

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

11,936,693

DECLARATION OF DR. CHUCK EASTTOM Ph.D., D.Sc.

TABLE OF CONTENTS

I.	Introduction.....	1
II.	LEGAL PRINCIPLES	5
	A. Person of Ordinary Skill in the Art.....	5
	B. Obviousness and Motivation to Combine.....	6
	C. Analogous Art.....	10
	D. Claim Construction	10
III.	Prior Art	11
	A. 10,949,406 (“Calvo”) is analogous, prior art to the ’693 Patent	11
	B. 11,558,414 (“Nguyen”) is analogous, prior art to the ’693 Patent	13
	C. 2012/0311696 (“Datsenko”) is analogous, prior art to the ’693 Patent	14
IV.	Technology Background.....	15
	A. Cloud Computing.....	15
	B. IP addresses, ports, and protocols.....	16
	C. Network Paths.....	18
	D. Routing Tables.....	21
	E. Attack Surfaces	22
	F. Penetration Testing	23
	G. Cybersecurity Policies	24
	H. PCI DSS.....	25
V.	Analysis.....	27
	A. Level of Ordinary Skill in the Art for ‘693 patent.....	27
	B. Overview of ‘693 patent	28
	C. Opinions Regarding Ground 1: Claims 1-7, 9-18, and 20-21 are Obvious Over Calvo and Nguyen.....	32
	1. Claim 1[pre]: A method for applying a policy on a network path, comprising:	32
	2. Claim 1[a]: selecting a reachable resource having a network path to access the reachable resource, wherein the	

reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment.....	32
3. Claim 1[b]: actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;	38
4. Claim 1[c]: storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network.....	48
5. Claim 1[d]: applying a policy on the valid path, wherein the policy includes a conditional rule;	52
6. Claim 1[e]: initiating a mitigation action, in response to determining that the conditional rule is not met; and	54
7. Claim 1[f]: applying the policy on another network path, in response to determining that the conditional rule is met	56
8. Claim 2: The method of claim 1, further comprising: initiating active inspection for each network path of a plurality of network paths; and applying the policy only on a network path of the plurality of network paths which is a valid path	61
9. Claim 3: The method of claim 2, further comprising: initiating active inspection by generating an access instruction for the reachable resource; and executing the access instruction on a network path.	63
10. Claim 4: The method of claim 2, further comprising: applying the policy only on each network path of the plurality of network paths which is a valid path.....	63
11. Claim 5: The method of claim 4, further comprising: initiating active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path.....	64
12. Claim 6: The method of claim 1, further comprising: initiating the mitigation action on the reachable resource.....	64
13. Claim 7: The method of claim 6, wherein the mitigation action includes any one of: revoking access to the	

reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.....	64
14. Claim 9: The method of claim 1, further comprising: initiating active inspection of the network path to detect an application path.....	65
Claim 10: The method of claim 9, further comprising: generating the mitigation action further based on the application path.....	66
15. Claim 11[pre]: non-transitory computer-readable medium storing a set of instructions for applying a policy on a network path, the set of instructions comprising:	66
16. Claim 11 [a] one or more instructions that, when executed by one or more processors of a device, cause the device to:	68
17. Claim 11[b]: select a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment;	72
18. Claim 11[c]: actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;	72
19. Claim 11[d]: storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network;	72
20. Claim 11[e]: apply a policy on the valid path, wherein the policy includes a conditional rule;	72
21. Claim 11[f]: initiate a mitigation action, in response to determining that the conditional rule is not met; and	72
22. Claim 11[g]: apply the policy on another network path, in response to determining that the conditional rule is met.	72
23. Claim 12[pre]: A system for applying a policy on a network path comprising:	73

24. Claim 12[a]: a processing circuitry; and.....	75
25. Claim 12[b]: a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to:	79
26. Claim 12[c]: select a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment;	80
27. Claim 12[d]: actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;	80
28. Claim 12[e]: store an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network;.....	81
29. Claim 12[f]: apply a policy on the valid path, wherein the policy includes a conditional rule;.....	81
30. Claim 12[g]: initiate a mitigation action, in response to determining that the conditional rule is not met; and	81
31. Claim 12[h]: apply the policy on another network path, in response to determining that the conditional rule is met.	81
32. Claim 13: The system of claim 12, wherein the memory contains further instructions which when executed by the processing 15 circuitry further configure the system to: initiate active inspection for each network path of a plurality of network paths; and apply the policy only on a network path of the plurality of network paths which is a valid path.	81
33. Claim 14: The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection by generating an access instruction for the reachable resource; and execute the access instruction on a network path.	81

34. Claim 15: The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: apply the policy only on each network path of the plurality of network paths which is a valid path.....	81
35. Claim 16: The system of claim 15, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path	82
36. Claim 17: The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate the mitigation action on the reachable resource.	82
37. Claim 18: The system of claim 17, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.....	82
38. Claim 20: The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection of the network path to detect an application path.....	82
39. Claim 21: The system of claim 20, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate the mitigation action further based on the application path.....	82
D. Opinions Regarding Ground 2: Claims 8 and 19 are Obvious Over Calvo, Nguyen, and Datsenko	83
1. Claim 8: Claim 8: The method of claim 1, further comprising: generating an exception to the policy based on a valid network path.	83

2.	Claim 19: The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate an exception to the policy based on a valid network path.	86
VI.	Conclusions.....	87

I. Introduction

1. My name is William C. Easttom II (Chuck Easttom), I have 30 years of experience in the computer science industry including extensive experience with computer science including cybersecurity. I have authored 44 computer science books, including textbooks used at over 60 universities around the world. I also have authored over 70 research papers and am an inventor with 27 computer science patents.

2. I hold a Doctor of Science (D.Sc.) degree in Cyber Security from Capitol Technology University (Dissertation Topic: “A Comparative Study of Lattice Based Algorithms for Post Quantum Computing”). I also hold a Doctor of Philosophy (Ph.D.) in Technology focused on nanotechnology (Dissertation Topic: “The Effects of Complexity on Carbon Nanotube Failures”) from Capitol Technology University. I also have a Doctor of Philosophy (Ph.D.) in Computer Science from the University of Portsmouth (Dissertation Topic: topic “A Systematic Framework for Network Forensics Using Graph Theory”). I also hold four master’s degrees (one in Applied Computer Science, one in Education, one in Defense and Strategic Studies, and one in Systems Engineering). I also hold over 80 computer industry certification in programming, networking, digital forensics, and cybersecurity.

3. I am currently an Adjunct Lecturer for Georgetown teaching graduate courses in requirements engineering, cybersecurity, artificial intelligence, and cryptography.

I am also an adjunct for Vanderbilt University teaching graduate computer science courses, specifically quantum computing, secure software engineering, and digital forensics. I also developed a graduate course in digital forensics for the University of Dallas and taught that course from 2019 to 2022.

4. I am a Senior member and Distinguished Speaker for the Association of Computing Machinery (ACM) and a Senior Member and Distinguished Visitor of the Institute for Electrical and Electronics Engineering (IEEE). The IEEE is the world's largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards for a wide range of engineering disciplines, including software development standards. I am also a Distinguished Visitor of the IEEE. I have been involved in IEEE standards creation for several years.

5. My full CV is included as **Appendix A**.

6. I am being compensated at my usual rate of \$550 per hour. My compensation is not dependent in any way upon my conclusions or the outcome of this matter. I have no financial interest in either Petitioner or Patent Owner in this matter.

7. As part of my work in forming my opinions in connection with this proceeding, I have reviewed the following materials. For the prior art listed below, it is my opinion that a person of ordinary skill in my field would have reasonably

relied on such prior art in forming opinions regarding the subject matter of this proceeding, as discussed further in the relevant sections of this Declaration:

Exhibit	Description
1001	U.S. Patent No. 11,936,693 (“’693 Patent”)
1002	Prosecution History for U.S. Patent No. 11,936,693 (“’693 Prosecution History”)
1004	U.S. Patent No. 10,949,406 to Calvo et al. (“Calvo”)
1005	U.S. Patent No. 11,558,414 to Nguyen (“Nguyen”)
1006	U.S. Patent Application Publication No. 2012/0311696 (“Datsenko”)
1007	U.S. Patent No. 11,418,528 to Deardorff et al. (“Deardorff”)
1008	Understanding Cloud Computing Basics, October 9, 2020, EU Online (“Cloud Computing Basics”)
1009	Introduction to Cloud Computing, Cloud Computing I, 15-319, Spring 2010, Majd F. Sakr (“Sakr”)
1010	Cloud Computing: An Overview, Ling Qian et al., 2009, LNCS 5931, 626-631 (“Qian”)
1011	The Introduction of Big Data in Cloud Computing, Austin Gruenberg, Minnesota State University Moorhead (“Gruenberg”)
1012	Cloud Computing Explained, Vangie Beal, May 21, 2010 (“Beal”)
1013	Study: Cloud Computing to Brighten Future of Data Centers, Martin LaMonica, March 10, 2008, CNET (“LaMonica”)
1014	Energy Aware Consolidation for Cloud Computing, Shekhar Srikantaiah et al. (“Srikantaiah”)
1015	Above the Clouds: A Berkeley View of Cloud Computing, Michael Armbrust et al, February 10, 2009 (“Armbrust”)
1016	Use of Cloud Computing Applications and Services, John Horrigan, September 12, 2008 (“Horrigan”)
1017	The NIST Definition of Cloud Computing, Publication 800-145, Peter Mell and Timoth Grance, U.S. Department of Commerce (“Mell”)
1018	NIST Cloud Computing Standards Roadmap, Publication 500-291, Version 2 (“Gallagher”)
1019	No Vacancy: IPv4 Address Depletion and Possible Solutions for the Expanding Internet, Illumin Magazine, June 27, 2011, Steve Wolfsohn (“Wolfsohn”)
1020	Internet Protocol, DARPA Internet Program Protocol Specification, September 1981, RFC: 791(“RFC 791”)

Exhibit	Description
1021	Internet Protocol, Version 6 Specification, December 1995 (“RFC 1883”)
1022	A Brief History of the Internet and Related Networks, Internet Histories, https://www.cs.kent.edu/~javed/internetbook/cerfs/cerf.html (“A Brief History of the Internet and Related Networks”)
1023	A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures, Zhijiang Chen et al., Big Data Research, 2015 (“Chen”)
1024	U.S. Patent Application Publication No. 2022/0360958 (“Cui”)
1025	Transmission Control Protocol, DARPA Internet Program Protocol Specification, September 1981, RFC: 793 (“RFC 793”)
1026	MegaLexica, Computer Dictionary of Information Technology (“MegaLexica”)
1027	U.S. Patent No. 10,205,638 to Angrish et al. (“Angrish”)
1028	European Patent Specification No. EP 3 013 016 to Murthy (“Murthy”)
1029	Cisco Configure Static Routing, Nexus 3000 Series Switches (“Cisco Static Routing”)
1030	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7 (“Cisco Firepower”)
1031	Cisco Routing Concepts (“Cisco Routing Concepts”)
1032	Analyzing the Internet’s BGP Routing Table, Geoff Huston, January 2001 (“Huston”)
1033	How Does the Internet Work? Rus Shuler, Pomeroy IT Solutions, 2002 (“Shuler”)
1034	Unicast Routing Principles, Microsoft TechNet (“Unicast Routing Principles”)
1035	Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networks’ Resilience Against Zero-Day Attacks, Mengyuan Zhang et al., IEEE Vol. 18, No. 1, January/February 2021 (“Zhang”)
1036	U.S. Patent Application Publication No. 2015/0058993 (“Choi”)
1037	U.S. Patent No. 10,509,909 to Andriani (“Andriani”)
1038	U.S. Patent No. 11,720,685 to Gwilliams (“Gwilliams”)
1039	U.S. Patent No. 11,336,555 to Soh et al. (“Soh”)
1040	U.S. Patent No. 9,621,595 to Lian et al. (“Lian”)

Exhibit	Description
1041	PCI Data Security Standard (PCI DSS), Version 1.1, September 2017 (“PCI DSS 1.1”)
1042	PCI Data Security Standard (PCI DSS), Version 1.2, March 2008 (“PCI DSS 1.2”)
1043	PCI Data Security Standard Requirements and Testing Procedures, Version 4.0, March 2022 (“PCI DSS 4.0”)
1044	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Matthew Scholl et al. (“Scholl”)
1045	European Patent Specification EP 2 869 535 to Scott et al. (“Scott”)

II. LEGAL PRINCIPLES

8. In forming my analysis and conclusions expressed in this Declaration, I have applied the legal principles described in the following paragraphs, which were provided to me by counsel for the Petitioner.

A. Person of Ordinary Skill in the Art

9. I understand that the factors considered in determining the ordinary level of skill in a field of art include: the level of education and experience of persons working in the field; the types of problems encountered in the field; the teachings of the prior art regarding solutions to such problems; and the sophistication of the technology at the time of the alleged invention. I understand that a person of ordinary skill in the art (“POSITA”) is not a specific real individual, but rather is a hypothetical individual having the qualities reflected by the factors above and knowledge of all relevant prior art references, including the references I cite below.

B. Obviousness and Motivation to Combine

10. I have been informed that a patent claim is invalid as “obvious” in light of one or more prior art references if it would have been obvious to a POSITA at the time of the alleged invention, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called “secondary considerations” of non-obviousness, which include: (i) “long-felt but unresolved need” for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) “copying” of the claimed invention by others.

11. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single prior art reference or multiple prior art references, there must be a reason that would have prompted a POSITA to modify or supplement the single prior art reference, or to combine two or more references, in a manner that provides the elements of the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference(s) themselves, the knowledge or “common sense” of a POSITA, or from the nature of the problem to be solved, and this reason may be explicit or implicit from the prior art as a whole. I have been informed that, under the law, the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable

results. I also understand it is improper to rely on hindsight in making the obviousness determination.

12. I understand that an obviousness determination also requires that a POSITA would have had a reasonable expectation of success. This concept has been explained to me as relating to the relative likelihood or predictability—from the perspective of a POSITA—of successfully modifying the prior art in the manner proposed, but that bodily incorporation is not necessary. I understand that the expectation of success need only be “reasonable” and, thus, does not require the absolute certainty gleaned from physically creating the proposed prior art modification.

13. I am informed that, in order to establish that a claimed invention was obvious based on a combination of prior art elements, a clear articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I am informed that, under the U.S. Supreme Court's *KSR* decision, a combination of multiple items of prior art renders a patent claim obvious when there was an apparent reason for a person having ordinary skill at the time of the invention to combine or modify the prior art. I am informed that such reasons may include, but are not limited to, one or more of the following rationales: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to

improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and/or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

14. I am informed that the test for obviousness is not necessarily whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference, but rather whether one of skill in the art at the time of the alleged invention would have been motivated to combine the teachings of the prior art references to achieve the claimed invention. I am informed that an invention that is a combination of prior art must do more than yield predictable results to be non-obvious and that, even where one or more motivations to combine exist, claims are not necessarily obvious unless a person having ordinary skill in the art would have had a reasonable expectation of success in implementing or applying the proposed combination at the time of the invention.

15. I also am informed that in conducting an obviousness analysis, a precise teaching directed to the specific subject matter of the challenged claim need not be sought out because it is appropriate to take account of the inferences and creative steps that a POSITA would employ. In other words, the prior art need not be directed towards solving the same specific problem as the problem addressed by the patent. Further, the individual prior art references themselves need not all be directed towards solving the same problem. The prior art considered can be directed to any need or problem known in the field of endeavor at the time of invention and can provide a reason for combining the elements of the prior art in the manner claimed. Common sense teaches that familiar items may have obvious uses beyond their primary purposes. I am informed that, under the *KSR* standard, common sense is important and should be considered in assessing obviousness.

16. I also am informed that the fact that a particular combination of prior art elements was “obvious to try” may indicate that the combination was obvious even if no one attempted the combination. If the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than innovation. I am further informed that in many fields it may be that there is little discussion of obvious techniques or combinations, and it often may be the case that market demand, rather than scientific literature or knowledge, will drive the design of an invention. When

there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a POSITA would have had a good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation, but of ordinary skill and common sense.

C. Analogous Art

17. I am informed that for a prior art reference to be proper for use in an obviousness rejection, the reference must be “analogous art” to the claimed invention. I am informed that a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to at least one problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). In order for a reference to be “reasonably pertinent” to a problem, it must logically have commended itself to an inventor’s attention in considering the inventor’s problem. In determining whether a reference is reasonably pertinent, one should consider the problem faced by the inventor, as reflected either explicitly or implicitly, in the patent.

D. Claim Construction

18. I understand that, for purposes of my analysis in this *inter partes* review proceeding, the terms appearing in the patent claims should be interpreted according

to their “ordinary and customary meaning.” In determining the ordinary and customary meaning, I understand that the words of a claim are first given their plain meaning that those words would have had to a person of ordinary skill in the art at the time of the alleged invention, in light of the patent as a whole, including the file history of the patent. Moreover, I understand that treatises and dictionaries may be used to inform the meaning attributed by a person of ordinary skill in the art to a claim term.

III. Prior Art

19. I have been informed that the earliest possible priority date for the ’693 Patent is April 13, 2022, and have been asked to assume such priority date for purposes of this analysis.

A. 10,949,406 (“Calvo”) is analogous, prior art to the ’693 Patent

20. I have been informed that because Calvo was filed March 25, 2019 and issued as a U.S. patent on March 16, 2021, that Calvo qualifies as prior art to the ’693 Patent under 35 U.S.C. §§ 102(a)(1) and (2).

21. In my opinion, Calvo is analogous prior art to the ’693 Patent because Calvo is in the same field of endeavor as the ’693 Patent and also because Calvo is reasonably pertinent to a problem that the inventors of the ’693 Patent were involved.

22. Calvo is in the same field of endeavor as the '693 Patent because a POSITA would have understood that both are directed to the field of cybersecurity. Calvo, Title, Abstract, 1:5-22, 2:7-36; '693 Patent, Title, Abstract, 1:20-32, 5:37-39. A POSITA would have understood that the field of cybersecurity includes concepts for protecting computing systems through, for example, inspection, policy application, compliance checks, network evaluations, etc. See e.g., Ex. 1007, Deardorff, 1:14-27. A POSITA would have understood that Calvo's policy application, compliance verification, and remediation disclosures for cloud networks to place Calvo in the field of cybersecurity. Calvo, Title, Abstract, 1:5-22, 2:7-36; '693 Patent, Title, Abstract, 1:20-32, 5:37-39; Ex. 1007, Deardorff, 1:14-27 (discussing defenses provisioned for cybersecurity defenses and countermeasures).

23. Calvo is also reasonably pertinent to a problem that the inventors of the '693 Patent were involved because a POSITA would have understood that both Calvo and the '693 Patent address problems related to policy application. '693 Patent, Title, Abstract, 2:44-62, 20:34-35, Fig. 9, Claims 1-21; Calvo, Title, Abstract, 1:6-22, 2:7-36. A POSITA would have also understood that both Calvo and the '693 Patent address problems related to managing networks at scale. '693 Patent, 1:59-2:17; Calvo, 1:19-22, 2:34-36.

B. 11,558,414 (“Nguyen”) is analogous, prior art to the ’693 Patent

24. I have been informed that because Nguyen was filed November 5, 2020 and issued as a U.S. patent on January 17, 2023, Nguyen qualifies as prior art to the ’693 Patent under 35 U.S.C. § 102(a)(2).

25. In my opinion, Nguyen is analogous prior art to the ’693 Patent because Nguyen is in the same field of endeavor as the ’693 Patent and also because Calvo is reasonably pertinent to a problem that the inventors of the ’693 Patent were involved.

26. Nguyen is in the same field of endeavor as the ’693 Patent because a POSITA would have understood that both are directed to the field of cybersecurity. Nguyen, Title, Abstract, 1:5-35; ’693 Patent, Title, Abstract, 1:20-32, 5:37-39. A POSITA would have understood that the field of cybersecurity includes concepts for protecting computing systems through, for example, inspection, policy application, compliance checks, network evaluations, etc. See e.g., Ex. 1007, Deardorff, 1:14-

27. Nguyen’s disclosures of penetration testing fall within the field of cybersecurity. A POSITA would have understood that the field of cybersecurity includes concepts for protecting computing systems through, for example, inspection, policy application, compliance checks, network evaluations, etc. See e.g., Ex. 1007, Deardorff, 1:14-27 (describing penetration testing); Nguyen, Title, Abstract, 1:5-35; ’693 Patent, Title, Abstract, 1:20-32, 5:37-39.

27. Nguyen is also reasonably pertinent to a problem that the inventors of the '693 Patent were involved because a POSITA would have understood that both Nguyen and the '693 Patent address problems related to determining network vulnerabilities/improving scanning techniques for attempting to infiltrate a network. '693 Patent, 1:43-50, 1:53-2:17; Nguyen, Title, Abstract, 1:5-35, 1:56-2:14, 11:56-58). A POSITA would have also understood that Nguyen and the '693 Patent address problems related to reducing time/resources/labor for cybersecurity protection processes. '693 Patent, 1:53-2:17; Nguyen, 1:18-25, 3:67.

C. 2012/0311696 (“Datsenko”) is analogous, prior art to the '693 Patent

28. I have been informed that because Datsenko was filed June 2, 2011 and published as a U.S. patent application publication on December 6, 2012, that Datsenko qualifies as prior art to the '693 Patent under 35 U.S.C. §§ 102(a)(1) and (2).

29. In my opinion, Datsenko is analogous prior art to the '693 Patent because Datsenko is in the same field of endeavor as the '693 Patent and also because Datsenko is reasonably pertinent to a problem that the inventors of the '693 Patent were involved.

30. Datsenko is in the same field of endeavor as the '693 Patent because a POSITA would have understood that both are directed to the field of cybersecurity. Datsenko, Title, Abstract, [0001]-[0003]; '693 Patent, Title, Abstract, 1:20-32, 5:37-

39. A POSITA would have understood that the field of cybersecurity includes concepts for protecting computing systems through, for example, inspection, policy application, compliance checks, network evaluations, etc. See e.g., Ex. 1007, Deardorff, 1:14-27. Datsenko's policy enforcement disclosures fall within the field of cybersecurity. See e.g., Ex. 1007, Deardorff, 1:14-27; Datsenko, Title, Abstract, [0001]-[0003].

31. Datsenko is also reasonably pertinent to a problem that the inventors of the '693 Patent were involved because a POSITA would have understood that both Datsenko and the '693 Patent address problems related to policy application. '693 Patent, Title, Abstract, 2:44-62, 20:34-35, 22:17-26, Fig. 9, Claims 1-21; Datsenko, Title, Abstract, [0001]-[0003], [0043]-[0044].

IV. Technology Background

32. In the following sub-sections, I briefly describe technology relevant to the '693 patent.

A. Cloud Computing

33. Cloud computing is the delivery of computing services, including servers, storage, databases, networking, software, analytics, etc.; over the Internet ("the cloud"). Ex. 1008, Cloud Computing Basics. Instead of owning their own computing infrastructure or data centers, companies can rent access to anything from applications to storage from a cloud service provider. Ex. 1009, Sakr. Users can

provision computing resources as needed automatically without requiring human interaction with each service provider. Ex. 1010, Qian. Cloud computing is thought to have begun in mid-2006, but it is recorded to have been brought up and discussed as early as the 1960s. Ex. 1011, Gruenberg. By 2009 cloud computing was well known and widely used. Ex. 1012, Beal; Ex. 1013, LaMonica; Ex. 1014, Srikantaiah; Ex. 1015, Armbrust. By 2008, research showed “‘Cloud computing’ takes hold as 69% of all internet users have either stored data online or used a web-based software application.” Ex. 1016, Horrigan.

34. NIST Special Publication 800-145 published September 2011 provides the NIST Definition of Cloud Computing. Ex. 1017, Mell. NIST Special Publication 500-291, Version 2 July 2013 NIST Cloud Computing Standards Roadmap. Ex. 1018, Gallagher.

B. IP addresses, ports, and protocols

35. The cloud is generally made up of “resources.” Ex. 1008, Cloud Computing Basics. A POSITA would have been very familiar with different types of cloud resources and how such resources are commonly identified.

36. An IP address (Internet Protocol address) is a unique identifier assigned to each device (resource) connected to a computer network that uses the Internet Protocol for communication. IP addresses help data find its destination on the internet or local networks. IP version 4 uses a 32 bit address space providing

approximately 4.2 billion addresses. IP version 6 uses a 128 bit address space. IP version 4 addresses were first created in 1983. Ex. 1019, Wolfsohn. The IP Protocol was standardized as RFC 791 in 1981. Ex. 1020, RFC 791. IPv6 was standardized as RFC 1883 in 1995. Ex. 1021, RFC 1883. By the end of 1991, the Internet has grown to include some 5,000 networks in over three dozen countries, serving over 700,000 host computers used by over 4,000,000 people. Ex. 1022, A Brief History of the Internet and Related Networks. In sum, there were a huge number of resources in cloud networks prior to the '693 Patent, and a POSITA would have known that IP addresses were one very common way to identify specific resources. See also Ex. 1023, Chen, Introduction.

37. Ports are another example of how resources can be identified. Ex. 1024, Cui, Abstract, [0036]; Ex. 1023, Chen, Introduction. For example, data packets need to know where to go and providing a port number, in addition to an IP address, is one exemplary resource identifier. Ex. 1023, Chen, Section 4.3.

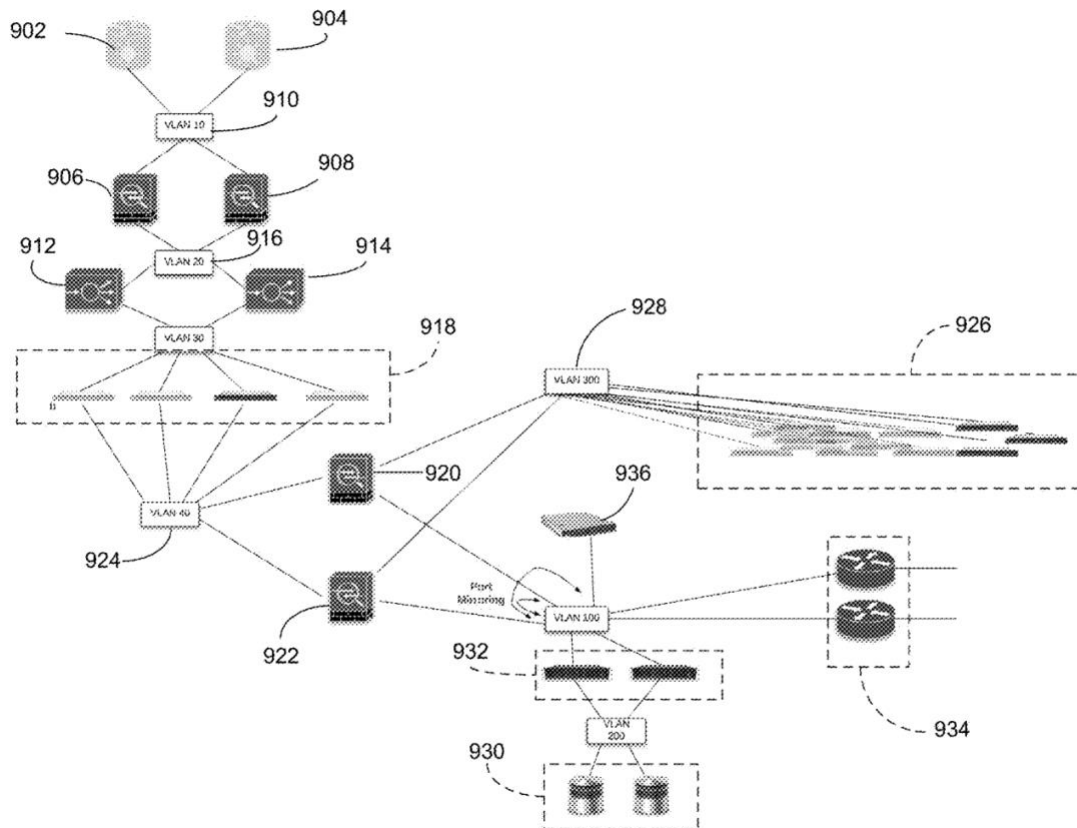
38. Protocols are agreed mechanisms by which network communication occurs. Network protocols are formal rules and conventions that define how data is transmitted and received across a network. TCP (Transmission Control Protocol) was first standardized as RFC 793 in 1981. Ex. 1025, RFC 793.

C. Network Paths

39. A POSITA would have understood a network path to be merely a connection of two or more resource nodes in a computing network, including in or partially in a cloud network. Ex. 1026, MegaLexica (defining “path” as “[a] path or explicitly routed Internet address; a node-by-node specification of a link between two machines.”).

40. Network paths can sometimes be presented in topology graphs (although this not necessary because any two computing resource nodes connected together connotes a network path). One such example is provided by Angrish:

FIG. 9



Ex. 1027, Angrish, Fig. 9.

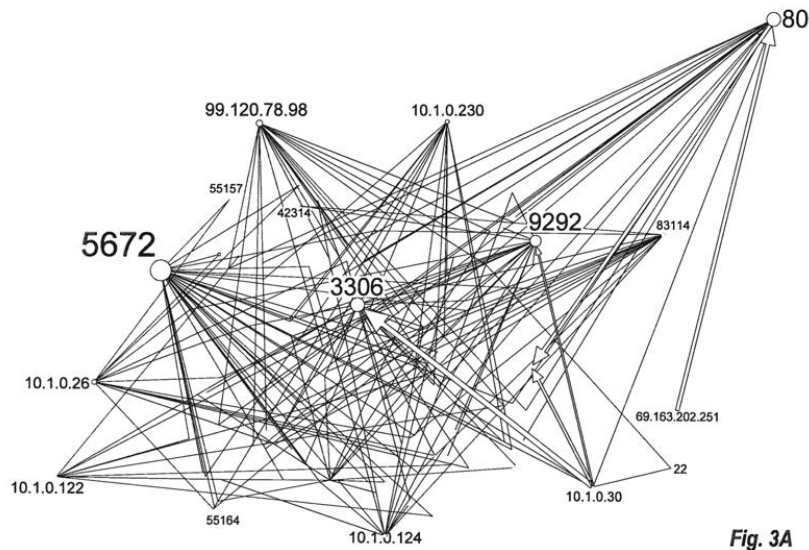
41. As Angrish explains in conjunction with its Figure 9:

One example of a complete virtual network topology that may be created by a user at the network segment level using the software architecture of FIG. 2 is shown in FIG. 9. Various functions may be separated from each other by strategically placed broadcast domains. Thus, gateway routers 902 and 904 are shown coupled to a pair of redundant dedicated or virtual firewalls 906 and 908 via VLAN 910. Load balancers 912 and 914 interface with the firewalls via VLAN 916. A virtual or dedicated server farm 918 is employed and separated from a second pair of firewalls 920 and 922 by VLAN 924. A virtual server cluster 926 interfaces with the firewall through VLAN 928. Dedicated cloud storage 930 and database servers 932 are also provided. A cloud bridge 934 and intrusion prevention system 936 round out the high-level topological features of the configuration shown in FIG. 9. This is

but one example of a customized virtual network that a consumer may configure based on the specific device level selections provided by the software interface architecture disclosed herein.

Ex. 1027, Angrish, 7:62-8:13.

42. Another well-known feature of network resources and their connections/paths is that parameters can be used to define a path. For example, Murthy depicts the following connection of resource nodes which are identified by IP addresses and ports:



Ex. 1028, Murthy, Fig. 3A.

43. As Murthy explains:

FIG. 3A illustrates an example network view that indicates one or more parameters included in the metric generated by the user interface engine 220. The network view includes nodes as illustrated with IP addresses and ports that represent the API interaction between nodes generated for the software code 134.

Ex. 1028, Murthy, [0049].

