UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.
Patent Owner.

Cases IPR2022-00182
Patent No. 9,917,856

DECLARATION OF MICHAEL T. GOODRICH, PH.D.
IN SUPPORT OF PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I. QUALIFICATIONS 1

II. SCOPE OF ASSIGNMENT AND APPROACH 6

III. APPLICABLE STANDARDS AND CONTROLLING PRINCIPLES 8

A. Anticipation 8

B. Obviousness 9

C. Person of Ordinary Skill in the Art 11

IV. BACKGROUND 12

A. State of the Art 12

1. Secure Communications 13

2. Network Security 15

B. Overview of Petitioner's Relied Upon References 19

1. Buruganahalli 19

a. Buruganahalli's Figure 3A Whitelist Embodiment Allows an Encrypted Session Without Applying Packet-Filtering Rules to Encrypted Packets 19

b. Buruganahalli's Figure 3A Blacklist Embodiment Blocks a Requested Encrypted Session Before Any Encrypted Packets are Received 20

c. Buruganahalli's Figure 3B Blacklist Embodiment Requires that Encrypted Packets be Decrypted Before Applying any Packet-Filtering Rules 22

1. Baehr 27

C. The '856 Patent's contributions to the art 29

D. The Challenged Claims 38

V. CLAIM CONSTRUCTION 41

A. "Network-Threat Indicators" 42

B. "Proxy System" 43

VI. IN MY OPINION PETITIONER HAS FAILED TO SHOW THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE 43

A. In My Opinion, Buruganahalli Does Not Teach Rule-Based Filtering of Encrypted Packets 44

1. In My Opinion, Buruganahalli Only Applies its Firewall Rules/Policies to Unencrypted or Decrypted Data 44

2. In My Opinion, Figure 3A Embodiment Does Not Involve Applying Packet-Filtering Rules to Encrypted Packets 48

3. In My Opinion, Petitioner Has Not Identified a Single Instance Where Buruganahalli Teaches Filtering Encrypted Packets 51

4. In My Opinion, Petitioner Attempts to Rewrite Buruganahalli's Decrypt-First Approach with Conclusory Statements About a Skilled Artisan's Understanding and Obviousness 53

B. In My Opinion, Petitioner Has Not Shown that Buruganahalli Teaches the Claimed "Network-Threat Indicators" 55

C. In My Opinion, the Prior Art Does Not Teach the Claimed Routing Filtered Packets to a Proxy System 58

1. In My Opinion, Buruganahalli Does Not Disclose the Claimed Routing Filtered Packets to a Proxy System 58

2. In My Opinion, a Skilled Artisan Would Not Have Been Motivated to or Would Reasonably Expect Success Modifying Buruganahalli in View of Baehr 61

a. In My Opinion, the Proposed Combination Does Not Meet the Claim Elements 61

b. In My Opinion, Petitioner Does Not Provide Any Persuasive Reason for Why a Skilled Artisan Would Implement its Proposed Combination Using Baehr 63

VII. IN MY OPINION, THE OBJECTIVE EVIDENCE OF NONOBVIOUSNESS ALSO DEMONSTRATES THAT THE CLAIMS ARE VALID 68

A. The ’856 Patent Satisfied a Long-Felt Need in the Industry and Received Substantial Industry Praise 68

VIII. CONCLUSION 68

I, Michael T. Goodrich, Ph.D., declare and state as follows:

I. QUALIFICATIONS

1. I make this Declaration based upon my own personal knowledge, information, and belief, and I would and could competently testify to the matters set forth herein if called upon to do so.

2. Attached hereto as Appendix A is a true and correct copy of my Curriculum Vitae (CV). I summarize some of the relevant information regarding my CV as follows.

3. I received a Bachelor of Arts degree in Mathematics and Computer Science from Calvin University, in Grand Rapids, Michigan, in 1983, a Master of Science (M.S.) degree in Computer Science from Purdue University, in West Lafayette, Indiana, in 1985, and a Ph.D. in Computer Science from Purdue University in 1987.

4. I am a Distinguished Professor in the Department of Computer Science at the University of California, Irvine, where I have been a faculty member since 2001. The Distinguished Professor title is a campus-level distinction and is reserved for faculty who have achieved the highest levels of scholarship over the course of their careers. I was a professor in the Department of Computer Science at Johns Hopkins University from 1987-2001.

5. I have authored or coauthored over 350 publications, including several widely adopted books, such as Data Structures and Algorithms in Java, Data Structures and Algorithms in C++, Data Structures and Algorithms in Python, Introduction to Computer Security, and Algorithm Design and Applications. My publications include contributions to data structures and algorithms, information visualization, networking, graph algorithms, computational geometry, distributed and parallel algorithms, cloud security, information security and privacy, and algorithm engineering. For example, I have published peer-reviewed research articles, including publications[1] J-63, J-71, J-78, C-80, C-83, C-85, C-91, C-100, and C-108, on stopping viruses in email attachments and on authenticating data that is downloaded from untrusted repositories. I have also published peer-reviewed research articles on the use of parallelism in computer systems, including publications J-5, J-7, J-12, J-16, J-19, and J-24. Also, several of my textbooks include entire chapters on software engineering, and several of my publications, including Ch-8, Ch-12, J-36, J-45, C-53, C-62, C-63, C-64, C-208, are on algorithm engineering. Altogether, my publications have, according to Google Scholar, been cited over 16,500 times. My research has been supported by grants from the Defense Advanced Research Projects Agency ("DARPA"), the National

[1] I am using the indexing scheme from my CV.

Security Agency ("NSA"), the Office of Naval Research ("ONR"), the Army Research Office ("ARO"), and the National Science Foundation ("NSF").

6. In addition, I have consulting experience in matters involving algorithms, cryptography, machine learning, digital rights management, computer security, mobile devices (including power management), networking, software, video streaming, and storage technologies.

7. I am a Fellow of the American Association for the Advancement of Science ("AAAS"), a Fellow of the Institute of Electrical and Electronics Engineers ("IEEE"), and a Fellow of the Association for Computing Machinery ("ACM"), as well as being named as a Foreign Member of the Royal Danish Academy of Sciences and Letters. I am also a recipient of a Fulbright Scholarship (for senior specialist service to University of Aarhus, Denmark). In addition, I am a recipient of the IEEE Computer Society Technical Achievement Award ("for outstanding contributions to the design of parallel and distributed algorithms for fundamental combinatorial and geometric problems") and the Pond Award for Excellence in Undergraduate Teaching. Also, I am an ACM Distinguished Scientist.

8. My study of computer and network security topics began as an undergraduate student and continued in graduate school, where my Ph.D. research involved the study of computer system components operating in parallel. My

study and interest in computer security continued after my Ph.D., as detailed above and in my CV. In addition, I have reviewed and evaluated research papers on computer security, including cryptography, beginning with work as an associate editor for Journal of Computer & System Sciences, as well as my service on program committees of peer-reviewed Computer Science conferences, including the Conference on Electronic Publishing and the Information Superhighway and the ACM Symposium on Theory of Computing (STOC), the latter for which I chaired and edited the conference proceedings.

9. I am a co-inventor on several U.S. patents, including U.S. Patent No. 7,257,711, "Efficient Authenticated Dictionaries with Skip Lists and Commutative Hashing," which discloses secure distributed data authentication schemes. I am also co-inventor of U.S. Patent No. 7,299,219, "High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling," which discloses a technology for quickly retrieving website data that can change frequently, so as to be stored in a search engine. I am also co-inventor of U.S. No. Patent 8,681,145, "Attribute Transfer Between Computer Models Including Identifying Isomorphic Regions in Polygonal Meshes," which teaches how to map one mesh-based computer model to another. In addition, I am co-inventor of U.S. Patent No. 9,152,716, "Techniques for Verifying Search Results Over a Distributed

Collection," which discloses a system for searching the Internet so as to produce verifiable search results that can be produced by a search engine.

10. I have taught courses at Johns Hopkins University, Brown University, and University of California, Irvine, at both the undergraduate and graduate levels. Topics of my courses have included computer security, algorithms, data structures, information visualization, computer graphics, networking, algorithm engineering, computational geometry, and parallel processing. In addition, I have mentored twenty-four (24) PhD students over the years, who have written their PhD theses on topics in algorithms, data structures, information visualizations, networking, parallel processing, and computer security and privacy.

11. I have served as an editor on several technical journals, including Computational Geometry: Theory and Applications, Journal of Computer & System Sciences, Journal of Graph Algorithms and Applications, Int. Journal of Computational Geometry & Applications, and Information Processing Letters. I have also served on many program committees (PCs) for top conferences and workshops in Computer Science, including serving as PC chair in several instances. Examples include ACM Symposium on Computational Geometry ("SoCG"), ACM Symposium on Theory of Computing ("STOC"), Workshop/Symposium on Algorithms and Data Structures ("WADS"), Algorithm Engineering and Experimentation ("ALENEX"), which I co-founded with Dr.

Catherine McGeoch in 1999), IEEE Symposium on Foundations of Computer Science ("FOCS"), ACM-SIAM Symposium on Discrete Algorithms (SODA), International Symposium on Graph Drawing ("GD"), International Colloquium on Automata, Languages, and Programming ("ICALP"), ACM Conference on Computer and Communications Security ("CCS"), European Symposium on Algorithms ("ESA"), IEEE International Parallel and Distributed Processing Symposium ("IPDPS"), ACM Symposium on Parallel Algorithms and Architectures ("SPAA"), ACM Symposium on Advances in Geographic Information Systems ("GIS"), IEEE Symposium on Security and Privacy ("S&P"), IEEE International Conference on Big Data, IEEE International Conference on Data Engineering ("ICDE"), and International Symposium on Algorithms and Computation ("ISAAC"), and DAGS Conference on Electronic Publishing and the Information Superhighway.

II. SCOPE OF ASSIGNMENT AND APPROACH

12. I understand that I am submitting a declaration in connection with the *Inter Partes* review ("IPR") proceedings IPR2022-00182 involving U.S. Patent No. 9,917,856 ("the '856 Patent", Ex. 1001).

13. I have been retained as an expert on behalf of Patent Owner, Centripetal Networks, Inc. ("Centripetal"), to provide information and opinions to the Patent Trial and Appeal Board (hereinafter "PTAB" or "the Board") to assist in

the determination of the validity of patent claims of the ’856 Patent for which the Board has instituted an IPR proceeding. Specifically, counsel for Centripetal asked me to provide opinions regarding the validity of Challenged Claims 1, 24, and 25 of the ’856 Patent in view of the prior art reference cited by Petitioner.

14. I have been informed by counsel and I understand that the analysis of whether a patent is anticipated or obvious is performed from the perspective of a person of ordinary skill in the art at the time of the patented inventions (or a “POSITA”). The relevant timeframe for the claims of the ’856 Patent is no later than December 23, 2015.

