Black, “Compare-by-Hash: A Reasoned Analysis”, *USENIX Annual Technical Conference — USENIX 2006*, 8 pages, 2006.
16. J. Black and M. Cochran, “MAC Reforgeability”, *Fast Software Encryption — FSE 2009*, Lecture Notes in Computer Science, Vol. 5665, Springer-Verlag, pp. 345–362, 2009.
17. J.H. Huang, J. Black, and S. Mishra, “Security and Privacy in a Sensor-Based Search and Rescue System,” *1st ICST/CREATE-NET International Conference on Ad Hoc Networks — ADHOCNETS 2009*, Vol. 28, Springer.
18. A. Sayler, D. Grunwald, J. Black, E. White, M. Monaco, “Supporting CS education via virtualization and packages: tools for successfully accommodating “bring-your-own-device” at scale,” *SIGCSE 2014*, pp. 313-318, 2014.

**Workshop
Publications
(Non-
Refereed)**

1. J. Black and P. Rogaway, “A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC.” *NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000*, 4 pages, Sep 2000.
2. J. Black and P. Rogaway, “OCB: Proposal to NIST.” *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 36 pages, Aug 2001.
3. J. Black and P. Rogaway, “PMAC: Proposal to NIST.” *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 27 pages, Aug 2001.

Selected Talks

1. Data Structures for Fast Graph Algorithms. Presented at the 1997 UC Davis Workshop on Computing, Davis, USA, October 1997. (See Conference Publication #1.)
2. UMAC: Fast and Secure Message Authentication. Presented at CRYPTO '99, Santa Barbara, USA, August 1999. (See Conference Publication #2)
3. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Presented at CRYPTO 2000, Santa Barbara, USA, August 2000. (See Conference Publication #3)
4. A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC. Presented at NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000, October, 2000; also presented at the 2nd NIST Modes Workshop in Santa Barbara, USA, August 2001.
5. Enciphering Finite Sets of Arbitrary Size. Presented at RSA-CT '02, San Jose, USA, February 2002. (See Conference Publication #5)
6. A Block-Cipher Mode of Operation for Parallelizable Message Authentication. Presented at EUROCRYPT 2002, Amsterdam, The Netherlands, May 2002. (See Conference Publication #6)
7. Side-Channel Attacks on Symmetric Encryption Schemes. Presented at USENIX Security 2002, San Francisco, USA, August 2002. (See Conference Publication #7)
8. Practical Cryptography and Autonomic Web Computing. Invited talk at the 47th meeting of the IFIP Working Group 10.4. Rincon, Puerto Rico, January 2005.
9. On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. Presented at EUROCRYPT 2005, Aarhus, Denmark, May 2005. (See Conference Publication #11)
10. The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function. Presented at FSE 2006, Graz, Austria, March 2006. (See Conference Publication #14)
11. Compare-by-Hash: A Reasoned Analysis. Presented at USENIX Technical Conference 2007, Boston, MA, June 2006. (See Conference Publication #15)

Patents

1. T. McSheery, J. Black, S. Nollet, J. Johnson, and V. Jivan. Distributed-Processing Motion Tracking System for Tracking Individually Modulated Light Points. US Patent 6,324,296 B1. November 2001.

Funding

1. NCHIA E-Team Grant. “Entrepreneurship for Undergraduates.” PI: John Black. Period: 2000-2001. Amount: \$6,000.
2. University of Nevada Junior Faculty Research Grant. “Fast, Provably-Secure Cryptography.” PI: John Black. Period: 2001-2002. Amount: \$10,000.
3. NSF CAREER Award. “Highly-Optimized Provably-Secure Cryptography.” PI: John Black. Period: 2002-2007. Amount: \$469,925.
4. NSF NeTS Grant. “NeTS ProWIN: Topology And Routing With Steerable Antennas.” PI: Dirk Grunwald. Co-PIs: John Black, Douglas Sicker. Period: 2005–2008. Amount: \$745,215.
5. NSF Cybertrust Grant. “Cryptography for Constrained Environments.” PI: John Black. Period: 2005–2008. Amount: \$294,887.

Teaching History

ECS 122A — Design and Analysis of Algorithms (UC Davis). Co-taught once with Professor Rogaway; subsequently taught the course independently.

CMPSC 290G — Intro to Cryptoanalysis (UCSB).

CS 365 — Discrete Mathematics (UNR).

CS 425 — Software Engineering (UNR).

CS 426 — Senior Projects (UNR). Supervised 11 group projects in topics ranging from fingerprint recognition to audio editing to GUI design.

CS 432 — Computer Networks (UNR). Introduction to low-level networking concepts with an emphasis on network security.

CS 665 — Graduate Analysis of Algorithms (UNR). A typical algorithms course with emphasis on complexity theory.

CS 709 — Modern Cryptography (UNR). A graduate course introducing cryptography and visiting some of the research front.

CS 791G — Computer Network Security (UNR). A seminar course covering various topics related to network security.

CSCI 2270 — Data Structures (CU); Program design, Object orientation, Java, Linked lists, Arrays, Stacks and Queues, Hash tables, Trees, Balanced Binary Trees, Multi-core programming.

CSCI 3104 — Algorithms (CU); Divide-and-conquer, Greedy, Graph Algorithms, NP-Completeness, Quantum Algorithms.