D. Routing Tables

44. Routers require tables that contain specific IP addresses that are reachable via specific router ports. Ex. 1029, Cisco Static Routing; Ex. 1030, Cisco Firepower; Ex. 1031, Cisco Routing Concepts. Routing tables include additional information about reachable IP addresses:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R -
       D - EIGRP, EX - EIGRP external, O - OSPF,
       N1 - OSPF NSSA external type 1, N2 - OSPF
       E1 - OSPF external type 1, E2 - OSPF exte
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
       * - candidate default, U - per-user static
       P - periodic downloaded static route

Gateway of last resort is not set
  10.0.0.0/24 is subnetted, 2 subnets
D       10.1.1.0/24 [90/2170112] via 209.165.200.224, 0:00:00, Ethernet0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.224, 0:00:00, Ethernet0/0
  192.168.10.0/24 is variably subnetted, 2 subnets
C       192.168.10.0/24 is directly connected, Ethernet0/0
L       192.168.10.1/32 is directly connected, Ethernet0/0
  192.168.11.0/24 is variably subnetted, 2 subnets
C       192.168.11.0/24 is directly connected, Ethernet0/0
L       192.168.11.1/32 is directly connected, Ethernet0/0
  209.165.200.0/24 is variably subnetted, 2 subnets
C       209.165.200.224/30 is directly connected, Ethernet0/0
L       209.165.200.225/32 is directly connected, Ethernet0/0
R1#
```

Id.

45. Cisco describes these routing tables as follows:

Static routes are those that you define explicitly. These are stable, normally high-priority routes, that you would use to ensure traffic to the route destination is always sent out the correct interface. For

example, you would create a default static route to cover all traffic not already covered by any other route, that is, 0.0.0.0/0 for IPv4 or ::/0 for IPv6. Another example would be a static route to an internal syslog server that you always want to use.

Dynamic routes are those learned through the operation of a routing protocol, such as OSPF, BGP, EIGRP, IS-IS, or RIP. You do not define the routes directly. Instead, you configure the routing protocol, and the system then communicates with neighbor routers, transmitting routing updates to them and receiving routing updates in turn.

Id.

46. Selecting a reachable resource, with an indicator that it is reachable has been a common feature of networks for many years. Ex. 1032, Huston; Ex. 1033, Shuler; Ex. 1034, Unicast Routing Principles.

E. Attack Surfaces

47. “The concept of attack surface has seen many applications in various domains, e.g., software security, cloud security, mobile device security, Moving Target Defense (MTD), etc.” Ex. 1035, Zhang, Abstract. A POSITA would have understood the concept of attack surface to mean the portions of a network which may be subject to cybersecurity attacks, namely through “entry and exit points[,]” “channels (e.g., TCP and UDP), and untrusted data items[,]” Ex. 1035, Zhang, Introduction. “[T]he concept of attack surface has [] seen many applications in other emerging domains, e.g., cloud security[.]” Ex. 1035, Zhang, Introduction; Ex. 1036, Choi (titled “System and Method for Discovering Optimal Network Attack Paths”).

F. Penetration Testing

48. Penetration testing, also known as pen-testing, was a well-known cybersecurity process for protecting against attackers infiltrating an internal network from the outside. Ex. 1037, Andriani, 1:23-26 (“The phrases ‘pentesting’ (penetration test) and ‘vulnerability scanning’ became synonymous with every organization's cyber security program for protecting their network against malicious infiltration.”).

49. Described another way, Deardorff discloses:

Penetration testing involves an authorized simulated attack on a computer system to evaluate the security of the computer system. For example, penetration testing can identify security vulnerabilities, including the ability of potentially malicious actors to gain access to the computer system and/or associated storage devices and/or network infrastructure. A penetration test identifies a target computing system and a particular goal, and then undertakes various exploit actions to attain the goal. By doing so, the penetration test can determine whether the target computing system is vulnerable to attack if cybersecurity defenses were provisioned adequately, and which cybersecurity countermeasures, if any, the penetration test defeated.

Ex. 1007, Deardorff, 1:14-27.

50. Penetration testing was also specifically known for use in cloud environments prior to the '693 Patent. *See, e.g.*, Ex. 1038, Gwilliams, 4:28-36 (“pentesting device 100 may be configured to perform a pentest on a target application 102. The target application 102 may include networks (for example, Wi-Fi networks, LANs, WANs, and cloud networks), hardware, software, data centers, web applications, servers (for

example, application servers and Internet servers), virtual machines, operating systems, communication devices (for example, routers switches), internet of things (IOT) devices, among other components.”); Ex. 1039, Soh, 1:25-42 (“With new computing environments such as cloud computing coming within the scope of the PCI DSS requirements, there is growing demand from various affected business units and stakeholders within an organization (e.g., a bank issuing credit cards) to perform PCI penetration tests.”).

51. And penetration testing of internal networks on “paths” was known to be accomplished by traversing resource nodes. Ex. 1007, Deardorff, Title, Abstract, 8:64-9:9.

G. Cybersecurity Policies

52. Cybersecurity policies can generally be used to protect and control access to critical data. For example, Lian first explains:

A hardware firewall is a network security system that controls incoming and outgoing network traffic. A hardware firewall generally creates a barrier between an internal network (assumed to be trusted and secure) and another network (e.g., the Internet) that is assumed not to be trusted and secure.

Attackers breach internal networks to steal critical data. For example, attackers target low-profile assets to enter the internal network. Inside the internal network and behind the hardware firewall, attackers move laterally across the internal network, exploiting East-West traffic flows, to critical enterprise assets. Once there, attackers siphon off valuable company and customer data.

Ex. 1040, Lian, 1:19-31.

53. Lian is one example reference disclosing cybersecurity policies. Ex. 1040, Lian, Title (“Conditional Declarative Policies”). Lian discloses an exemplary

firewall rule set which may include: receiving a declarative policy associated with a computer network security policy; collecting information from at least one external system of record; generating a firewall rule set using the declarative policy and information, the firewall rule set including addresses to or from which network communications are permitted, denied, redirected, and/or logged, the firewall rule set being at a lower level of abstraction than the declarative policy; and provisioning the firewall rule set to a plurality of enforcement points of a distributed firewall, the firewall selectively policing network communications among workloads using the firewall rule set.

Ex. 1040, Lian, 1:35-48.

54. In sum, a POSITA would have understood a cybersecurity policy could be one or more rules about network access to one or more computing nodes in a network. Ex. 1040, Lian, 1:35-4.

H. PCI DSS

55. PCI DSS is a security standard that represents an example of a security compliance policy. Ex. 1004, Calvo, 2:5-24. Specifically, “Payment Card Information Data Security Standard (PCI DSS) outlines detailed requirements for securing cardholder data that is stored, processed, or transmitted by merchants, banks, and other organizations.” Ex. 1039, Soh, 1:20-24.

56. As Soh explains, **penetration testing is a requirement for PCI DSS:**

One of the requirements in the PCI DSS is performance of network-layer penetration testing on the organization's network segmentation

structure. Under Section 11.3.4.1 of the PCI DSS, this penetration testing must be conducted at least annually and after any significant infrastructure or application upgrade or modification; and at least every six months and after any changes to network segmentation controls or methods. Network segmentation refers to the process of dividing a network into smaller segments in such a way that limits or prevents communication between them. It is a security practice that enables the merchant, bank or other organization to protect its cardholder data.

With new computing environments such as cloud computing coming within the scope of the PCI DSS requirements, there is growing demand from various affected business units and stakeholders within an organization (e.g., a bank issuing credit cards) to perform PCI penetration tests.

Ex. 1039, Soh, 1:25-42.

57. A POSITA would have been well-aware that penetration testing is a requirement for PCI DSS, as it was well-known before the '693 Patent and several versions of PCI DSS (before the '693 Patent) each required and discuss penetration testing. Ex. 1041, PCI DSS 1.1; Ex. 1042, PCI DSS 1.2; Ex. 1043, PCI DSS 4.0; Ex. 1039, Soh, 1:25-42.

58. Not only is penetration testing an annual requirement, but penetration testing must be conducted after significant infrastructure or application changes, including network segmentations. *Id.*

59. Penetration to comply with PCI DSS was known to be increasingly important with the rise of cloud computing networks. Ex. 1039, Soh, 1:25-42.

60. PCI DSS explains the “[p]urpose” of the required penetration testing as follows:

Attackers spend a lot of time finding external and internal vulnerabilities to leverage to obtain access to cardholder data and then to exfiltrate that data. As such, entities need to test their networks thoroughly, just as an attacker would do. This testing allows the entity to identify and remediate weakness that might be leveraged to compromise the entity's network and data, and then to take appropriate actions to protect the network and system components from such attacks.

Ex. 1043, PCI DSS 4.0, p. 245.

61. In addition to PCI DSS, penetration testing was recommended for HIPPA compliance. Ex. 1044, Scholl.

V. Analysis

62. This section contains my analysis of U.S. Patent 11,936,693 ('693 patent) and its invalidity in light of the prior art.

A. Level of Ordinary Skill in the Art for '693 patent

63. A person of ordinary skill in the art as of the '693 patent's earliest priority claim would have a bachelor's degree in an academic area emphasizing computer science (i.e. computer science, computer information systems, computer engineering, etc.) and (2) at least two years of experience in the field of cybersecurity. Additional education could substitute for less experience and vice versa.

64. Based on my education, training, professional experience, and additional experience summarized in Section I above and provided in full in my curriculum vitae attached as **Appendix A**, I am familiar with the level and abilities of a POSITA

at the time of the claimed invention in the '693 Patent. Additionally, I met at least these minimum qualifications to be a POSITA to the '693 Patent before April 13, 2022. Further, although my qualifications may exceed those of the hypothetical POSITA defined above, my analysis and opinions regarding the '693 Patent have been rendered from the perspective of a POSITA at the time of the claimed invention.

B. Overview of '693 patent

65. US Patent 11,936,693 was granted March 19, 2024 based on application 18/357,845 filed July 24, 2023. It is a continuation in part of application No. 17/818,898 filed August 10, 2022, and a continuation in part of application No. 17/659.163. filed on Apr. 13, 2022, and a continuation-in-part of application No. 17/659.164, filed on Apr. 13, 2022 and a continuation in part of application No. 17/659.165 filed on April 13, 2022.

66. The '693 patent involves accessing reachable resources including cloud resources. By examining the network path, the '693 can determine if the resource is accessible from the external network ('694 patent, 2:44-52). The '693 uses active inspection for network paths ('693 patent, 2:63-3:3). The '693 also applies policies ('693 patent, 34:36-46). Figure 1 of the '693 is a diagram of a cloud computing environment monitored by an active inspector, implemented in accordance with an embodiment:

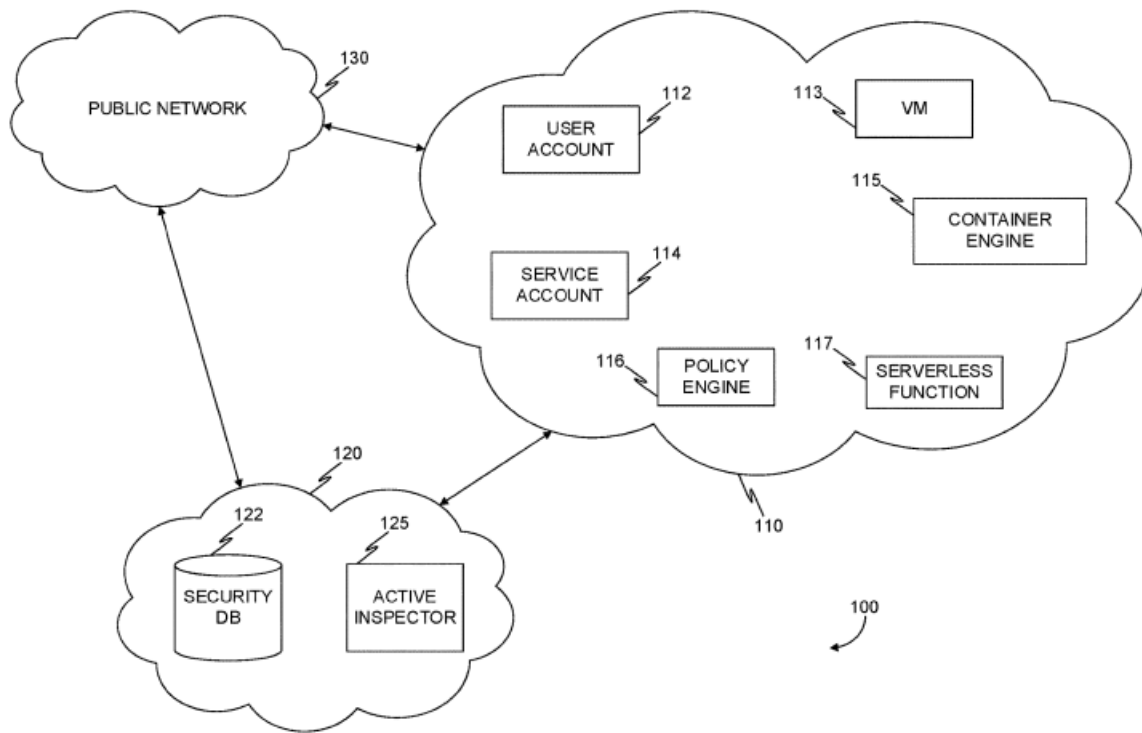


FIG. 1

67. The '693 involves generating instructions directed to a resource over a network path and receiving a response. For example, using the SSH protocol.

68. The '693 Patent is generally directed to cybersecurity. '693 Patent, Title, Abstract, 1:20-32, 1:43-45, 5:37-51, Claims 1-21.

69. Regarding resource inspection, the '693 Patent describes “external attack surface management (EASM) is a term which for a technology field and best practices which are utilized in cybersecurity to describe what vulnerabilities an organization has within their network infrastructure[.]” ('693 Patent, 1:27-32). The '693 Patent purports to disclose an “efficient way” of EASM through a process the '693 Patent refers to as “active inspection.” ('693 Patent, 5:40-55). Per the '693

Patent, “active inspection” determines which theoretical vulnerabilities are “indeed vulnerable” by trying to access internal cloud resources from an external resource (’693 Patent, 10:66-11:6, 20:44-48) by sending instructions and receiving responses (’693 Patent, 5:40-44, 8:2-7, 9:62-63, 9:64-10:6). If the resource can be successfully accessed from an external network, the network path to such resource is determined to be a valid/viable network path (’693 Patent. ’693 Patent, 10:50-53, 10:56-58, 11:10-14, 20:3-6, Claim 1).

70. The ’693 Patent discloses a process for applying a policy (after determining a network path is valid per active inspection), checking for compliance of such policy, and then either (A) mitigating in an instance of noncompliance or (B) continuing to apply the policy on other paths in an instance of compliance:

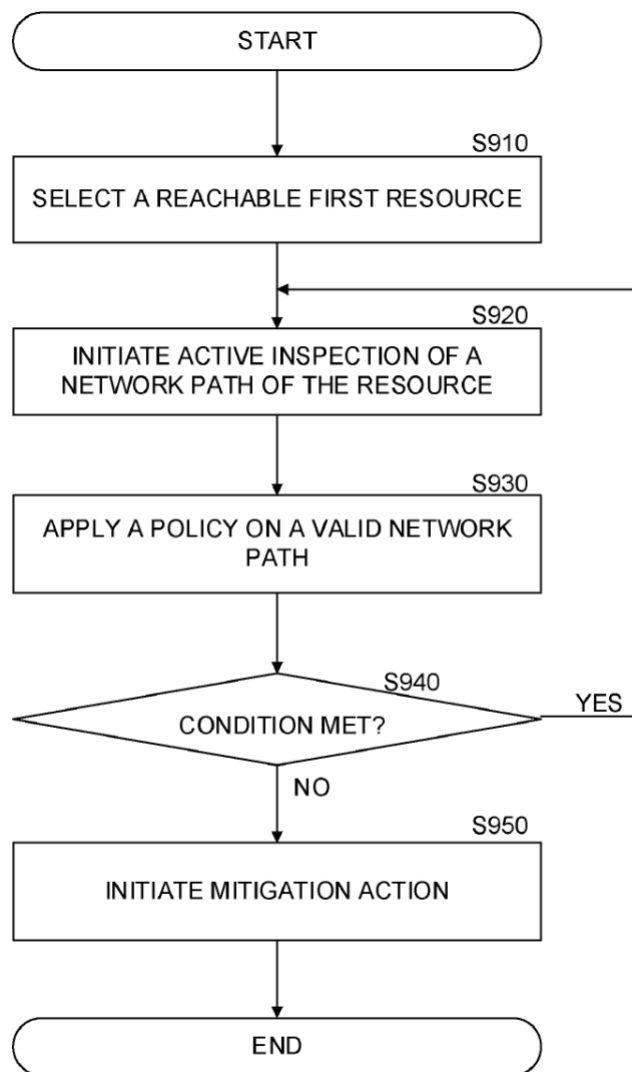


FIG. 9

71. '693 Patent, Fig. 9, Claim 1, 5:21-22, 20:34-22:57.

72. The '693 Patent provides the following exemplary scenario for “a policy [] applied on a valid network path” ('693 Patent, 21:56, Fig. 9 at S930): “a policy includes a statement that a network path to/from a first reachable resource should only be accessible via a predefined port (e.g., port 80) using a predefined protocol (e.g., HTTPS). In some embodiments, where a viable network path is detected, the

policy is applied to determine if the network path adheres to the policy or not.” ’693 Patent, 22:2-8; *see also* ’693 Patent, 5:43-51 (using “port 22” as an example).

C. Opinions Regarding Ground 1: Claims 1-7, 9-18, and 20-21 are Obvious Over Calvo and Nguyen

1. Claim 1[pre]: A method for applying a policy on a network path, comprising:

73. I have been informed that the preamble is not generally construed as limiting and that neither party has proposed the preamble as limiting here.

74. Regardless, in my opinion, Calvo in view of Nguyen renders obvious Claim 1[pre]. For example, Clavo’s disclosures of applying/deploying a compliance pack to cloud-based resources which have specific paths to/from external network such as the Internet teach applying a policy on a network path, as claimed. This is explained below in Claims 1[a]-1[d].

2. Claim 1[a]: selecting a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment

75. In my opinion, Calvo’s disclosures of selecting target cloud-based resources which have specific paths to/from external network such as the Internet teach selecting a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud

computing environment, having access to an external network which is external to the cloud computing environment, as claimed.

76. Calvo's resource teaches a resource as it is in the '693 Patent. Compare Calvo, 3:30-41, with '693 Patent 6:37-47.

77. Calvo teaches selecting a reachable resource. In general, Calvo teaches methods "for compliance lifecycle management for cloud-based resources." Calvo, 2:7-9. In a specific example, Calvo discloses that "[t]he client may also use a resource selection component 130 to select a set of target resources 185 from the resources 180 of the provider 20 network 190." Calvo, 4:17-20. This is shown in multiple Figures, for example Figs. 1A-1B ("Resource Selection 130"), Figs. 2A-2B ("Select target resources for deployment of the selected compliance pack 210").

78. The '693 Patent explains what it means by "reachable resource" in the following excerpts: "[a] reachable resource is a resource which includes at least a viable network path, having reachability parameters which allow access from an external network to the resource, the resource deployed in a cloud computing environment." '693 Patent, 16:56-60; *see also* '693 Patent, 5:43-46, 5:66-6:2, 7:50-53, 9:28-31, 10:20-21, 18:66-19:3. "In an embodiment, a network path may be stored as a data string which includes one or more reachability parameters. Such parameters include host names, protocols, IP addresses, ports, usernames, passwords, and the like." '693 Patent, 7:50-53.

79. Calvo discloses that Calvo's target resources may be in "one or more multitenant provider networks, including one or more regions of such networks." Calvo 2:42-45; *see also* Calvo 3:29-41, 4:17-20, 8:1-5. Furthermore, Calvo discloses a network interface 3040 using network protocols to communicate with other device(s) 3060 via network(s). Calvo, 14:64-15:6, Fig. 8. As was discussed in section IV.B of this declaration, IP addresses, ports, and network protocols have been well known for decades, and a POSITA would have certainly been familiar with them.

80. A POSITA would have readily understood that IP addresses and ports are part of typical network communication. Specifically, A POSITA would have understood Calvo's system to utilize network interface 3040 and common network protocols, including a parameter (i.e., IP address, port number, etc.) to communicate with reachable resources, such as Calvo's target resources.

81. The '693 Patent explains a network path is "a connection of two or more security objects[.]" '693 Patent, 12:46-47. For example, the network path "may be a path from a virtual machine (VM), connected to a NIC, connected to a load balancer, connected to a firewall." '693 Patent, 13:57-59. Example security graph 200 (Fig. 2) of the '693 Patent illustrates a network path consisting of a plurality of nodes (i.e., firewall node 220, API gateway node 230, VM node 240, container engine node 250,

etc.) connected to at least another node by an edge which may represent access connection between said nodes ('693 8:30-39, 8:63-9:15):

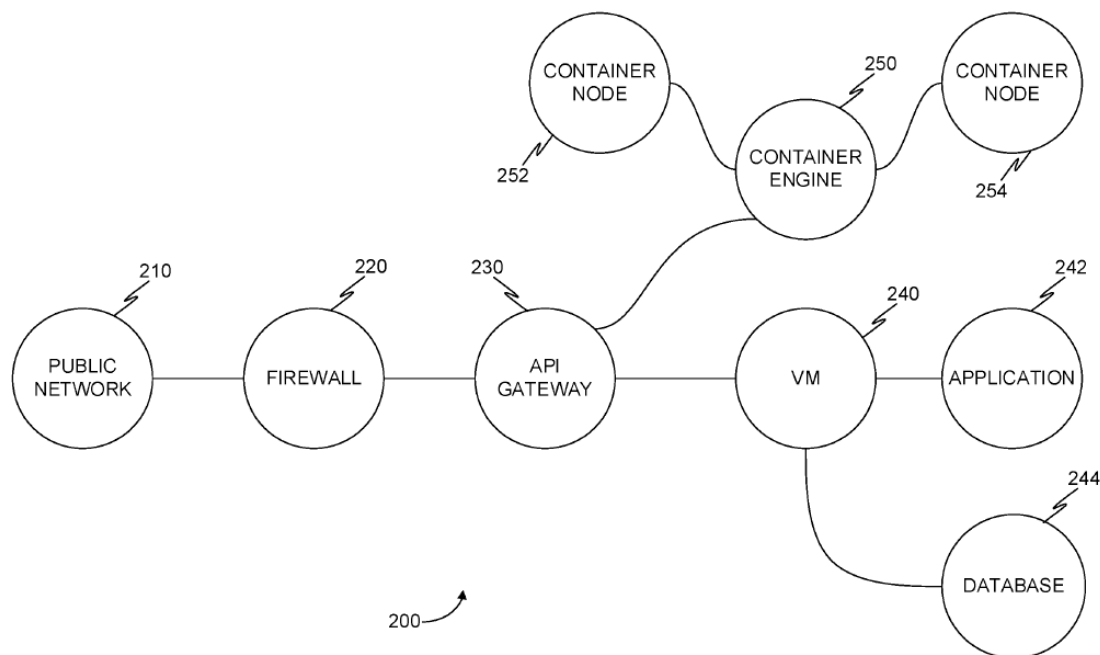


FIG. 2

'693 Patent, Fig. 2. The exemplary nodes depicted above (i.e., firewall node 220, API gateway node 230, VM node 240, container engine node 250, etc.) are each a resource as defined by the '693 Patent. *See* '693 Patent, 6:37-40 (“A resource is a cloud entity which supplies functionality, such as processing power, memory, storage, communication, and the like.”), 6:41-44 (“Resources may include [] virtual machines (VMs) [] container engines [] serverless functions”), 8:57-67 (“API gateway node 230 [] represents an API [] gateway. An API gateway is a workload, for example a serverless function”). A POSITA would have understood Figure 2 of the '693 patent to depict at least the following network path: public

network>firewall>API gateway>additional resources (including as few as two such connected resource nodes).

82. As I will discuss further below, Calvo teaches at least the following exemplary network path to access the reachable resources: public Internet>firewall>port 22>resource(s).

83. In discussion of the rules of Clavo's compliance pack, Calvo says,

Remedial actions 175A in a compliance pack 171A may include automated tasks or workflows to be performed for resources found to be noncompliant. Remedial actions for noncompliance may include notifying relevant users, modifying a configuration of a resource, isolating a resource, and so on. **For example, a rule in an InfoSec compliance pack may be used to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the relevant rule.** Using a single compliance pack, such rules may be applied to disparate resources throughout an enterprise in a consistent manner. In one embodiment, a data structure for a compliance pack action may indicate a CompliancePackID, ActionName, ActionResourceNumber, ActionArtifactsRepositoryLocation, CreationTime, LastUpdatedTime, and UpdatedBy.

Calvo, 6:30-45 (emphasis added). Within the above example (and whole paragraph), a POSITA would have understood Calvo's disclosed Internet, firewall, port, and subsequent resource(s) to all be "resources" per the '693 Patent. And because each of these resources represent computing nodes connected together in one or more networks (e.g., public external network/Internet and internal cloud-based network), a POSITA would have further understood such Calvo resources to represent one or

more network paths per the '693 Patent. Additionally, as I explained previously, network paths were known to merely be a connection of more than one computing node, usually evidenced by parameters such as port numbers; routing tables for example use these parameters to route data to the appropriate locations via specific network paths. Section IV.B (IP addresses, ports, and protocols); Section IV.C (network paths); Section IV.D (routing tables).

84. Accordingly, Calvo teaches a reachable resource having a network path to access the reachable resource. Calvo teaches that its selected target resources (e.g., resources on the internal network side of Calvo's firewall) include one or more reachability parameters (e.g., Calvo's port 22) which may provide access from an external network (for example, through Calvo's firewall from the public Internet), where Calvo's selected cloud-based target resources have one or more reachability parameters per the '693 Patent. Calvo, 6:35-39, 3:37-41.

85. Calvo teaches that the reachable resource is a cloud object deployed in a cloud computing environment. Calvo, 2:9-12, 2:37-40, 3:24-41, Figs. 1A-1B.

86. Calvo teaches its selected cloud-based resources have access to an external network which is external to the cloud computing environment. Calvo's selected target resources are "cloud-based resources" that are "hosted in the cloud," and such resources may be "hosted in one or more provider networks" or "one or more multi-tenant provider networks, including one or more regions of such networks." Calvo,

Abstract, 3:33-35, 2:44-45, 3:35-37 (“The resources 180 may be hosted in one or more multi-tenant provider networks such as networks 190 and 191.”), Fig. 1B. Calvo specifically discloses “[t]he resources 180 may be accessed from inside or outside the provider networks (e.g., via one or more public networks such as the Internet and/or one or more private networks by resource owners or other provider network clients, such as clients 10.” Calvo, 3:37-41, 9:3-8, Fig. 1B. A POSITA would have understood that accessing the resources from “outside the provider networks” via “the Internet” to mean the resources have access to an external network which is external to the cloud computing environment.

87. For at least these reasons, Calvo teaches this claim limitation.

3. Claim 1[b]: actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network;

88. In my opinion, Calvo in view of Nguyen teaches actively inspecting the network path to determine if the network path of the reachable resource is accessible from the external network at least because Nguyen’s discloses a process of pen-testing targets/potential vulnerabilities to determine if such are actual vulnerabilities by sending instructions and receiving responses).

89. The ’693 Patent discloses that “[p]erforming an active inspection of a cloud environment allows to determine which of the reachability paths (i.e., network paths) are indeed vulnerable, meaning that paths that can be used to gain access into the

cloud environment, and which reachability paths (network paths) are not vulnerabilities since the active inspector could not gain access to the resource, therefore the reachability path is not possible in practice.” ’693 Patent, 10:66-11:6. Additionally, the ’693 Patent states that “it is advantageous to determine if a network path is a valid network path, i.e., a network path through which a resource is really reachable, as opposed to an invalid network path, which seems reachable, but in practice cannot be used to access the resource.” ’693 Patent, 20:44-48. A POSITA would have understood that active inspection per the ’693 Patent determines which theoretical vulnerabilities of network paths are real vulnerabilities.

90. The ’693 Patent discloses that “[a]ctive inspection allows to generate instructions directed at the reachable resource over a network path, which when received by the reachable resource cause the reachable resource to send a response. For example, a reachable resource may have indicated that port 22 is an open port.” ’693 Patent, 5:40-44; *see also* ’693 Patent, 9:62-63, 10:50-53, 10:56-58, 11:10-14, 20:3-6. Furthermore, the ’693 Patent explains that the generated instruction “may be to send a data packet to an IP address of the resource, and receive an acknowledgement (ACK) response.” ’693 Patent, 8:2-7. More specifically, the ’693 Patent states “**the instruction includes one or more access parameters. Such parameters may include, but are not limited to, a host name, an IP address, a communication protocol, a port, a username, a password, and the like, or**

combination thereof. **A communication protocol may be, for example, HTTP or UDP (user datagram protocol). For example, the instruction may be a ping, GET, CONNECT, or TRACE request over HTTP.**” ’693 Patent, 9:64-10:6 (emphasis added).

91. Similarly, Nguyen teaches determining which “targets” represent “actual vulnerabilities” by performing pen-testing. Nguyen’s process includes sending instructions and receiving responses to identify actual threats from external surfaces in the same manner as the ’693 Patent. *Compare* Nguyen, 4:46-50, 10:52-11:6, 12:29-13:44, 16:1-4, *with* ’693 Patent 5:40-44, 8:2-7, 9:62-63.

92. Nguyen discloses that “[t]he reconnaissance component 210 performs reconnaissance on a desired scope (e.g., all applications and computing systems owned, operated, and/or controlled by the entity 106) to map a relevant external surface 244. The relevant external surface 244 identifies the potential targets within the desired scope that are publically accessible (e.g., via a network, such as the Internet)[.]” Nguyen, 5:15-21; *see also*, 2:9-14, 2:45-51, 15:6-16. Where the “reconnaissance component 210 may use public information obtained from public sources to map the relevant external surface 244” and “may be characterized as identifying [] what the bad guys see[.]” Nguyen, 5:27-29, 6:50-51. Nguyen defines the term “external surface” as “all of the targets within a particular scope through which an external actor may attempt to take advantage of a potential vulnerability.”

Nguyen, 4:11-15. Nguyen defines the term “target[s]” as “public facing access point[s] or endpoint[s].” Nguyen, 2:5-6. “Examples of targets include an IP address, an interface component (e.g., a user input), an application programming interface (“API”) endpoint, a Uniform Resource Identifier (“URI”) endpoint, and the like.” Nguyen, 2:6-9.

93. Nguyen teaches to “generate [] test plans” and “execute [] test plan” instructions to “identify actual security risks and, at the same time, eliminate falsely identified potential vulnerabilities.” Nguyen, 4:46-50; *see also* Nguyen, 12:29-31, 12:57-58, 13:29-32, 16:1-4. **“A potential vulnerability is determined to be an actual vulnerability when the test elicits a specific response indicative of the presence of a particular vulnerability[.]”** Nguyen, 10:52-54 (emphasis added). Nguyen discloses that “the test plan eliminates false positives or potential vulnerabilities that are not actual vulnerabilities[.]” and that “[t]he test plan(s) 350 may be configured to test portions of the relevant external surface[.]” Nguyen, 10:58-60, 11:5-6.

94. A POSITA would have understood Nguyen’s test plan instructions use instructions (HTTP methods, GET, TRACE, CONNECT) and access parameters (e.g., IP addresses, TCP/UDP protocols, port number) that are also identified in the ’693 Patent. Nguyen, 11:1-4, 13:14-16, 13:22-25, 13:45-47; ’693 Patent, 5:40-44, 8:2-7, 9:62-10:6, 10:50-58, 11:10-14, 20:3-6.

95. Nguyen teaches that **“a potential vulnerability is determined to be an actual vulnerability when the test elicits a specific response indicative of the presence of a particular vulnerability[.]”** Nguyen, 10:52-54 (emphasis added); *see also* Nguyen, 13:38-44.

96. In my opinion, these Nguyen disclosures teach active inspection as explained in the '693 Patent.

97. I have been informed that the parties have offered the following claim constructions for the active inspection claim limitation: “sending a data packet over the network path” and “gathering information regarding the network path.” In my opinion, Nguyen as explained above teaches the active inspection claim limitation under each of these constructions. First, these Nguyen disclosures teach “sending a data packet over the network path” because a POSITA would have known that sending instructions to/over/through networks is accomplished by sending data in the form of packets. Ex. 1045, Scott, Title, [0001]. Specifically, Scott discloses:

The invention is specified by the independent claims 1, 5, and 6. Further embodiments are specified in the dependent claims 2-4. One embodiment provides a packet-forwarding device that operates in an information-centric network (ICN), and facilitates executing instructions included in a packet to manipulate one or more local resources. Specifically, each packet includes a name. The packet's name can have a fixed length, or can have an arbitrary length. The packet's name can be hierarchical (e.g., includes an ordered sequence of name elements), or can be a flat name (e.g., a hash value). The packet can also carry instructions that can manipulate resources at network devices that receive, process, store, and/or forward the packet. This allows the control plane of a router architecture to be governed by the

packet's name and instructions, and not by preprogrammed instructions at the various network nodes, as occurs in US 2012/314580 A1. In some embodiments, the packet can also carry a payload. Thus, for example, a router in a content centric network (CCN) does not need to process separate packet types for Interests and Content Objects. A packet's instructions can cause a packet-forwarding device to process the packet as an Interest, to process the packet as a Content Object, or to process the packet in a custom way.

Ex. 1045, Scott, [0001]. As evidenced by Scott, for example in this passage, packets are used to send and execute instructions to interact with network resources. *Id.* And a POSITA would have understood the Nguyen disclosures above to teach “gathering information regarding the network path” because Nguyen sends instructions, receives responses, and makes determinations about verified vulnerability threats. Nguyen, 10:52-54, 13:38-44.

98. A POSITA would have been motivated to combine Calvo and Nguyen, and specifically to include Nguyen's pen-testing process into Calvo's method/system with a reasonable expectation of success, as I explain in the following paragraphs.

99. Calvo is directed at ensuring compliance with regulations such as HIPAA, GDPR, PCI, etc. (Calvo 5:20-39). One aspect of Calvo is policy compliance (Calvo 5:60-62; 7:19-22; 9:30-35). Nguyen is directed towards automated penetration testing. Nguyen also performs threat modeling (Nguyen 2:58-64). A POSITA would have recognized that Nguyen's penetration testing and threat modeling would improve (and in certain cases be necessary to accomplish) Calvo's policy compliance. In fact, Calvo specifically discloses PCI compliance (Calvo, 2:7-24),

and PCI requires penetration testing. Ex. 1039, Soh, 1:20-33; see also Sections IV.F-H. Calvo also discloses HIPAA compliance. In 2024 HIPAA was modified to require penetration testing¹, however, prior to that penetration testing was recommended. *Id.* Therefore, a POSITA would readily see an advantage to combining Nguyen with Calvo.

100. Calvo's disclosures also provide multiple motivations to combine Calvo and Nguyen. For example, Calvo discloses that "as the scale and scope of typical distributed systems has increased, the tasks of provisioning, administering, and managing the computing resources have become increasingly complicated" and that prior art approaches "were complex, time-consuming, resource-consuming, and potentially prone to human error when manually implemented." Calvo, 1:19-22, 2:30-36. A POSITA reading Calvo would have been motivated to ensure that the selected resources for policy deployment posed true threats as opposed to merely theoretical threats and understood that Nguyen disclosed an exemplary process to determine which potential vulnerabilities are actual vulnerabilities. Furthermore, Calvo discloses that its "techniques ... may be used for managing the compliance lifecycle of resources hosted in the cloud in a simplified and efficient manner" (Calvo, 2:37-40) and that its disclosures provide the "technical advantage[]" of "improving use of computation resources by providing simplified selection." Calvo,

¹ <https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html>

3:6–10. A POSITA would have easily recognized that Nguyen’s autonomous pen-testing process would have furthered Calvo’s goal for simplified and efficient policy applications and selections. This is because Nguyen outlines an automated process that can rule out “false positives or potential vulnerabilities that are not actual vulnerabilities[,]” enabling future processing to focus solely on confirmed external attack vulnerabilities. Such would have saved considerable processing power in large systems that continuously monitor for policy compliance, like in Calvo. In other words, if a large system or network had a large amount of resources or sensitive data, considerable time, effort, and processing power could be saved by eliminating aspects of the network which did not pose true threats (as identified by penetration testing). Moreover, Calvo discloses that “resource selection 130 may be performed according to a scope” and that “the scope may identify a class of resources to which the pack should be deployed, and the resource selection 130 may automatically select such resources that are accessible to the user account.” Calvo, 4:22-25. A POSITA would have understood that Nguyen’s autonomous pen-testing method would have been a known way to accomplish automatic resource selection, and indeed one that would focus on real external threats rather than theoretical threats.

101. Nguyen’s disclosures also provide an express teaching to combine Calvo and Nguyen. For example, Nguyen discloses a focused selection and verification of resources through testing, which “ensures that computing resources and/or testers

are pentesting those of the applications that pose the greatest risk.” Nguyen, 3:4-12. Accordingly, a POSITA would have understood that incorporating Nguyen’s autonomous pen-testing process into Calvo’s method/system would have provided the benefit of focusing on resources that posed the greatest risk and furthered Calvo’s goal for simplified and efficient policy applications and selections. Nguyen also discloses that “[m]any companies own and operate hundreds or thousands of IP address that host multiple applications each” and that “companies may own and operate hundreds or thousands of publicly facing domain names. In other words, companies have large external surfaces that would require a long time to properly pentest using prior art manual methods.” Nguyen, 4:18-24. A POSITA would have understood that Nguyen’s autonomous pen-testing process would have been beneficial for large networks with large surface exposures, as it false positive vulnerabilities. This would have allowed network administrators to focus policy application efforts on only verified threats.

102. Additionally, a POSTIA would have understood that combining Calvo’s resource selection and policy application process with Nguyen’s pen-testing process (to verify that the selected resources correspond to actual vulnerabilities) to be combining prior art elements according to the known methods of pen-testing (by sending instructions and receiving response) to yield predictable results, in this case, determining resources that are real vulnerabilities.

103. Further, a POSITA would have understood that applying Nguyen's pen-testing (to determine resources that correspond with real vulnerabilities) would have improved Calvo's device (which selects resources for policy deployment and then applies policies) would improve Calvo's device in the same way as Nguyen's by eliminating false positive vulnerabilities from further cybersecurity processing, and that such a combination therefore would have constituted the use of a known technique to improve a similar device in the same way.

104. A POSITA would have also had a reasonable expectation of success in incorporating Nguyen's pen-testing into Calvo's system and method. For example, pentesting was well-known and a requirement of PCI DSS as explained above. Therefore, such additional would have been trivial. Further both Calvo and Nguyen represent examples of working processes and their integration would have only required minor modifications in software or simply sending instructions. Both Calvo and Nguyen describe automated processes for resource selection. I also note that both Calvo and Nguyen were initially applications submitted by the same Amazon Technologies, Inc. entity, which further demonstrates their compatibility because Amazon was known in the art before the '693 Patent to be a sophisticated cloud-computing company.

4. Claim 1[c]: storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network

105. In my opinion, Calvo in view of Nguyen teaches storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network at least because Nguyen's discloses storing test results indicating which potential vulnerabilities are actual vulnerabilities.

106. The '693 Patent discloses that "based on the determined viability of network paths" a stored security graph may be updated. '693 Patent, 11:38-40. The '693 Patent explains that "if a resource is successfully accessed [] this result can be stored[.]" '693 Patent, 11:40-44.

107. As explained above in Claim 1[b], Nguyen's pen-testing process that determines which targets (potential vulnerabilities) are actual vulnerabilities by sending instructions to such targets and receiving responses, teaches active inspection per the '693 Patent. *See above*, Claim 1[b].

108. Like the '693 Patent, Nguyen teaches storing the results of active inspection, including the results indicating which targets (potential vulnerabilities) have been determined to be real vulnerabilities based on Nguyen's pen-testing process (sending and receiving instructions). Specifically, Nguyen discloses that "results obtained from performing tests on targets" (i.e., the results of pen-testing a target) "may

identify one or more actual vulnerability[.]” and the results are stored in “a vulnerabilities database 380[.]” Nguyen, 11:16-17, 16:12-13; *see also* Nguyen, 11:65-67, 12:2-5, 13:1-5, 13:52-54, Fig. 3.

109. Nguyen’s disclosures teach a valid path because Nguyen’s pen-testing process “eliminates false positives or potential vulnerabilities that are not actual vulnerabilities” (Nguyen, 10:58-60) and determines which resources are actual vulnerabilities by sending instructions and receiving responses to verify real vulnerabilities and store the results of the determined vulnerabilities. Nguyen, 11:16-17, 16:12-13, 13:1-5; *see also above* Claim 1[b].

110. As previously discussed, A POSITA would have been motivated to include Nguyen’s pen-testing process into Calvo’s method and system to determine actual vulnerabilities with a reasonable expectation of success. *See above*, Claim 1[b]. This combination would have included storing the results of pen-testing, and therefore, the combination explained above teaches Claim 1[c].

111. Further, a POSITA would have been motivated to specifically include storing the test results of pentesting as taught by Nguyen. As a preliminary matter, this would have been a matter of common sense. If pentesting was performed, and specifically performed to determine true threats and eliminate “false positive” (Nguyen, 10:58-60) threats as disclosed by Nguyen (and explained above), the results of such process would be useless unless the results were stored. Storing the

results of Nguyen's pentesting process would have allowed for Calvo's policy application process to be more efficient and not wasteful. This efficiency would have extended to policy application, compliance verification, and potential remediation, within the Calvo-Nguyen system, particularly given that Calvo discloses a continuous policy application process. Calvo, 4:49-52, 5:1-5. Calvo also discloses an association between the compliance pack and the target resources: "In deploying a compliance pack to a set of resources, the package deployment 140 may store an association between the selected compliance pack 171A and the target resources 185." (Calvo 4:49-52). This stored association would have represented an additional, specific motivation to combine Nguyen's storing feature into the Calvo-Nguyen combination explained above. Nguyen discloses "The relevant external surface 244 identifies the potential targets within the desired scope that are publicly accessible (e.g., via a network, such as the 20 Internet) and associates each of the potential targets with at least one of the applications 104." (Nguyen, 5:18-22). A POSITA would understand that determining that a target is publicly accessible requires some indication that the network path is valid

112. A POSITA would have also understood that in implementing the Calvo-Nguyen system, it is not possible to apply a compliance package to one or more resources on a network without first having an indication that the network path is valid through sending instructions to and receiving instructions from the one or more

resources. A POSITA would have recognized that this association must include the network path to the resource, and this discloses an indicator to indicate the network path is valid. This association is further disclosed in Calvo in the following excerpt: “In the case of continuous compliance management, the stored association between the compliance pack 171A and the target resources 185 may be re-used in performing the rule evaluation 150 (and automated remediation 160) repeatedly over time.” Calvo, 5:1-5; see also Calvo, 9:1-8 (“The system 100, repository 170, and/or target resources 185 may be hosted in or otherwise associated with a provider network 190. A provider network may represent a network operated by an entity such as a business or a public sector organization to provide one or more services (such as various types of cloud-based computing or storage) accessible via the Internet and/or other networks to a distributed set of clients. The services may collaborate to provide, virtualized resources to clients.”).

113. In addition to the prior art cited, a POSITA would be aware that routing tables have had indicators that a path is valid for decades prior to the ‘693 patent, as discussed in section IV.C.

114. A POSITA would have also had a reasonable expectation of success in combining Nguyen with Calvo for the same reasons as discussed in Claim 1[b]. Additionally, a POSITA would have readily known how to store results of cybersecurity tests/processes. See generally, Nguyen.

5. Claim 1[d]: applying a policy on the valid path, wherein the policy includes a conditional rule;

115. In my opinion, Calvo in view of Nguyen teaches applying a policy on the valid path, wherein the policy includes a conditional rule at least because the Calvo-Nguyen combination explained above teaches applying Calvo's compliance pack to prevent access from the public Internet to the internal cloud-based resource(s) through firewall port 22, where such has been stored as an actual vulnerability via Nguyen's pen-testing process, wherein Calvo's compliance pack contains rules.

116. The '693 Patent describes that "a policy includes a statement, a conditional rule, a combination thereof, and the like" ('693 Patent, 8:22-29), and that "applying a policy on a network path includes applying a conditional rule." '693 Patent, 21-62-67. The '693 Patent further explains, "the condition of the policy, such as a conditional rule[,] includes determining if the policy is adhered to by the network path. In some embodiments, this is determined [] by applying a rule and checking the result of the outcome[.]" '693 Patent, 22:39-45. Additionally, the '693 Patent provides the following example of "a policy applied on a valid network path" ('693 Patent, 21:56): "For example, according to an embodiment, a policy includes a statement that a network path to/from a first reachable resource should only be accessible via a predefined port (e.g., port 80) using a predefined protocol (e.g., HTTPS). In some embodiments, where a viable network path is detected, the policy

is applied to determine if the network path adheres to the policy or not.” ’693 Patent, 22:2-8.

117. Calvo teaches a policy that includes a conditional rule. Calvo discloses that “[a] compliance pack 171A may include a plurality of rules 172A that can be evaluated to determine the policy compliance of a resource” (Calvo 5:60-62), and that “[a] compliance package [] may include settings, rules, artifacts (e.g., documentation of compliance standards), and remedial actions to be taken if resources are found to be noncompliant.” Calvo, 5:46-51.

118. A POSITA would have understood that Calvo teaches policy application and compliance verification of such policies. Calvo, Fig. 2B. To determine whether a policy rule has been complied with, a POSITA would have understood that such rule would involve a condition, and the compliance check would be seeing if such condition was met or not met. In Calvo’s following example: “a rule in an InfoSec compliance pack may be used to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the relevant rule[,]” a POSITA would have understood that the conditional rule present is “port 22 [] is not accessible to the Internet.” Calvo, 6:35-39.

119. Calvo teaches applying a policy on the path. Calvo teaches that a “compliance pack 171A may be deployed to the selected resources” and applied (Calvo, 4:47-49;

see also Calvo, 2:42-45, 4:2-9, 2:64-3:1, Fig. 2B), where a compliance pack includes “a plurality of rules 172A that can be evaluated to determine the policy compliance of a resource” Calvo 5:60-62. As I explained in Section IV.C-D, paths in networks represent a connection of computing nodes (or resources/devices). In Calvo’s example, resources are part of a network path from the public Internet to the selected cloud-based resource through firewall and port 22. Calvo, 6:35-39; *see also* Calvo, 3:37-41, 4:35-37, 2:46-51, 2:60-62, 5:60-62. A POSITA would have understood that applying compliance rules (for example, to restrict external network access) would be applied on nodes (i.e., resources) of a network because the nodes represent computing objects. Computing objects are the features in a network which can execute instructions. And the path is made up of a connection of resources. Instructions cannot be applied on simply the vertices between resource nodes. Rather, instructions are applied on the nodes to restrict aspects of network access. This is further explained in Sections IV.C-D above. Thus, A POSITA would have understood that applying a rule to prevent access from the Internet to internal cloud resource via firewall port 22 teaches policy application on a path.

6. Claim 1[e]: initiating a mitigation action, in response to determining that the conditional rule is not met; and

120. Calvo teaches initiating a mitigation action, in response to determining that the conditional rule is not met because Calvo’s discloses remedial action taken in response to a determination of rule noncompliance), as claimed.

121. The '693 Patent describes a mitigation action includes “revoking access to the reachable resource, revoking access from the reachable resource, **closing a port of the reachable resource, generating a notification**, generating an alert[.]” ’693 Patent, 22:53-57 (emphasis added).

122. Calvo discloses deploying compliance packs including conditional rules. *See above*, Claim 1[d]. Furthermore, Calvo discloses a rule evaluation process performed for each target resource to “determin[e] whether a resource is compliant or noncompliant with the rule.” Calvo, 4:52-58. Calvo’s Figure 2B at steps 240 and 250 shows that remedial actions are taken if a resource is not compliant (where noncompliance means a conditional rule is not met). Calvo, Fig. 2B. Calvo also discloses that “[f]or resources found to be noncompliant, the system 100 may perform automated remediation 160. The automated remediation 160 may include performing one or more remedial actions[.]” Calvo, 4:58-61; *see also* Calvo, 4:9-13, 10:44-51. Calvo specifically discloses that “remedial actions for noncompliance may include notifying relevant users, modifying a configuration of a resource, isolating a resource” Calvo, 2:60-64 (emphasis added); *see also* Calvo, 4:63-65, 10:51-61. Calvo also teaches closing a port as an exemplary remediation action: “For example, a rule in an InfoSec compliance pack may be used to ensure that port 22 on any firewall or security group (cloud-based or on-premises) is not accessible to the Internet, and the port may be closed if it is found to be noncompliant with the

relevant rule.” Calvo, 6:35-39. APOSITA would have understood that Calvo’s remedial actions teach mitigation actions.

123. Additionally, Calvo is directed towards ensuring that systems that access resources are in compliance with any required regulations such as HIPAA, GDPR, or PCI-DSS and includes compliance packs to mitigate non-compliance. Calvo, 2:9-24, 5:20-39.

7. Claim 1[f]: applying the policy on another network path, in response to determining that the conditional rule is met

124. Clavo teaches applying the policy on another network path, in response to determining that the conditional rule is met at least because Calvo discloses a continuous compliance verification process which applies the compliance pack on a subsequent resource (which a POSITA would have known to have subsequent network path per the ’693 Patent) in response to compliance being confirmed for a previous resource (which a POSITA would have known to have a previous network path per the ’693 Patent).

125. The ’693 Patent discloses “a method for applying a policy on a network path” shown in an example flow chart (’693 Patent, 5:21-22):

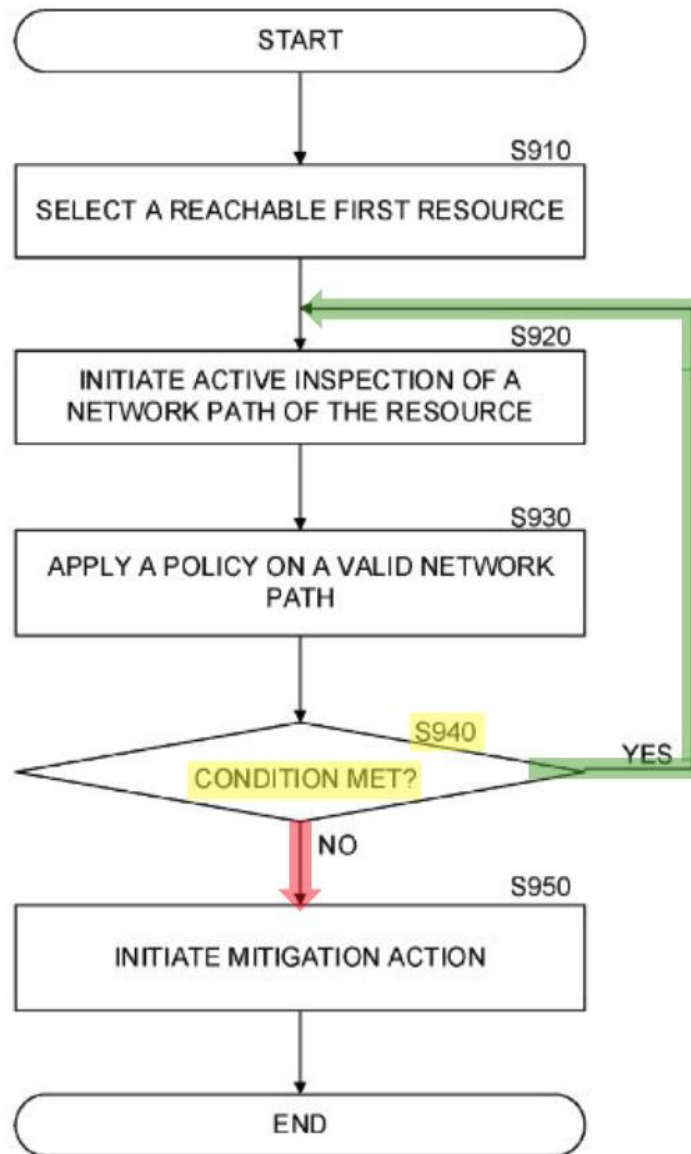


FIG. 9

'693 Patent, Fig. 9 (annotated). Figure 9 outlines the steps for applying a policy on a network path, “[a]t S910, a reachable first resource is selected” ('693 Patent, 21:1), “[a]t S920, active inspection of a network path is initiated” (*Id.*, 21:30), “[a]t S930, a policy is applied on a valid network path” (*Id.*, 21:56), “[a]t S940, a check is

performed to determine is a condition is met” (*Id.*, 22:39-40). *See generally*, ’693 Patent, 21:1-22:40.

126. At step 940 (annotated by yellow in the figure above) of the Figure 9 flow chart, there are two options following the check to determine is a condition is met: (1) “YES”—“[w]here the condition is satisfied (e.g., the network path adheres to the policy), execution continues at S920[;]” and (2) “NO”—“where the condition is not satisfied (e.g., the network path does not adhere to the policy), execution continues at S950.” ’693 Patent, 22:45-50, Fig. 9. Following the “NO” option (annotated by red arrow in the figure above) of S940 continues to “S950, [where] a mitigation action is initiated.” ’693 Patent, 22:51, Fig. 9. Following the “YES” option (annotated by green arrow in the figure above) of S940 continues to execute S920.

127. In my opinion, Calvo teaches this process as disclosed in the ’693 Patent and claimed in Claim 1[f]. Calvo’s “continuous compliance verification” process (i.e., applying Calvo’s rule(s) on a resource, evaluating rule compliance, and repeating for subsequent resources), shown for example in Figure 2B via the “No” path at step 240 (annotated in green below) is an example of applying a policy on another network path in response to determining a conditional rule is met:

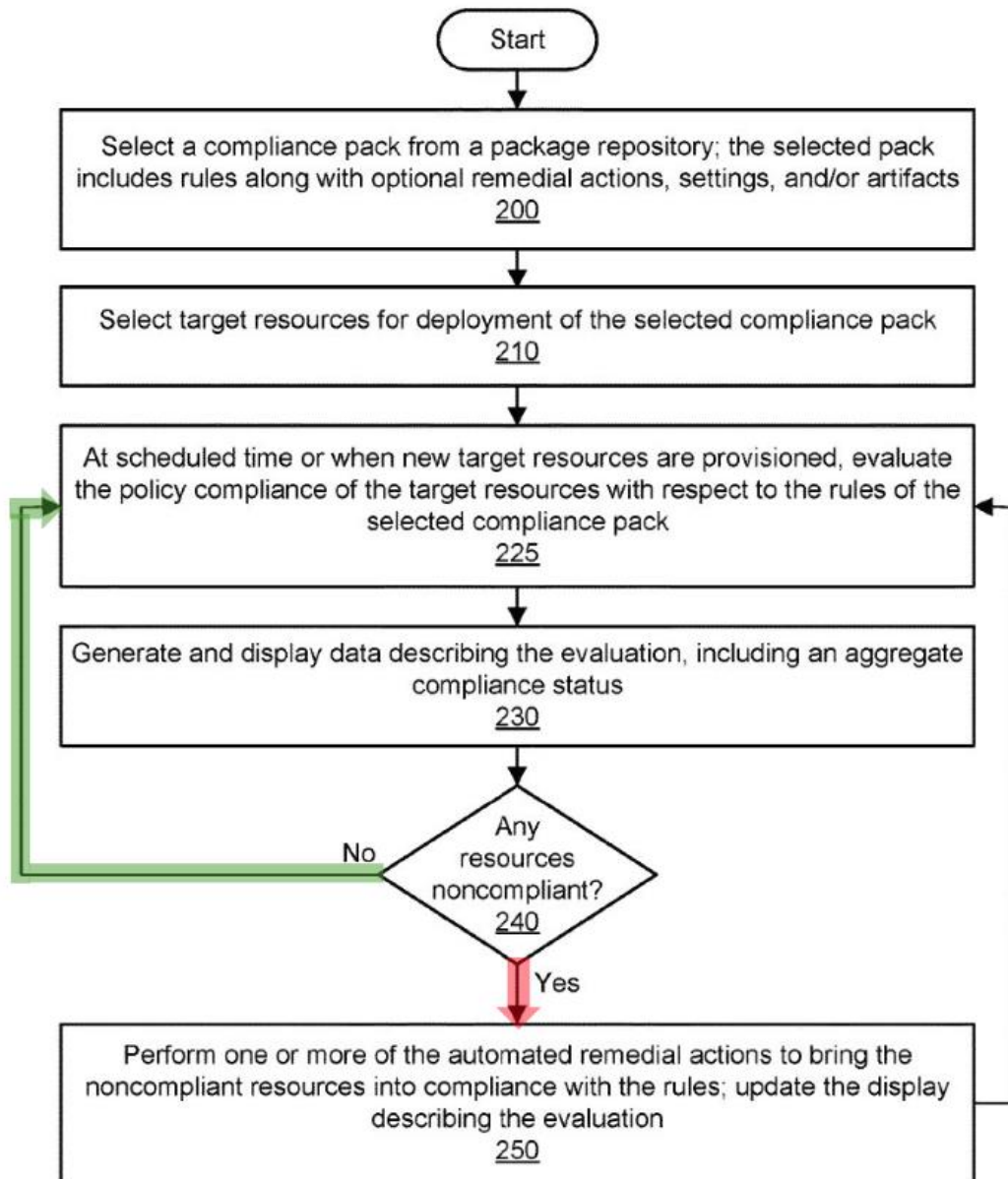


FIG. 2B

Calvo, Fig. 2B (annotated); *see also* Calvo, 4:35-37, 4:52-54, 5:1-9, 7:33-36, 7:51-60, 10:41-43.

128. Following Calvo’s Figure 2B, a “flowchart[] illustrating methods for compliance lifecycle management for cloud-based resources” (Calvo, 9:29-31):

from step 200 to step 225, a compliance pack is deployed, and rule evaluation for a resource is performed (*Id.*, 9:31-33, 9:48-49, 10:67-11:2). At step 240, “the method may determine whether any resources were found to be noncompliant with any of the rules in the deployed compliance pack” (Calvo, 10:44-46), where there are two options “Yes” and “No” dependent on the resources compliance to policy, similar to S940 of the ’693 Patent. Option (1)—“No,” there are not any resources noncompliant (annotated in green in the above figure)—leads to step 225 to perform rule evaluation after the compliance pack is deployed (Calvo, Fig. 2B, 10:67-11:6); Option (2)—“Yes,” there are resources noncompliant (annotated in red in the above figure)—leads to step 250 to perform remediation actions. This second option is the subject previously discussed in Claim 1[e], and the first option teaches applying the same compliance pack (with the same at least one conditional rule) to another resource in response to determining the rule was complied with for a previous resource (annotated in green in the above figure).

129. Calvo’s application of the same rule(s) on a subsequent resource teaches applying the policy on another network path because the subsequent resource would have a different network path than the first resource, as disclosed in the ’693 Patent. ’693 Patent, 12:46-47 (“A network path is a connection of two or more security objects”), 8:30-39. This description of a network path in the ’693 Patent is in line with how a POSITA would have understood network path; for example, as I

explained in Section IV.C, a network path is a connection of two or more computing nodes/devices/resources. *See also*, Claim 1[a].

130. Calvo teaches that “a user may deploy a compliance pack ... across an entire enterprise, and have access to a unified view of compliance across the target resources,” where there are “one or more resources in one or more provider networks or regions of provider networks.” Calvo, 3:1-5, 3:67-4:2 (emphasis added); *see also* Calvo, 6:39-41 (“Using a single compliance pack, such rules may be applied to disparate resources throughout an enterprise in a consistent manner.”). A POSITA would have understood each resource across an entire enterprise to have a unique network path. Section IV.C; ’693 Patent, 12:46-47, 8:30-39. Accordingly, each of Calvo’s resources has a distinct network path per the ’693 Patent and per the understanding of POSITA before the ’693 Patent.

131. Calvo further discloses applying the policy in response to determining the condition is met: "Settings 173A may include configuration recorder settings, result aggregation settings, delivery channel settings, and the reporting frequency. Settings 172A may apply to the entire pack 171A or to individual rules 172A. In one embodiment, a data structure for a compliance pack setting may indicate a SettingID, DeliveryChannel, ConfigRecorder, optional Config Aggregator, ServiceRule, CreationTime, LastUpdatedTime, and UpdatedBy." (Calvo 6:8-16)

**8. Claim 2: The method of claim 1, further comprising:
initiating active inspection for each network path of a plurality of**

network paths; and applying the policy only on a network path of the plurality of network paths which is a valid path

132. Calvo in view of Nguyen teaches the method of claim 1, further comprising: initiating active inspection for each network path of a plurality of network paths and applying the policy only on a network path of the plurality of network paths which is a valid path at least because: (1) Nguyen discloses a process of pen-testing multiple resources/targets/potential vulnerabilities with multiple paths to determine if such are actual vulnerabilities by sending instructions to the such and receiving responses; (2) Nguyen rules out false positive paths; and (3) Calvo discloses applying compliance packs on a resource which Nguyen has verified is an actual vulnerability and not false positive potential vulnerabilities ruled out by Nguyen.

133. As I discussed above, Nguyen's process of pen-testing targets/potential vulnerabilities to determine if such are actual vulnerabilities by sending instructions and receiving responses teaches active inspection per the '693 Patent. *See above*, Claim 1[b]. This Calvo-Nguyen combination teaches multiple of Calvo's resources (with multiple paths) being selected for Nguyen's pen-testing because each such resource has its own network path per the '693 Patent, as discussed above (*See above* Claim 1[f]; Section IV.C). Accordingly, Nguyen's pen-testing of such multiple resources (with multiple paths) teaches active inspection for each network path of a plurality of network paths. *See also* Nguyen, 2:43-49 ("Unlike prior art pentesting, which is performed manually, autonomous pentesting is performed by a computing

system. Autonomous pentesting may begin with the computing system performing reconnaissance on a desired scope (e.g., a number of applications or an entire organization). During reconnaissance, the computing system identifies all of the potential targets within the desired scope."), 2:54-57, 4:46-50, 5:13-18, 9:18-23, 14:44-46, 15:67-16:5; Claim 1[b].

**9. Claim 3: The method of claim 2, further comprising:
initiating active inspection by generating an access instruction for
the reachable resource; and executing the access instruction on a
network path.**

Calvo in view of Nguyen teaches the method of claim 2, further comprising: initiating active inspection by generating an access instruction for the reachable resource and executing the access instruction on a network path because Nguyen discloses generating and executing of test instructions to determine which potential vulnerabilities are actual vulnerabilities using the same exemplary instructions and parameters as the '693 Patent. *See* Claim 1[b].