15. I have reviewed in detail the ’856 Patent; the Petition for *Inter Partes* Review of the ’856 Patent filed in Case No. IPR2022-00182 (the “Petition”); Dr. Dr. Jon Weissman’s declaration filed in Case No. IPR2022-00182 (Ex. 1003, the “Weissman Decl.”); the Board’s Institution Decision for Case No. IPR2022-00182 (Paper 11, the “Institution Decision”); and the deposition transcript of Dr. Weissman (Ex. 2027, “Weissman Tr.”). I have also reviewed United States Patent No. 9,680,795 to Buruganahalli et al. (Ex. 1004, “Buruganahalli”), United States Patent No. 5,878,231 to Baehr et al. (Ex. 1005, “Baehr”), the file history for the ’856 Patent (Ex. 1002), along with the other exhibits listed on Petitioner’s Exhibit List. I have also reviewed the exhibits listed on Patent Owner’s Exhibit List and cited in Patent Owner’s Response in IPR2022-00182.

16. To the extent that I am presented with new information concerning the subject matter of this declaration or affecting any assumptions made herein, I reserve the right to supplement this declaration accordingly.

III. APPLICABLE STANDARDS AND CONTROLLING PRINCIPLES

A. Anticipation

17. Counsel has informed me, and I understand, that an issued patent claim is invalid as anticipated if each and every element of that claim is disclosed in a single prior art reference that enables a person of ordinary skill in the art to make the allegedly anticipating subject matter. I understand that to be anticipatory, a reference must enable one of skill in the art to practice an embodiment of the claimed invention without undue experimentation.

18. Counsel has informed me, and I understand, that if a prior art reference does not disclose a given element expressly, it may do so inherently. I have been informed by counsel and I further understand that a prior art reference will inherently anticipate a claimed invention if any claim elements or other information missing from the reference would nonetheless be known by the person of ordinary skill in the art to be necessarily present in the subject matter of the reference.

B. Obviousness

19. Counsel has informed me, and I understand, that an issued patent claim is invalid as obvious if it can be shown that the differences between the patented subject matter and the prior art are such that the subject matter as a whole would have been obvious, at the time the invention was made, to a person having ordinary skill in the art. Relevant considerations include the level of ordinary skill in the art; the scope and content of the prior art; differences between the prior art and the claims at issue; and the so-called objective indicia, or secondary considerations, of nonobviousness.

20. Counsel has informed me, and I understand, that in order to evaluate the obviousness of any claim of the ’856 Patent over a given prior art combination, I should analyze whether the prior art references, included collectively in the combination, disclose each and every element of the allegedly invalid claim as those references are read by the person of ordinary skill in the art at the time of the invention. Then I am to determine whether that combination makes the claims of the ’856 Patent obvious to the person of ordinary skill in the art by a preponderance of the evidence, at the time of the inventions. I understand that such preponderance of the evidence is satisfied if the proposition is likely to be true than not true.

21. Counsel has informed me, and I understand, that the obviousness inquiry requires that the prior art be considered in its entirety.

22. Counsel has informed me, and I understand, that even where all of the claim limitations are expressly disclosed in the prior art references, there must be some showing that a person of ordinary skill in the art would have been motivated to combine such prior art references and that there would have been a reasonable expectation of successfully achieving the claimed invention from such combination.

23. Counsel has informed me, and I understand, in considering the obviousness of a claimed invention, one should not view the invention and the prior art with the benefit of hindsight. It is for that reason, I am informed and I understand, that obviousness is assessed by the person of ordinary skill in the art at the time the invention was made. In this regard, I am informed and I understand that the invention cannot be used as a guide to selecting and understanding the prior art. I understand that the appropriate standard is to determine whether a person of skill in the art *would* be motivated to combine references, not whether they could.

24. Counsel has informed me, and I understand, that obviousness cannot be predicated on what was unknown at the time of the invention, even if the inherency of a certain feature is later established. Counsel has also informed me,

and I understand, that unknown properties of the prior art may not be relied upon to provide the rationale for modifying or combining the prior art to reach the claimed subject matter.

25. Counsel has informed me, and I understand, that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.

C. Person of Ordinary Skill in the Art

26. Counsel has informed me, and I understand, that the "person of ordinary skill in the art" ("POSITA") is a hypothetical person who is presumed to be familiar with the relevant scientific field and its literature at the time of the invention. This hypothetical person is also a person of ordinary creativity capable of understanding the scientific principles applicable to the pertinent field.

27. I am informed by counsel and I understand that the level of ordinary skill in the art may be determined by reference to certain factors, including (1) the type of problems encountered in the art, (2) prior art solutions to those problems, (3) the rapidity with which innovations are made, (4) the sophistication of the technology, and (5) the educational level of active workers in the field. I further understand that in a given case, every factor may not be present, and one or more factors may predominate.

28. In my opinion, a person of ordinary skill in the art in the field of the '856 Patent as of its priority date would be someone with a bachelor's degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or a related field. This description is approximate, and more work experience could compensate for less education or more education could compensate for less work experience.

29. Based on my training and experience, I believe that I am a person of greater-than-ordinary skill in the relevant art, and have been since at least the priority date of the '856 Patent, which permits me to give an opinion about the qualifications of one of ordinary skill at the time of the invention.

30. In my opinion, my definition of a POSITA is similar to that of Dr. Weissman. *See, e.g.*, Weissman Decl. at ¶¶ 1-12, 24-30. Thus, the opinions contained in this declaration would not change were I to use the definition of a POSITA offered by Dr. Weissman.

IV. BACKGROUND

A. State of the Art

31. The following analysis shows that detecting cyberattacks in encrypted traffic was considered "unsolvable" and provides additional analysis as to why Buruganahalli in view of Baehr does not render obvious claims 1, 24, and 25. Ex. 2013 at 1; Ex. 1027 at 61-64. Typical firewalls—like Buruganahalli—could only

analyze unencrypted data. With the rise in popularity of encrypted communications, cyberattacks became embedded inside encrypted communications, obfuscating the cyberattacks. Ex. 1001 at 1:17-18; Ex. 2005 at ¶ 0018. Conventional wisdom addressed this problem by configuring firewalls to decrypt the encrypted communications, just like Buruganahalli. Ex. 2005 at ¶ 0019; Ex. 2015 at 2:47-59. Such a firewall functions as a "trusted man-in-the-middle,"[2] intercepting, decrypting, analyzing, and then re-encrypting the encrypted communications. Ex. 2015 at 2:47-5:12. But decryption and re-encryption is difficult to perform in real-time and undesirably slows down network traffic and consumes computing power. Weissman Tr. at 53:25-54:2 ("Decryption is an expensive operation, and the firewall has to process packets very quickly.").

1. Secure Communications

32. HTTP and SMTP communications over the Internet (which are, respectively protocols for web pages and email) are often secured using the Transport Layer Security ("TLS") protocol. The TLS protocol is an upgrade of another widely known protocol, known as the Secure Sockets Layer ("SSL"). SSL is a transport layer protocol that provides for:

[2] A person of ordinary skill in the art would understand that a "man-in-the-middle" is often a type of cyber-attack; hence, the distinction of a "trusted man-in-the-middle."

1) the client computer sends a request to a server computer to initiate a handshake procedure;

2) the server computer responds by sending a digital certificate, which typically includes the server's name, a certificate authority, and a public key that will be used to encrypt the transmission of a random number;

3) the client may contact the certificate authority to validate the certificate;

4) if the client is satisfied that the certificate is valid, it sends a random number encrypted with the server's public key to the server computer; and

5) both the client computer and the server computer then generate a unique session key using this random number that is subsequently used for the encryption and decryption of all further communications between the client and the server.

33. While other variations exist to this method, the above-described method is the typical procedure for initiating a secure communication by generating and exchanging a private session key. Because the communications are encrypted with this private key, it is very difficult, in practice virtually impossible, to read the communications. The use of TLS/SSL to secure HTTP communications is known as "HTTPS" and is sometimes referred to as HTTP over TLS, HTTP over SSL, or HTTP Secure. HTTPS is essentially encrypting the same HTTP data with a shared secret session key that is determined after an initial "hello" protocol, which includes sharing the public key(s) of a client and server.

TLS/SSL therefore encrypts traffic and other communications over a network. For example, TLS/SSL information is encrypted so that when it is sent over the Internet no one but the recipient will be able to decrypt that information (barring someone breaking the encryption scheme being used). While this encrypted traffic provides certain protection to networks and enterprises – by, for example, protecting sensitive information – it also is vulnerable to manipulation by potential attackers, e.g., if the content that is encrypted contains malware or if the encrypted content is modified so that its decryption comprises a threat.

2. Network Security

34. With the expansion of networks and connectivity, network security is a continually growing and significant consideration and concern for larger enterprises and corporations. Data centers, in particular, are at the focus of protecting such networks as data centers serve as the primary hosts of applications underlying companies' business and business operations. Thus, protection at the data center, and in particular, detecting and ensuring the network is not subject to malicious threats or attacks is critical. These attacks include enterprise wide phishing attacks, malicious worms, exploits, botnet, hijacked IPs, and other such threats that are becoming more pervasive across industries.

35. One of the challenges faced with monitoring traffic in connection with the data centers is the volume and path of the traffic. *See, e.g.,* the Ex. 1001 at 1:7-

20. Monitoring tools, therefore, that are able to assess the traffic within the data center and utilize information and insights from other networks and devices provide for the ability to maximize efficiency in protecting a network's security.

36. For example, analyzing traffic for malicious threats can be accomplished through packet filtering. In particular, as packets enter a network, a packet filtering tool can analyze the packet header for information that may signal that a threat or attack is being attempted. Packet header information includes, as I describe in this Declaration, IP destination address; IP source address; protocol (that is, whether the packet is a UDP, TCP or ICMP packet); TCP or UDP destination port and/or source port; and ICMP message type. Comparing the detected packet header information against rules or policies that a network has access to allow for these packet to be stopped before they can compromise the network. In particular, as disclosed in the '856 Patent,[3] a database and list of threat indicators can be aggregated from within the network and from other networks so that if an outside network is aware of a threat that the given network is currently unaware of, it will be able to detect it within a packet without having had encountered it yet. This allows for every packet or traffic coming through to be analyzed therefore providing for even greater security and protection for the

[3] *See, e.g.,* the Ex. 1001 at 1:7-20.

network particularly for bigger enterprises taking advantage of larger intranet connectivity. When a threat is detected based on the information in the packet header, based on the packet filtering rules, certain actions may be taken such as dropping, forward, or routing the packet.

37. Applications are an example of a threat vector for attacking networks. Applications may contain malicious links or attachments, particularly for newer applications that are unknown to a network. By launching an application, the end user may inadvertently compromise the network. This potential compromise is similar to when an end user clicks on a malicious URL link or attachment in a "spoof" e-mail sent by a hacker who makes the message appear to come from a person that the end user would normally trust. As such, as discussed, utilizing techniques of identifying known applications – or threats – based on previous information and policies helps to ensure that the use of applications do not compromise a computer or network of computers.

38. A goal of a security gateway is to be a mediator of the communication between computing devices in the internal network and the computing devices in the external network, or two networks within an internal network, and to make security decisions about the communication according to a security policy. For example, a security gateway could block all the communication originating from external computing devices and allow only internal computing devices to originate

requests or send emails to the outside. This setup is the most common configuration for home routers: the internal hosts connected to the router can connect to the Internet, but external hosts on the Internet cannot open connections to the hosts behind the router.