CSCI 3753 — Operating Systems (CU); Scheduling, Virtual Memory, Filesystems, Multi-core systems, Pthreads, Kernel data structures, virtualization, Security.

CSCI 4830 — Network Security (CU); a new course developed to introduce basics of cryptography and network security. Covers SSL, PKI, DDOS attacks, wireless security, buffer overruns, and more.

CSCI 4900 — Solving Puzzles with Computers (CU); a one-unit undergraduate course describing some hard combinatorial puzzles and how computers can be used to attack them.

CSCI 5413 — Ethical Hacking (CU); Network security, nmap, netcat, Kali Linux, Buffer overruns, Format string vulnerabilities, Race Conditions, Web Security, SQL Injections, XSS, CSRF, Wireless.

CSCI 6268 — Foundations of Computer and Network Security (CU); an introductory course covering basic cryptography, cryptographic protocols, attacks, and principles, as well as core network security attack and defense.

CSCI 7000 — Cryptography Seminar (CU); A graduate course introducing basic cryptographic definitions and then making some forays to the research front.

CSCI 7000 — Cryptanalysis Seminar (CU); A graduate course introducing students to cryptanalysis. Differential and linear cryptanalysis, square attack, RSA basics, factoring, protocol errors, lattices, Coppersmith's algorithm.

CSCI 7000 — Quantum Computing (CU); Introduction to quantum circuits, number theory, Shor's Algorithm, Grover's Algorithm.

Graduate Students

Rakhi Motwani, M.S., Completed: Spring 2002.

Scott Fritzinger, M.S., Completed: Summer 2002.

Hector Urtubia, M.S., Completed: Spring 2003.

Hiba Fayoumi, M.S., Completed: Summer 2004.

Mary Hedges, M.S., Completed: Spring 2007.

Joeseph Dunn, Ph.D., co-advisor with John Bennett, Completed: Summer 2007.

Martin Cochran, Ph.D., Completed: Spring 2008.

Jared Nishikawa, Ph.D., Completed: Spring 2016.

Undergraduate Students Troy Trimble, University of California at San Diego. REU Student, Summer 2003.
Gagan Sekhon, California State University at Hayward. REU Student, Summer 2003.
Ryan Gardner, University of Colorado at Boulder. REU Student, Summer 2004.
Trevor Highland, University of Texas at Austin. REU Student, Summer 2005.

**External
Service**

Secretary, International Association for Cryptologic Research, 2005–2007.
Program Committee, ACNS 2015.
Program Committee, CT-RSA 2015.
Program Committee, FSE 2014.
Program Committee, CT-RSA 2014.
Program Committee, CT-RSA 2013.
Program Committee, Eurocrypt 2012.
Program Committee, FSE 2011.
Program Committee, PKC 2011.
Program Committee, CANS 2010.
General Chair, CRYPTO 2009.
Program Committee, CRYPTO 2008.
Program Committee, ACNS 2008.
Program Committee, RSA-CT 2007.
Program Committee, ISC 2007.
Program Committee, ACNS 2007.
Program Committee, ACM CCS 2006.
Program Committee, CANS 2006.
Program Committee, ICISC 2006.
Program Committee, SECURE 2006.
Program Committee, ACSAC 2006.
Program Committee, CRYPTO 2005.
Program Committee, SAC 2005.
Program Committee, ICISC 2005.
Program Committee, CANS 2005.
Program Committee, IEEE SISW 2005.
Program Committee, CRYPTO 2004.
Program Committee, EUROCRYPT 2004.
Program Committee, RSA-CT 2003.
NSF CISE Panelist, 2001, 2003, 2005, 2006, 2007, 2009.
Referee for Journal of Cryptography, 1999–2006.
Referee for Software: Practice and Experience, 2005.
Referee for IEEE Communications Magazine, 2005.
Referee for IEEE Transactions on Circuits and Systems I, 2005.
Referee for IEEE Computer, 2005.
Referee for Journal of Computer Security, 2004.
Referee for IEEE Transactions on Information Theory, 2003.
Referee for IEEE Transactions on Computers, 2002.
Reviewer for CRYPTO 1999–2002, SODA 1998, SPAA 2002, Asiacrypt 2004, EURO-CRYPT 2006.

Developed **CryptoStats** web site: an application which tracks publication rates by year, by author, by conference in the two main cryptography conferences. It was heavily used in my community (on average 240 hits per month), 2003–2009.

ACM Programming Contest problem composer, 2003–2007.
ACM Programming Contest site administrator, 2005.

Graduate Student Mixer organizer, CRYPTO 2005.

**Internal
Service**

Chair, Computing Committee, 2010–2011, 2012–2015.

Chair, Space Committee, 2012–2015.

Liaison, Casey Feldman Foundation, 2010–2015.

Member, Departmental Executive Committee, 2003–2005, 2007–2009, 2013–2015.

Member, Executive Committee, Computer and Communications Security Center, 2003–2006.

Member, Departmental Search Committee, 2003–2006, 2012–2014.

Chair, Departmental Search Committee, 2008–2009.

Member, Graduate Committee, 2005–2006.

Developed departmental voting software, now used for all departmental votes and college votes.