**10. Claim 4: The method of claim 2, further comprising:
applying the policy only on each network path of the plurality of
network paths which is a valid path**

134. Clavo in view of Nguyen teaches the method of claim 2, further comprising: applying the policy only on each network path of the plurality of network paths which is a valid path at least because the Calvo-Nguyen combination described above applies compliance packs on Nguyen's verified threats and not the ruled out false positive vulnerabilities. *See* Claim 2.

**11. Claim 5: The method of claim 4, further comprising:
initiating active inspection on each network path of the plurality
of network paths to determine if the network path is a valid
network path.**

135. Calvo in view of Nguyen teaches the method of claim 4, further comprising initiating active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path at least because the Calvo-Nguyen combination described above teaches active inspection on multiple network paths to determine which paths are valid paths and rule out false positives. See Claims 1-4.

**12. Claim 6: The method of claim 1, further comprising:
initiating the mitigation action on the reachable resource.**

136. Calvo in view of Nguyen teach the method of claim 1, further comprising: initiating the mitigation action on the reachable source at least because Calvo discloses remedial actions, including notifying relevant users, modifying a resource isolating a resource, and closing a port, as claimed. Calvo, 2:60-64, 6:35-39, 3:6-17.

**13. Claim 7: The method of claim 6, wherein the mitigation
action includes any one of: revoking access to the reachable
resource, revoking access from the reachable resource, closing a
port of the reachable resource, generating a notification,
generating an alert, and any combination thereof.**

137. Calvo in view of Nguyen teaches the method of claim 6, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable

resource, generating a notification, generating an alert, and any combination thereof at least because Calvo's remedial actions include notifying users, modifying a configuration of the resource, isolating the resource, and closing a port. Calvo 2:60-64, 6:35-39, 10:54-56.

**14. Claim 9: The method of claim 1, further comprising:
initiating active inspection of the network path to detect an
application path.**

138. Calvo in view of Nguyen teach the method of claim 1, further comprising: initiating active inspection of the network path to detect an application path at least because the scope of Nguyen's reconnaissance targets includes applications, and Calvo teaches its resources include applications.

139. As previously discussed, the Calvo-Nguyen process teaches active inspection of the network path per the '693 Patent. *See above*, Claim 1[b]. Nguyen's pen-testing process in the Calvo-Nguyen combination further teaches initiating active inspection of the network path to detect an application path. Specifically, Nguyen's pen-testing process includes reconnaissance on a scope of potential targets, where "[t]he scope may include an application". Nguyen, 4:14; *see also* Nguyen, 2:9-14, 2:45-51, 4:11-18, 5:15-21, 15:6-16. Furthermore, Figure 5 of Nguyen discloses block 506 performed by the system, "Select Application to Pentest," where "the command and control module 130 selects the portion 102 of applications 104 to pentest." Nguyen,

Fig. 5, 15:33-35. Additionally, Calvo's cloud-based resources include "applications." Calvo, 2:9-12, 3:29-33, 9:48-53.

Claim 10: The method of claim 9, further comprising: generating the mitigation action further based on the application path.

140. Calvo in view of Nguyen teach the method of claim 9, further comprising: generating the mitigation action further based on the application path at least because Calvo teaches remedial actions are taken in response to a determination of rule noncompliance of an application resource, and the scope of Nguyen's pen-testing process includes applications. *See* Claims 1[e], 1[f], 9; Calvo, Fig. 2B, 2:9-24, 3:29-33, 5:20-39, 9:48-53.

15. Claim 11[pre]: non-transitory computer-readable medium storing a set of instructions for applying a policy on a network path, the set of instructions comprising:

141. Calvo teaches a non-transitory computer-readable medium storing a set of instructions for applying a policy on a network path, the set of instructions at least because Calvo discloses non-transitory computer-readable medium storing program instructions for implementing its disclosed method/system.

142. Calvo illustrates a computing device, as shown in figure 8:

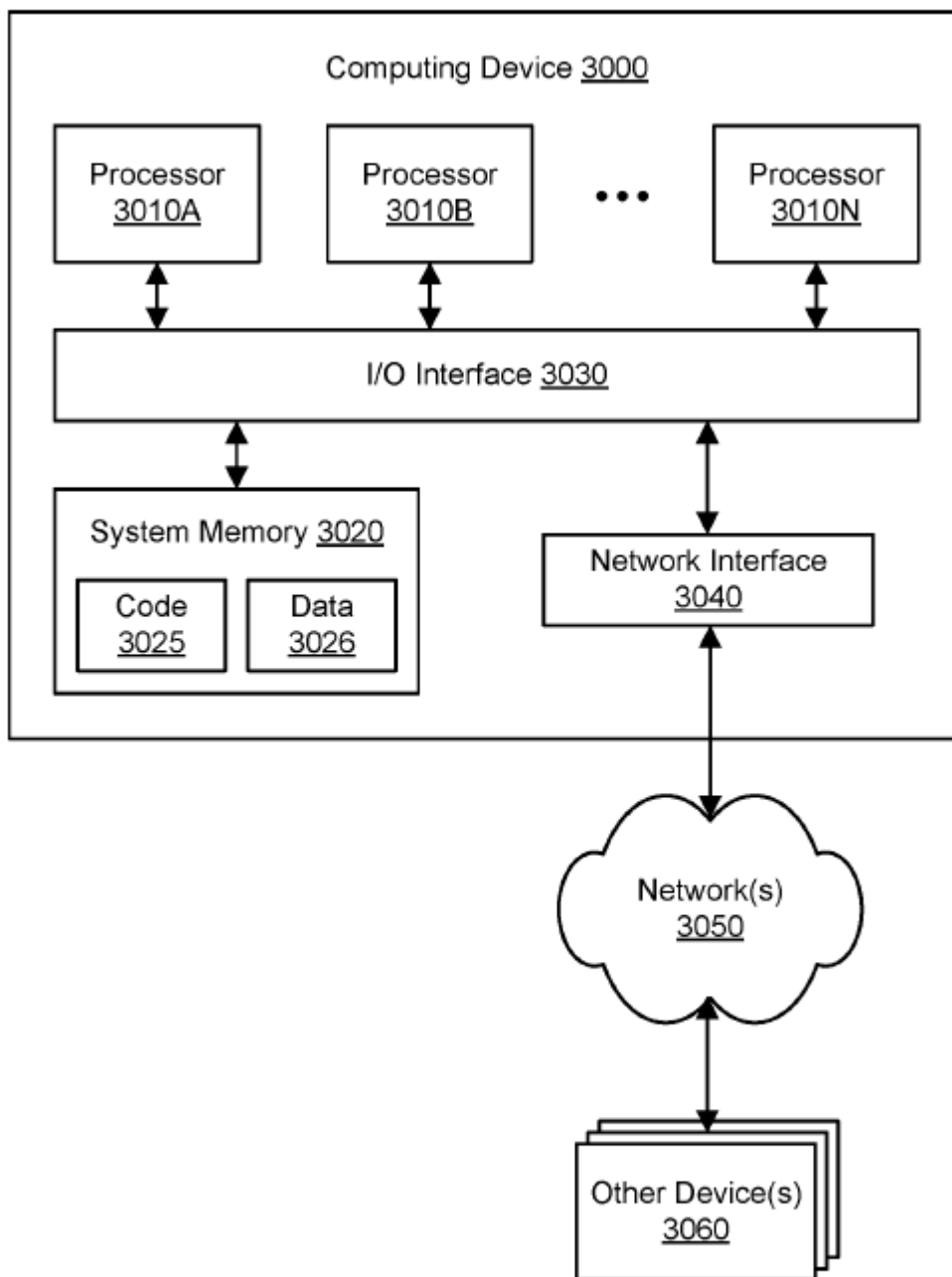


FIG. 8

143. Calvo discloses System memory is non-transitory computer readable medium via Calvo's disclosures of system memory, and Calvo discloses program instructions. Calvo, 14:5-17, 14:5-15, Claim 13.

144. Nguyen also discloses non-transitory computer readable storage "is a non-transitory computer-readable storage medium that excludes transitory signals (e.g., a propagating transient electric or electromagnetic transmission) but includes non-transitory data storage circuitry (e.g., buffers, cache, and queues) within transceivers of transitory signals" (Nguyen 22:21-26).

145. Nguyen further discloses the non-transitory computer-readable storage medium in claims 14, 15, 16, 17, 18, 19, and 20.

16. Claim 11 [a] one or more instructions that, when executed by one or more processors of a device, cause the device to:

146. Calvo teaches one or more instructions that, when executed by one or more processors of a device at least because Calvo teaches program instructions executed by processors of Calvo's computing device.

147. Figure 8 of Calvo discloses one or more processors:

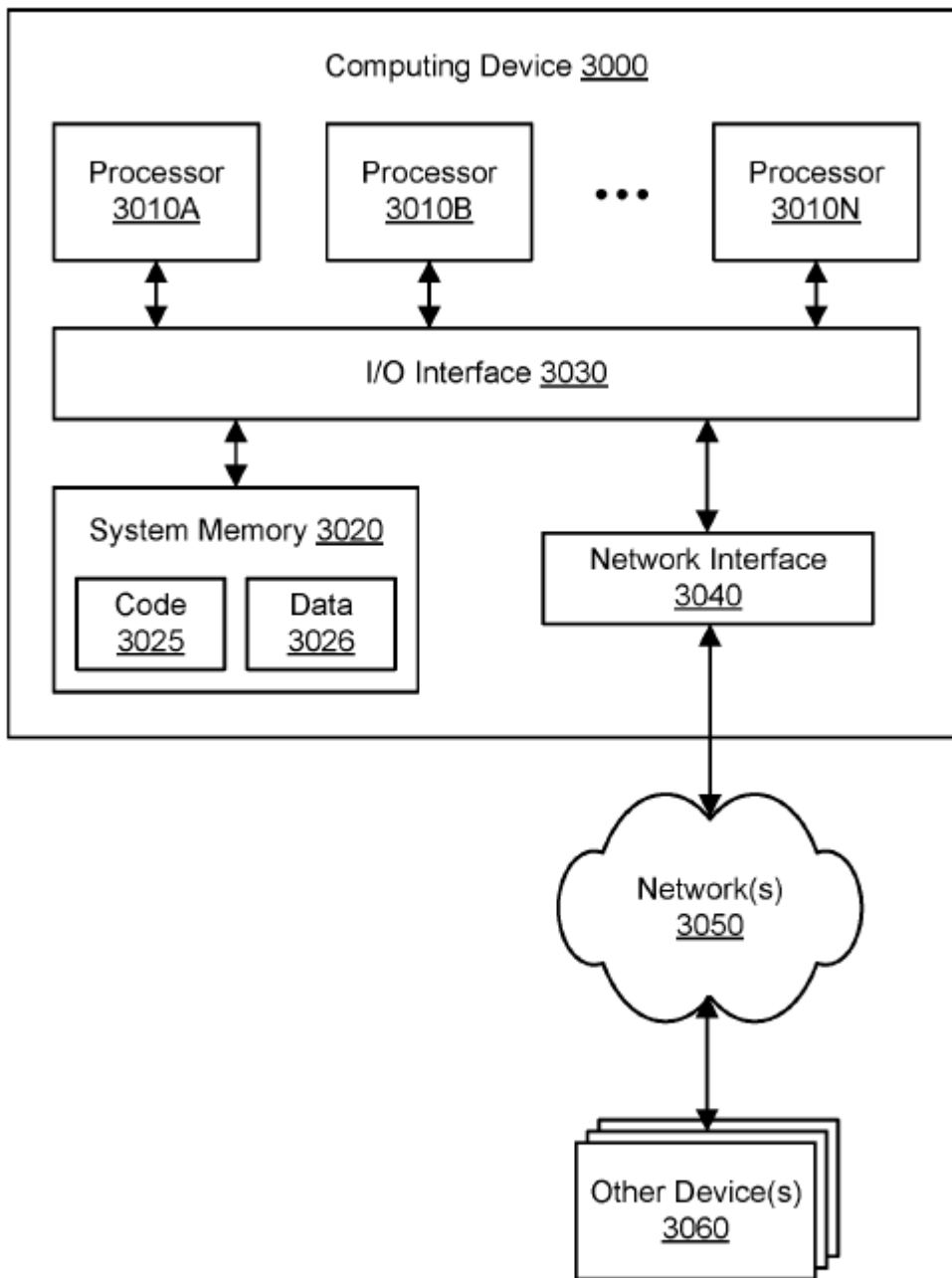


FIG. 8

148. Calvo further discloses one or more processors in the following excerpt "In various embodiments, computing device 3000 may be a uniprocessor system

including one processor or a multiprocessor system including several processors 3010A- 3010N (e.g., two, four, eight, or another suitable number)." (Calvo 14:16-19)

149. Figure 4 of Nguyen discloses one or more processors:

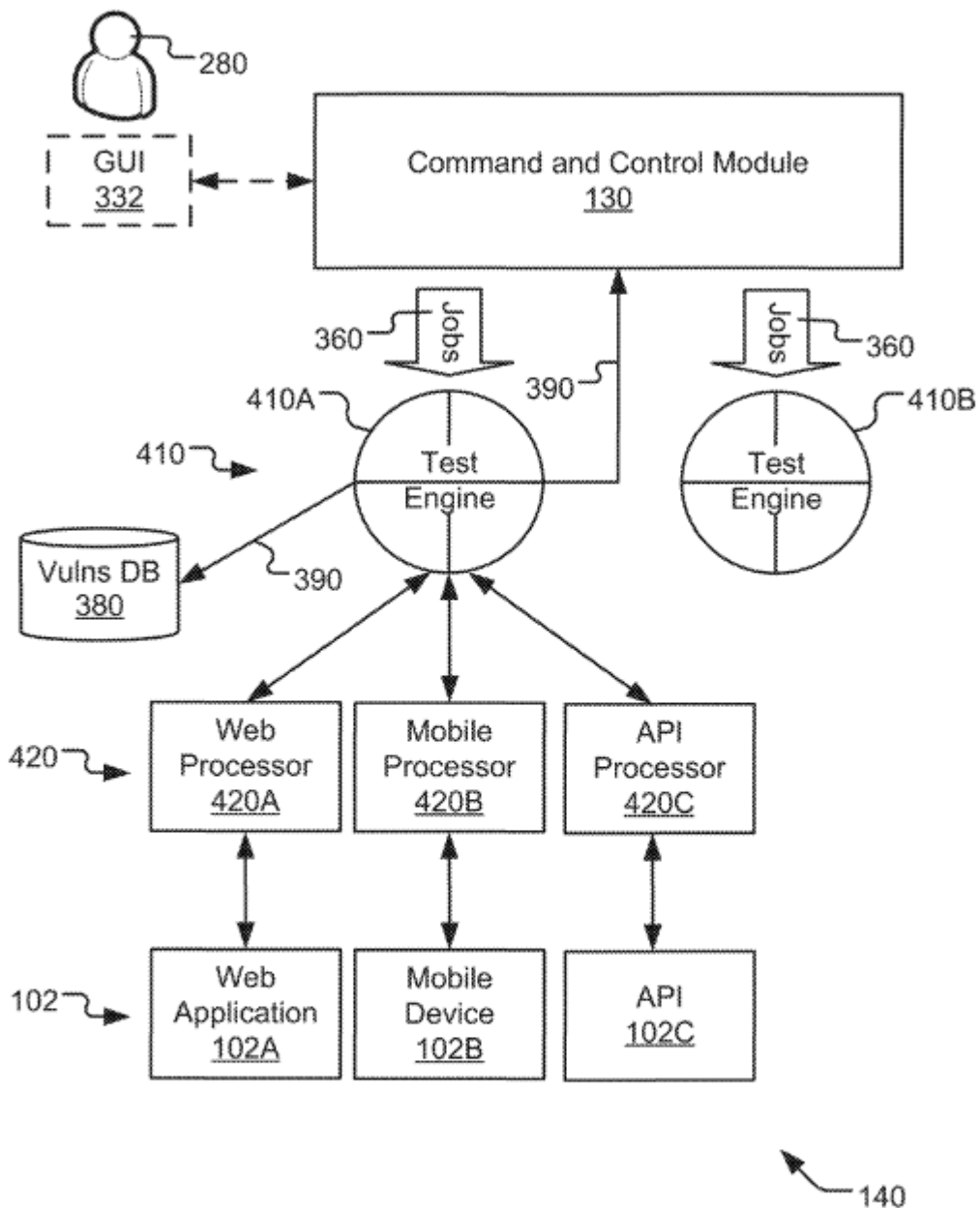


FIG. 4

150. Nguyen further discloses one or more processors in the following excerpt

"The computing system automatically generates jobs based on the test plan and

forwards the jobs to one or more test engines that instruct one or more processors to perform the tests listed in the test plan." (Nguyen 3:26-29). *See also* Claim 11[pre].

17. Claim 11[b]: select a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment;

151. *See above* Claim 1[a].

18. Claim 11[c]: actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;

152. *See above* Claim 1[b].

19. Claim 11[d]: storing an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network;

153. *See above* Claim 1[c].

20. Claim 11[e]: apply a policy on the valid path, wherein the policy includes a conditional rule;

154. *See above* Claim 1[d].

21. Claim 11[f]: initiate a mitigation action, in response to determining that the conditional rule is not met; and

155. *See above* Claim 1[e].

22. Claim 11[g]: apply the policy on another network path, in response to determining that the conditional rule is met.

156. *See above* Claim 1[f].

23. Claim 12[pre]: A system for applying a policy on a network path comprising:

157. Calvo in view of Ngueyn teach a system for applying a policy on a network path at least because Calvo discloses a system and the Calvo-Nguyen combination described above teach applying a policy on a network path.

158. Figure 8 of Calvo discloses a computer system:

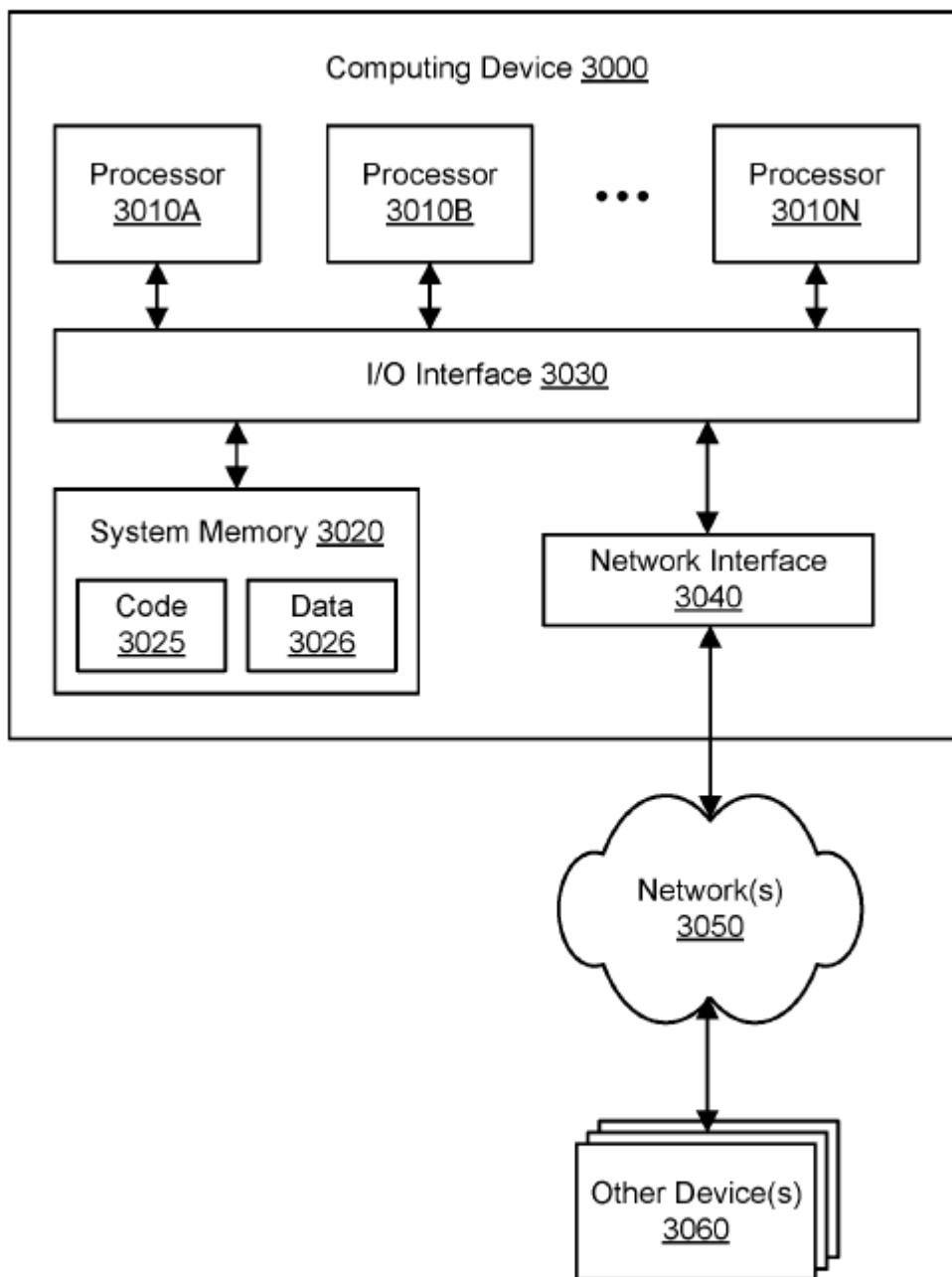


FIG. 8

159. And as explained above, the Calvo-Ngueyn combination teaches applying a policy on a network path. Claim 1.

24. Claim 12[a]: a processing circuitry; and

160. Calvo in view of Ngueyn teach a processing circuitry at least because Calvo discloses processors that implement its teachings.

161. A POSITA would understand that a processor is, by definition, processing circuitry. Figure 8 of Calvo discloses one or more processors:

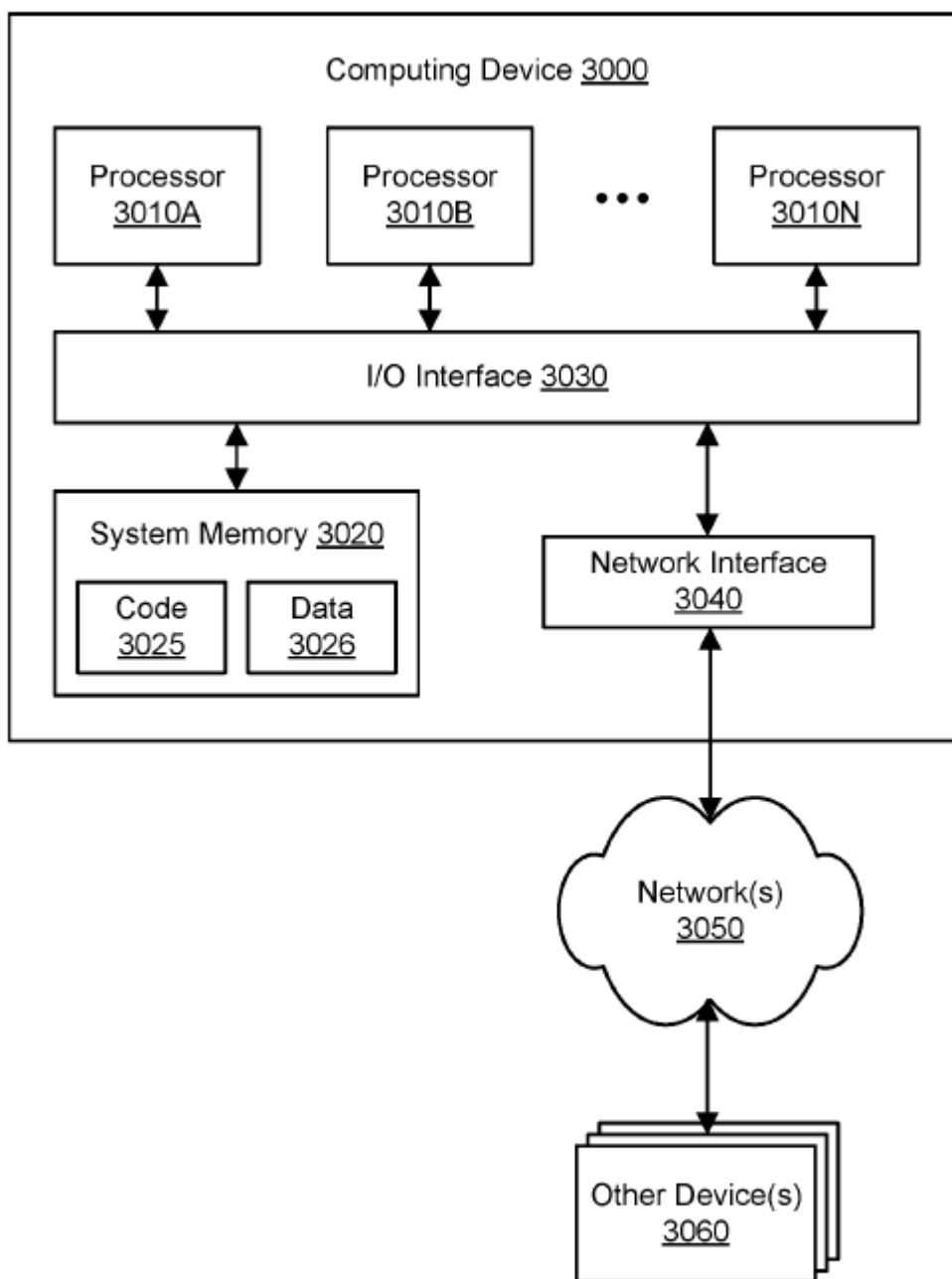


FIG. 8

162. Calvo further discloses one or more processors in the following excerpt "In various embodiments, computing device 3000 may be a uniprocessor system

including one processor or a multiprocessor system including several processors 3010A- 3010N (e.g., two, four, eight, or another suitable number)." (Calvo 14:16-19)

163. Figure 4 of Nguyen discloses one or more processors:

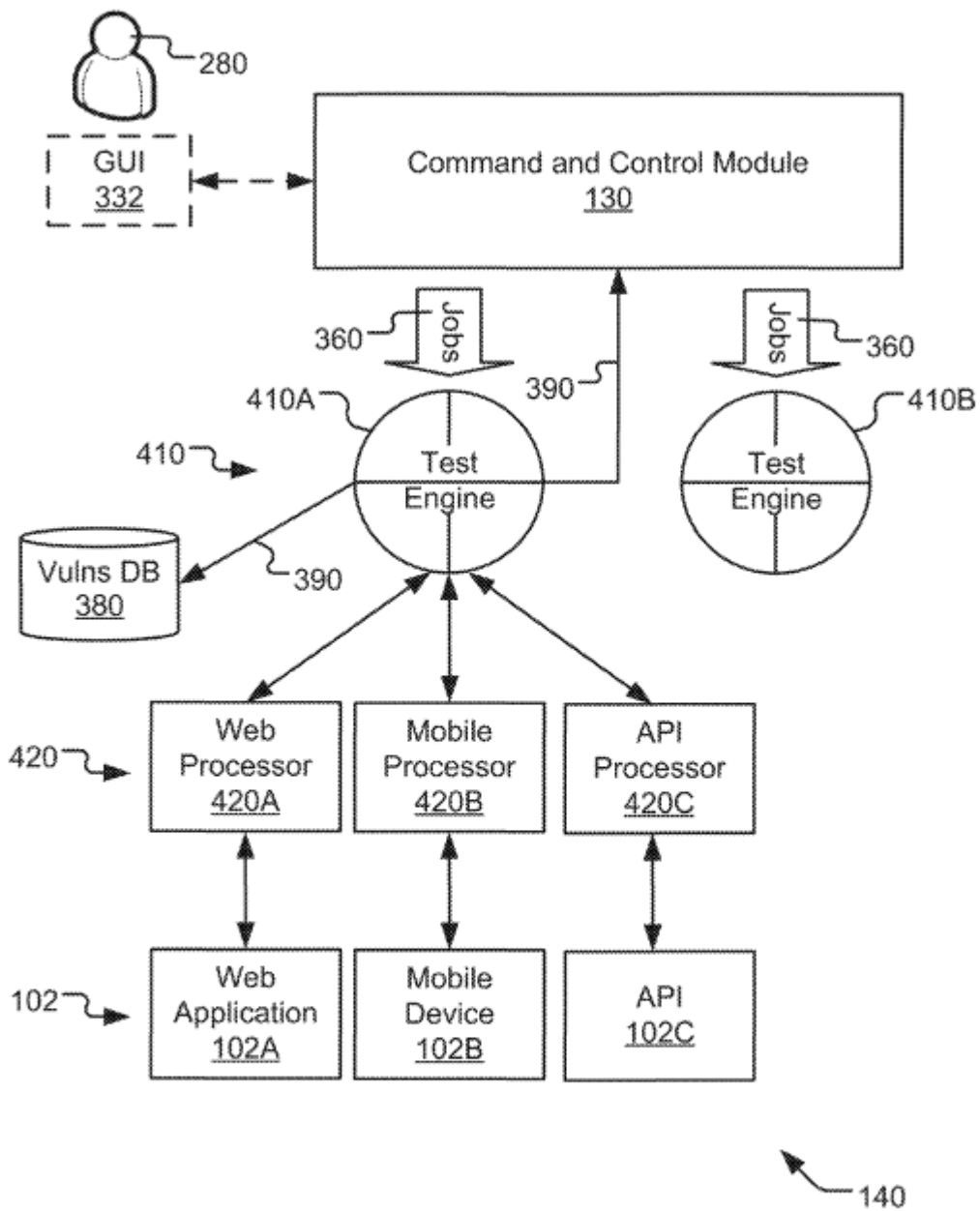


FIG. 4

164. Nguyen further discloses one or more processors in the following excerpt

"The computing system automatically generates jobs based on the test plan and

forwards the jobs to one or more test engines that instruct one or more processors to perform the tests listed in the test plan." (Nguyen 3:26-29).

25. Claim 12[b]: a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to:

165. Calvo in view of Nguyen teach a memory, the memory containing instructions that, when executed by the processing circuitry at least because Calvo teaches system memory that holds program instructions that are executed by Calvo's processors.

166. Calvo discloses memory "In the illustrated embodiment, computing device 3000 includes one or more processors 3010A-3010N coupled to a system memory 3020 via an input/output (I/O) interface 3030. In one embodiment, computing device 3000 further includes a network interface 3040 coupled to I/O interface 3030." (Calvo 14:10-15)

167. Calvo further discloses that said memory contains instructions that are executed by the processing circuitry: "In one embodiment, system memory 3020 may be configured to store program instructions and data accessible by processor(s) 3010A-3010N." (Calvo 14:29-31) This is further disclosed in the following excerpt "In some embodiments, system memory 3020 may be one embodiment of a computer-readable (i.e., computer-accessible) medium configured to store program

instructions and data as described above for implementing embodiments of the corresponding methods and apparatus." (Calvo 15:7-11)

168. Nguyen also discloses memory storing instructions: "In an embodiment, each server typically includes an operating system that provides executable program instructions for the general administration and operation of that server and includes a computer-readable storage medium (e.g., a hard disk, random access memory, read only memory, etc.) storing instructions that, if executed by a processor of the server, cause or otherwise allow the server to perform its intended functions (e.g., the functions are performed as a result of one or more processors of the server executing instructions stored on a computer-readable storage medium)." (Calvo 15:7-11)

26. Claim 12[c]: select a reachable resource having a network path to access the reachable resource, wherein the reachable resource is a cloud object deployed in a cloud computing environment, having access to an external network which is external to the cloud computing environment;

169. *See above* Claim 1[a].

27. Claim 12[d]: actively inspect the network path to determine if the network path of the reachable resource is accessible from the external network;

170. *See above* Claim 1[b].

28. Claim 12[e]: store an indicator to indicate that the network path is a valid path, in response to determining that the reachable resource is accessible from the external network;

171. *See above* Claim 1[c].

29. Claim 12[f]: apply a policy on the valid path, wherein the policy includes a conditional rule;

172. *See above* Claim 1[d].

30. Claim 12[g]: initiate a mitigation action, in response to determining that the conditional rule is not met; and

173. *See above* Claim 1[e].

31. Claim 12[h]: apply the policy on another network path, in response to determining that the conditional rule is met.

174. *See above* Claim 1[f].

32. Claim 13: The system of claim 12, wherein the memory contains further instructions which when executed by the processing 15 circuitry further configure the system to: initiate active inspection for each network path of a plurality of network paths; and apply the policy only on a network path of the plurality of network paths which is a valid path.

175. *See above* Claim 12 and Claim 2.

33. Claim 14: The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection by generating an access instruction for the reachable resource; and execute the access instruction on a network path.

176. *See above* Claim 13 and Claim 3.

34. Claim 15: The system of claim 13, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: apply the

policy only on each network path of the plurality of network paths which is a valid path.

177. *See above* Claim 13 and Claim 4.

35. Claim 16: The system of claim 15, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection on each network path of the plurality of network paths to determine if the network path is a valid network path

178. *See above* Claim 15 and Claim 5.

36. Claim 17: The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate the mitigation action on the reachable resource.

179. *See above* Claim 12 and Claim 6.

37. Claim 18: The system of claim 17, wherein the mitigation action includes any one of: revoking access to the reachable resource, revoking access from the reachable resource, closing a port of the reachable resource, generating a notification, generating an alert, and any combination thereof.

180. *See above* Claim 17 and Claim 7.

38. Claim 20: The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: initiate active inspection of the network path to detect an application path.

181. *See above* Claim 12 and Claim 9.

39. Claim 21: The system of claim 20, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate the mitigation action further based on the application path.

182. *See above* Claim 20 and Claim 10.

D. Opinions Regarding Ground 2: Claims 8 and 19 are Obvious Over Calvo, Nguyen, and Datsenko

1. Claim 8: Claim 8: The method of claim 1, further comprising: generating an exception to the policy based on a valid network path.

183. Calvo in view of Nguyen and Datsenko teach the method of claim 1, further comprising: generating an exception to the policy based on a valid network path at least because Datsenko teaches generating exceptions to policies for reasons why a user may need to access an otherwise blocked portion of a network and the Calvo-Nguyen combination described above teaches policies on valid network paths.

184. Datsenko teaches an “Override for Policy Enforcement System,” which includes “a mechanism for assisting a user in obtaining an exception to a given policy.” Datsenko, Title, Abstract, [0003], [0009], [0021] (“Embodiment 100 is an example of a device that may monitor access to a resource, then launch an exception management system that may or may not issue an exception to the access policy.”), [0023] (“The exception management system may provide a work around or exceptions to the access control policy for certain situations.”), [0037], [0048] (“exception management system 126 may generate an exception”). Datsenko’s teachings also apply to policy exceptions based on the network path. Datsenko, [0003] (“each exception may have one or more paths by which the exception may be granted. The policy enforcement system may be used for any type of access control to any resource, including URL resources, physical peripherals or networks,

data or applications, or any other resource”), [0013] (“policy enforcement system may operate at a resource or at a gateway to a resource. For example, a network may have a gateway through which devices on the outside of the network may request access to the network.”).

185. Further, claim 8 of Calvo states "The method as recited in claim 5, wherein the compliance pack is customized according to user input based at least in part on one or more predefined compliance packs, wherein one or more customizations in the compliance pack represent *an inclusion or exclusion of one or more rules in the one or more predefined compliance packs.*" (emphasis added); see also Calvo, Claim 4. A POSITA would understand that an exclusion of one or more rules is an exception to the policy.

186. A POSITA would have been motivated to combine Datsenko with the Calvo-Nguyen combination described above, and specifically to incorporate Datsenko’s policy exception mechanism into the Calvo-Nguyen combination. For example, Datsenko discloses that “[t]he exception mechanism may capture a reason or set of reasons why a user wishes to access the resource that is otherwise restricted.” Datsenko, [0010]. Datsenko goes on to provide one example of a legitimate reason why an exception to a policy may be needed. Datsenko, [0043] (describing an example of a marketing professional who may need to gain access to an otherwise blocked social media site). A POSITA would have understood that there could be

several reasons why an exception to an otherwise valid policy may be needed, not just this example from Datsenko. For example, compliance requirements (e.g., PCI DSS) change over time. Exs. 1041-1044. A POSITA would know that compliance requirements change over time (*Id.*) and therefore would have known that exceptions to previously applied/existing policies may be needed, for example as taught by Datsenko. See generally, Datsenko. Additionally, a POSITA would have understood that incorporating Datsenko's policy exception mechanism into the Calvo-Nguyen combination would have constituted combining prior art elements according to known methods to yield predictable results and also the use of a known technique to improve a similar device in the same way. For example, Datsenko's policy exception mechanism represents just one example of known policy exceptions in the art and being able to utilize policy exceptions provides the benefit of having a more flexible system and granting access to users who may legitimately need it.

187. A POSITA would have had a reasonable expectation of success in incorporating Datsenko's policy exception mechanism into the Calvo-Nguyen combination because each reference represents known, working systems in the art. Such an incorporation would have required minor modifications in software that a POSITA would have known how to accomplish. In other words, adding in policy exceptions to policy systems would be a trivial addition. For example, Datsenko discloses that its "policy enforcement system may operate at a resource or at a

gateway to a resource. For example, a network may have a gateway through which devices on the outside of the network may request access to the network.” Datsenko, [0013]. And Datsenko discloses that its “policy enforcement system may be used for any type of access control to any resource, including URL resources, physical peripherals or networks, data or applications, or any other resource.” Datsenko, [0003], [0035], [0016] (“some or all of the subject matter may be embodied in hardware and/or software (including firmware, resident software, micro-code, state machines, gate arrays, etc.)”).

2. Claim 19: The system of claim 12, wherein the memory contains further instructions which when executed by the processing circuitry further configure the system to: generate an exception to the policy based on a valid network path.

188. *See* Claims 8 and 12.

VI. Conclusions

189. Based on the analysis described in this declaration, combined with my extensive education and experience, it is my opinion that a POSITA would have found the claims of the '693 obvious in view of Calvo, Nguyen, and Datsenko.

A handwritten signature in blue ink, appearing to read "Chuck Easttom", is written over a faint, rectangular stamp. The signature is fluid and cursive.

Dr. Chuck Easttom

03 June 2025

Date

APPENDIX A

Education

University Degrees

- **B.A.** Southeastern Oklahoma State University. Major Communications with Minors in Chemistry and Psychology. Extensive coursework in science (chemistry, physics, and biology) as well as specific courses in neuroscience (neurobiology of memory, cognitive science, etc.). Also, additional coursework in computer science including programming and database courses. While attending I was named to the National Dean's List.
- **M.Ed.** Southeastern Oklahoma State University. Coursework included technology related courses such as digital video editing, multimedia presentations, and computer graphics. A statistics course was also part of the coursework. While attending I was named to Who's Who in Colleges and Universities.
- **M.B.A.** Northcentral University in Applied Computer Science. Extensive course work in graduate computer science including graduate courses in C++ programming, C# programming, Computer Graphics, Web Programming, Network communication, Complex Database Management Systems, and Artificial Intelligence. Approximately 30 graduate hours of graduate computer science courses. Additionally, a doctoral level statistics course was included. A semester research project in electronic medical software was also part of the curriculum. I also took several research courses beyond the requirements for the degree.
- **MSSE Master of Science in Systems Engineering.** University of Texas at El Paso. The coursework includes studies in software & system requirements; system integration, verification, and validation; system architecture and design; and systems modeling & simulation. While attending I became a member of Phi Kappa Phi Honor Society and a member of the Gold Key Honor society.
- **MSDS Master of Strategic and Defense Studies** University of El Paso. Course work includes cyber warfare, information warfare, national security, space operations, low intensity conflict, strategic theory, studies of particular regions (Europe, Asia, Africa, etc.), etc.
- **D.Sc. Doctor of Science** in Cyber Security from Capitol Technology University. The curriculum included a broad coverage of cybersecurity issues. My dissertation topic was "A Comparative Study of Lattice Based Algorithms for Post Quantum Computing". This research focused on analyzing quantum resistant cryptography algorithms.
- **Ph.D. Doctor of Philosophy** in Technology from Capitol Technology University. The focus of this program was on nanotechnology used in bioengineering. More specifically my studies focused on carbon nanotubes used in bioengineering. Dissertation topic "The Effects of Complexity on Carbon Nanotube Failures". Specifically, this research focused on the impact that complexity in carbon nanotube structures had on the emergence of Stone-Wales defects in the nanotubes. The focus was particularly on nanotubes used in biomedicine such as

- genetic engineering and pharmaceutical delivery.
- **Ph.D. Doctor of Philosophy** in Computer Science from University of Portsmouth in England. The emphasis was on computer networking and the application of applied mathematics. Dissertation topic “A Systematic Framework for Network Forensics Using Graph Theory”. The study applied a broad spectrum of graph theory tools including algebraic graph theory and spectral graph theory to the modeling of network intrusions.

Industry Certifications

The following is a list of engineering and computer industry certifications I have earned.

Engineering Certifications

Note: some of these appear also in computer industry certifications

1. Associate of Systems Engineering (ASEP) from INCOSE (International Council on Systems Engineering) 275062.
2. Microsoft Certified Systems Engineer (MCSE) Windows Server 2000 Certification Number: A527-9552 (this certification is now retired)
3. EC Council Certified Application Security Engineer - .Net
4. EC Council Certified Application Security Engineer – Java
5. CISSP- ISSEP Information Systems Security Engineering Professional #387731

Hardware and Networking Related Certifications

1. CompTIA (Computer Technology Industry Associations) A+ Certified D76DTT4107
2. CompTIA Network + Certified COMP10163630
3. CompTIA Server+ Certified COMP10163630
4. CompTIA I-Net+ Certified COMP10163630
5. CompTIA Cloud+ Certified COMP001021522764
6. JN0-103 Juniper Networks Certified Associate, Junos JNCIA-Junos
7. Cisco 100-490 Supporting Cisco Routing and Switching Network Devices
8. CompTIA IT Operations Specialist (CIOS) COMP10163630
9. CompTIA Cloud Admin Professional (CCAP) COMP10163630
10. CompTIA Network Infrastructure Professional – CNIP COMP10163630

Operating System Related Certifications

11. CompTIA Linux + Certified COMP10163630
12. CompTIA Systems Support Specialist (CSSS) COMP10163630
13. CompTIA Linux Network Professional – CLNP COMP10163630
14. CompTIA Secure Infrastructure Specialist (CSIS) COMP10163630
15. Microsoft Certified Professional (MCP) – Windows Server 2000 Professional Certification Number: A527-9546

16. Microsoft Certified Systems Administrator (MCSA) Windows Server 2000 Certification Number: A527-9556 (this certification is now retired)
17. Microsoft Certified Systems Engineer (MCSE) Windows Server 2000 Certification Number: A527-9552 (this certification is now retired)
18. Microsoft Certified Technology Specialist (MCTS) Windows Server 2008 Active Directory Microsoft Certification ID: 1483483
19. Microsoft Certified Technology Specialist (MCTS) Windows 7 Microsoft Certification ID: 1483483
20. Microsoft Certified IT Professional (MCITP) Windows 7 Microsoft Certification ID: 1483483 (this certification is now retired)
21. Microsoft Certified Solutions Associate Windows 7 Microsoft Certification ID: 1483483 (this certification is now retired)
22. National Computer Science Academy Windows 8 Certification Certificate : 4787829

Programming and Web Development Related Certifications

23. Microsoft Certified Professional (MCP) – Visual Basic 6.0 Desktop Applications Microsoft Certification ID: 1483483 (this certification is now retired)
24. Microsoft Certified Professional (MCP) – Visual Basic 6.0 Distributed Applications Microsoft Certification ID: 1483483 (this certification is now retired)
25. Microsoft Certified Application Developer (MCAD) - C# Microsoft Certification ID: 1483483 (this certification is now retired)
26. Microsoft Certified Trainer (MCT 2005-2021) Microsoft Certification ID: 1483483
27. Microsoft Certified Technology Specialist (MCTS) Visual Studio 2010 Windows Application Microsoft Certification ID: 1483483
28. Microsoft Certified Technology Specialist (MCTS) Visual Studio 2010 Data Access Microsoft Certification ID: 1483483
29. National Computer Science Academy HTML 5.0 Certification Certificate : 4788000.
30. National Computer Science Academy ASP.Net Certification Certificate : 4788342
31. Certified Internet Webmaster (CIW) Associate CIW0163791
32. EC Council Certified Application Security Engineer - .Net
33. EC Council Certified Application Security Engineer – Java
34. Dynamics 365 Business Central Functional Consultant Associate
35. Microsoft Dynamics 365 Fundamentals Microsoft Certification ID: 1483483
36. Microsoft Certified: Azure AI Fundamentals Microsoft Certification ID: 1483483

37. Section 508 Standards for Web (Web accessibility course/certification from US DOJ Civil Rights Division).
38. What is Section 508 and Why Is It Important (Web accessibility course/certification from US DOJ Civil Rights Division).
39. Certified Secure Software Lifecycle Professional (CSSLP) 387731
40. Certified Professional in Accessibility Core Competency (CPACC) Certification Number 24JFCWE059

Database Related Certifications

41. Microsoft Certified Database Administrator (MCDBA) SQL Server 2000
Microsoft Certification ID: 1483483 (this certification is now retired)
42. Microsoft Certified Technology Specialist (MCTS) Implementing SQL Server
2008 Microsoft Certification ID: 1483483
43. Microsoft Certified IT Professional (MCITP) SQL Server Administration
Microsoft Certification ID: 1483483
44. DP-203 - Data Engineering on Microsoft Azure Microsoft Certification ID: 1483483
45. CompTIA Data+ (Data mining and Data science certification)
46. CompTIA DataSys+

Security and Forensics Related Certifications

47. CIW Certified Security Analyst CIW0163791
48. EC Council Certified Ethical Hacker v5 (CEH) ECC942445
49. EC Council Certified Hacking Forensics Investigator v4 (CHFI) ECC945708
50. EC Council Certified Security Administrator (ECSA) ECC947248
51. EC Council Certified Encryption Specialist (ECES)
52. EC Council Certified Instructor
53. CISSP – Certified Information Systems Professional #387731
54. CISSP – ISSAP – Certified Information Systems Architecture Professional #387731
55. CISSP – ISSEP Information Systems Security Engineering Professional #387731
56. CISSP – ISSMP Information Systems Security Management Professional #387731
57. CCFP – Certified Cyber Forensics Professional #387731 (Certification has been retired)
58. Certified Criminal Investigator (CCI) 2015-2017
59. Forensic Examination of CCTV Digital VTR Surveillance Recording Equipment
60. Oxygen Phone Forensics Certified
61. Access Data Certified Examiner (ACE) 2014-2017
62. OSForensics Certified Examiner (OSFCE)
63. Certified Forensic Consultant (CFC) 2015-2017
64. CompTIA Certified Advanced Security Practitioner (CASP) COMP10163630

- 65. CompTIA Certified Cybersecurity Analyst (CySA+) COMP001021522764
- 66. CompTIA Pentest+ COMP001021522764
- 67. CompTIA Security+ COMP001021522764
- 68. CompTIA SecurityX COMP001021522764
- 69. CompTIA Security Analytics Specialist-CSAP COMP001021522764
- 70. CompTIA Secure Cloud Professional-CSCP COMP001021522764
- 71. CompTIA Network Vulnerability Assessment Professional-CNVP COMP001021522764