39. Often times, the determination as to what will be blocked or allowed is based on rules. In large enterprises, the security gateway can inspect traffic within a network to determine whether a threat exists and to block the traffic from being sent from the malicious entity or block traffic being sent to the malicious entity. For example, a security gateway or security device can inspect packets and determine that they are being sent to an illegitimate place which may be evidence of a worm. On the other hand, a security gateway may inspect traffic on a network that is being sent to a target on the network in an attempt to overload the target which may be evidence of a denial-of-service attack.

40. The security gateway can perform various actions with respect to the communication between an internal host and an external host. For example, a security gateway can examine each TCP/IP packet and determine whether the packet should be forwarded to its destination. This determination could be based on, but is not limited to, rules or security policies and log entries based on information pertaining to the received and transmitted packets. These rules, as I described above, are often defined by conditions or sets of conditions that establish

actions to be taken if and when those conditions are met.

B. Overview of Petitioner's Relied Upon References

1. Buruganahalli

41. Buruganahalli (Ex. 1004) relates to "[t]echniques for destination domain extraction for secure protocols." Ex. 1004 at Abstract. Buruganahalli extracts the destination domain from an unencrypted client hello message of the Transport Layer Security (TLS) protocol. *Id.* at 4:45-67. The unencrypted client hello message is sent by a client at the start of the TLS handshake process. *Id.* at 5:6-10, 7:19-25. The hello message includes a Server Name Indication (SNI) field indicating the destination domain.[4] *Id.* at 4:59-5:10. Buruganahalli's firewall uses this destination domain to apply a whitelist/blacklist policy. *Id.* at 7:12-51.

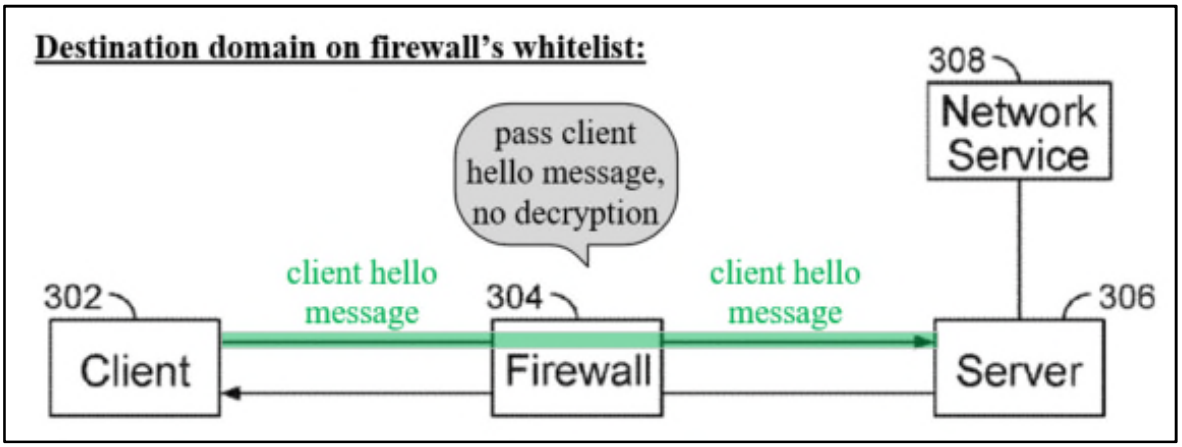
42. A POSITA reading Buruganahalli would understand that Buruganahalli describes several scenarios of whitelisting and blacklisting, and I describe these scenarios as follows.

a. Buruganahalli's Figure 3A Whitelist Embodiment Allows an Encrypted Session Without Applying Packet-Filtering Rules to Encrypted Packets

43. Buruganahalli's figure 3A (which I have annotated below) depicts the first scenario, if a destination domain is on the whitelist, the firewall allows the

[4] The SNI is an extension to the TLS protocol that allows a server to present a digital certificate for a domain specified in the hello message. The desired domain is not encrypted. *See, e.g.,* https://en.wikipedia.org/wiki/Server_Name_Indication.

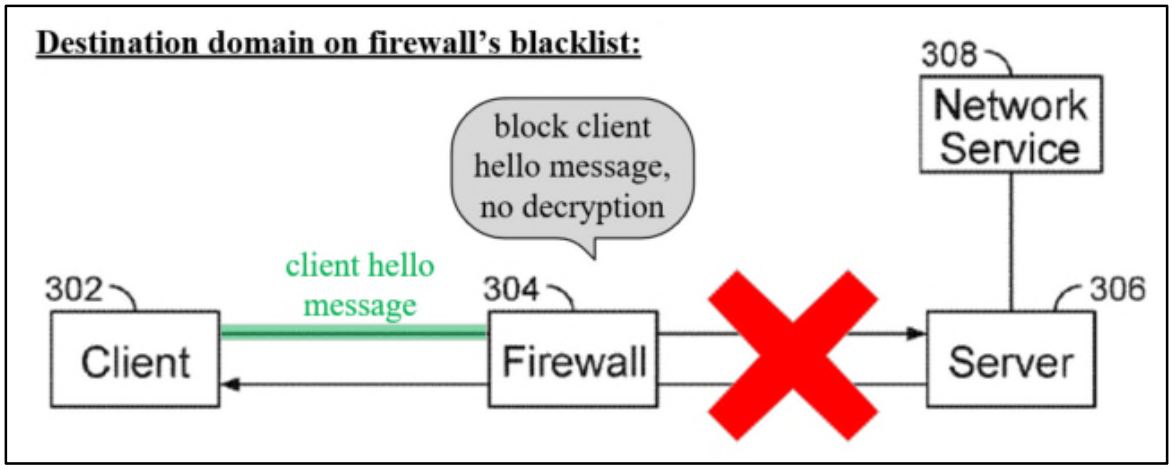
client hello message to pass through to the server and allows a secure connection to be established between the client and server. Ex. 1004 at 5:43-51, 6:1-11, 7:52-59, 10:54-11:6, 16:35-41, Fig. 3A. A POSITA would understand that in this first scenario, subsequent encrypted traffic is simply forwarded without decryption or filtering. *Id.*



Buruganahalli, Fig. 3A (annotated).

b. Buruganahalli's Figure 3A Blacklist Embodiment Blocks a Requested Encrypted Session Before Any Encrypted Packets are Received

44. In the second scenario (which I have annotated in figure 3A below), if the destination domain is on the blacklist, the firewall blocks the unencrypted **client hello message** from passing through to the server. *Id.* at 5:64-6:11, 10:54-11:19, 4:31-44. A POSITA would understand that there is no secure connection established and no encrypted packets are received by the firewall. Ex. 1004 at 5:64-6:11, 10:54-11:19, 4:31-44.

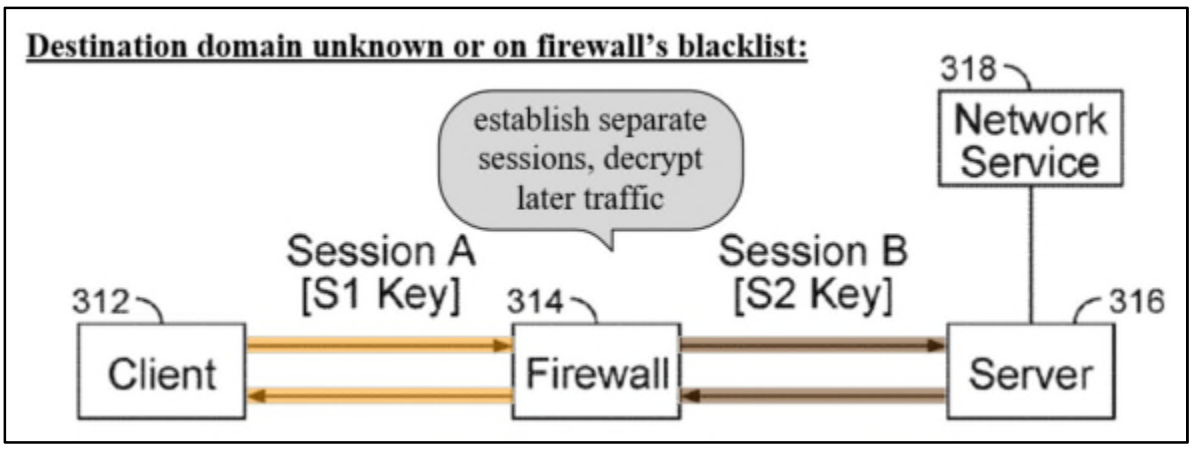


Buruganahalli, Fig. 3A (annotated).

45. In this scenario, Buruganahalli explains that a firewall can apply a policy "without having to decrypt" traffic because no secure, encrypted session is ever started, and no encrypted packets are received. Ex. 1004 at 11:7-19, 4:31-44. I understand that Petitioner readily acknowledges this fact in its argument about how Buruganahalli discloses filtering packets comprising unencrypted data. Pet. at 37 (arguing that unencrypted traffic is filtered "based on the determination of whether 'the destination domain is included in the blacklist'" which occurs "prior to the establishment of the secure communication channel/tunnel after which any data communications intercepted between the client and the remote server would be encrypted"). Buruganahalli further clarifies that because firewall 304 does not perform decryption of encrypted packets, it "cannot detect such firewall policy/rule violation(s)" in the encrypted packets. Ex. 1004 at 11:2-6.

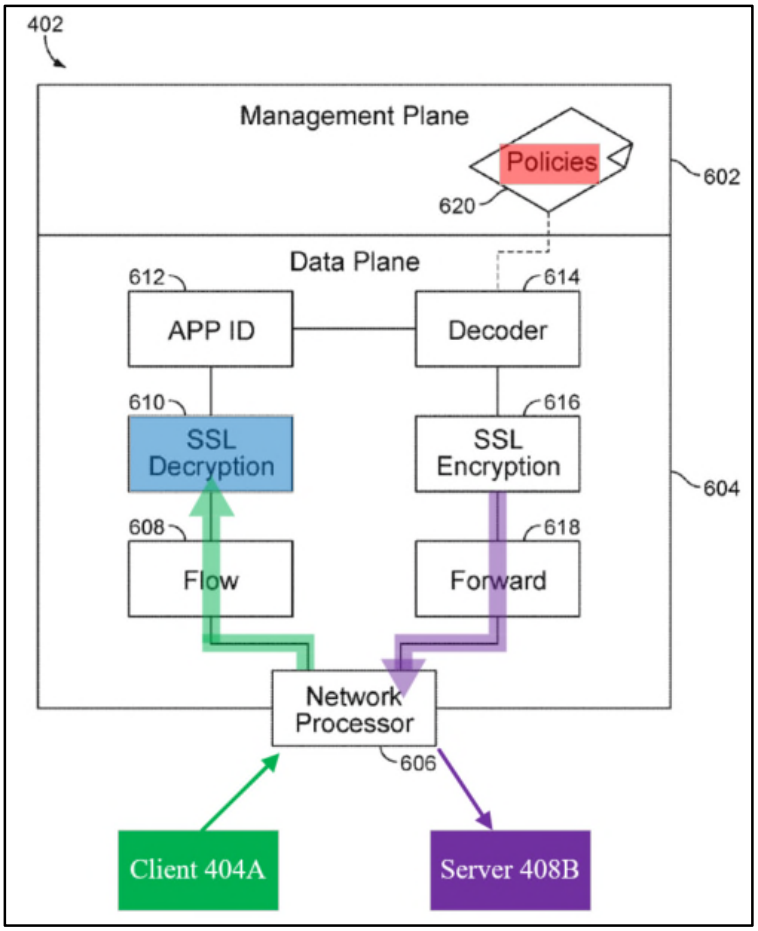
c. Buruganahalli's Figure 3B Blacklist Embodiment Requires that Encrypted Packets be Decrypted Before Applying any Packet-Filtering Rules

46. In a third scenario (which I have annotated in figure 3B below), if the destination domain is on the blacklist (or unknown because it is not on the whitelist or blacklist), the firewall may initially allow the client hello message but require decryption thereafter. *Id.* at 6:12-38, 7:60-67, 8:25-44, 11:59-12:64. A POSTIA would understand that a secure connection is split into two sessions: **Session A** and **Session B**, as depicted in annotated Figure 3B below. *Id.* This allows the firewall to **decrypt** encrypted packets for further analysis. *Id.* at 12:4-61 ("[a]fter the session set-up handshaking is completed for each of Session A and Session B, any data that is communicated from the client 312 to the firewall 314 is **decrypted** using a session key S1 and is then inspected by the firewall 314"; "[s]imilarly, traffic coming from the server is **decrypted** with the session key S2, inspected by the firewall 314, and then encrypted using the session key S1 and forwarded to the client 312") (emphasis added). Thus, the firewall 314 becomes a "man-in-the-middle" with respect to the communication between client 312 and server 316, which, and this scenario the firewall 314 is considered a "trusted" man-in-the-middle. *Id.* at 9:61-10:9, 11:59-12:3, 12:4-55.



Buruganahalli, Fig. 3B (annotated).

47. In my opinion, none of these three scenarios involves rule-based filtering of encrypted packets because Buruganahalli only applies packet-filtering rules to unencrypted packets or decrypted packets. *Id.* Buruganahalli states that "techniques for decrypting such secure communications are **needed** in order to monitor such encrypted data communications **and to apply filtering based on a policy**." *Id.* at 4:20-22 (emphasis added). Buruganahalli reinforces this fundamental fact about how encrypted communications were handled before the '856 Patent throughout its disclosure. For example, in figure 6, security device 402 (*e.g.*, firewall) has a management plane storing **policies 620** and a data plane for handling packets. *Id.* at 14:8-20, 14:58-60, Fig. 6.

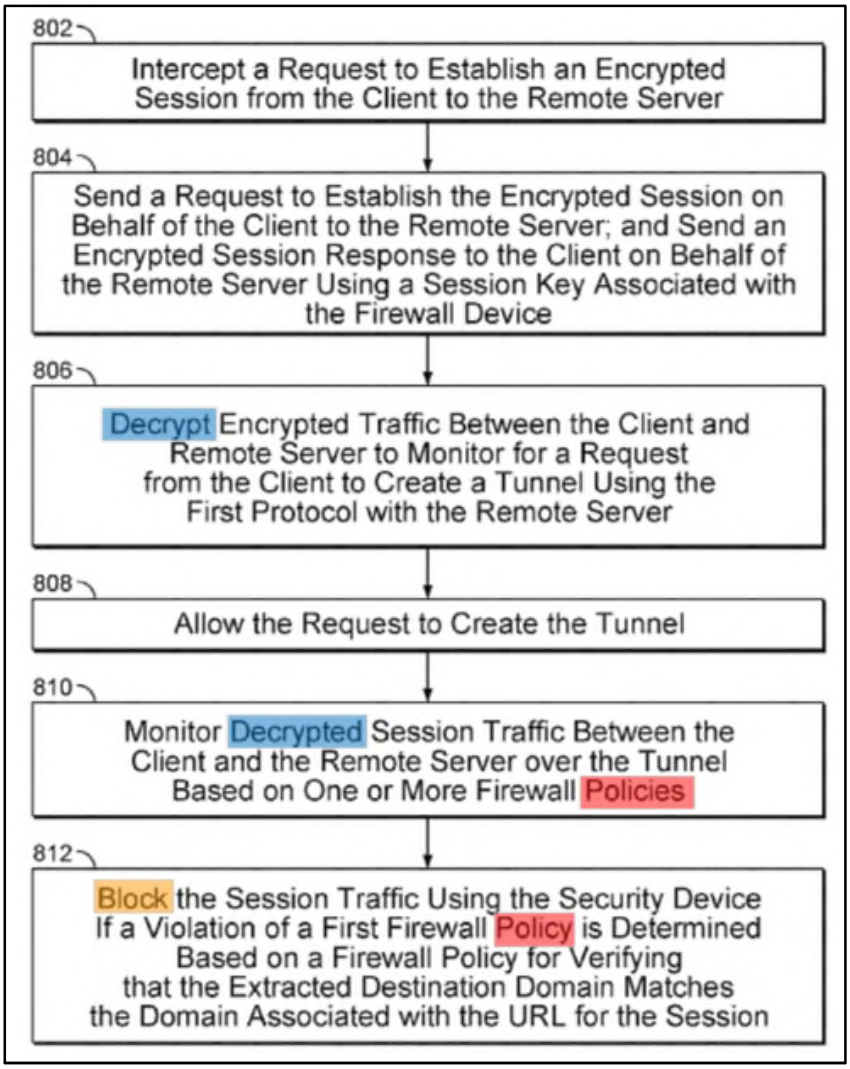


Buruganahalli, Fig. 6 (annotated)

48. Network processor 606 receives a packet from **client 404A** intended for **server 408B**. Ex. 1004 at 14:21-22. The packet may be assigned to a flow 608 that is newly created (*e.g.*, if the packet is an unencrypted packet for a new session/flow) or previously created (*e.g.*, if the packet is a subsequent packet like an encrypted packet) based on a flow lookup (using an IP address—not a domain name). *Id.* at 14:25-28, 9:25-30 (describing use of IP address); Weissman Tr. at 35:4-25 (testifying a packet is correlated to a particular flow using "the IP address and port"). A POSITA would recognize reading Buruganahalli that if an encrypted

packet does not belong to a whitelisted flow/session, it is dropped (and no filtering is applied) or it is decrypted by an **SSL decryption engine 610** before applying any policies. Ex. 1004 at 14:33-38. **Policies 620** to allow or block that decrypted data are not applied until the decrypted data is decoded by decoder 614, as evidenced by the dashed line in Figure 6 connected to the decoder. Ex. 1004 at 14:50-58, 14:21-22, Fig. 6; *see id.* at 9:44-10:28, Fig. 1 (policy engine 120 applies policies after receiving results from decrypting and decoding encrypted traffic).

49. Finally, regarding Figure 8, Buruganahalli provides a flow diagram showing that encrypted traffic is **decrypted** and the **decrypted** traffic is monitored using **policies**, which may result in **blocking** the traffic. *Id.* at 15:22-45, Fig. 8, Fig. 8.

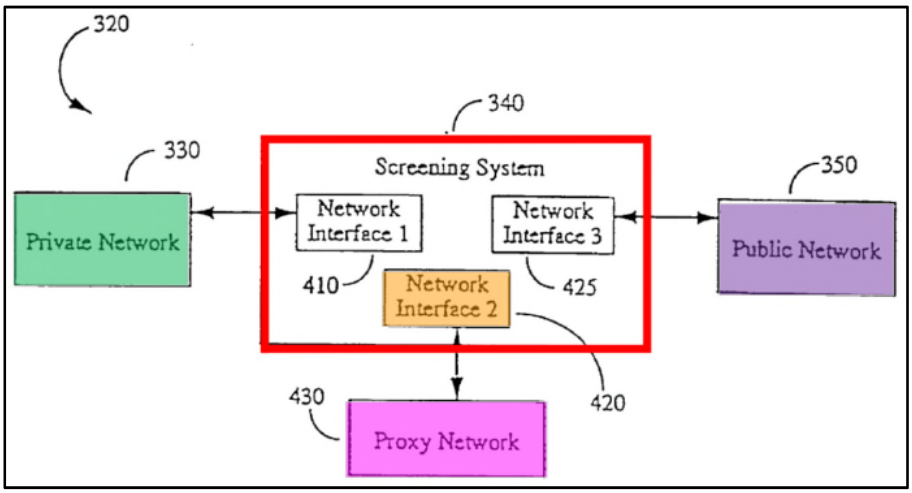


Buruganahalli, Fig. 8 (annotated).

50. In my opinion, in every instance Buruganahalli only applies policies to unencrypted packets or decrypted data—never to encrypted packets because decryption is fundamental to Buruganahalli's firewall, which is designed to split a secure session so the firewall can act as a "trusted man-in-the-middle" to decrypt encrypted packets. Ex. 1004 at 4:16-22, 9:61-10:9, 11:59-13:4, claims 1, 6-10.

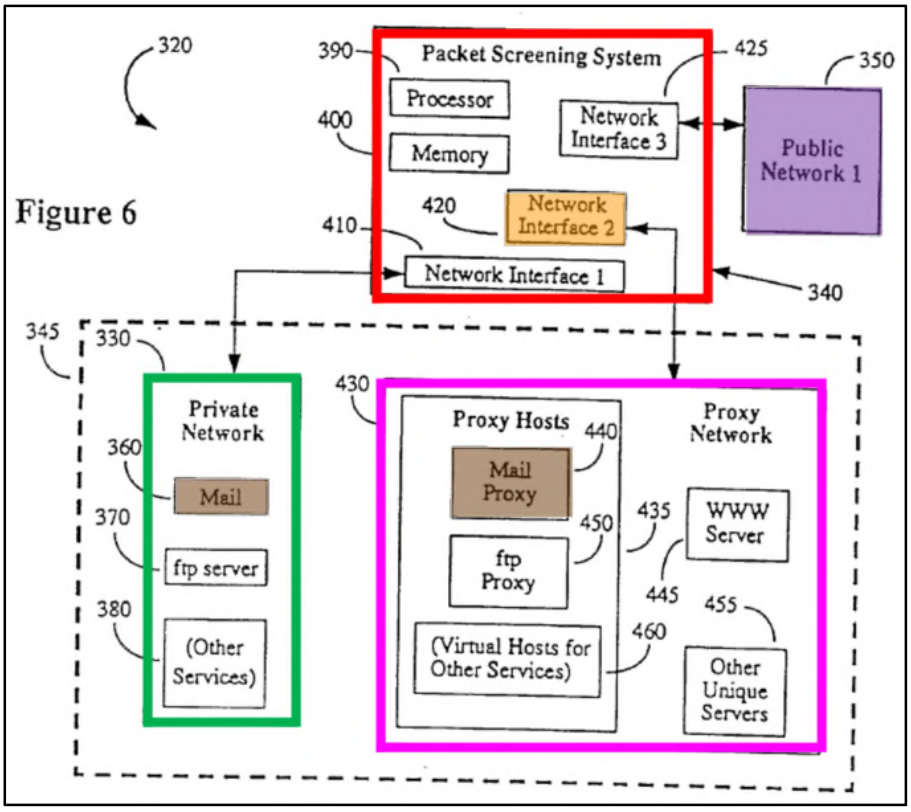
1. Baehr

51. Baehr (Ex. 1005) relates to a system for screening packets transmitted between a **private network** and a **public network**. Ex. 1005, Abstract, 1:9-17, 2:10-17, Fig. 5 (which I have annotated below). Baehr describes adding **network interface 420** to **screening system (or "screen") 340** for coupling it to **proxy network 430**. *Id.* at 3:51-64.