- 72. CompTIA Security Infrastructure Expert -CSIE COMP001021522764
- 73. CompTIA Security Analytics Expert-CSAE COMP001021522764
- 74. CompTIA Security Network Professional – CNSP
- 75. JN0-230 – Juniper Security Associate (JNCIA-SEC)
- 76. JN0-334 – Juniper Security Specialist (JNCIS-SEC)
- 77. JN0-635 – Juniper Security, Professional (JNCIP-SEC)
- 78. Certified Cloud Security Professional (CCSP) #387731
- 79. SC-300 - Microsoft Identity and Access Administrator

Software Certifications

- 80. National Computer Science Academy Microsoft Word 2013 Certification
Certificate #: 5078016
- 81. National Computer Science Academy Microsoft Word 2000 Certification
Certificate #: 5078187

Other Certifications

- 82. CompTIA Project+ COMP10163630

Licenses

Texas State Licensed Private Investigator. Registration Number 827827. Associated with Allegiant Investigations & Security License Number: A18596

Publications

Books

- 1. Easttom, C. (2003). Moving from Windows to Linux. Newton Center, MA: Charles River Learning. 1st Edition, Charles River Media.
- 2. Easttom, C. & Hoff, B. (2006). Moving from Windows to Linux, 2nd Ed. Newton Center, MA: Charles River Learning. 1st Edition, Charles River Media.
- 3. Easttom, C. (2003). Programming Fundamentals in C++. Newton Center, MA: Charles

- River Learning. 1st Edition, Charles River Media.
4. Easttom C. (2002). JFC and Swing with JBuilder 8.0. Plano, Texas: WordWare Publishing.
 5. Easttom, C. (2002). JBuilder 7.0 EJB Programming. Plano, Texas: WordWare Publishing.
 6. Easttom, C. (2001). Beginning JavaScript, 1st Edition. Plano, Texas: WordWare Publishing.
 7. Easttom, C. (2002). Beginning VB.Net. Plano, Texas: WordWare Publishing.
 8. Easttom, C. (2001). Advanced JavaScript, 2nd Edition. Plano, Texas: Wordware Publishing.
 9. Easttom, C. (2005). Introduction to Computer Security. New York City, New York: Pearson Press.
 10. Easttom, C. (2006). Network Defense and Countermeasures. New York City, New York: Pearson Press.
 11. Easttom, C. (2005). Advanced JavaScript, 3rd Edition. Plano, Texas: Wordware Publishing.
 12. Easttom, C. & Taylor, J. (2010). Computer Crime, Investigation, and the Law. Boston, Massachusetts: Cengage Learning.
 13. Easttom, C. (2011). Introduction to Computer Security, 2nd Edition. New York City, New York: Pearson Press.
 14. Easttom, C. (2013). Essential Linux Administration: A Comprehensive Guide for Beginners. Boston, Massachusetts: Cengage Learning.
 15. Easttom, C. (2012). Network Defense and Countermeasures, 2nd Edition. New York City, New York: Pearson Press.
 16. Easttom, C. (2013). System Forensics, Investigation, and Response, 2nd Edition. Burlington Massachusetts: Jones & Bartlett.
 17. Easttom, C. (2014). CCFP Certified Cyber Forensics Professional All-in- One Exam Guide. New York City, New York: McGraw-Hill Publishing.
 18. Easttom, C. & Dulaney, E. (2015). CompTIA Security+ Study Guide: SY0-401. Hoboken, New Jersey: Sybex Press.
 19. Easttom, C. (2015). Modern Cryptography: Applied Mathematics for Encryption and Information Security. New York City, New York: McGraw-Hill Publishing.
 20. Easttom, C. (2016). Computer Security Fundamentals, 3rd Edition. New York City, New York: Pearson Press.
 21. Easttom, C. (2017). System Forensics, Investigation, and Response, 3rd Edition. Burlington Massachusetts: Jones & Bartlett.
 22. Easttom, C. & Dulaney, E. (2017). CompTIA Security+ Study Guide: SY0-501. Hoboken, New Jersey: Sybex Press.
 23. Easttom, C. (2018). Penetration Testing Fundamentals: A Hands-on Guide to Reliable Security Audits. New York City, New York: Pearson Press.
 24. Easttom, C., & Christy, R. (2017). CompTIA Security+ Review Guide: SY0-501. Hoboken, New Jersey: Sybex Press.
 25. Christy R., Easttom, C. (2018). CompTIA Security+ Practice Tests: Exam SY0-501. Hoboken, New Jersey: Sybex Press.
 26. Easttom, C. & Roberts, R. (2018). Networking Fundamentals, 3rd Edition. Goodheart-Wilcox Publishing.
 27. Easttom, C. (2018). Network Defense and Countermeasures, 3rd Edition. New York City, New York: Pearson Press.
 28. Easttom, C. (2019). Computer Security Fundamentals, 4th Edition. New York City, New York: Pearson Press.
 29. Easttom, C & Johnson, R. (2020). Security Policies and Implementation Issues, 3rd

Edition. Jones and Bartlett.

30. Alsmadi, I., Easttom, C., Tawalbeh, L. (2020). NICE Cyber Security Framework Cyber Security Management. Springer Press.
31. Easttom, C. (2020). Modern Cryptography: Applied Mathematics for Encryption and Information Security 2nd Edition. New York City, New York: Springer Press.
32. Easttom, C. (2021). Digital Forensics, Investigation, and Response, 4th Edition. Burlington Massachusetts: Jones & Bartlett.
33. Easttom, C. (2021). Quantum Computing Fundamentals. New York City, New York: Pearson Press.
34. Easttom, C. (2021). An In-Depth Guide to Mobile Device Forensics. CRC Press.
35. Easttom, C. (2021). Certified Ethical Hacker v11 Exam Cram. Pearson Press.
36. Easttom, C. (2022). Networking Fundamentals, 4th Edition. Goodheart-Wilcox Publishing.
37. Easttom, C. (2022). Modern Cryptography: Applied Mathematics for Encryption and Information Security 3rd Edition. New York City, New York: Springer Press.
38. Easttom, C. (2023). Machine Learning for Neuroscience. CRC Press.
39. Easttom, C. (2023). Computer Security Fundamentals, 5th Edition. New York City, New York: Pearson Press.
40. Easttom C., Roberts, R. (2023). Computer Service and Repair, 6th Edition. Goodheart-Wilcox Publishing.
41. Easttom, C. (2023). Network Defense and Countermeasures, 4th Edition. New York City, New York: Pearson Press.
42. Easttom, C., Butler, B., Zehra, N., Phelan, J., Stuber, S., Balkissoon, V., Rodriguez, K. (2024). Comprehensive Windows Forensics. Springer Press.
43. Easttom, C. (2024). Quantum Hardware. Springer Press.
44. Easttom, C. (2021). Digital Forensics, Investigation, and Response, 4th Edition. Burlington Massachusetts: Jones & Bartlett. Writing is done, will be published in 2025.

Papers & articles.

1. Easttom, C. (2010). RSA and its Challenges. EC Council White Paper.
2. Easttom, C. (2010). Finding Large Prime Numbers. EC Council White Paper
3. Easttom, C. (2010). A Method for Finding Large Prime Numbers. Hacking Magazine. Hands-On Cryptography Issue.
4. Easttom, C. (2014). A method for finding large prime numbers. Open-Source Article published by Academia.edu 2014.
5. Easttom, C. (2011). The RSA Algorithm - The ups and Downs. CryptoMagazine.
6. Easttom, C. (2011). Feistel Ciphers - An Overview. Presentation at Cast Security Conference. Washington, D.C.
7. Easttom, C. (2011). Steganography- History and Modern Applications. Presentation at Takedown Security Conference. This includes image, sound and video steganography.

8. Easttom, C. (2012). Problems with RSA. Presentation at Takedown Security Conference – Dallas, TX.
9. Easttom, C. (2013). Cryptanalysis. Presentation at Takedown Security Conference. Huntsville, Alabama.
10. Easttom, C. (2014). An Overview of Cryptographic S-Boxes used in Block Ciphers. Research Gate. DOI RG.2.2.14084.94088.
11. Easttom, C. (2014). Cryptographic Backdoors. Presentation at ISC2 Security Congress. Atlanta, Georgia.
12. Easttom, C. (2014). Cryptographic Backdoors. Presentation at University of Texas Dallas ACM Chapter Conference.
13. Easttom, C. (2014). Windows Registry Forensics. Research Gate. DOI RG.2.2.29603.86561
14. Easttom, C. (2014). Artificial Intelligence, Fuzzy Logic, Neural Networks and Fuzzy Neural Networks and their impact on Electronic Medical Records. Academia.edu.
15. Easttom, C. (2014). A Basic Overview of Electro-Magnetic Interference. Academia.edu.
16. Easttom, C. (2014). An Overview of Targeted Malware. Academia.edu.
17. Easttom, C. (2014). An Introduction to Mobile Forensics. Academia.edu.
18. Easttom, C. (2015). Cryptographic Backdoors. Academia.edu.
19. Easttom, C. (2015). The History of Computer Crime in America. Academia.edu.
20. Easttom, C. (2015). Spyware Techniques. Academia.edu.
21. Easttom, C. (2015). Recovering Deleted Files from NTFS. Academia.edu.
22. Easttom, C. (2015). Multi-dimensional analysis of cyber-forensic evidence. Academia.edu.
23. Easttom, C. (2016). Spyware coding techniques. Journal of Information Security Science & Digital Forensics (HJISSDF), 1 (1)
24. Easttom, C. (2016). Cryptographic Backdoors – an introduction. Journal of Information Security Science & Digital Forensics (HJISSDF), 1 (1)
25. Easttom, C. (2016). A Look at Spyware Techniques. 2600 Magazine, 33(3). Autumn issue 2016.
26. Easttom, C. (2016). Multi-Dimensional Analysis of Digital Forensic Evidence. Forensic Examiner Journal, 25 (4).
27. Easttom, C. (2016). Applying Graph Theory to Evidence Evaluation. Research Gate DOI: RG.2.2.23391.0528
28. Easttom, C. (2017). An Overview of Pseudo Random Number Generators. Research Gate. DOI: RG.2.2.13941.58087
29. Easttom, C. (2017). A Model for Penetration Testing. Research Gate. DOI: RG.2.2.36221.15844
30. Easttom, C. (2017). The RSA Algorithm Explored. International Journal of

- Innovative Research in Information Security. (IJIRIS). 4(1).
31. Easttom, C. (2017). Utilizing Graph Theory to Model Forensic Examination. International Journal of Innovative Research in Information Security (IJIRIS), 4(2).
 32. Easttom, C. (2017). Applying Graph Theory to Modeling Investigations. IOSR Journal of Mathematics (IOSR-JM) 13,2 PP 47-51. doi:10.9790/5728-130205475
 33. Easttom, C. (2017). Enhancing SQL Injection with Stored Procedures. 2600 Magazine. 34(3).
 34. Easttom, C. (2017). An Overview of Key Exchange Protocols. IOSR Journal of Mathematics (IOSR-JM). 13(4). DOI: 10.9790/5728-1304021618.
 35. Easttom, C. (2017). An Overview of Quantum Cryptography with Lattice Based Cryptography. IOSR Journal of Mathematics, 13(6).
 36. Easttom, C. (2018). A Generalized Methodology for Designing Non-Linear Elements in Symmetric Cryptographic Primitives. In Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual. IEEE.
 37. Easttom, C. (2018). The role of weaponized malware in cyber conflict and espionage. In 13th International Conference on Cyber Warfare and Security ICCWS, 2018.
 38. Easttom, C. (2018) An Overview of Cryptographic Backdoors. Journal of Information System Security, 13 (3), 177-185.
 39. Easttom, C. (2018). The Daubert Standard as a Framework for Digital Forensics. Digital Forensics Magazine, 35.
 40. Easttom, C. (2018, May). An Examination of Inefficiencies in Key Dependent Variations of the Rijndael S-Box. In Electrical Engineering (ICEE), Iranian Conference on (pp. 1658-1663). IEEE.
 41. Easttom, C. (2018, May). A Study of Cryptographic Backdoors in Cryptographic Primitives. In Electrical Engineering (ICEE), Iranian Conference on (pp. 1664-1669). IEEE.
 42. Easttom, C. (2018). Bluetooth Hacking 101. 2600 Magazine 35(1).
 43. Easttom (2018). An Examination of the Operational Requirements of Weaponized Malware. Journal of Information Warfare 17 (2).
 44. Easttom, C. (2018). A Method for Using Historical GPS Phone Records. Digital Forensics Magazine, 36.
 45. Easttom, C. (2018). A Systems Approach to Indicators of Compromise Utilizing Graph Theory. 2018 IEEE International Symposium on Technologies for Homeland Security.
 46. Easttom, C. (2018). How to model digital forensics investigations with graph theory. Digital Forensics Magazine, 37.
 47. Easttom, C. (2019). Conducting Investigations on the Dark Web. Journal of Information Warfare 18 (1).

48. Easttom, C. (2019). An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives. 2019 IEEE 9th Annual Computing and Communication Conference.
49. Easttom, C., Butler, W. (2019). A Modified McCumber Cube as a Basis for a Taxonomy of Cyber Attack. 2019 IEEE 9th Annual Computing and Communication Conference.
50. Alsmadi, I, Easttom, C. (2019). The Analysis of Sub-Communities Behavior in Social Networks. American Journal of Science and Engineering, 1(1).
51. Easttom, C. (2019). Integrating Machine Learning algorithms in the Engineering of Weaponized Malware. European Conference on the Impact of Artificial Intelligence and Robotics, Oxford University, England.
52. Easttom C. (2019). On the relationship of emergence and non-linear dynamics to machine learning and synthetic consciousness. European Conference on the Impact of Artificial Intelligence and Robotics, Oxford University, England.
53. Easttom, C. (2019). A Methodological Approach to Weaponizing Machine Learning. 4th International Conference on Computer Science and Information Engineering in Beijing China.
54. Easttom, C. (2019). On the Application of the Complexity Zeta Function to Quantify Complexity in Bioengineering Systems. 4th International Conference on Computer Science and Information Engineering in Beijing China.
55. Alsmadi, I, Easttom, C. (2019). Using Maximum Weighted Cliques in the Detection of Sub-Communities' behaviors in OSNs. Proceedings of the Future Technologies Conference 2019.
56. Easttom, C. (2019). SecML: A Proposed Modeling Language for Cybersecurity. IEEE 10th Annual Computing and Communication Conference UEMCON.
57. Easttom, C., Mei, N. (2019). Mitigating Implanted Medical Device Cybersecurity Risks. IEEE 10th Annual Computing and Communication Conference UEMCON.
58. Easttom, C., Sanders, W. (2019). On the Efficacy of Using Android Debugging Bridge for Android Device Forensics. IEEE 10th Annual Computing and Communication Conference UEMCON.
59. Easttom, C. (2020). Mathematically modeling cyber-attacks utilizing engineering techniques 15th International Conference on Cyber Warfare and Security ICCWS
60. Easttom, C., Butler, W. (2020). Applying systems engineering principles to penetration testing. 15th International Conference on Cyber Warfare and Security ICCWS
61. Easttom, C. (2020). On the Application of Algebraic Graph Theory to Modeling Network Intrusions. 2020 IEEE 10th Annual Computing and Communication Conference.
62. Easttom, C., Thapa, S., Lawson, J. (2020). A Comparative Study of Machine Learning Algorithms for Use in Breast Cancer Studies. 2020 IEEE 10th Annual Computing and Communication Conference.
63. Easttom, C. (2020). On the Application of the Complexity Zeta Function to

- Modelling Complexity and Emergence in Neuro-Engineering. 2020 IEEE 10th Annual Computing and Communication Conference.
64. Easttom, C. (2020). A professional Engineering Approach to Penetration Testing. PenTest Magazine, March 2020.
 65. Easttom, C. Adda, M. (2020). An Enhanced View of Incidence Functions for Applying Graph Theory to Modeling Network Intrusions. WSEAS Transactions on Information Science and Applications. DOI: 10.37394/23209.2020.17.12
 66. Easttom, C., Ibrahim, A., Chefronov, C., Alsmadi, I., Hanson, R. (2020). Towards a deeper NTRU analysis: a multi modal analysis. *International Journal on Cryptography and Information Security (IJCIS)*. 10(2).
 67. Easttom, C. Adda, M. (2020) The Creation of Network Intrusion Fingerprints by Graph Homomorphism. WSEAS Transactions on Information Science and Applications. 17(2020). DOI: 10.37394/23209.2020.17.15
 68. Easttom, C. (2021). Mathematically modelling victim selection in cybercrimes. 16th International Conference on Cyber Warfare and Security - ICCWS 2021
 69. Easttom, C. (2021). A methodology for smart TV Forensics. 16th International Conference on Cyber Warfare and Security - ICCWS 2021
 70. Easttom C. (2021). On the Use of the SSIM Algorithm for Detecting Intellectual Property Copying in Web Design. IEEE 11th Annual Computing and Communication Conference.
 71. Easttom, C., Adda, M. (2021). Application of the Spectra of Graphs in Network Forensics. IEEE 11th Annual Computing and Communication Conference.
 72. Pelosi, M., & Easttom, C. (2021). Identification of LSB image Steganography using Cover Image Comparisons. *Journal of Digital Forensics, Security and Law*, 15(2), 6.
 73. Easttom, C., Butler, W. (2021). The Iran-Saudi Cyber Conflict. *International Journal of Cyber Warfare and Terrorism (IJCWT)*
 74. Easttom, C., Bianchi, L., Valeriani, D., Nam, C., Hossaini, A., Zapala, D., Roman-Gonzalez, A., Singh, A., Antonietti, A., Sahonero-Alvarez, G., Balachandran, P., (2021). A Functional Model for Unifying Brain Computer Interface Terminology. *IEEE Open Journal of Engineering in Medicine and Biology*.
 75. Easttom, C. (2021). Applying Mathematics and Engineering Techniques to Cyber Security. In *Actas del Congreso Internacional de Ingeniería de Sistemas* (pp. e5575-e5575).
 76. Easttom, C., Bianchi, L., Valeriani, D., Nam, C. S., Hossaini, A., Zapala, D., ... & Balachandran, P. (2021). A functional BCI model by the P2731 working group: control interface. *Brain-Computer Interfaces*, 8(4), 154-160.
 77. Easttom, C., Alsmadi, I (2022). A Comparative Study of Machine Learning Algorithms for Identifying Mental States from EEG Recordings. IEEE 12th Annual Computing and Communication Conference.
 78. Easttom, C. (2022). NTRU & LASH Implemented for Quantum Resistant Blockchain. IEEE 12th Annual Computing and Communication Conference.
 79. Easttom, C. (2024). Utilizing ChatGPT to Improve Quantum Algorithms. IEEE 14th Annual Computing and Communication Workshop and

Conference (CCWC)

80. Easttom, C. (2025). Majorana Nanowires for Topological Quantum Computing. IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC).
81. Easttom, C. (2025). Malicious Use of Artificial Intelligence. IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC).
82. Lee, B., Easttom, C. (2025). A Novel Framework for Malware Analysis: Integrating Large Language Models with Heuristic Techniques. IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC).
83. Easttom, C. (2025). Quantum Resistant Cryptography and Cyberwarfare. ICCWS, 20th International Conference on Cyber Warfare and Security.
84. Easttom C. (2025). Understanding Deepfakes and Countermeasures. ICCWS, 20th International Conference on Cyber Warfare and Security.

Patents

1. U.S. Patent No. 8,527,779 B1 Method and apparatus of performing distributed steganography of a data message.
2. U.S. Patent No. 8,713,067 Stable File System
3. U.S. Patent No. 8,819,827 B1 Method and apparatus of performing data executable integrity verification.
4. U.S. Patent No. 8,825,845 B1 Managing a network element operating on a network.
5. U.S. Patent No. 8,825,810 B1 Domain name service based remote programming objects.
6. U.S. Patent No. 8,984,639 Method and apparatus of performing data executable integrity verification.
7. U.S. Patent No. 9,405,907 Method and apparatus of performing data executable integrity verification (a continuation patent of '639)
8. US Patent No. 9,313,167 Domain name service based remote programming objects.
9. US Patent No. 9,619,656 Method and apparatus of performing distributed steganography of a data message (continuation patent of 8,527,779 B1)
10. US Patent No. 9,686,227 Domain Name Service based remote programming objects (continuation patent of U.S. Pat. No. 9,313,167)
11. US Patent No. 9,755,887 Managing a network element operating on a network.
12. US Patent No. 9,754,108 Method and apparatus of performing data executable integrity verification.
13. US Patent No. 9,753,957 System and method for document tracking
14. US Patent No. 9,984,229 Method and apparatus providing a multiple source evidence application trust model.

15. US Patent No. 10,122,573 Managing a network element operating on a network.
16. US Patent No. 10,242,188 Method and apparatus of performing data executable integrity verification.
17. US Patent No. 10,360,354 Method and apparatus of performing distributed steganography of a data message. A continuation patent of U.S. Pat. No. 9,619,656.
18. U.S. Patent No. 10,469,441 Domain name service based remote programming objects. A continuation patent of U.S. Patent 9,686,227.
19. U.S. Patent No. 10,467,208 System and method for document tracking. A continuation patent of U.S. Patent 9,753,957.
20. US Patent No. 10,621,149 Stable File System. A continuation patent of U.S. Pat. No. 8,713,067.
21. U.S. Patent No. 10,635,815 Method and apparatus of performing data executable integrity verification.
22. U.S. Patent No. 10,708,118 Managing a network element operating on a network.
23. U.S. Patent No. 11,080,396 Secure Downloads
24. U.S. Patent No. 11,165,629 Managing a network element operating on a network.
25. U.S. Patent No. 11,204,999 Method and apparatus of performing data executable integrity verification.
26. US Patent 11,775,477 Stable file system. A continuation patent of U.S. Pat. No. 8,713,067.
27. US Patent 12,155,523 B1 Managing a Network Element Operating on A Network

Standards and Certification Creation

1. Chair of IEEE P3123 Standard for Artificial Intelligence and Machine Learning (AI/ML) Terminology and Data Formats from 2021 to 2024.
2. Vice Chair of IEEE P23026 - Systems and Software Engineering -- Engineering and Management of Websites for Systems, Software, and Services Information from 2018-2021.
3. Member of IEEE Software & Systems Engineering Standards Committee. Working on DevOps 2675 from 2017-2020.
4. Member of the IEEE Engineering in Medicine and Biology Standards Committee. Standard for Unified Terminology for Brain-Computer Interfaces P2731.
5. Member of IEEE Artificial Intelligence Standards Group
 1. Editor in Chief for the *American Journal of Science and Engineering* 2017 to 2022
 2. Editorial board for the Journal Artificial Intelligence in Medical Imaging
 3. Editorial Review Board for *International Journal of Cyber Warfare and*

Terrorism (IJCWT)

4. Reviewer for Journal of Modern Mechanical Engineering and Technology – EBM
5. Reviewer for scientific papers submitted to *IEEE Security & Privacy* and the *IEEE Open Access Journal*.
6. Reviewer for the *International Journal of Network Security (IJNS)* 2018-2019
7. Reviewer for the *International Journal of Computer Science and Security (IJCSS)* 2018-2019
8. Reviewer for the *Journal of Information Warfare (JIW)* for 2019
9. Reviewer for scientific papers submitted to *Digital Forensics magazine* for 2016 to 2018.
10. Editorial board member for the year 2016 for *Journal of Information Security Science & Digital Forensics*.
11. Editorial board for the year 2016 member for *The Forensic Examiner*.
12. Subject matter expert for the Computer Technology Industry Association (CompTIA) Server + exam creation team. I was part of the team that helped create the CompTIA Server+ certification test.
13. Subject matter expert for the Computer Technology Industry Association (CompTIA) Linux+ exam review team. I was part of the team that helped create the CompTIA Linux+ certification test.
14. Subject matter expert for the Computer Technology Industry Association (CompTIA) Security+ exam Job Task Analysis team. I was part of the team that helped create the CompTIA Security+ certification test.
15. Subject matter expert for the Computer Technology Industry Association (CompTIA) Certified Technical Trainer exam revision team.
16. Created the EC Council Certified Encryption Specialist course and certification test. Then I revised the course and certification in 2017.
17. Created the EC Council CAST Advanced Encryption course.
18. Created the EC Council advanced forensics courses for Dark Web investigations; Memory and Malware Forensics; and Cell Phone Forensics.
19. Created the EC Council IoT and IoT security courses.
20. Worked on the Job Task Analysis Team for the Certified Ethical Hacker v8 test.
21. Created the video courses for EC-Council CASE (Certified Application Security Engineer) courses for Java and .Net.
22. Member of the advisory board for Embry Riddle University cyber security program within the Homeland Security degree program 2016-2018.
23. Created the OSCFE (OS Forensics Certified Forensic Examiner) course and test.
24. Advisory board committee for your DOE- National Nuclear Security Administration (NNSA)'s solicitation, "Minority Serving Institution Partnership Program (MSIPP), title TAMUK Cybersecurity Minor / Certificate Program for DOE / NNSA Workforce. Texas A&M University Kingsville.

Professional Awards and Memberships

1. Participated in the University of Arizona Research Leadership Institute (RLI), mentoring a younger professor in launching a research career.
2. Participated in the 2nd Lt J.P. Blecksmith Research Fellowship program, mentoring a Lieutenant in developing research.
3. Distinguished Speaker of the Association of Computing Machinery (2017 to 2020)
4. Distinguished Visitor of the IEEE Computer Society (for the term of 1 January 2020 through 31 December 2022)
5. Senior Member of the IEEE (Institute of Electronics and Electrical Engineers) 92862378
6. Senior Member of the ACM (Association of Computing Machinery) 0447967
7. Member of the ACM Special Interest Group on Artificial Intelligence
8. Member of the International Association of Cryptological Research (IACR)
9. International Association of Accessibility Professionals
10. Member of the ACM Special Interest Group on Security, Audit and Control
11. Member of the IEEE Nanotechnology Society
12. Member of the IEEE Engineering in Medicine and Biology Society
13. Member of the International Council of Systems Engineers (INCOSE) 275062
14. Affiliate Member of the National Academy of Forensic Engineers
15. Member of the American Physical Society (APS). Member of both the Quantum Information and Nuclear Physics divisions from 2018 to 2023.
16. Member of the Association for the Advancement of Artificial Intelligence
17. Associate Member of the American Academy of Forensic Sciences (2015 to 2018)
18. Member of InfraGard (FBI-Civilian group for cyber security) 2013- 2019
19. 1992-1993 National Dean's List
20. Who's Who in American Colleges and Universities 1998
21. Marquis Who's Who in America
22. Marquis Who's Who in Education
23. Marquis Who's Who in Science and Engineering
24. Phi Kappa Phi Honor Society # 12618300
25. Gold Key Honor Society #900058595

Speaking Engagements

1. Mid-Cities PC Users Group September 19, 2003. The topic was computer security

- in general.
2. The Harvard Computer Society April 5, 2004. The topic was computer security.
 3. The ACM Chapter of Columbia University November 15, 2005. The topic was computer viruses.
 4. DeVry/Keller University in Dallas December 2009 Commencement Speaker.
 5. Public presentation on computer crime in McKinney Texas in July 2008.
 6. Southern Methodist University Computer Science and Engineering Colloquium September 2010. The topic was organized computer crime and computer terrorism. I was an invited speaker.
 7. Takedowncon security conference in Dallas Texas, May 2011. The topic was steganography. I was an invited speaker. This included image, audio, and video steganography.
 8. An Overview of Modern Cryptography, May 5, 2011, Webinar
 9. CAST Conference in Washington D.C. August 2011. The topic was Cryptography: Feistel Ciphers. The audience was primarily Department of Defense personnel and contractors. I was an invited speaker.
 10. Digital Certificates: An Expert View, January 12, 2012, Webinar
 11. Takedown security conference in Dallas Texas, May 2012. The topic was RSA cryptography. I was an invited speaker.
 12. Problems with RSA, November 4, 2012, Webinar
 13. Takedowncon security conference in Huntsville Alabama, July 15, 2013. The topic was cryptanalysis. The audience was primarily Department of Defense personnel and contractors. I was an invited speaker.
 14. September 25-26, I conducted a 2-day master class in hacking techniques, in Singapore for Clariden Global. I was an invited speaker.
 15. March 2014, I conducted a presentation for the University of Texas ACM chapter. The topics were distributed steganography and cryptographic backdoors.
 16. May 26-27, 2014. I conducted a 2-day workshop in software testing in Singapore for Clariden Global. I was an invited speaker.
 17. June 2014, I conducted a public talk on computer crime and internet safety in Melissa Texas, sponsored by the Melissa Police Department.
 18. October 1, 2014, presentation of a talk on cryptographic backdoors at the ISC2 Security Conference in Atlanta Georgia.
 19. October 5, 2014, presentation of a talk on cryptographic backdoors at the Hakon convention in Indore, India. I was an invited speaker.
 20. October 17, 2014, U.S. Secret Service, North Texas Electronic Crimes (N-TEC) Task Force presenting a talk on the history and current state of computer crime. I was an invited speaker.
 21. November 7, 2014, North Texas Crime Commission-Healthcare Cyber Security Symposium presenting a talk on health care breaches. I was an invited speaker.
 22. January 27, 2015: Collin County Sheriff's Alumni Association.
"Cybercrime and online predators".
 23. April 14, 2015, Brighttalk webinar "What you don't know about Cryptography and how it can hurt you".
 24. May 4, 2015, North Texas Crime Commission-Healthcare Cyber Security Symposium presenting a talk on the causes and remediation of health care

- breaches. I was an invited speaker.
25. May 12, 2015, SecureWorld Houston “What you don’t know about Cryptography and how it can hurt you”.
 26. August 20, 2015. Southwest Financial Crimes Forum “7 biggest mistakes of incident response.” I was an invited speaker.
 27. September 30, 2015, ISC2 Security Congress “Cryptanalysis for Forensics”.
 28. October 3, 2015. Conducted a 1-day workshop in Malware at Hakon India. I was an invited speaker.
 29. October 4, 2015. Hakon India Indore India. 2015 “Cyberwar and Terrorism”.
 30. November 4, 2015, iSMG Fraud Summit in Dallas Texas “Business Email Masquerading: How Hackers Are Fooling Employees to Commit Fraud”. I was an invited speaker.
 31. November 5, 2015, SWACHA Electronic Payments Summit in Irving Texas “Emerging Trends in Cyber Crime”. I was an invited speaker.