Baehr, Fig. 5 (annotated). The annotation depicts that packets received at the **screening system** (*e.g.*, from the **public network**) are allowed, dropped, or sent to a host on the **proxy network**. Ex. 1006 at Abstract, 10:46-49.

52. Baehr's Figure 6 (which I have annotated below) provides a more detailed view of **screen 340**. *Id.* at 4:12-63, Fig. 6. A proxy host (*e.g.*, **mail proxy 440**) of **proxy network 430** mirrors a host (*e.g.*, **mail host 360**) on **private network 330** to perform functions as though it is the private network host to which packets are destined. *Id.* at Abstract, 4:26-63, 8:13-17, 8:36-46.



Baehr, Fig. 6 (annotated).

53. In my opinion, there is nothing distinguishable about Baehr's use of a proxy as compared to other proxy systems considered during prosecution. First, Baehr does not disclose the proxy performing decryption. *Id.* Second, Baehr does not describe rule-based filtering of encrypted packets. *Id.* Further, Baehr was filed in 1997, which is before TLS was introduced by the IETF in 1999; hence, Baehr does not disclose a system that is designed to work with TLS (which is required for the SNI in Buruganahalli).

C. The ’856 Patent’s contributions to the art

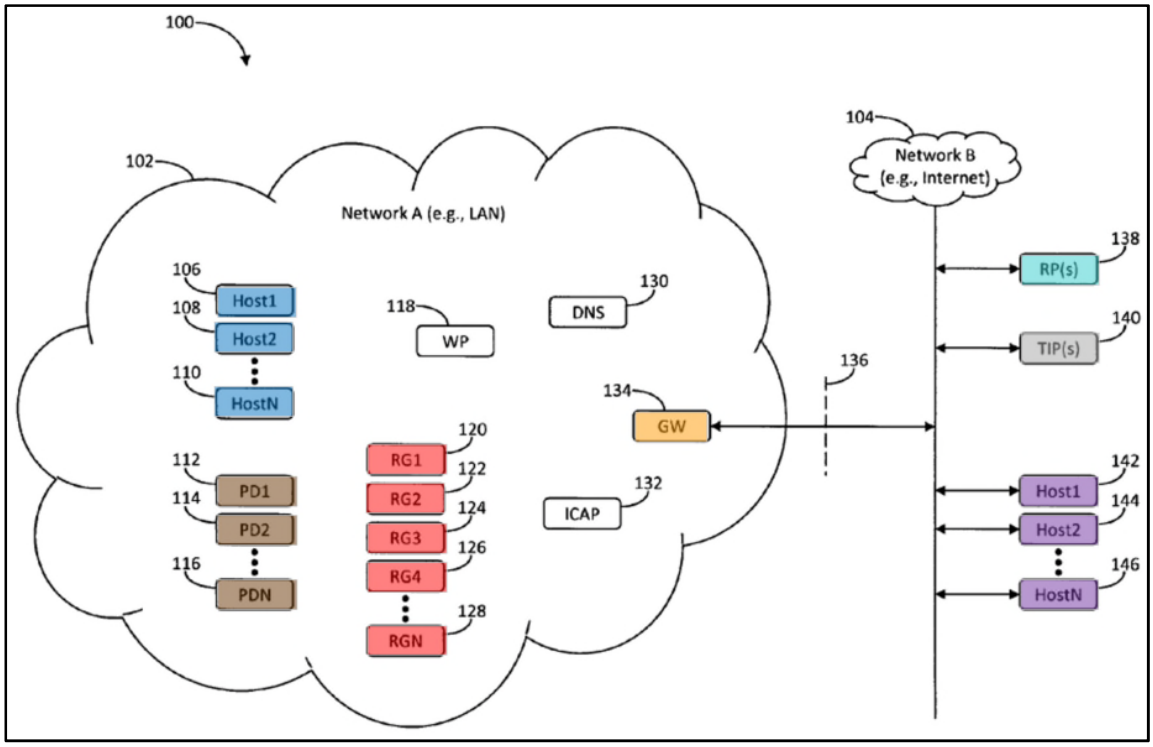
54. Prior to the ’856 Patent, firewalls either filtered unencrypted packets to block certain secure sessions before they started or decrypted encrypted packets in order to filter the decrypted data, as performed by Buruganahalli. Ex. 1004 at 11:2-6. With the ’856 Patent’s inventive approach, rule-based network-threat detection of encrypted packets is performed on encrypted traffic without decryption. Ex. 1001 at 9:66-10:14, 11:51-65.

55. The ’856 Patent reconfigures rules based on encrypted-packet log data that otherwise would not be collected because, *e.g.*, under prior approaches, the secure session would be blocked before encrypted packets were received. Ex. 1001 at 14:4-18, 20:22-27, 22:18-19, 23:58-62, Figs. 3A-6B. The ’856 Patent’s approach of filtering encrypted packets accounts for possible rule updates that are received after a secure session is initiated. Ex. 1001 at 14:19-16:26 (describing use of reconfigured rules), 22:20-51 (same).

56. This added flexibility gives firewalls and other network devices the ability to: (i) end a secure session that is later deemed to be a threat per an updated rule, or (ii) allow a secure session to pass through without any further processing per an updated rule that indicates the secure session is not a threat. Ex. 1001 at 14:19-16:26, 22:20-51. Another advantage of a firewall or other network device implementing the ’856 Patent’s technology to perform rule-based filtering of

encrypted packets is that it can allow a secure session initially and end it after a time or data limit is exceeded because such device continues to log encrypted packets. Ex. 1001 at 9:33-46, 11:28-35. This means such device can prevent too much data from being extracted by bad actors if the secure session turns out to be a threat.

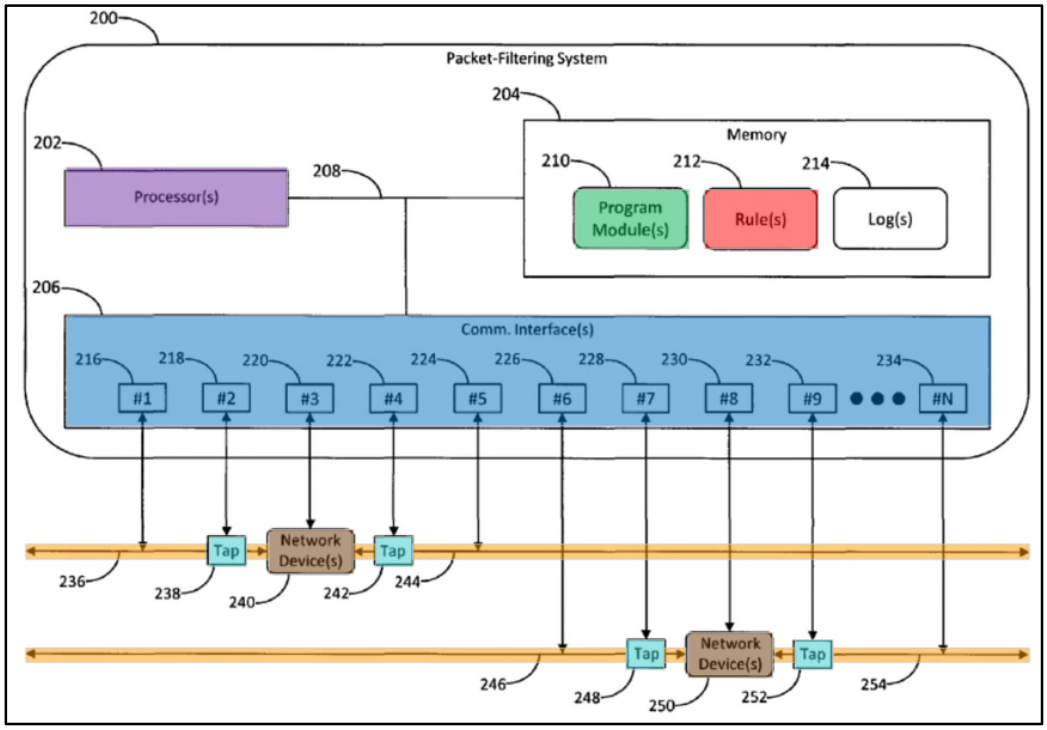
57. Figure 1 (which I have annotated below) depicts an illustrative environment using the inventive approach to protect network 102 from threats in network 104. *Id.* at 2:20-34, Fig. 1.



Ex. 1001, Fig. 1 (annotated). The annotated depiction shows that **gateway 134** interfaces network 102 with network 104. *Id.* at 2:50-53. Network 102 includes one or more **hosts 106, 108, 110** for communicating with one or more **hosts 142,**

144, 146 in network 104. *Id.* at 2:35-53. Network 102 also includes **proxy devices 112, 114, 116** and **rule gates 120 122, 124, 126, 128**. *Id.* at 2:35-43. The rule gates receive data indicating network-threat indicators (*e.g.*, domain names) from **rule providers 138** based on reports from **threat-intelligence providers 140**. *Id.* at 3:65-4:9. Using this data, the **rule gates** configure rules to control a packet-filtering system. *Id.* at 4:16-21.