 32. May 25, 2016 “Improving Professional Standards in Cyber Forensics” Keynote speaker for Association of Digital Forensics Security and Law. I was an invited speaker.
 33. June 22, 2016, the topic was “Cyber Security Issues Facing Business” Texas Security Bank Business Institute meeting. I was an invited speaker.
 34. August 4, 2016 “Steganography: The in’s and Out’s” DefCon 24, Las Vegas. This included image, audio, and video steganography.
 35. September 12, 2016, USMCOC Third North American Sustainable Economic Development Summit Cyber Security, Information Technology & Innovation Panel. I was an invited speaker.
 36. September 13, 2016, Tarleton State University CyberSecurity Summit at the George W. Bush Institute. The topic was "A template for incident response". I was an invited speaker.
 37. September 28, 2016, Secure World Dallas. A presentation on "Analyzing Forensic Evidence -Applications of graph theory to forensic analysis”.
 38. October 2, 2016, Hakon India (Indore India). A presentation on “The Dark Web Markets – Implications for Law Enforcement and Counter Terrorism”. I was an invited speaker.
 39. October 18-19, 2016, Jordan Cyber Security & Forensics Forum (JCSFF-2016) Presenting two presentations. The topics were “Zero Day Exploits” and “How to forensically analyze Zero Day Exploits”. I was an invited speaker.
 40. December 1-2. I conducted a 2-day advanced workshop on cyber-threat intelligence in Singapore for Clariden Global. I was an invited speaker.
 41. January 17, 2017, the 2nd International Congress of the International Association of Law and Forensic Science (IALFS), in Cairo Egypt January 17, 18, 19. The topics were “Improving Digital Forensics” and “Applying Graph Theory to Model Forensic Examinations”. I was an invited speaker.
 42. February 11, 2017. North Texas Cyber Security Association bimonthly meeting. Speaking on Dark Web Markets and their impact for law enforcement and intelligence agencies. Plano Texas Collin College Courtyard Campus.
 43. February 17, 2017. American Academy of Forensic Sciences 69th Annual Meeting. Speaking on a novel approach JTAC phone forensics.

44. March 3, 2017. University of North Texas. A presentation on Applying Graph Theory to Analyzing Digital Evidence.
45. May 24, 2017. Enfuse 2017 conference in Las Vegas. A presentation on Applying Graph Theory to Analyzing Digital Evidence.
46. July 27, 2017. Defcon 25 2017 conference in Las Vegas. A presentation entitled "Windows: The Undiscovered Country" on undocumented features of Windows and SQL Server that can be used for hacking and penetration testing.
47. September 25, 2017, ISC2 Security Congress in Austin Texas. A presentation on "Applying Graph Theory to Analyzing Digital Evidence".
48. September 27 and 28, 2017. Secure Jordan conference in Amman. I presented two talks. The first is "An overview of current challenges in phone forensics". The second is "How to address dark web markets".
49. October 18-19 SecureWorld Dallas 2017. A presentation on "Cryptography, what you don't know and how it can hurt you".
50. January 8 to 10th Annual IEEE Computing and Communication Workshop at the University of Nevada in Las Vegas, a presentation on my paper "A Generalized Methodology for Designing Non-Linear Elements in Symmetric Cryptographic Primitives". I also chaired a session on Artificial Intelligence, and another session on Computer Architecture and VLSI.
51. February 2018, Provost Marshal General's Annual Army Worldwide Antiterrorism Training Seminar. I spoke on terrorism and the dark web.
52. March 8 to 9 ICCWS conference (13th International Conference on Cyber Warfare and Security) presenting my paper "The Role of Weaponized Malware in Cyber Conflict and Espionage". Also presenting a research poster on "A Modified McCumber Cube as a Basis for a Taxonomy of Attacks"
53. March 23, 2018, presenting "Penetration Testing as a Profession Rather than a Dark Art". at the ISC2 Dallas Chapter Meeting in Murphy Texas.
54. April 11, 2018, University of Texas at Dallas ACM chapter hosted my Distinguished Speaker of the ACM Talk "Quantum Computing and Lattice Based Cryptography."
55. May 7, 2018, Princess Sumaya University for Technology in Amman Jordan hosted my Distinguished Speaker of the ACM Talk "Applying Graph Theory to Digital Forensics."
56. May 17, 2018. SecureWorld Houston 2018. Presentation on "Quantum Computing and Cryptography."
57. May 17, 2018, speaking on "Quantum Computing and Post Quantum Cryptography" at SecureWorld Houston.
58. September 17-19, 2018, I presented presenting "Dark Web Market Investigations" at the San Antonio Techno Security & Digital Forensics Conference
59. September 25, 2018, I presented "Dark Web Market Investigations" at the Global Security Exchange (GSX) 2018 (formerly the Annual Seminar and Exhibits) in Las Vegas Tuesday, September 25, 2018 (11 am Session 5127)
60. October 8-10, 2018 "An exploration of quantum computing and post quantum cryptography" ISC2 Security Congress in New Orleans.
61. October 10-11, 2018, speaking on "Quantum Computing and Post Quantum Cryptography" at SecureWorld Dallas.

62. October 23-24, 2018, IEEE International Symposium on Technologies for Homeland Security. Presenting my paper "A Systems Approach to Indicators of Compromise Utilizing Graph Theory"
63. January 7-9, 2019. On 9 January at 10:30 I was the keynote speaker at the IEEE CCWS conference in Las Vegas presenting a talk on "The impact of complexity and emergent properties on engineering". During the conference I am also presenting my papers "A Modified McCumber Cube as a Basis for a Taxonomy of Cyber Attacks" and "An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives"
64. February 11th, an invited talk on "Application of Graph Theory for Digital Forensics" at Seton Hall University.
65. March 7-8, 2019, The International Conference on Data Sciences, Security and Applications (ICDSSA, 2019) Delivering two invited talks: "Overview of Cryptographic Backdoors" and "S-Box Design in symmetric cryptographic primitives" as part of the Distinguished Speakers of the ACM program.
66. March 14-15, 2019. Future of Information and Communication Conference (FICC) 2019 in San Francisco. I presented my Distinguished Speaker of the ACM talk: "Quantum Computing and Lattice Based Cryptography" as an invited keynote speaker.
67. April 4, 2019, Cyberintelligence Summit - Identifying Emerging Threats & Defenses. Fayetteville Arkansas. Speaking on "What Computer Science and Digital Forensics Can and Cannot Do for You in any Case". This is at the University of Arkansas School of Law, Fayetteville, Arkansas.
68. April 5, 2019, Cyberintelligence Summit - Identifying Emerging Threats & Defenses. Fayetteville Arkansas. Speaking on "What Computer Science and Digital Forensics Can and Cannot Do for You in any Case". This is at the Arkansas Bar Center, Little Rock, Arkansas.
69. May 23-24, 2019. ACM Colloquium on Information Assurance, Cybersecurity, and Management CIACAM in Minneapolis. Delivered my Distinguished Speaker of the ACM talk on "Quantum Computing and Lattice Based Cryptography".
70. September 27-28. ICCSIE –International Conference on Computer Science and Information Engineering in Beijing China. Presenting two papers as well as a keynote address "The current state of Quantum Computing"
71. October 11, 2019. Hacker Halted, presenting a talk on "The State of Dark Web Investigations".
72. October 26, 2019, Colloquium on Analytics, Data Science and Computing (CADSCOM 2019). Keynote talk on Quantum Computing and AI.
73. October 28-30, 2019. ISC2 Security Congress. Presenting on machine learning and cybersecurity.
74. November 6, 2019. IEEE Quantum Education Summit 2019. Speaking on master's degree curriculum in quantum computing.
75. February 26-27, 2020. 5th International Conference on Quantum and Particle Physics in London, England. Delivering a talk entitled "Space-Time and Gravity as Emergent Quantum Properties."
76. September 2, 2020, National Centers for Academic Excellence invited talk:

- "Quantum Computing and how it relates to security."
77. September 10, 2020. International IOT, Electronics and Mechatronics Conference
Delivering a keynote address "The impact of complexity and emergence on engineering."
 78. November 19, 2020. Distinguished Visitor of the IEEE talk on "The impact of Emergence, Nonlinear Dynamics, and Chaos Theory on Engineering."
 79. December 18, 2020. US-Korea Conference Sustainable Development & the Future. I am an invited speaker presenting on "Applications of Machine Learning to BCI (Brain Computer Interface)"
 80. February 12, 2021. Arizona ISACA Meeting. I spoke on criminal activity on the Dark Web.
 81. 24 February 2021. "The Current Status of Quantum Computing" This is an IEEE Distinguished Visitor Program talk presented to the IEEE Region 4.
 82. 25 March 2021. "The Current Status of Quantum Computing" This is an IEEE Distinguished Visitor Program talk presented to IEEE Rock River Valley Computer Society chapter and IEEE Rock River Valley Section and IEEE Women in Engineering.
 83. 25 April 2021 "Applications of Machine Learning to Cybersecurity" GIDS 2021 conference.
 84. September 21, 2021. Delivered a talk on Quantum Resistant Cryptographic Algorithms for the Silicon Valley/SF Bay Area IEEE Computer Chapter.
 85. October 5, 2021. Delivered a talk at Hacker Halted on The Impact of Machine Learning on Cybersecurity.
 86. October 27, 2021, Keynote speaker at CHIS2021 conference. Delivered a talk on Bringing Mathematical Rigor to Cybersecurity.
 87. December 3-5, 2021, Keynote speaker at International Symposium on Automation, Information and Computing (ISAIC 2021) Delivering a talk on Fuzzy logic and its impact on machine learning and AI.
 88. October 3, 2022, Speaker at Hacker Halted on the topic of Quantum Computing and its impact on cybersecurity.
 89. December 08, 2023, Speaker at an ICAC Conference. ICAC is the Internet Crimes Against Children task force. I spoke on malicious applications of artificial intelligence and machine learning.
 90. January 10, 2024, Speaker at ICAC national conference. ICAC is the Internet Crimes Against Children task force. I spoke on malicious applications of artificial intelligence and machine learning.
 91. March 1, 2024, Speaker at Indiana ICAC meeting. ICAC is the Internet Crimes Against Children task force. I spoke on malicious applications of artificial intelligence and machine learning.
 92. October 30, 2024, Keynote speaker at Hacker Halted 2024 "AI uses by malicious actors."
 93. February 18, 2025. "The Future of Computing: Exploring Quantum Leaps and Incremental Advances" – IEEE Distinguished Lecturer Program IEEE Computer Society, Mohan Babu University India.
 94. May 20, 2025 "The current state of quantum computing and cryptography" – IEEE Distinguished Lecturer Program IEEE Computer Society, IEEE

Litigation Support Experience

I have worked for both plaintiffs and defendants in computer science related cases. These cases include software copyright, trade secret cases, patent cases, and computer crime related cases. In patent cases I have opined on both infringement and validity issues. I have also testified as to the valuation of computer software.

1. 2004-2005 AVG v. Microsoft, consulting for the firm of McKool Smith on behalf of the plaintiff AVG. This was a patent infringement case involving six patents. I was the testifying expert for one patent (the '286 patent) and a consulting expert for the others. This case involved software analysis for several hundred gigabytes of software source code as well as preparation of claim charts. This case concluded.
2. 2006 Harrison v. Comtech Solutions Worldwide Inc., consulting for the firm of Winthrop & Weinstein on behalf of Comtech Solutions. This was a software copyright infringement case. I was a consulting expert for this case.
3. 2006 The Weidt Group v. Cold Spring Granite Company, consulting for the firm of Winthrop & Weinstein on behalf of The Weidt Group. This was a software copyright infringement case. I was a consulting expert for this case. This case concluded.
4. 2008 Countryman v. NextMedia Inc., consulting for the firm Siebman, Reynolds, Burg, & Phillips on behalf of the plaintiff, Countryman. This case involved an alleged breach of network security. I was a testifying expert, the case settled before trial.
5. 2008-2009 Virnetx v. Microsoft, consulting for firm of McDermott, Will, and Emery on behalf of the plaintiff Virnetx. This was a patent infringement case. This case involved software analysis for several hundred gigabytes of software source code. I was a consulting expert for this case. The case went to trial in 2010.
6. Virnetx v Apple, case 6:10-cv-00417 consulting for firm of McDermott, Will, and Emery on behalf of the plaintiff Virnetx. This was a patent infringement case. This case involved software analysis for several hundred gigabytes of software source code. I was a consulting expert for this case.
7. 2010 SSL Services LLC v. Citrix Systems Inc., consulting for the firm of Dickstein and Shapiro LLC on behalf of the plaintiff SSL Services. This was a patent infringement case. I was a consulting expert for this case. Case No. 2-08-cv-158 (E.D. Tex.).
8. 2009-2012 Uniloc v. multiple defendants, consulting for the firm of Ethridge Law Group on behalf of Uniloc. This was a patent infringement case. I consulted and performed the analysis of over 100 potential defendants, determining if the products in question infringed. This involved analyzing the

- software utilizing standard network forensics techniques as well as reviewing source code. The case also required me to prepare over 100 claim charts. This was a patent case. Case numbers including No. 6:14-cv-00415 (E.D. Tex.) (ArcSoft, Inc.), No. 6:14-cv-00420 (E.D. Tex.) (Canon U.S.A., Inc.), No. 6:14-cv-00424 (E.D. Tex.) (Embarcadero Technologies, Inc.).
9. 2011-2012 Virnetx v. Cisco et al.; Virnetx v Mitel, et al., consulting for the firm of McKool Smith on behalf of Virnetx. This was a patent infringement case. I was a consulting expert for this case. This case involved software analysis for over 20 gigabytes of software source code for various Cisco products. This was a patent case. I also worked on the related Alcatel case and reviewed source code for those products as well. Case No. 6:10-cv-00417 (E.D. Tex.)
 10. 2011 Parallel Networks v. Abercrombie & Fitch, multiple defendants, and multiple law firms on behalf of approximately 80 defendants. This was a patent infringement case. Most of the defendants I was working on behalf of won summary judgement Case No. 6:10-cv-00111 (E.D. Tex.). This case concluded.
 11. 2011 Nuance v. Vlingo, consulting for the firm of Hays, Bostic, & Cronnin, on behalf of Vlingo. This was a patent infringement case. I was a consulting expert for this case that involved extensive source code review. Case No. 1:09-cv-11414 (D. Mass.). This case concluded.
 12. 2011 Eolis v. Adobe Systems Inc., et al., Consulting for the firm of Locke, Lord, Bissel, and Liddell on behalf of defendant Citibank. This was a patent infringement case. I was a consulting expert for this case. Case No. 6:09-cv-00446 (E.D. Tex.). Case settled.
 13. 2012 Smartphone case v. Apple on behalf of the firm of Hayes, Bostic, and Cronin on behalf of Smartphone. This was a patent infringement case. I was a consulting expert for this case. This was a patent case. As part of my work on this case I reviewed Apple iOS source code. Case No. 6:13-cv-00196 (E.D. Tex.). Case settled.
 14. 2012 Smartphone case v. Android (HTC and Sony) on behalf of the firm of Nelson, Bumgardner, and Castro on behalf of Smartphone. This was a patent infringement case. I was a consulting expert for this case. As part of my work on this case I reviewed source code for several Android based phones. This was a patent case. Case No. 6:10-cv-00580 (E.D. Tex.). Case settled.
 15. 2012-2013 Market One Models v. Tekcenture. For the plaintiff. This was a software copyright infringement case. This case also involved valuation of software and intellectual property. I was a testifying expert in this case. The case was settled during trial. Dallas County CAUSE NO. CC-10-05682-A.
 16. 2012-2013 Allstate v. Nationwide consulting for the firm Banner & Whitcoff, on behalf of AllState. This was a patent infringement case; I was a consulting expert for this case. My work on this case involved software source code review for insurance applications. The case was settled before trial. Case No. 1:12-cv-03609 (N.D. Ill.).
 17. 2012 Unified Messaging Solutions LLC v. Facebook Inc., Google Inc., Intuit, etc. consulting for the firm of Nelson, Bumgardner, and Castro on behalf of

- Unified Messaging Solutions LLC. This was a patent infringement case. I was a consulting expert for this case. This case involved extensive software source code analysis. Cases No. 6:11-cv-00120 (E.D. Tex.) (Facebook), No. 6:12-cv-00085 (E.D. Tex.) (Intuit), No. 6:11-cv-00464 (E.D. Tex.) (Google).
18. 2012- 2013 DN Lookup Technologies v. Charter Communications et al. Consulting for the firm of Lee, Jorgensen, Pyle & Kewalraman on behalf of DN Lookup Technologies. This was a patent infringement case. I was a consulting expert for this case. Case No. 1:11-cv-01177 (D. Del.).
 19. 2013 Droplets v. Amazon, et al Consulting for the firm of Wilson, Sonsini, Goodrich, & Rosati on behalf of the defendants E-Trade, Charles Schwab, Ameritrade, and Scottrade. This was a patent infringement case. I was a consulting expert for this case. The case was settled before trial. Case No. 3:12-cv- 03733 (N.D. Cal.).
 20. 2013 Andrews v. Medical Excesses LLC. Consulting for the firm of Maynard, Cooper & Gale on behalf of the defendant. This was a liability case involving a breach of network security. The case was settled before trial. Case No. 2:11-cv- 1074 (M.D. Ala.).
 21. 2013 Macro Niche Software, Inc., and Michael j. Ruthemeyer v. 4 Imaging Solutions, L.L.C., Protech Leaded Eyewear, Inc. And Imaging Solutions of Australia consulting for the firm of Kevin R. Michaels, P.C on behalf of the plaintiff. This was a software copyright infringement case. This case also involved valuation of software and intellectual property. I was a testifying expert in this case. The case was settled before trial. Case No. 4:12-cv-2292 (S.D. Tex.).
 22. 2013 Geotag v. Frontier Communications et al. Consulting for the firm of Reese, Gordon, & Marketos on behalf of the plaintiff. This was a patent infringement case involving multiple defendants. I was a testifying expert in this case. The case involved extensive source code and product analysis. This was a patent case. The cases settled before trial. Case No. 2:10-cv-00265 (E.D. Tex.).
 23. 2013-2014 Geotag v. Starbucks et al. Consulting for the firm of Reese, Gordon, & Marketos on behalf of the plaintiff. This was a patent infringement case involving multiple defendants. I was a testifying expert in this case. This was a patent case. The case involved extensive source code and product analysis. The cases settled before trial. Case No. 2:10-cv-00572 (E.D. Tex.).
 24. 2013-2014 Geotag v. AT&T et al. Consulting for the firm of Malouf & Nockels LLP and the Winstead law firm, on behalf of the plaintiff. This was a patent infringement case. I was a testifying expert in this case. This was a patent case. The case involved extensive source code and product analysis. The case was settled before trial. Case No. 3:13-cv-00169 (N.D. Tex.).
 25. 2013 MCNE, Inc. and David Todd McGee v Amarone Partners LLC, et al. District Court of Dallas County. Consulting for the firm of Howie Law PC on behalf of the defendant. This was a software copyright infringement case. I was a testifying expert in this case, but the case settled before trial. Case Dallas County, Texas DC-11-03860.

26. 2013 PiNet v. J.P. Morgan Chase. Consulting for the firm of Puziniak Law Office on behalf of the plaintiff. This was a patent infringement case. I was a testifying expert on invalidity issues. The case was settled before trial. Case 1:12-cv-00282 (D. Del.).
27. 2013. Future Ads LLC v. Gillman, No. SACV13905DOCJPRX.
28. 2014 Pragmatus Telecom LLC v Volkswagen Group of America. Working for the defendant on behalf of the firm Locke Lord LLP. This was a patent case. I was a consulting expert. The case was settled before trial. Case 1:12-cv-01559 (D. Del.).
29. 2014 API Technical Services LLC vs Anthony Francis et al. working for the defendant on behalf of the Wade Law Firm. I was a testifying expert in this case, the case settled before trial. Case 4:13-cv-627 (E.D. Tex.).
30. 2014 Ameranth, Inc. v. Genesis Gaming Solutions, Inc., for the defendant Genesis Gaming Solutions. This was a patent infringement case. I was a testifying expert in this case, the case settled before trial. This case was in the Central District of California. Case 8:13-cv-00720 (C.D. Cal.).
31. 2014 Ameranth, INC v. ITCS INC., for the defendant ITCS. This was a patent infringement case. I was a testifying expert in this case, settled before trial. This case was in the Central District of California SA 8:13-00720 AG. Case 8:13-cv-00720 (C.D. Cal.).
32. 2014 Neomedia Inc. vs Dunkin Brands Inc. Civil Action No.: 13-cv-02351-RM-BNB. I was retained by the firm of Nutter law on behalf of the defendant Dunkin Brands Inc. This was a patent case. The case was settled before trial. Case 1:13-cv-02351 (D. Colo.).
33. Neomedia v Marriott Intl. Inc. Civil Action No. 14-cv-001752-KLM. I was retained by the firm of Ballard Spahr LLP for the defendant. This was a patent case. The case was settled before trial. Case 1:13-cv-001752 (D. Colo.).
34. 2014 Federal Trade Commission vs Boost Software Inc. for the defendant. Case 14-cv-81397 (S.D. Fla.). The case concluded at trial.
35. 2014 Federal Trade Commission vs PC Cleaner Pro Inc. for the defendant. Case 14-cv-81395 (S.D. Fla.). The case concluded at trial.
36. 2015 E AutoXchange LLC vs Academy, LLC. I was retained on behalf of the defendant for the law firm of Wolfe & Wyman LLP. This was a software copyright infringement case. Case 1:14-cv-01278. The case was settled.
37. 2015 Attorney General of Florida v ASAP Tech Help LLC, Working for the firm of Lubell & Rosen for the defendant. This case was settled before trial. Case 2015 CA002751XXXXMB. Case concluded.
38. 2015 SNA1 S.p.A. v Barcrest Group Ltd. For the firm of Winget, Spadafora, & Schwartzberg on behalf of Illinois Insurance Company. I was a consulting expert. The case was settled.
39. 2015 Suncoast Post-Tension LTD vs Peter Scoppa, et al. US District Court Houston. For the firm of Macdonald Devin P.C., on behalf of the defendant. Case No. 4:13-cv-03125. This case involved trade secrets and computer forensics. Case concluded.
40. 2015-2017 Walmart Stores Inc. v. Cuker Interactive LLC. for the Henry Law

- Firm on behalf of Cuker Interactive LLC. Software trade secrets are the underlying matter in the case. Case has concluded.
41. 2015 United States of America vs. Anastasio N. Laoutaris. District Court for the Northern District of Texas, Dallas Division case no 3:13-CR-00386-B. Working for the firm of Law Office of John R. Teakell on behalf of the defendant. This was a criminal case involving alleged violation of 18 U.S.C. 1030 (a)(5)(A) and (c)(4)(B)(i). Case concluded at trial.
 42. 2016 VPN Multicast Technologies LLC vs AT&T Corp., Civil Action No.: 3:15-cv-02943-M. Patent infringement case. For the firm of The Simon Law Firm on behalf of the plaintiff. This case was settled.
 43. 2015-2016 Bradium Technologies vs Microsoft Cause 35:27 Patent infringement case. For the firm of Kenyon & Kenyon LLP on behalf of the plaintiff. This case was settled.
 44. 2016 United States v Michael Thomas. Eastern District of Texas Sherman Division Case No 4:13CR227. For the firm of Tor Ekeland, P.C. on behalf of the defense. This was a cybercrime case. Case concluded at trial.
 45. 2016 Motio Inc. v. BSP Software LLC, Brightstar. United States District Court for the Northern District of Texas Dallas Division Civil Action No. 3:16-cv-00331-O. For the firm of Walsh Law on behalf of the plaintiff. The case was settled.
 46. 2016-2017 Sanders et al. v. Knight et al. For the firm of Bradley, Murchison, Kelley, and Shea. This case has settled.
 47. 2016-2017. Suzanne Zacharius vs Kensington Publishing. Supreme Court of the state of New York. Index No. 652460/2012. Hired by the firm of Fox Rothschild LLP, for the defendant. This was a document forensics case. This case has settled.
 48. 2016 – 2017 Thomas Sisoian v. IBM. United States District Court for the Western District of Texas Austin Division Case No. 1-14-CV-565-SS. For the firm of DiNovo Price Ellwanger & Hardy LLP on behalf of the plaintiff. This was a software copyright case. This case was settled.
 49. 2016 – 2017 Evicam International, Inc. v. Enforcement Video, LLC, d/b/a WatchGuard Video. US District Court for the Eastern District of Texas, Sherman Division Case No. 4:15-cv-00105-ALM. For the firm of Reese, Gorden, and Marketos on behalf of the defendant WatchGuard Video on the topic of patent invalidity. The case has concluded at trial.
 50. 2016 – 2018 Various patent cases on behalf of Uniloc USA with the law firms of Prince Lobel and Tyre as well as the Ethridge Law Group. The cases have included Uniloc USA v Cisco Systems Inc. Civil Action No. 6:15-cv-1175; Uniloc USA v Facebook Inc. Civil Action No. 6:15-cv-223; Uniloc USA Inc. v Apple Inc. Case No.: 4:18-cv-00362-PJH; Huawei, Facebook, and others. The cases I worked on have settled or are suspended.
 51. 2017-2018. Bascom Global Internet Service Inc., v AT&T Corp. Case No. 3:14-CV-3942-M. I was hired by the firm of Susman Godfrey LLP on behalf of the plaintiff. This case has settled.
 52. 2017-2018. Dale Oliver v Bruce Johanson, Blair Johanson, and DB Squared LLC. United States District Court for the Western District of Arkansas,

- Fayetteville Division. Case No. 5:17-cv-05129-TLB. Hired by the Mark Henry Law firm for the defendant/counter claimant. The case included software copyright matters. This case has been tried.
53. Uniloc vs Samsung Case No. 2:17-cv-00651-JRG in the Eastern District of Texas, Marshall Division. This was a patent case. This case has settled.
 54. 2017-2018. Kathy Whiting v Gurjit Singh Dhillon, C.H. Robinson Worldwide, Inc. District Court of Lincoln County State of Oklahoma. Case No. CJ-2013-120. Hired by the firm of Kane, Russell, Colman, and Logan PC for the defendant. This case was settled.
 55. 2017-2018. John M. Money, LLC dba Auditors Recovery Service v. AmWins Specialty Auto, Inc. Cause No. DC-16-05483 101st Judicial District Court, Dallas County Texas. Hired by the firm of Kessler Collins for the defendant. This case was settled.
 56. Neutral forensic expert, working for the court (not for a particular party) in the matter of Mallory Pounds, et al. v. Joshua Freise, et al. This case has settled.
 57. Array Technologies Inc. vs. Mitchell, NextTracker, et al., United States District Court for the District of New Mexico. Case No. 1:17-cv-00087-JAP-LF. Retained on behalf of Array Technologies Inc. regarding security of trade secrets. This case has settled.
 58. Luminati Networks Ltd. vs. Biscience inc. In the United States district court for the eastern district of Texas Marshall Division civil action no. 2:18-cv-483- jrg. This was a patent case. The case was settled.
 59. Beaton v SpeedyPC Software. Case No. 1:13-cv-08389 United States District Court Northern District of Illinois, Eastern Division. Retained on behalf of Beaton. This case has settled.
 60. Randy L. Rasmussen, Andre Gerard, Thomas Collier, and Mark E. Millwee vs Texas Children's Hospital. Civil Action No. 4:19-cv-00268 Southern District of Texas Houston Division. I was hired by the defendant to opine on computer industry certifications. The case was settled before trial.
 61. Adams Wealth Advisors, LLC, et al., vs Tanner Dance et al. Case No. 20010002 First Judicial District Court Cache County, Utah. I was hired by the firm of Maschoff Brennan on behalf of the defendant to perform digital forensic analysis. The case was settled before trial.
 62. Madison Inc. vs. Lederer. I was hired by the plaintiffs to perform digital forensics investigations. This case has settled.
 63. Mid America Mortgage, Inc. Red Rock Mortgage, vs. Kelly Grigs, Greg Mahaney, and Interline Mortgage Services LLC. Hired by Kessler Collins P.C. on behalf of the plaintiff. This case involved digital forensics and theft of trade secrets. This case concluded.
 64. Uniloc 2017 LLC v. Samsung Electronics Civil Action No. 2:18-cv-508 (JRG- RSP) United States District Court for the Eastern District of Texas Marshall Division. Retained on behalf of Uniloc. This was a patent case. Case settled.
 65. Ida Marie Estrada vs. HEB LP 2018 Hidalgo County District Court Cause No. C-4093-18-J. Retained on behalf of Ida Marie Estrada by the Acevedo Law Firm, PLLC, to perform forensic analysis of security videos. This case has

- settled.
66. Gardiner v. Walmart Inc. et al Case 4:20-cv-04618. I was hired by the firm of Wilshire Law Firm, PLC to determine if Walmart customer data was for sale on the Dark Web, and if it appeared Walmart had been breached.
 67. Uniloc 2017 LLC v Motorola Mobility LLC United States District Court Delaware case 1:18-cv-01844-RGA-SRF. Retained on behalf of Uniloc. This case is stayed.
 68. Integrated Dentistry, P.A. v. Integrative Dental Specialists, Pllc, In the United States District Court for The Western District of Arkansas Fayetteville Division Case 5:19-CV-05090 Hired by Henry Law firm on behalf of the plaintiff. This matter has settled.
 69. Icon Health & Fitness, Inc. v. Peloton Interactive, Inc. In The United States District Court for The District of Delaware. Hired by the firm of Mashoff Brennan on behalf of the plaintiff. This was a patent case, case settled.
 70. WhereverTV, INC. v. Comcast LLC. United States District Court of Florida, Ft. Myers Division 2:18-cv-529-JLB-NPM. Hired by the firm of Reese, Marketos, LLP on behalf of the plaintiff. This was a patent case. Case concluded at trial.
 71. The Douglas Stewart Company v. HIQO Solutions. US District Court for the Southern District of Georgia Civil Action: 4:20-cv-00101-WTM_CLR. Hired by the firm of Lewis Brisbois for the defendant. This case has settled.
 72. Maritz Holdings Inc., V Certain Underwriters at Lloyd's London Subscribing to Policies Numbered B122f0115115 and Fi0115116, Et Al., United States District Court for The Eastern District of Missouri Eastern Division Case No. 4:18-cv-00825-RWS. Hired by the firm of Lewis Rice on behalf of the defendant. This case has settled.
 73. Huawei Technologies Co., LTD vs Verizon Communications. In the United States District Court Western District of Texas Waco Division. Civil Action No. 6:20-cv-00090. Hired by the firm of Fish & Richardson P.C. on behalf of Huawei. This is a patent infringement case. This case has settled.
 74. Callrail, Inc. v. Phonewagon, Inc., et al. Litigation. US District Court for the Northern District of Georgia No. 1:18-cv-02207-AT. Hired by the firm of Lewis Brisbois for the defendant. This case involves code analysis. This case has settled.
 75. Vault Data, LLC Vs Karl J. Cama Cause No. 153-307467-19. Hired by the firm of Friedman, Suder & Cooke for the defense. This case has settled.
 76. CyberX Group, LLC, And David E. Lindsey Vs. Christopher Pearson, CyberX, LLC, Troy Van Zile, Pearson Holdings, Inc., Operation 29, LLC, Landon Jordan, Graford Business Management, LLC, And Vzlivin LLC. Northern District of Texas Dallas Division Case No. 3:20-cv-2501-B. Hired by the firm of Platt Cheema Richmond PLLC, for the plaintiff. This case involved code analysis. This case has settled.
 77. Louisiana Workers' Compensation Corporation vs Insurity Inc. Case No: 1-19-0004-2033. Hired by the firm of Nixon Peabody LLP, for the defendant. This case involved code analysis. This case was concluded at arbitration.
 78. Hunter Aldridge v. Kenny Nation, et al. Hired by the Simon Law firm for the

- Defendant. This case involves phone forensics. This case has settled.
79. Sopris Systems, LLC V South Texas Electric Cooperative, Inc Cause No. 19-05-84418-B Hired by the firm of Carter Arnett for the Plaintiff. This case is a software dispute.
 80. Pro Marketing Sales, Inc. Vs. Secturion Systems, Inc.; And Richard J. Takahashi, United States District Court for The District of Utah Case No. 1:19-cv-00113. Hired by the firm of Ray Quinney & Nebeker on behalf of the defense. This case involves ownership of patents including both source code analysis and computer chip analysis.
 81. Cisco Systems, Inc. and Cisco Technology, Inc., V Jedd Williams. Hired by McDermott, Will, and Emory for the defense. This case was settled.
 82. Hasko Trading Inc V Agro LLC. Cause No. 20-09227 In the District Court 68th Judicial District Dallas County Texas. Hired by the Law Office of Paul Clevenger for the Plaintiff. This case was settled.
 83. Appian Corporation v Pegasystems Inc. and Mr. Youyong Zou. This case is in the Circuit Court of Fairfax County Virginia, Civil Action No. 2020 07216. Was retained by the firm of Choate, Hall & Stewart LLP on behalf of the defendant. This case involved alleged theft of trade secrets. This case concluded at trial.
 84. CPC Patent Technologies PTY LTD, v. Apple Inc. This case is in the Western District of Texas Waco Division Case No. 6:21-cv-00165-ADA. I was retained by the firm of K&L Gates LLP on behalf of the plaintiff. This is a patent case. This case involves both source code analysis and computer chip/CPU analysis. The case concluded.
 85. CPC Patent Technologies PTY LTD, v. HMD Inc. This case is in the Western District of Texas Waco Division Case No.6:21-cv-00166-ADA. I was retained by the firm of K&L Gates LLP on behalf of the plaintiff. This is a patent case. This case involves both source code analysis and computer chip/CPU analysis. The case concluded.
 86. Peloton Interactive, Inc. vs. iFIT INC. In The United States District Court for the District of Delaware C.A. No. 1:20-cv-1535. I was hired by the firm of Foley & Lardner LLP on behalf of the defendant. This was a trade secrets case. The defendant won summary judgement in this case.
 87. Allscripts Healthcare, LLC. v Andor Health LLC US District Court of Delaware C.A. No. 1:21-cv-00704-MAK. This case involves cloud computing (Azure) and computer security/forensics issues. This case was settled.
 88. Todd Rands vs Jason T. Saur Circuit Court of St. Louis County, State of Missouri Cause No. 20SL-CC00536. Hired by the firm of Simon Law on behalf of the plaintiff. This case involved phone forensics. The case concluded.
 89. Soter Technologies, LLC v. IP Video Corporation, et al. This case was in the United States District Court Eastern District of New York. Civ. No. 2:20- cv-02989(GRB)(AKT). I was hired by the firm of Chiesa Shahinian & Giantomasi PC on behalf of the plaintiff. This case concluded.
 90. Boxcast Inc. v Resi Media LLC. This case is in the United States District

Court Eastern District of Texas Marshall Division Civil Action No. 2:21-cv-00217. I was hired by the firm of Munck, Wilson, Mandala on behalf of the defendant. This is a patent case. The two patents in the suit were rendered invalid by the PTAB.

91. Walter Peters v Apple Inc. Case No. 19STCV21787. This case involves cybersecurity and open-source intelligence. The case concluded.
92. Arkeyo, LLC vs Saggezza INC Northern District of Illinois Case No. 19-cv-08112. I was hired by the firm of Jayaram on behalf of the defendant. The case involves allegations of software copyright infringement and trade secrets misappropriation. The defendant won summary judgment.
93. F45 TRAINING PTY LTD vs BODY FIT TRAINING USA INC., Hired by the firm of Willkie Farr & Gallagher LLP for the defendant. This is a patent infringement case. US District Court of Delaware C.A. No. 20-1194-WCB. Defendant won summary judgement.
94. Cisco v Wilson Chung, Poly, Case No. 4:19-cv-07562-PJH Northing District of California-Oakland. Hired by the firm of McDermott, Will, and Emery on behalf of the defendant. The case involves digital forensics and trade secrets. The defendant won summary judgement.
95. James Feliciano Vs BLC Abstract & Title, LLC A/K/A Ellyson Abstract Ellyson Abstract & Title Co. LLC District Court of Brewster County, Texas. Hired by the plaintiff. The case involved cybersecurity and digital forensics. The case concluded.
96. Brian M. Douglas & Associates, LLC V Conquest Solutions, LLC, In the State Court of Cobb County State of Georgia Civil Action File No 21-A-2215. This was a Cybersecurity Case. Hired By the Firm of Hill Kertscher & Wharton LLP. The case concluded.
97. Healthcare Advanced Risk Technologies, Inc., And Inspirien Holding Corp., V Terence Mills, Ai.Io Corp., Jane Nemcova, And Veuu, Inc., United States District Court Eastern District Of New York Case No.: 2:22-cv-04192-JS-AYS. This is a software copyright and trade secrets case. I was hired by the firm of Fox Rothschild on behalf of the plaintiff. The case was settled before trial.
98. James Feliciano V BLC Abstract & Title, LLC hired by the Johnson Law Firm on behalf of the plaintiff. The case concluded.
99. Anyplace Management and Diagnostics, Inc. D/B/A Anyplace Md, Healthcare Billing Solutions, Inc., In the United States District Court for The Western District of Texas Austin Division Vs Anyplace Management and Diagnostics, Inc. D/B/A Anyplace Md, Healthcare Billing Solutions, Inc., Civil Action No. 1:22-Cv-353-Ly Hired by the Farrell Law Group. This is a cybersecurity case. Case settled.
100. Jacqueline Delling vs R & C Transportation, LLC and Michael Wilkinson State of Missouri Cause No. vs. 21SL-CC03800. Hired by the firm of Simon Law Firm on behalf of the plaintiff. The case involved forensics examination of cell phone records. The case concluded.
101. Cardware Inc. vs. Samsung Electronics Co., Ltd. And Samsung Electronics America, Inc., In the United States District Court for The

- Eastern District of Texas Marshall Division Case No. 2:22-Cv-00141-Jrg-Rsp hired by the firm of Reichman Jorgensen Lehman & Feldberg LLP on behalf of the plaintiff. The case involved patent infringement and validity. Case settled.
102. Juan Alcazar vs. Fashion Nova Inc. CASE NO.: 3:20-cv-01434-TSH. Hired by the firm of Wilshire Law. The case involves ADA compliance for the website. The case has settled.
 103. BaseCap Analytics Inc., vs Robert Amenn, United States District Court Southern District Of New York, case 1:23-cv-09370-MKV. Hired by the firm of Ballard Spahr for the plaintiff. The case involves theft of trade secrets and digital forensics. Case settled.
 104. Juul Labs, Inc. Antitrust Litigation United States District Court Northern District of California Case No. 3:20-Cv-02345-Who Hired by The Firm of Joseph Saveri Law Firm, LLP on behalf of the plaintiff. The case concluded.
 105. Blue Bear Waste Services, LLC, Vs Bond Enterprises, INC., Hired by the firm of Campbell, Killin, Brittan, & Ray for the plaintiff. The case involves software quality issues. Case concluded at arbitration.
 106. Convexity Limited, vs Ivan Novikov, Wallarm, INC., and Does 1-100. Superior Court of The State of California County of San Francisco. Case No. CGC-20-584174. This case involved cybersecurity including security audits and penetration tests. Case settled.
 107. Ceiva Opc, LLC V Amazon.Com Inc in The United States District Court Central District of California Case No.: 2:22-CV-02709-AB (MAA). Hired by the firm of Munk Wilson to work on patent validity issues. Case settled.
 108. Taasera Licensing LLC, V Musarubra Us LLC, D/B/A Trellix, In the United States District Court for The Eastern District of Texas Marshall Division Civil Action No. 2:22-Md-03042-Jrg. Hired by the firm of Jackson Walker LLP for the defense to work on infringement and validity issues. Case settled.
 109. Dickson Furniture Manufacturers LLC, v Specialty Bedding LLC In the District of Harris County Texas 11th Judicial District. Cause No. 2021-78803. Cybersecurity case. Case settled.
 110. Villasport LLC, a Colorado limited liability company, and SYUFY Enterprises LP, A California Limited Partnership V MOBOMO LLC, A Maryland Limited Liability Company. Superior Court of California County of Marin. Hired by Gordon, Rees, Scully, & Mansuchani for the defendant. This was a software case. Case has settled.
 111. Digital Doors, INC v IBM. Retained by the firm of Global IP Law Group, LLC on behalf of Digital Doors. I worked on multiple IPRs. The case has settled.
 112. Commondoay Futures Trading Commission Vs Sam Ikkurty A/K/A Sreeniv as I Rao, Ravishankar Avadhanam, And Jafia LLC. United States District Court Northern District of Illinois Case: 1:22-cv-02465. I was asked to opine on cryptocurrency. Case settled.
 113. Malloreay Tomczak, Luis Rivera-Solis, Kalitha Head, Josephine Walker,

And Leslie Wyatt, on behalf of themselves and all others similarly situated vs United Services Automobile Association, USAA Casualty Insurance Company, USAA General Indemnity Company, And Garrison Property and Casualty Insurance Company United States District Court District Of South Carolina Case No. 5:21-cv-01564-MGL My role was consulting on big data analysis.

114. Dynapass IP Holdings v Wells Fargo Eastern District of Texas Marshall C.A. NO. 2:22-cv-00217-JRG-RSP. Hired by the firm of McGuire Woods on behalf of the defense. This was a patent infringement case. Case settled.
115. In Re Edward D. Jones & Co., L.P. Securities Litigation, United States District Court Eastern District of California CASE NO. 2:18-cv-00714-DJC-AC. Hired by the firm on behalf of the plaintiff. My role in this case involved databases, data stores, and extracting data.
116. Transcend Company, Inc., a Michigan Corporation vs Jesse Kessler. Hired by the firm of Honigman LLP on behalf of the plaintiff. This case involved a cyberbreach and digital forensics. Case settled.
117. Western Digital Technologies, Inc. vs. Viasat, Inc., United States District Court Northern District of California Oakland Division Case No.: 4:22-Cv-4376-Hsg. This is a patent infringement case; I am working on both infringement and validity issues.
118. Gabriela Miguel, Emilio Pensado, Jr., And Robert Herrera, Individually, And on Behalf of All Others Similarly Situated, V. Apple Inc. Superior Court for The State of California County of Los Angeles Case No. 21STCV08348. Hired by Wilshire Law Firm for the Plaintiff
119. Considerate Commerce, INC. v. ISP Electronics, LLC. Rockwall County - 439th District Court case no 1-23-1236. My work involves digital forensics and trade secrets evaluation.
120. William Morgan, Kathleen Dorety, Michael Viscardi in the matter of William Morgan, Kathleen Dorety, Michael Viscardi v. Government Employees Insurance Company d/b/a GEICO, GEICO Casualty Company, GEICO Indemnity Company, and GEICO General Insurance. Hired by the firm of Berger Montague for the plaintiffs. This is a cybersecurity case.
121. Mastercard Incorporated and Mastercard International Incorporated Petitioner V Ov Loop, INC. Patent Owner IPR2023-01289. Hired by the firm of B.C. Law Group for the patent owner.
122. Arcadia Anesthesia, P.A. And Suresh Valloppillil, M.D., Plaintiffs, vs Tu Xuan Dao, M.D., And Orthomed Staffing, LLC Defendants Cause No. 296-06050-2022 In the District Court 296th Judicial District Collin County Texas. Hired by The Law Offices of Welsh and Kampas, PLLC on behalf of the plaintiff. This is a cybersecurity case. Case Settled.
123. LM Healthcare v. Natalie Pantano, et al, In the United States District Court for The District Of New Jersey. Civ. No.: 2:22-CV-0048-JKS-AME. Hired by the firm for the petitioner. Hired by the firm of Ballard Spahr. My role was digital forensics. Case settled.
124. William Childers v. Cox Communications. National Arbitration and Mediation Case No. 1000266371. Hired by the firm of Taylor-Copeland Law

- for the plaintiff. This is a cybersecurity case. Case settled.
125. Technology Ventures, LLC v Vyla, INC., a Colorado Corporation. Hired on behalf of the plaintiffs. JAG Case No.: 2024-0438A. The case went to arbitration.
 126. IonQ vs. Patrick Yang. Hired by the firm of Quinn Emanuel. This is a trade secrets case.
 127. Adeia Guides INC. v Videotron (Canadian Court). Hired by the plaintiffs' attorney Goodmans LLP. This is a patent infringement case.
 128. Mary Heather McAfee, Zaher Murray and George Wright, On Behalf of Themselves and All Similarly Situated Individuals, Plaintiffs in The United States District Court for The Eastern District of Virginia Richmond Division Civil Action No. 3:23-Cv-439 V. Meridianlink, Inc., Defendant. Hired by the firm of Berger Montague on behalf of the plaintiff. This case relates to cybersecurity issues.
 129. Edge Networking Systems LLC v. Amazon.Com, Inc., et al. in support of IPR OF U.S. Patent No. 11,695,823. Hired by the firm of Latham & Watkins LLP.
 130. Intellectual Ventures v American Airlines and Southwest Airlines in support of the IPR of U.S. Patent No.7,324,469. Hired by the firm of McKool Smith.
 131. Intellectual Ventures v American Airlines and Southwest Airlines in support of the IPR IPR2025-00987 of U.S. Patent No. 8,407,722. Hired by the firm of Munck Wilson Mandala LLP
 132. Intellectual Ventures v American Airlines and Southwest Airlines in support of the IPR2025-00987 of U.S. Patent No. 8,027,326. Hired by the firm of Munck Wilson Mandala LLP.
 133. XMISSION, L.C., A Utah Company Vs PRIMAL HEALTH, LP, UNITED STATES DISTRICT COURT DISTRICT OF UTAH, CENTRAL DIVISION Case No.: 2:21cv539-HCN-JCB. The case involves the CAN-SPAM act. Hired by the firm of Cameron Ringwood for the plaintiff.
 134. April Kay Moore, Yvette Mckinley, Kimberly Joy, individually and on behalf of all others similarly situated v Centrelake Medical Group, Inc Superior Court for the State of California County Of Los Angeles. This was a cybersecurity breach case. I was hired by the firm of Wilshire Law Firm, PLC on behalf of the plaintiff. Case has settled.
 135. Cognipower LLC vs Fantasia Trading, LLC D/B/A ANKERDIRECT and Anker Innovations Limited in The United States District Court for The District of Delaware. C.A. No. 19-cv-2293-JLH-SRF. Hired by the firm of Nixon Peabody LLP for the defendant. My role was a digital forensics examination. My role in the case has concluded.

Testifying Experience

I have testified at 72 depositions, 12 trials, 4 arbitrations, and 9 hearings. Specifics are listed below.

1. May 2, 2025. My deposition was taken in the matter of Western Digital Technologies, Inc. v Viasat, Inc., United States District Court Northern District of California Oakland Division Case No.: 4:22-Cv-4376-Hsg
2. February 5-6, 2025, I testified at the trial of Adeia Guides INC. v Videotron (Canadian Court).
3. October 14, 2024, I testified at the arbitration of Technology Ventures, LLC v Vyla, INC.
4. August 13, 2024, my deposition was taken in the matter of Mastercard Incorporated and Mastercard International Incorporated Petitioner v Ov Loop, INC. IPR2023-01289.
5. June 28, 2024, my deposition was taken in the matter of Childers v Cox Communications.
6. May 5, 2024, my deposition was taken in the matter of Gabriela Miguel, Emilio Pensadof Jr., And Robert Herrera, Individually, and on Behalf of All Others Similarly Situated, v Apple Inc. Superior Court for The State of California County of Los Angeles Case No. 21STCV08348.
7. January 10, 2024, testified in the arbitration hearing regarding Blue Bear Waste Services, LLC, v Bond Enterprises, INC.
8. December 20, 2023, my deposition was taken in the matter of Convexity Limited, v Ivan Novikov, Wallarm, INC.
9. November 28, 2023. My deposition was taken in the matter of Blue Bear Waste Services, LLC, v Bond Enterprises, INC.
10. November 21, 2023. I testified in a hearing in the matter of BaseCap Analytics Inc., v Robert Amenn, United States District Court Southern District Of New York, case 1:23-cv-09370-MKV.
11. November 14, 2023. My deposition was taken in the matter of Ceiva Opco, LLC v Amazon.Com Inc in The United States District Court Central District of California
12. November 7, 2023. My deposition was taken in the matter of Juan Alcazar v Fashion Nova Inc.
13. October 25th, 2023. My deposition was taken in the matter of Sopris Systems, LLC v South Texas Electric Cooperative.
14. September 7, 2023. My deposition was taken in the matter of In Re Edward D. Jones & Co., L.P. Securities Litigation,
15. May 11, 2023, my deposition was taken in the matter of Brian M. Douglas & Associates, LLC v Conquest Solutions, LLC.
16. April 18 through April 25th, 2023, I testified in the trial of WhereverTV v Comcast on both patent infringement and invalidity. United States District Court of Florida, Ft. Myers Division.
17. April 13, 2023, my deposition was taken in the matter of Jacqueline

Delling vs R & C Transportation, LLC, and Michael Wilkinson State of Missouri Cause No. v 21SL-CC03800.

18. April 4, 2023, my deposition was taken in the matter of IPR2022-00600 Apple Inc. v CPC Patent Technologies PTY LTD. I was retained by CPC Patent Technologies.
19. February 2023, my deposition was taken in the matter of IPR2022-00601 and IPR2022-00602 Apple Inc. v CPC Patent Technologies PTY LTD. I was retained by CPC Patent Technologies.
20. January 30, 2023, my deposition was taken in the matter of CPC Patent Technologies PTY LTD, v HMD Inc. regarding validity issues.
21. January 12, 2023, my deposition was taken in the matter of CPC Patent Technologies PTY LTD, v HMD Inc. regarding infringement issues.
22. November 14, 2022, my deposition was taken in an IPR related to Boxcast INC. v Resi Media LLC.
23. October 19, 2022, my deposition was taken in the matter of Cisco v Wilson Chung/Poly.
24. September 8, 2022, my deposition was taken in the matter of Arkeyo, LLC v Saggezza.
25. August 31, 2022, my deposition was taken in the matter of F45 TRAINING PTY LTD v BODY FIT TRAINING USA INC.,
26. July 14, 2022, my deposition was taken in an IPR related to Boxcast INC. v Resi Media LLC.
27. June 21 and June 22, 2022, I testified at a Markman hearing in the matter of WHEREVERTV, INC. v Comcast LLC.
28. June 13, 2022, my deposition was taken in the matter of Walter Peters v Apple Inc. Case No. 19STCV21787.
29. May 2, 2022, I testified in the trial of Appian Corporation v Pegasystems INC. and Mr. Youyong Zou
30. May 1, 2022, my deposition was taken in the matter of Allscripts Healthcare, LLC. v Andor Health
31. March 24, 2022, my deposition was taken in the matter of Hunter Aldridge v Kenny Nation. The case involves phone forensics.
32. March 11, 2022, my deposition was taken regarding pre-sale bar in the matter Boxcast Inc. v Resi Media LLC.
33. March 10, 2022, my deposition was taken in the case of Todd Rands v Jason T. Saur Circuit Court of St. Louis County, State of Missouri No. 20SL-CC00536. The case involves phone forensics.
34. February 18, 2022, my deposition was taken regarding claim construction in the matter Boxcast Inc. v Resi Media LLC.
35. January 17, 2022, I testified in the arbitration hearing in the matter of LWCC v Insurity.

36. January 15, 2022, my deposition was taken in the matter of Appian v Pegasystems.
37. January 5, 2021, my deposition was taken in the matter of Boxcast INC. v Resi Media LLC.
38. December 22, 2021, my deposition was taken in the matter of Peloton vs. iFit regarding trade secrets.
39. November 5, 2021. I testified in an arbitration hearing in the matter of Cuker v Pillsbury, Winthrop, Shaw, Pittman. AAA CASE NO. 01-18-0001-5005
40. November 1, 2021, my deposition was taken in the matter of IPR2021-00342 Petition
41. October 15, 2021, my deposition was taken in the matter of OnQuest Concierge LLC v App Quest Technologies LLC, et al., hired by the firm of Platt Cheema Richmond PLLC on behalf of the plaintiff.
42. September 17, 2021, my deposition was taken in the matter of Cisco v Williams.
43. July 27, 2021, my deposition was taken in the matter of WhereverTV v Comcast.
44. July 7, 2021, my deposition was taken in the matter of The Douglas Stewart Company v HIQO Solutions.
45. July 5, 2021, my deposition was taken in the matter of Huawei v Verizon.
46. December 21, 2020, I testified at a hearing in the matter of Icon Health & Fitness, Inc. v Peloton Interactive, Inc.
47. November 18, 2020, my deposition was taken in the matter of Icon Health & Fitness, Inc. v Peloton Interactive, Inc.
48. November 10, 2020, my deposition was taken in the matter of Mid America Mortgage, Inc. Red Rock Mortgage, v Kelly Griigs, Greg Mahaney, and Interline Mortgage Services LLC.
49. September 1, 2020, I testified in an evidentiary hearing in the case of Madison Inc. v Lederer.
50. July 14, 2020, my deposition was taken in the matter of Ida Marie Estrada v HEB LP Cause No. C-4093-18-J.
51. My deposition was taken on April 1 & 2, 2020. My deposition was taken in the matter of Uniloc 2017 LLC v Samsung Inc. Case No. 2:18-cv-00508-JRG.
52. February 25, 2019, my deposition was taken in the matter of Uniloc 2017 v Samsung Civil Action No. Case No. 18-cv-00506.
53. December 12, 2019, my deposition was taken in the matter of Uniloc 2017 LLC v Motorola Mobility LLC.
54. June 25, 2019, my deposition was taken in the matter of Array Technologies Inc. v Mitchell, NextTracker, et al.,
55. January 10, 2019, my deposition was taken on the matter of IPR2018-00361.
56. December 20 & 21, 2018 my deposition was taken in the matter of Uniloc v Samsung, Civil Action No. 2:17-cv-651-JRG on patent infringement and

- validity issues.
57. October 12, 2018. My deposition was taken in the matter of IPR2018-00294.
 58. September 21, 2018. My deposition was taken in the matter of IPR2017-02148.
 59. August 6, 2018. My deposition was taken in IPR2017-01799, IPR2017-01800, IPR2017-01801 and IPR2017-01802.
 60. August 3, 2018. My deposition was taken in IPR2017-01797 and IPR2017-01798.
 61. July 25, 26, and 27 2018 I testified at trial in the matter of Dale Oliver v Bruce Johanson Blair Johanson, and DB Squared LLC. Case No. 5:17-cv-05129-TLB.
 62. July 19, 2018. My deposition was taken in the matter of Uniloc USA, Inc. v Apple Inc., Case No.: 3:18-cv-00365-WHA.
 63. June 28, 2018. My deposition was taken in Google LLC v Uniloc regarding the following IPR2017-01683, IPR2017-01684, IPR2017-01685. Google LLC v Uniloc IPR 2017-02080, and IPR 2017-02081.
 64. March 02, 2018. My deposition was taken in the matter of Dale Oliver v Bruce Johanson, Blair Johanson, and DB Squared LLC.
 65. December 22, 2017, I testified at a hearing in the matter of John M. Money, LLC dba Auditors Recovery Service v AmWins Specialty Auto, Inc. Cause No. DC-16-05483 101st Judicial District Court.
 66. November 27, 2017. My deposition was taken in the case of: Case IPR2017-00221, U.S. Patent 7,535,890; Case IPR2017-00222, U.S. Patent 8,243,723; and Case IPR2017-00225, U.S. Patent 8,995,433.
 67. July 13 and 14, 2017. I testified at trial regarding patent invalidity in the case of Evicam International, Inc. v Enforcement Video, LLC, d/b/a WatchGuard Video.
 68. June 27, 2017. My deposition was taken in the case of Thomas Sisoian v IBM. United States District Court for the Western District of Texas Austin Division Case No. 1-14-CV-565-SS.
 69. June 17, 2017. My deposition was taken in the case of Evicam International, Inc. v Enforcement Video, LLC, d/b/a WatchGuard Video, on the issues of patent invalidity.
 70. April 17 and 18, 2017. I testified at trial in the case of Walmart Stores Inc. v Cuker Interactive LLC. July 12, 2016. Case No. 5:14-CV-5262.
 71. December 12, 2016. I testified at a hearing regarding multiple motions in the case of Walmart Stores Inc. v Cuker Interactive LLC. Case No. 5:14-CV-5262
 72. July 12, 2016. My deposition was taken in the case of Walmart Stores Inc. v Cuker Interactive LLC. Case No. 5:14-CV-5262
 73. June 7, 2016. I testified in the trial of United States v Michael Thomas.
 74. My deposition was taken in the case of Federal Trade Commission and State of Florida v Inbound Call Experts, LLC, et al. Case No. 14-81395-CIV-Marra/Matthewman US District Court Southern District of Florida.
 75. October 9, 2015. I testified in the trial of Suncoast Post-Tension LTD v

- Peter Scoppa, et al.
76. September 25, 2015, and September 28, 2015, I testified in the trial of United States of America v Anastasio N. Laoutaris.
 77. August 27, 2015, my deposition was taken in the Suncoast Post-Tension LTD v Peter Scoppa, et al. case.
 78. May 22, 2015, my deposition was taken in the Attorney General of Florida v ASAP Tech Help LLC case.
 79. December 17, 2014, I testified at a non-jury trial/hearing in the Federal Trade Commission v PC Cleaner Pro Inc. case.
 80. November 24, 2014, I testified at a non-jury trial/hearing in the Federal Trade Commission v Boost Software Inc. case.
 81. On November 13, 2014, my deposition was taken in the Neomedia Inc. v Dunkin Brands Inc. case relating to patent indefiniteness/invalidity issues.
 82. July 9, 2014, my deposition was taken in the Geotag v AT&T case relating to validity issues.
 83. June 11, 2014, my deposition was taken in the Geotag v AT&T case relating to infringement issues on.
 84. May 15, 2014, my deposition was taken in the Geotag v Starbucks et al. case relating to invalidity issues regarding the defendants Dominos and Darden.
 85. May 14, 2014, my deposition was taken in the Geotag v Starbucks et al. case relating to infringement issues regarding the defendant Darden.
 86. 24 January 2014, my deposition was taken in the Geotag v. Frontier Communications et al. case relating to infringement issues regarding the defendants Gander Mountain and Abercrombie and Fitch.
 87. 23 January 2014, my deposition was taken in the Geotag v Frontier Communications et al. case relating to infringement issues regarding the defendants Trane and Genesco.
 88. 22 January 2014, my deposition was taken in the Geotag v Frontier Communications et al. case relating to infringement issues regarding the defendants Cinemark, Spencer's Gifts, and Regis Corp.
 89. 21 January 2014, my deposition was taken in the Geotag v Frontier Communications et al. case relating to infringement issues regarding the defendants Walmart, Nike, and Advanced auto.
 90. January 2014, my deposition was taken in the PiNet v J.P. Morgan Chase case relating to invalidity.
 91. My deposition was taken in the Geotag v. Frontier Communications et al. case relating to infringement issues regarding the defendants in Judge Gilstrap's court in December 2013. This was multiple defendants.
 92. My deposition was taken in the Microsoft v Geotag case regarding Google in December 2013.
 93. I testified at an evidentiary hearing in the matter of Macroniche Software Inc. v 4 Imaging Solutions LLC, et al. Southern District of Texas Houston Division.
 94. I testified at the trial of Market One v Tekcenture case in the Dallas County Courts in February 2013.

95. My deposition was taken in the Geotag v Frontier Communications case regarding the defendant Yellow Pages in September 2013.
96. My deposition was taken in the Market One v Tekcenture case in December 2012.
97. My deposition was taken in 2011 in Eolas Tech. Inc. v Adobe Systems, Inc., et al., Civil Action No. 6:09-cv-446 (E.D. Tex.) (On behalf of defendant, Citibank).

Academic Experience

1. I am currently an adjunct professor for Vanderbilt University in their Master of Computer Science program. Specifically, I am teaching graduate courses in quantum computing; quantum algorithms and information theory; secure software engineering, and digital forensics.