58. I have annotated the packet-filtering system 200 in Figure 2 (annotated below) for illustration.

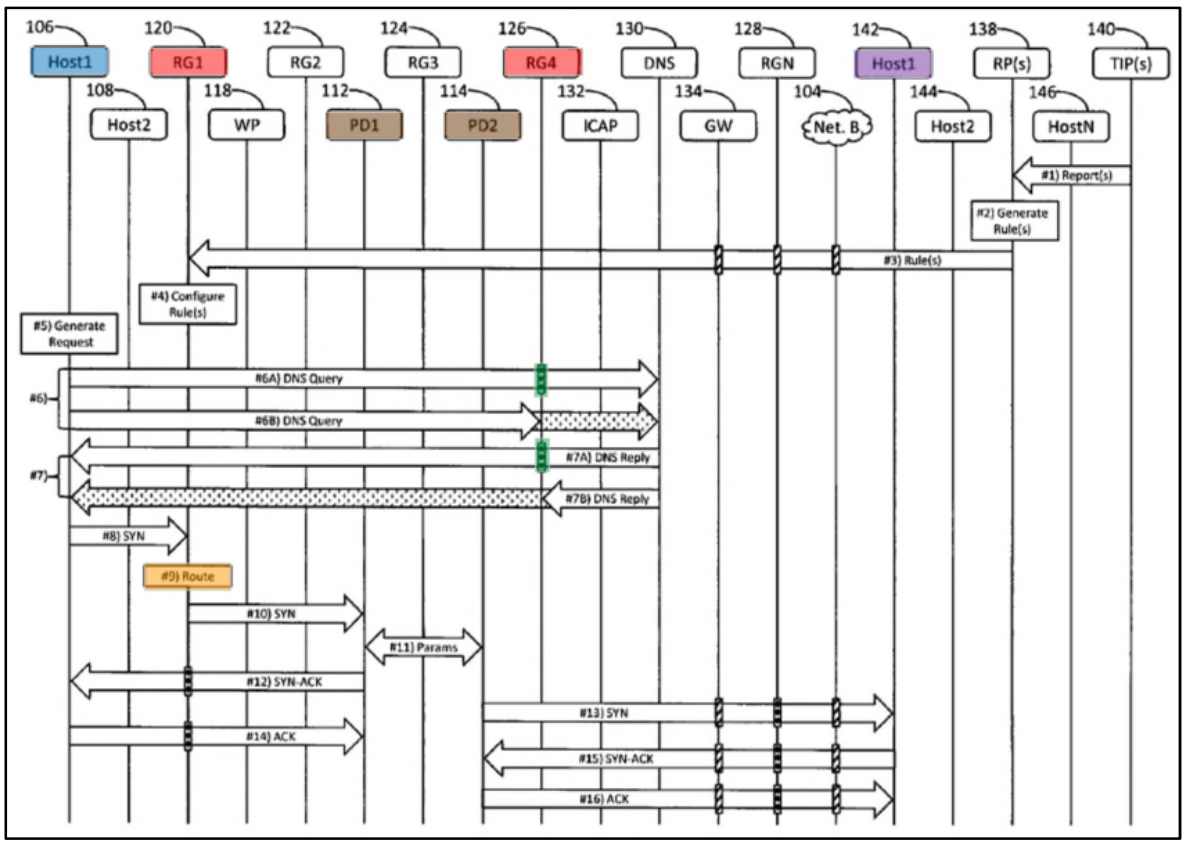


Ex. 1001, Fig. 2 (annotated)

59. In the above illustration, packet-filtering system 200 includes **processor(s) 202** for executing **program module(s) 210** for performing rule-based network-threat detection using **rules 212**. Ex. 1001 at 2:66-3:14. It also includes a

communication interface 206 for interfacing with **communication links 236, 244, 246, 254** directly or indirectly through **tap devices 238, 242, 248, 252** or **network devices 240, 250**. *Id.* at 3:15-56. The **rules 212** are deployed throughout the system so that filtering is performed by various devices (*e.g.*, tap device 238). *Id*.

60. Figures 3A-3C, 4A-4C, 5A-5B, and 6A-6B show different event sequences to illustrate capabilities of the system. Ex. 1001 at 1:64-67. Regarding Figures 3A-C, the ’856 Patent teaches **rule gate 120** receiving data (step #3) and configuring packet-filtering rules (step #4). *Id.* at 3:65-4:21, Fig. 3A (I have annotated below).

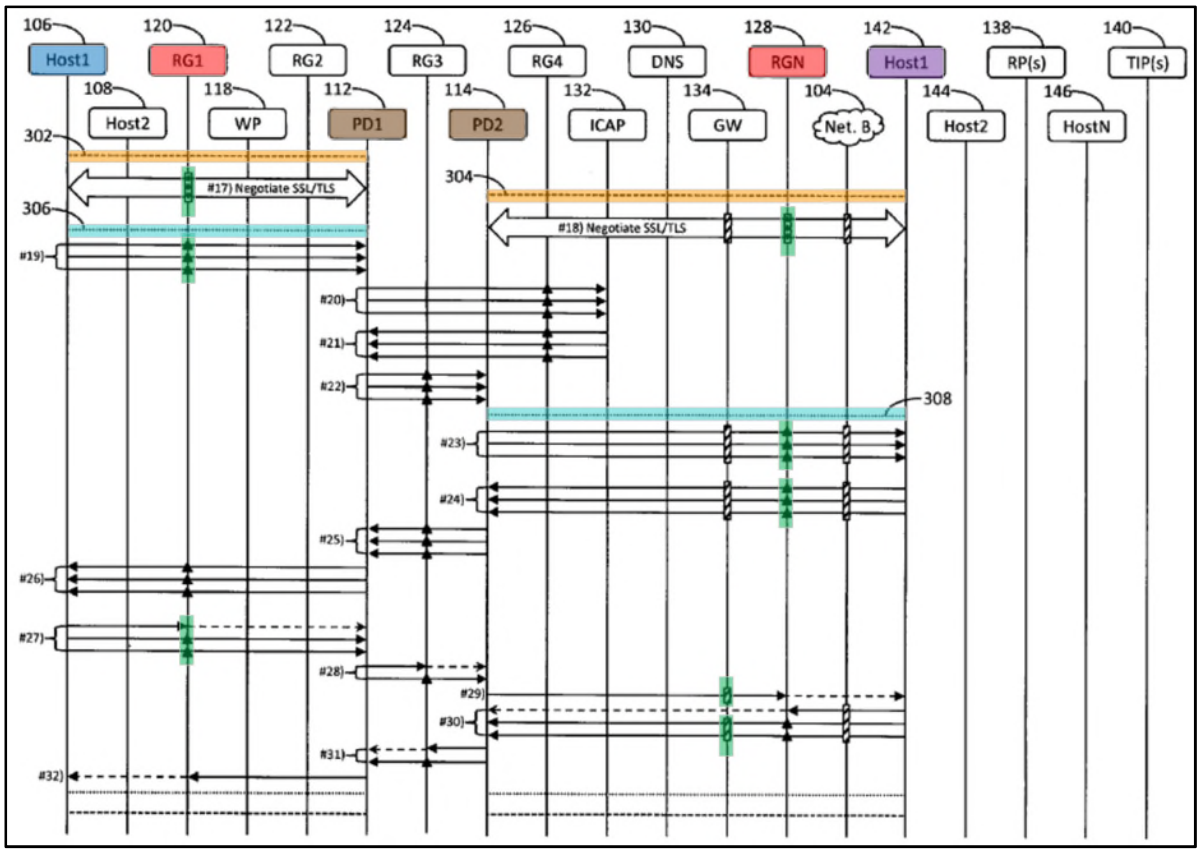


Ex. 1001, Fig. 3A (annotated).

61. When a user of **host 106** (*e.g.*, personal computer) requests a webpage associated with a domain name (step #5), a DNS query including the domain name is transmitted to a domain name system (DNS) (step #6) which responds with a DNS reply (step #7) providing a network address (*e.g.*, for **host 142**) associated with the domain name. *Id.* at 4:22-5:9. The packet-filtering system, specifically **rule gate 126** in this example, **filters** the DNS query or DNS reply. *Id.* at 4:28-6:16. Assuming the DNS reply is received, **host 106** sends (step #8) a SYN message (a Transmission Control Protocol (TCP) handshake message). *Id.* at 6:17-21. The packet-filtering system, specifically **rule gate 126**, **routes** (steps #9-10)

the SYN message to **proxy device 112** based on the packet-filtering rules. *Id.* at 6:33-7:32..

62. After receiving the SYN message, **proxy device 112**, in conjunction with **proxy device 114**, sets up two separate connections (steps #11-16): **connection 302** (*e.g.*, a TCP connection) between **the proxy system** and **host 106** and **connection 304** (*e.g.*, another TCP connection) between **the proxy system** and **host 142**. *Id.* at 7:33-8:64, Figs. 3A, 3B (I have annotated below).



Ex. 1001, Fig. 3B (annotated).

63. Handshake messages are exchanged over both connections 302 and 304 to establish two separate encrypted communication sessions (steps #17-18):

encrypted communication session 306 (*e.g.*, SSL/TLS session) between the **proxy system** and **host 106** and **encrypted communication session 308** (*e.g.*, another SSL/TLS session) between the **proxy system** and **host 142**. *Id.* at 8:65-9:65, Fig. 3B. These handshake messages include, *e.g.*, a client hello message having unencrypted data, such as a domain name. *Id.* at 9:16-33. **Rule gate 120** using rules may **filter** the handshake messages based on the domain name. *Id.* at 9:2-46. Similarly, **rule gate 128** using rules may **filter** the handshake messages for establishing encrypted communication session 308. *Id.* at 9:47-65.

64. A POSITA would understand reading the '856 Patent that once **encrypted communication sessions 306, 308** are established, encrypted packets may be communicated in those sessions. For example, encrypted packets are sent from **host 106**, **filtered** by **rule gate 120** using rules, and delivered to **proxy device 112** (step #19). Ex. 1001 at 9:66-10:14. This filtering includes correlating the encrypted packets with previous packets (*e.g.*, previous unencrypted packets) determined to comprise data corresponding to network threat indicators and then logging or dropping the encrypted packets. *Id.* at 10:2-14.

65. Even though an encrypted packet may be passed by **rule gate 120** at the beginning of a secure session (step #19), **rule gate 120** continues to **filter** encrypted packets and may later drop another encrypted packet of that session (step #27). *Id.* at 12:28-42. Similar **filtering** is performed by **rule gate 128** on

encrypted packets during encrypted communication session 308 (steps #23, 24, 29, 30). *Id.* at 11:36-65, 12:58-13:22. I note that these filtering steps use rules to filter encrypted packets without decryption—an important difference over Buruganahalli as it was during prosecution and the Cisco litigation.

66. In my opinion, this difference is captured by each independent claim. For example, representative claim 1 recites "determining, by the packet-filtering system and **based on a portion of the unencrypted data corresponding to one or more network-threat indicators** of the plurality of network-threat indicators, packets comprising **encrypted data that corresponds to the one or more network-threat indicators**;" and "**filtering**, by the packet-filtering system and **based on** at least one of a uniform resource identifier (URI) specified by **the plurality of packet-filtering rules**, data indicating a protocol version specified by **the plurality of packet-filtering rules**, data indicating a method specified by **the plurality of packet-filtering rules**, data indicating a request specified by **the plurality of packet-filtering rules**, or data indicating a command specified by **the plurality of packet-filtering rules**: …**the determined packets comprising the encrypted data** that corresponds to the one or more network-threat indicators." *Id.* at 25:24-45 (claim 1) (emphasis added). This rule-based filtering of encrypted packets marks a significant advancement over the prior art.

67. The data logged from filtering encrypted packets (as shown above in Figure 3B) can be used to **reconfigure rules** (step #34), as shown in Figure 3C (which I have annotated below). Ex. 1001 at 14:4-18, Figs. 3B, 3C.

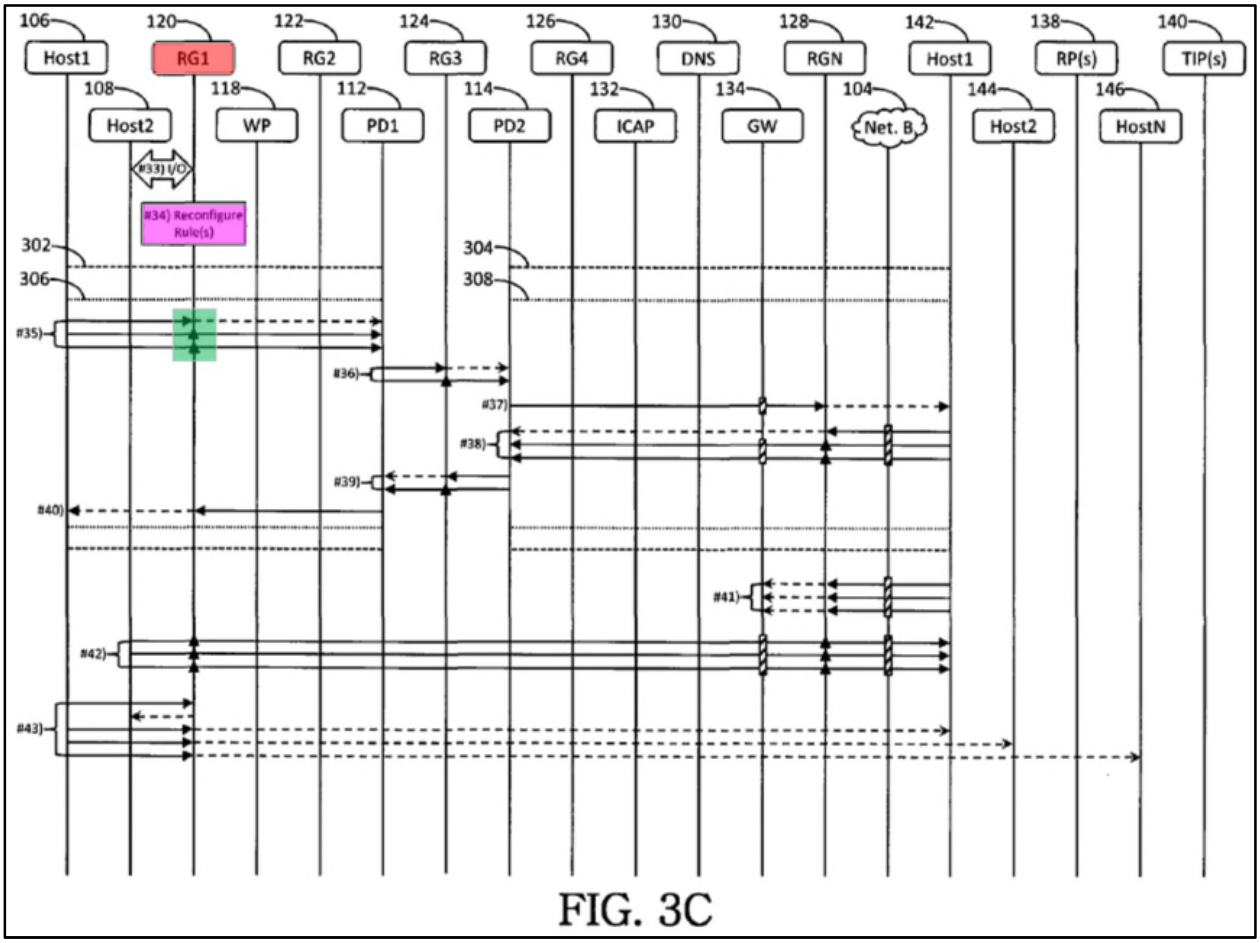


FIG. 3C

Ex. 1001, Fig. 3C (annotated). In my opinion, this improves cyberthreat analysis by enabling **rule gate 120** to act on updated rules. Figure 3C shows **rule gate 120 filtering** based on the reconfigured rules to drop an encrypted packet after the secure session is established (step #35). Ex. 1001 at 14:19-34.

D. The Challenged Claims

68. I understand that claims 1, 24, and 25 of the ’856 Patent are at issue in the IPR proceeding. For reference, these claims are as follows (using the indexing as used by Petitioner):

> [1.pre] A method comprising:
>
> [1.a] receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprises a domain name identified as a network threat
>
> [1.b] identifying packets comprising unencrypted data;
>
> [1.c] identifying packets comprising encrypted data;
>
> [1.d] determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;
>
> [1.e] filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:
>
> [1.f] packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and
>
> [1.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

[1.h] routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

[24.pre] A packet-filtering system comprising:

[24.a] at least one hardware processor; and memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

[24.b] identify packets comprising unencrypted data;

[24.c] identify packets comprising encrypted data;

[24.d] determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

[24.e] filter, based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

[24.f] packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

[24.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

[24.h] route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

[25.pre] One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to

[25.a] receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of network-threat indicators comprise a domain name identified as a network threat;

[25.b] identify packets comprising unencrypted data;

[25.c] identify packets comprising encrypted data;;

[25.d] determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

[25.e] filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:;

[25.f] packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

[25.g] the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

[25.h] route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

V. CLAIM CONSTRUCTION

69. I have been informed through counsel that during this *inter partes review* proceeding (because this petition for *inter partes* review was filed on or after November 13, 2018), claims terms should be given their "ordinary and customary meaning as would be understood by a person of ordinary skill in the art in question at the time of the invention." I have further been informed that for determining the meaning of a disputed claim term, it is appropriate to "look principally to the intrinsic evidence of the record, examining the claim language itself, the written description, and the prosecution history." I further understand that extrinsic evidence is less significant than the intrinsic record in determining the meaning of the claim language.

70. In its Institution Decision, the Board determined that regarding any explicit constructions that might be provided by the Board that "no claim term requires an explicit construction to decide whether Petitioner satisfies the 'reasonable likelihood' standard for instituting trial." Institution Decision at p. 48. Further, in its Institution Decision, the Board references and reviews the Cisco district court case, *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, No. 2:18-cv-00094, Dkt. 621 (E.D. Va.). Institution Decision at pp. 13-14. Thus, I understand that the Board has not provided any explicit claim constructions in contradiction to those in the Cisco district court case and that the Board acknowledges the Cisco

district court case; hence, I am guided in my analysis by claim constructions in the Cisco district court case for relevant claim terms explicitly not construed by the Board.

A. "Network-Threat Indicators"

71. I understand that the district court in *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, No. 2:18-cv-00094, Dkt. 621 (E.D. Va.) adopted the following construction for the term "network-threat indicators" to mean:

District Court's Construction
Indicators of packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like.

Ex. 1027 at 39.

72. I understand that Petitioner proposes that the term "network-threat indicators" should be construed to mean "indicators that represent the identity of a resource associated with a network threat." (Petition at p. 17) However, as I note above, in its Institution Decision, the Board explicitly did not adopt this construction and provided no claim constructions in contradiction to those in the Cisco district court case. Institution Decision at p. 48.

73. For the purposes of my patentability analysis, I apply the district court's construction.

B. "Proxy System"

74. I understand that the district court adopted the following construction for the term "proxy system" to mean:

District Court's Construction
a proxy system which intervenes to prevent threats in communications between devices.

Ex. 1027 at 39.

75. I understand that Petitioner does not provide a proposed construction for this term. *See, e.g.,* Institution Decision at p. 48. Further, as I note above, in its Institution Decision, the Board did not provide any explicit claim constructions in contradiction to those in the Cisco district court case. Institution Decision at p. 48.

76. For the purposes of my patentability analysis, I apply the district court's construction.

VI. IN MY OPINION PETITIONER HAS FAILED TO SHOW THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

77. I understand that Petitioner challenges only independent claims 1, 24, and 25 and each challenged claim has similar limitations including: (1) "filtering" based on information specified by packet-filtering rules "the determined packets comprising the encrypted data;" (2) "network-threat indicators;" and (3) "routing, by the packet-filtering system, filtered packets to a proxy system based on a

determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators." Ex. 1001, cl. 1.

78. In my opinion, Petitioner fails to show that Buruganahalli alone or in combination with Baehr renders obvious the Challenged Claims for the following reasons.

A. In My Opinion, Buruganahalli Does Not Teach Rule-Based Filtering of Encrypted Packets

79. Buruganahalli does not teach rule-based filtering of encrypted packets, as recited in each of the Challenged Claims. '856 Patent, Claim 1 ("filtering… the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators"). Because, in my opinion, Buruganahalli expressly requires that encrypted packets be decrypted prior to applying its firewall policies/rules. Ex. 1004 at 7:39-51 (disclosing a whitelist/blacklist embodiment in which "a session associated with the network communications between the client and the remote server are decrypted if the destination domain is included in the blacklist"); *id*. at 7:60-67 (same).

1. In My Opinion, Buruganahalli Only Applies its Firewall Rules/Policies to Unencrypted or Decrypted Data

80. I note that Petitioner relies entirely on Buruganahalli for the claimed "filtering" of encrypted data. I understand that Petitioner equates Buruganahalli's firewall policies/rules, including the blacklist policy, to the claimed "plurality of

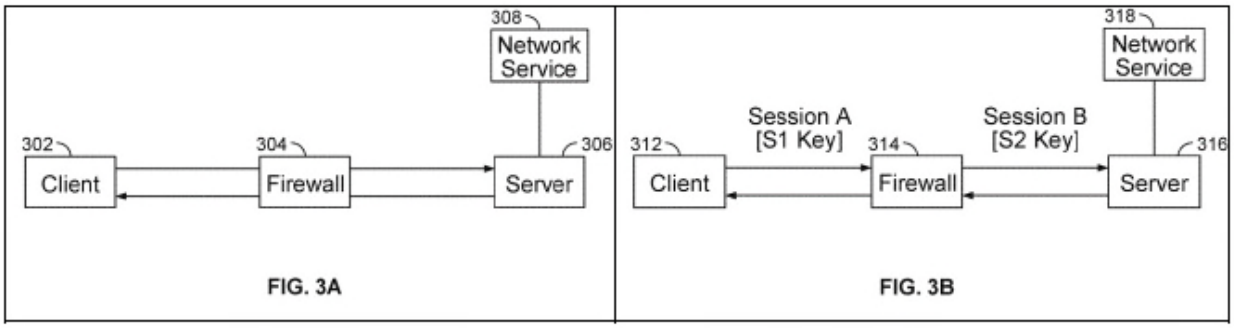
packet-filtering rules." *See* Pet. 29-30. Petitioner specifically cites to policies 620 in Buruganahalli's Figure 6. Pet. 29 (citing Ex. 1004 at 14:58-60, Fig. 6).

81. But a POSITA would understand that **policies 620** (which I have annotated in **red** below) are used by decoder 614 after decryption is performed by **SSL decryption engine 610**. Ex. 1004 at 14:8-15:3, Fig. 6. Further, a POSITA would understand that these policies are not applied to encrypted packets during the "handshake processing."

82. When encrypted packets are received by Buruganahalli's security device 402 (*e.g.*, a firewall), security device 402 performs decryption before using these policies for filtering. *Id.*; *see id.* at 12:29-32 (explaining that, in Fig. 3B, after setting up Sessions A and B, "any data that is communicated from the client 312 to the firewall 314 is decrypted using a session key S1 and is then inspected by the firewall 314"). A POSITA would understand that Buruganahalli's policy-based filtering is performed on ***decrypted*** data, not "packets comprising encrypted data" as claimed.[5]

[5] A POSITA would also understand that if the received packet is unencrypted, then decryption would not be necessary and **SSL decryption engine 610** would not be used. Ex. 1004 at 14:37-38. Either way, only unencrypted/decrypted packets are filtered.