2. I am currently an adjunct lecturer for Georgetown University. I teach graduate courses in cybersecurity, cryptography, and systems engineering courses.
3. I developed a graduate digital forensics course for the University of Dallas. I also taught this course for the University as an adjunct professor from 2019 to 2022.
4. I have taught classes at community colleges, technical colleges, universities, and corporate environments since 1998. These classes include programming courses (C, Java, C++, Objective C, C#/.Net, and others), software engineering, computer networking, system security, and digital forensics courses.
5. During 2019 I was a Professor of Practice with Capitol Technology University teaching graduate courses (master's and doctoral) in computer science, cybersecurity, electrical engineering, and research methods as well as chairing several doctoral dissertation committees. I was also the director for the Quantum Computing and Cryptography Research Laboratory at Capitol Technology University. I have chaired the following students to successful defense of their doctoral dissertations:
 - a. Dr. Kellep Charles, dissertation title "A quantitative approach using the experimental design to evaluate the effects automated vulnerability security scanners have on cent-os server system services."
 - b. Dr. Natalie Marini-Wear, dissertation title "A qualitative case study: software security in devops"
 - c. Dr. Tomas Pena, dissertation title "A deep learning approach to detecting covert channels in the domain name system."
6. I have worked on numerous scientific conference committees. The following is a sample:
 - a. At the 2018 Annual IEEE 8th Annual Computing and Communication Conference at the University of Nevada in Las Vegas, I chaired a session on Artificial Intelligence, and another session on Computer Architecture and VLSI.

- b. At the 2019 Annual IEEE 9th Annual Computing and Communication Conference I was a keynote speaker presenting a talk on "The impact of complexity and emergent properties on engineering". I also chaired a session on "IOT, Robotics and Machine Vision" as well as a session on "Mobile and Wireless Communication, Network".
 - c. On the technical committee for "Wireless & Sensor Networks & Cybersecurity; Mobile Computing and Security" IEEE IEMCON 2019 Conference.
 - d. Technical Program Co-Chair for the 2019 International Symposium on Blockchain Computing and Applications
 - e. On the technical committee for "Wireless & Sensor Networks & Cybersecurity; Mobile Computing and Security" IEEE Ubiquitous Computing, Electronics & Mobile Communications Conference (UEMCON) 2019 Conference.
 - f. Technical program chair for International Conference on Cyber Security: Recent Threats and Trends (ICCSTT) 2019
 - g. Program committee member for 2020 The 1st Workshop on Verification & Validation of Quantum Applications.
 - h. General Chair for the 2020 Quantum Computing and Engineering Conference (CQEC).
 - i. Technical program committee member for the inaugural IEEE International Conference on Quantum Computing and Engineering (QCE) 2020.
7. I have presented research talks at University of Texas at Dallas, Texas A&M San Antonio, Seton Hall University, Southern Methodist University, Columbia ACM Chapter, Harvard Computer Society, and Princess Sumaya University in Amman Jordan.
8. I am currently or have been previously a reviewer for several scientific journals:
- a. Editor in Chief for the *American Journal of Science and Engineering* (2017 to 2020).
 - b. Editorial board for the Journal of Artificial Intelligence in Medical Imaging
 - c. Reviewer for the *International Journal of Cyber Warfare and Terrorism (IJCWT)* (2016 to 2020).
 - d. Reviewer for scientific papers submitted to *IEEE Security & Privacy* and the *IEEE Open Access Journal*.
 - e. Reviewer for the *International Journal of Network Security (IJNS)*
 - f. Reviewer for scientific papers submitted to the *Journal of Information Warfare*
 - g. Reviewer for scientific papers submitted to the *International Journal of Network Security*.

Professional Experience

From: 2005
To: Present
Organization: Chuck Easttom Consulting
Title: Computer Scientist/Consultant

As an independent consultant, I have developed 2 electronic medical records software solutions, several small financial and web-based applications, microcontroller programming, and consulted with various companies on networking and security issues. My consulting work has included security audits, penetration tests, and forensic analysis. I have also done corporate training and college teaching in a wide range of topics including network administration, network security, web development (HTML, JavaScript, CSS, ASP, ASP.Net etc.), programming (C, C++, C#, Rust, Python, Perl, Java, VB, etc.) and database operations (MS SQL Server, MySQL, PostGres, Microsoft Access, Oracle, etc.).

I have worked extensively on cybersecurity projects including authentication (with smart cards, multi factor, digital certificates, etc.), zero-trust, security audits, penetration tests, and related topics.

I also developed the advanced cryptography course for the EC- Council. I developed the EC Council Certified Application Security Engineer courses for .Net, Java, and C++. I developed training courses for various companies such as SkillSoft and SimpliLearn in topics such as NoSQL, MongoDB, VMWare cloud, Information Systems Auditing, CSSLP certification prep, Secure software engineering, CISA certification prep, and others.

I frequently consult with various companies on computer security, cryptography, forensics, machine learning/artificial intelligence, DevOps, blockchain, software engineering, and related issues.

I work extensively in software engineering. That includes teaching and consulting on DevOps, secure software engineering, software standards including, but not limited to: NIST SP 800-27 – Life Cycle; IEEE 830-1993; IEEE 29148:2011; IEEE 15288; IEEE 829-1998 IEEE Standard for Software Test Documentation; IEEE 1008-1987 (R1993) IEEE Standard for Software Unit Testing; IEEE 1012-1998 Standard for Software Verification and Validation; IEEE 1028-1997.

My consulting activities have included a variety of government agencies including U.S. and Foreign governments. Consulting topics have included software engineering, cybersecurity, digital forensics, AI/ML, and computer networking. My consulting clients have included:

- Visa: Working on cybersecurity onboarding for their acquired entities. Conducting training in zero trust security, cloud security, and related topics.
- EC Council - Creating and teaching cybersecurity courses. I have worked on the EC Council cryptography courses, secure software engineering courses, blockchain courses, and advanced forensics courses.
- Skillsoft - Creating a range of technology-related training videos. This includes software engineering, database, and cybersecurity related courses.
- Collin County College - Teaching a range of computer science and security courses.
- Saudi Aramco - Teaching and consulting on cybersecurity issues
- Consulting with DoD related groups on a variety of engineering and cybersecurity projects
- Brand Protect - training and consulting on Dark Web investigations.
- SimpliLearn - Creating cybersecurity courses.
- TSTC - Tshukudu Technology College (Netherlands) - Teaching a variety of cybersecurity and cryptography courses.
- Allegiant Investigations- performing digital forensics investigations. Including smart phone, macOS, Windows, video, and image forensics.
- College of the Ozarks - Threat Intelligence Consulting

From: 2003
 To: 2013
 Organization: Collin College (Professional Development Department)
 Title: Adjunct Instructor (Part Time)

I taught professional development courses to IT professionals in programming (C, Java, C++, and C#), web development (HTML, JavaScript, CSS, and .net), networking, and network security. I have also designed and taught computer security courses for the college. These courses include:

- CompTIA Security+ Certification Prep.
- CISSP Certification Prep
- Hacking & Penetration Testing
- Computer Forensics
- Network Administration

Note from 2013 to 2019 I was paid as an outside training provider

From: 2003
 To: 2005
 Organization: Great American Insurance Company- Professional Liability Division
 Title: Systems Director

Summary: In this position I oversaw all application development including complex insurance Windows applications, web development including extensive online systems, database administration with SQL Server, network administration on a Windows based network, and network security for a division of an insurance company. This role combined management with hands-on work in all of these areas. I was first hired as Systems Manager, then after 12 months promoted to Systems Director. While in this role I oversaw and participated in the development of a web portal to allow customers to apply for insurance, renew policies, and check status. This includes software processes, such as Agile, and other methods.

I personally developed an extensive reporting application. I also oversaw and participated in a complete re-writing of the underwriting application used by our underwriters. Development was primarily using .Net with Microsoft SQL Server as a backend.

I was responsible for all network administration and security. This included securing endpoints, security policies, security technology, authentication methodologies, etc.

From: 2000
To: 2003
Organization: Remington College
Title: Department Chair for Computer Information Systems department
Summary: I was initially hired as an instructor but was later promoted to department chair. I taught a variety of computer science courses and managed the Computer Information Systems department. I taught courses in programming (software design, Java, C++, etc.), systems analysis, web development (HTML, JavaScript, Java Applets, and .Net), e-commerce, and information security.

From: 1999
To: 2000
Organization: Digital Speech Systems Inc.
Title: Senior Software Engineer
Summary: I began at digital speech as a software engineer and was later promoted to senior software engineer. My duties included developing voicemail and related software as well as mentoring new programmers. The programming work included work on voicemail server software, unified messaging software, and related applications. I worked extensively with C, Visual C++, SQL Server, and Visual Basic.

From: 1998
To: 1999
Organization: Southeastern Oklahoma State University
Title: Director of Academic Computing
Summary: I began as the Director of Educational Technology for the School of Arts and Letters but then took over the management of the entire university's information systems when I was promoted to the Director of Academic Computing for Southeastern Oklahoma State University. In this position I managed all technical support for the campus as well as overseeing all network administration, network security, and web development.

From: 1996
To: 1998
Organization: Alegis Corporation Systems Group
Title: Software Engineer
Summary: I began as a programmer/analyst and was later promoted to Software Engineer. I worked developing Windows based financial and collections applications for companies such as Boatman's Bank of St. Louis, Chrysler Financial, and Western Union. I worked extensively with C, C++, and Visual Basic (Versions 4.0 and 5.0). I also developed and oversaw the website or the company using HTML, JavaScript, and Cascading Style Sheets

From: 1995
To: 1996
Organization: Boeing Aerospace Operations
Title: Contract Programmer/Analyst
Summary: I worked as part of a team developing a Windows application to manage the maintenance and engineering tasks for the NATO AWACS. I worked with C, C++ and Visual Basic (starting with version 3.0) as well as Microsoft SQL Server.

From: 1991
To: 1995
Organization: Worked various technical support and computer related jobs while attending college. From late 1993 to 1995 a great deal of time was spent developing websites with HTML (1.0), JavaScript (beginning with its release in late 1995). Among the websites I created were websites for: a computer store, two martial arts studios, a quarter horse ranch, and a university chess club. During that same time period I worked extensively with some of the early browsers such as Mosaic and Netscape (late 1994). Prior to 1992, in 1991 to 1993 I worked building and repairing PC's.

From: 1987
To: 1991
Organization: United States Army
HHC 5/21 Infantry Battalion
7th Light Infantry Division
Title: Highest rank E-4
Summary: Awards received – Army Service Ribbon, National defense medal, marksman badge with grenade component. Honorable discharge.

Continuing Professional Education

I am always interested in updating and expanding my education, and therefore participate in seminars, webinars, online courses, continuing education/professional development training, etc. In some cases, I retake introductory or intermediate courses as a refresher. Here is an exemplary list of such courses.

- Paul Deitel, Teaching Strategies for Visual C# 2008 from Pearson Publishing – 2010.
- Design and Analysis of Algorithms from Massachusetts Institute of Technology – 2012.
- Parallel Computing from Massachusetts Institute of Technology – 2013.
- Microsoft Technet - Windows 7 Feature Overview – 2011.
- Programming Methodology from Stanford University Center for Professional Development – 2012.
- Perl fundamentals from the Association of Computing Machinery 2012.
- Key Issues in Distributed Systems from Stanford University Center for Professional Development – 2013.
- Introduction to HTML5 and CSS3 from the Association of Computing Machinery – 2013.
- Software Program Control Flow Fundamentals from the Association of Computing Machinery – 2013.
- Harvard Extension School CS 50 Intensive Introduction to Computer Science. This was an intensive coverage of C, PHP, MySQL, Algorithms, and Data Structures. I took this course as a refresher – 2014.
- The Fundamentals of Conducting an Internal Investigation from Guidance Software (webinar) – 2015
- Carnegie Mellon University Software Engineering Institute - Trends and New Directions in Software Architecture (webinar)- 2015
- Analyzing Evidence from Mobile Devices, Including Hidden and Deleted Data. Oxygen Forensics (webinar) – 2015
- Technical Debt in Large Systems: Understanding the Cost of Software Complexity. Massachusetts Institute of Technology (webinar) – 2015
- Current Trends in Computer Security. Stanford University (webinar) – 2015

- Windows FE and Live Forensic Triage (webinar) Forensic Magazine. – 2015
- American College of Forensic Examiners course - Forensic Examination of CCTV Digital VTR Surveillance Recording Equipment. 2015
- American College of Forensic Examiners course - Developmental and Motivational Factors of Transnational Terrorists. 2015
- American College of Forensic Examiners course - Psychological Profiles of Terrorists. 2015
- Oxygen Forensics Trainer Certification Course – 2015
- Access Data FTK Online training course – 2015
- American College of Forensic Examiners course - Digital Forensics in the 21st Century – 2016
- Specialized Forensic Photography and Diagramming – June 2017
- IEEE Course: Integrated Circuit Digital Design Methodology November 2017
- IEEE Course: Integrated Circuit Digital Design Methodology: Advanced Analysis and Simulation November 2017
- IEEE Course: 4G Broadband LTE December 2017
- IEEE Course Analyzing the Security of Bluetooth Low Energy. 2021
- IEEE Course BlueScan: Boosting Wi-Fi Scanning Efficiency Using Bluetooth Radio. 2021
- IEEE Continuing education course "Thermo-Mechanical and Mechanical Reliability of Electronics" 2021
- IEEE Course Bottleneck Analysis of Traffic Monitoring using Wireshark. 2021
- IEEE Continuing education course “Making and Qualifying Reliable Extreme Environment Electronics” 2022
- 2023 Private Investigator Continuing Education Course on DNA Evidence
- 2023 Private Investigator Continuing Education Course on Ethics
- 2023 Private Investigator Continuing Education Course on Suspicious Death and Bodily Injury Investigations.
- 2023 Private Investigator Continuing Education Course on Motor Vehicle and Bodily Injury Investigations.
- 2024 IEEE Continuing Education Course “5G System Principles 1.1 What Makes a 5G System.”
- 2025 Private Investigator Continuing Education on DNA and Fingerprint Identification.
- 2025 Private Investigator Continuing Education on Motor Vehicle Death & Serious Bodily Injury Investigations
- 2025 Private Investigator Continuing Education on Scene Investigations in Death & Serious Bodily Injury
- 2025 Private Investigator Continuing Education on Identity Theft: Detection, Prevention and Protection
- 2025 Private Investigator Continuing Education on DNA and Fingerprints: Evidence and Identification
- 2025 Microsoft’s Accessibility fundamentals course¹
- 2025 Dequeue University -Fast Tack to Accessibility for Web Developers Part I: Core Concepts.

¹ <https://learn.microsoft.com/en-us/training/paths/accessibility-fundamental/>

- 2025 Dequeue University -Fast Track to Accessibility for Web Developers, Part 2: Advanced Concepts
- 2025 Dequeue University - Accessibility Fundamentals - Disabilities, Guidelines, and Laws
- 2025 Dequeue University - WCAG 2.2: Semantic Structure and Navigation

References to my work

The following sections are provided as examples of the impact my work in computer science has had in the field.

Media References

My computer science expertise has been sought out by reporters including:

- CNN Money interviewed me regarding alleged unbreakable cryptography http://money.cnn.com/2011/09/02/technology/unhackable_code/
- CBS SmartPlanet interviewed me regarding NSA and cryptography <http://www.smartplanet.com/blog/bulletin/nsa-proof-products-protective-or-a-profit-motive/>
- "NSA proof products: protective or a profit motive?" also appeared on ZDNet.
- E-book's directory lists my "Moving from Windows to Linux" book as one of the top 10 Linux books <http://www.e-booksdirectory.com/linux/top10.html>.
- Lawrence Journal World interviewed me for a hacking story that was published August 6, 2006. The article was entitled "Hacker's infiltrate Web site".
- GoCertify.com Author Interview "Author Interview: CCFP Certified Cyber Forensics Professional All-in-One Exam Guide" January 2015
- ISMG interviewed me regarding the JP Morgan Chase Breach of 2015 <http://www.bankinfosecurity.com/interviews/what-jpmorgan-chase-breach-teaches-us-i-2982>
- CIO Magazine (Nov 14, 2016) in the article "12 steps to lower your espionage risk" references my book Computer Security Fundamentals 3rd Edition.
- Forensic Focus Magazine (June 2017) interviewed me regarding my work in applying graph theory to digital forensics.
- Sputnik Press Interviewed (June 2021) me regarding the Biden-Putin cybersecurity talks. <https://sputniknews.com/analysis/202106161083169993-putin-biden-cybersecurity-talk-may-mark-end-of-wild-west-era-in-cyberspace-expert-says/>
- Bank Info Security interviewed me (2015) regarding the JP Morgan Breach <https://www.bankinfosecurity.com/interviews/lessons-from-chase-breach-i-2982>.
- Lara Logan has no Agenda "Privacy in the Digital Age" July 2021.
- Vice The Motherboard Guide to Steganography interviewed me regarding steganography <https://www.vice.com/en/article/m7e9n3/the-motherboard-guide-to-steganography>

References to publications

My books and articles have been referenced by numerous computer scientists, including being referenced in several Ph.D. dissertations and master's Thesis'.

My books are used as textbooks at over 60 universities around the world.

Training

Since the late 1990's I have been teaching at least on a part-time basis. I have taught courses at colleges, technical schools, corporate training environments, and on site for companies and government agencies. Some of my training courses are through my own training company CEC-LLC, which is approved by the U.S. Department of Homeland Security National Initiative for Cyber Security Careers and Studies (NICCS)

<https://niccs.us-cert.gov/training/search/cec-security-llc>

I have taught courses in the following topics:

1. HTML (including HTML 5 and CSS3)
2. JavaScript (including advanced courses)
3. Java
4. C and C++
5. VB.Net, ASP.Net, and C#
6. Objective C/SWIFT iPhone programming
7. Microsoft SQL Server
8. Oracle
9. DevOps
10. Containers (Docker and Kubernetes)
11. Microsoft Access
12. NoSQL (including MongoDB and CouchDB)
13. Computer Networks (routers, switches, virtualization, SDN, NFV, etc.)
14. Computer Hardware (motherboards, chips, etc.)
15. JTAG techniques for phone forensics
16. Certification preparation courses for the following certifications: CompTIA A+, CompTIA Network+, CompTIA Security+, CISSP, ISSAP, CEH, CISA, CSSLP, ECES, CND, and CHFI.
17. Computer forensics (phone forensics, Windows forensics, general forensic science, etc.)
18. Computer security (principles, IDS/IPS, Honey Pots, policies, DRP/BCP, SIEM, cyber threat intelligence, etc.)
19. Cryptology (including advanced courses)
20. Math for cryptography including statistics, number theory, combinatorics, abstract algebra, graph theory, and related topics.
21. Windows Server (NT 4.0, Server 2003, Server 2008, Server 2012, Server 2019)
22. Secure programming (including web programming)
23. Linux
24. Hacking and penetration testing
25. Machine learning
26. Systems Engineering
27. Cloud Computing

- 28. Embedded systems
- 29. Systems Engineering

I have conducted computer security (computer forensics, network security, penetration testing cryptography, etc.) related courses for a variety of government and law enforcement agencies, various law enforcement officers, friendly foreign governments, and a variety of corporations. I volunteer my time teaching digital forensics and related materials to organizations that combat crimes against children such as the Internet Crimes Against Children Taskforce (ICAC) and have done so in Texas, North Dakota, Utah, and Illinois.

I have also created a number of video courses for companies such as Skillsoft and Pearson Press on topics such as Secure Programming, MongoDB, NoSQL, DevOps, Virtualization, Cloud computing, Digital Forensics, Quantum Computing, and other topics.

Technical Skills

The Following is an exemplary list of technologies. This is not meant to be an exhaustive list, but rather to provide a sample of areas within which I have expertise. I have experience and/or knowledge with:

Computer Hardware: CPU architecture, motherboard structure, chip programming/testing (using HDLs, System Verilog, etc.), battery power (Lithium-Ion, NiCad, Nickel-hydrogen, Nickel-Metal-Hydride, Lithium Polymer, etc.), and testing, etc.

Quantum Computing: Quantum concepts, quantum physics, quantum programming (QASM, Q#, Qiskit, Qiskit metal, etc.), quantum algorithms, quantum information theory, quantum hardware (ion trap, Bose Einstein condensate, nitrogen vacancy, superconducting, photon based, etc.).

Embedded Systems: Arduino, SystemC, SpecC, System Verilog, etc.

Electronic Cards: Smart cards, near field communications, ISO/IEC 7810 standard for identification cards, ISO/IEC 7816 standard for electronic cards for identification, ISO/IEC 14443 standard for contactless integrated circuit cards, etc. EMV, and related standards and technologies.

Alternate Computer Systems: Neuromorphic computing, molecular computing, etc.

Container Technology: Containers such as Docker, Kubernetes, gVisor, Singularity (for High Performance Computing), Podman (for Red Hat Linux originally but now also for MacOS and Windows), etc.

Programming Languages: C, C++, Assembly, .Net (C#, VB.Net, etc.), Go, Swift, Rust,

Pascal, Python, PHP, Ruby, Perl, Objective C, Java, Kotlin, and SmallTalk. This list is exemplary and not exhaustive.

Software Engineering: Design and testing methodologies. ISO 9000, ISO 15504, ISO 27001, Software Process Improvement Capability Determination (SPICE), UML, SWEBOK, software complexity measurements, etc.

Web development technologies: HTML, JavaScript, PHP, CSS, ColdFusion, Flash, and Dream Weaver. Web compliance with ADA, WCAG (2.0-2.2), Section 508, F18, and ISO/IEC 40500:2012 standards. Also experienced with web servers including Apache and IIS.

Engineering Methods: Systems architecture, systems modeling, engineering processes, requirements engineering, reliability engineering, circuit design, chip design, and related topics.

Artificial Intelligence: Expert systems, Fuzzy Logic, and AI Programming. Machine learning includes TensorFlow, Python, LLM, and similar tools. I also have experience in large language models (LLM), deep fake videos, and related AI topics.

Blockchain: Bitcoin, ethereum, decentralized apps (DApps), Decentralized Autonomous Organization (DAO), and related topics.

Internet of Things (IoT): IoT operating systems, protocols, and networking. I have experience with IoT protocols such as MQTT (Message Queuing Telemetry Transport); CoAP (Constrained Application Protocol); AMQP (Advanced Message Queuing Protocol); 6LoWPAN; NB-IoT (Narrowband IoT); NB-IoT (Narrowband IoT); etc. I have experience with IoT operating systems including: Contiki; RIOT OS; FreeRTOS; Apache Mynewt; LiteOS; Tizen; etc.

Software: Expertise with medical software including Electronic Medical Records, financial software, banking software, Business Process Management software (BPM), as well as other types of software.

Business Intelligence: Business intelligence methods, trade secret protection, and related topics.

Cryptography: I have extensive knowledge of cryptographic algorithms such as: DES, Blowfish, Twofish, AES, Serpent, RSA, Diffie-Hellman, ElGamal, MQV, ECC, GOST, KRYSTALS-KYBER, NTRU, Lattice Based Cryptography, and others. Also, Cryptographic hashes, message authentication codes, and cryptographic protocols.

Mathematics: Discrete math, number theory, graph theory, linear algebra, statistics, and algorithm analysis, etc.

Compression Algorithms: Lempel-Zev, Lempel-Ziv-Welch, Burrows Wheeler, Adaptive Transform Acoustic Coding (ATRAC), Huffman coding, Cartesian Perceptual

Compression, etc.

Mobile Devices: I am experienced with iOS and Android. I have worked with both operating systems extensively, including teaching programming for both operating systems and reviewing source code for both operating systems. I am also familiar with the hardware for both devices, including details regarding integrated circuits, batteries, display, etc, in both devices.

Networking: Network protocols, routers, switches, servers, IPv4, IPv6, Network models and concepts (TCP/IP, OSI, etc.), telecommunications, and network management. Networking protocols including ANT+, Bluetooth, Zigbee, 6LowPAN, etc. I am also familiar with video related networking protocols such as Quadrature Amplitude Modulation (QAM), Carrierless amplitude phase modulation (CAP), etc. Also, I am very familiar with cloud computing with both theoretical knowledge and hands-on experience with VMWare cloud, Azure, and AWS.

Satellite communications: L-Band (1-2 GHz): Used for GPS, maritime, and aviation communications; S-Band (2-4 GHz): Used for weather and some scientific satellites; C-Band (4-8 GHz): Used for satellite TV and VSAT systems; X-Band (8-12 GHz): Used primarily for military and deep-space communication; Ku-Band (12-18 GHz): Used for satellite broadcasting and internet services; Ka-Band (26.5-40 GHz): Used for high-speed satellite internet and advanced communication systems; Modulation: BPSK, QPSK, 8PSK, 16QAM, etc. Protocols such as LTP (Licklider Transmission Protocol);DVB-S/DVB-S2 (Digital Video Broadcasting-Satellite);CFDP (CCSDS File Delivery Protocol);Inter-Satellite Links (ISL), etc.

Video: Video transmission protocols and standards including DOCSIS (Data Over Cable Service Interface Specification), MoCA (Multimedia over Coax Alliance), NTSC (NTSC-M, N, J, etc.), Phase Alternating Line (PAL), SMPTE 2110, etc. Broadcast and streaming methodologies, set top boxes, OTT programming, interactive programming guides (IPGs), etc.

Databases: MySQL, SQL Server, DB2, PostGRES, Progress, Microsoft SQL Server, MS Access, Oracle, and SQL Anywhere. I have also worked with NoSQL databases including MongoDB, Hadoop, and CouchDB. This experience includes data mining and data analysis. I have worked with data stores that are used for medical data, financial data, banking data, educational data, and other data domains.

Computer/Network Security: PCI standards, Common Criteria, cybersecurity standards, penetration testing, computer viruses and other malware, disaster recovery planning, cryptology, firewalls, IDS, Honey Pots, chip security, cyber threat intelligence, competitive business intelligence, penetration testing, and security policies & procedures.

Biometrics: Fingerprint, facial recognition, voice recognition both algorithms and hardware.

Cyber Forensics: PC forensics, network forensics, cell phone forensics (including JTAG). I have experience with a wide range of tools, including but not limited to: Guidance Software Encase, Access Data FTK, Cellebrite, Paraben Sim Seizure, Oxygen Forensics, OSForensics, WindowsFE, and various open-source tools.

Domains: The domains within which I have practical IT experience include finance & banking, insurance, education, customer management, geographical mapping/tracking, defense department applications, and medical applications (including electronic medical records and medical billing).

Soft Skills: I have experience in valuing software and intellectual property as well as IT management related issues.