83. As I noted above, Buruganahalli provides figures 3A and 3B, neither figure illustrates rule-based filtering of encrypted packets: (1) using policies to filter unencrypted packets (*i.e.*, hello messages) without needing decryption (Fig. 3A); and (2) using policies to filter data only after decrypting encrypted packets (Fig. 3B):



Buruganahalli, Figs. 3A (left) and 3B (right). I note that the Board correctly acknowledges that "Figure 3B's embodiment differs from Figure 3A's embodiment." ID at 70. These figures cover the three scenarios (which I discussed above) of whitelisting based on an unencrypted packet (Fig. 3A), blacklisting and blocking a session before it starts (Fig. 3A), and blacklisting based on an unencrypted packet but allowing and decrypting the subsequent encrypted session (Fig. 3B).

84. In my opinion, rather than performing policy-based filtering of encrypted packets, Buruganahalli splits the secure session and performs trusted man-in-the-middle decryption to apply its policies to **decrypted** data. Ex. 1004 at 8:45-54, 9:61-10:9, 11:59-12:61, 15:22-45, Figs. 3B, 8.

85. This is because firewall 304 "typically cannot decrypt the encrypted secure tunnel session traffic and, thus, cannot detect such firewall policy/rule violation(s)" without this approach. Ex. 1004 at 11:2-6, Fig. 3A. This decrypt-first approach is consistent with other portions of Buruganahalli describing this same process. Ex. 1004 at 5:62-6:1 ("if a new flow . . . violate[s] a policy prior to the set-up of the encrypted data communication . . . , then the flow can be blocked and decryption is not required"), 5:24-51 (early application of policy to the SNI extension of an unencrypted hello message so "the rest of the stream can be forwarded without any decryption"), 7:1-9 (no decryption required because the firewall uses "the SNI field [of unencrypted hello message] for applying a policy"), 7:39-51 (communications "are not decrypted if the destination domain is included in the whitelist").

86. Buruganahalli requires decryption to monitor encrypted packets. For example, Buruganahalli describes that "techniques for decrypting such secure communications are needed in order to monitor such encrypted data communications and to apply filtering based on a policy." Ex. 1004 at 4:19-22; *see id.* at 4:51-55 (destination domain information in encrypted data determined by "waiting until application data associated with the flow is decrypted"). Elsewhere Buruganahalli's system decrypts before filtering based on policies. *Id.* At 6:17-22, 7:7:39-51, 8:1-54, 9:61-10:9, 11:66-12, 12:29-32, 12:52-55, 12:59-61, 14:33-36,

14:60-15:3, 15:30-37, cl. 1 (communications "are decrypted" to verify that the destination domain extracted from the unencrypted client hello matches another domain), cl. 7 ("decrypt a monitored encrypted network communications"), cl. 8 ("decrypt encrypted traffic").

87. A POSITA would understand that Figure 3B only involves applying policies to decrypted packets. Ex. 1004 at 11:59-12:64, Fig. 3B. I understand that the Board rightly acknowledges this fact. ID 70-71 ("Buruganahalli explains that 'any data that is communicated from the client 312 to the firewall 314 is decrypted [. . .] and is then inspected by the firewall 314,' e.g., 'to monitor the session traffic for firewall policy/rule compliance.'") (citing Ex. 1004 at 12:29–32, 12:42–44).

2. In My Opinion, Figure 3A Embodiment Does Not Involve Applying Packet-Filtering Rules to Encrypted Packets

88. I understand that in view of Petition failing to show that Buruganahalli's firewall policies/rules are applied to encrypted packets, the Board turned to Figure 3A's embodiment,[6] relying on a statement that policies are applied "without 'having to decrypt'" encrypted communications. ID 71 (discussing

[6] I note that Petitioner never maps any disclosures related to Figure 3A to filtering encrypted packets. *See* Pet. at 38-39 (citing no disclosures from Ex. 1004 at 10:54-12:3).

applying rules to "hello message[s]") (citing Ex. 1004 at 11:7-19); *see* ID 22, 41, 53. I respectfully disagree with the Board's finding.

89. A POSITA looking at Buruganahalli's figure 3A embodiment would recognize that packet-filtering rules are never applied to encrypted packets, *with or without* decryption. This is because Buruganahalli discloses that the "typical firewall" of figure 3A "typically cannot decrypt the encrypted secure tunnel session traffic and, thus, cannot detect such firewall policy/rule violation(s)." Ex. 1004 at 10:57-61, 11:2-6. Buruganahalli's solution to this problem is to extract a destination domain from the unencrypted handshake traffic so that its "firewall policies/rules" may be applied "*prior to and/or without having to decrypt* the encrypted secure tunnel session traffic." *Id*. At 11:7-19. This technique, which is explained more fulsomely earlier in Buruganahalli, refers to the firewall's ability to determine whether a new flow "violate[s] a policy *prior to the set-up* of the encrypted data communication" so that "the flow can be blocked and decryption is not required," whereas the session is allowed without any filtering of encrypted packets if the domain is trusted. Ex. 1004 at 5:62-6:11; *see also id.* At 7:52-59 ("a session associated with the network communications between the client and the remote server are not decrypted if the destination domain is included in a whitelist of the whitelist/blacklist policy").

90. Buruganahalli's disclosure of a typical firewall applying policies to secure protocol communications "prior to and/or without having to decrypt the encrypted secure tunnel session traffic" does not mean that any packet-filtering rules satisfying the "filtering" limitations are applied to encrypted packets. Ex. 1004 at 11:17-19. Instead, the policies are applied to **unencrypted** packets before an encrypted session ever begins (prior to beginning the encrypted session), making decryption entirely unnecessary because the session is either allowed without subjecting the encrypted packets to any filtering or blocked before any encrypted packets are received (without having to decrypt the encrypted packets). Specifically, the firewall applies a policy to an unencrypted hello message[7] and then decides whether to prevent the entire encrypted session before it ever begins, and if the session is allowed, encrypted packets are passed without decryption or filtering Ex. 1004 at 10:57-61 ("In that session, a typical firewall can initially just inspect the handshake traffic (e.g., the initial negotiation to setup a secure communication channel/tunnel between a client and a remote server), as all the application data is encrypted."); *see also* 10:54-11:58; *see id.* At 4:16-44, 5:24-6:1.

[7] I note that Petitioner admits a hello message is unencrypted. Pet. 30 (relying on hello message as "unencrypted data"); Ex. 1004 at 5:27-35.

91. As such, the policies in figure 3A are applied "prior to and/or without having to decrypt" any encrypted traffic, but also without applying packet-filtering rules to encrypted packets. Ex. 1004 at 11:7-19 ("prior to and/or without having to decrypt" encrypted packets"), 4:31-44 (policy-based filtering is "prior to the set-up of the encrypted data communication."). Given that Buruganahalli only applies policies to unencrypted packets to block a secure session before encrypted packets are received or to decrypted data, it is my opinion that Buruganahalli does not teach the claimed rule-based filtering of encrypted packets.

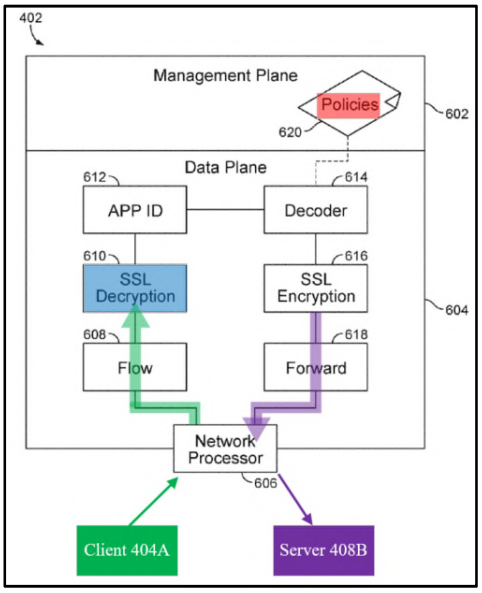
3. In My Opinion, Petitioner Has Not Identified a Single Instance Where Buruganahalli Teaches Filtering Encrypted Packets

92. Although Petitioner never asserts a combination of Buruganahalli's Figures 3A and 3B, I note that the institution decision seemingly combines them, alleging: "Buruganahalli discloses using techniques according to Figure 3A's embodiment separately or together with techniques according to Figure 3B's embodiment." ID 71 (citing Ex. 1004 at 11:7-12:3). I respectfully disagree.

93. Buruganahalli merely suggests that firewall 304 may switch from operating as shown in Figure 3A's embodiment (filtering unencrypted packets or just passing encrypted packets if whitelisted) to operating as shown in Figure 3B's embodiment (splitting the secure session to perform man-in-the-middle decryption). Ex. 1004, 6:12-38, 7:39-67, 8:25-54, 9:61-10:4, 11:59-12:64. In my

opinion, this still does not fix the issue, as neither Figure 3A or 3B filter encrypted packets using policies.

94. I also note that the Board incorrectly relied on Buruganahalli's flow lookup related to the TLS handshake and operation of decoder 614 in Figure 6. ID 69 (citing Ex. 1004 at 14:21-33, 14:50-55). As an initial matter, the Petition and Board's institution decision both point to Buruganahalli's flow lookup for limitations [1.b] and [1.c] of "identifying" unencrypted and encrypted packets, respectively. Pet. 30-32; ID 60-62. However, there is another separate intermediate step (*i.e.*, the "determining" step). As shown in figure 6, Buruganahalli's flow lookup 608 is performed on encrypted packets without applying **policies**, **decryption engine 610** decrypts the encrypted packets, and then decoder 614 applies **policies** to the decrypted data:



Buruganahalli, Fig. 6 (annotated)

Ex. 1004 at 14:8-15:3, Fig. 6. I note that Buruganahalli never discloses (and the Petition never asserts) that flow lookup uses policies to filter encrypted packets. Ex. 1004 at 14:25-33.

95. It is my opinion that in no instance does Buruganahalli apply its policies to encrypted packets. And neither the Petition nor the institution decision identify any contrary disclosure. Buruganahalli always decrypts encrypted packets before applying its policies.

4. In My Opinion, Petitioner Attempts to Rewrite Buruganahalli's Decrypt-First Approach with Conclusory Statements About a Skilled Artisan's Understanding and Obviousness

96. It is my opinion that Petitioner recognizing that Buruganahalli does not disclose filtering encrypted data, Petitioner tries twice to fill this gap: by first making conclusory statements about a skilled artisan's understanding and second alleging a motivation to rewrite Buruganahalli. Pet. 38.

97. First, Petitioner states that "a POSITA would have understood that the packets communicated as part of a secure session are filtered after a determination that a handshake message that initiates the session includes data that corresponds to the network threat indicator (*e.g.*, a blacklisted destination domain)." Pet. 38. This is wrong.

98. Petitioner's statement ignores that the claims require filtering encrypted data based on specific rules and that Buruganahalli's "packets

communicated as part of a secure session" are decrypted before any policy-based filtering. *See* Ex. 1004 at 11:2-6, 12:29-32, 12:59-61, 15:35-45.

99. Petitioner also makes another unsupported statement that the destination domain in the handshake message and encrypted data are correlated: "the handshake message comprises data (e.g., destination domain) that also applies to the encrypted data of the session, such that the security risks associated with the handshake message and encrypted data are correlated." Pet. 38. This too is incorrect.

100. Buruganahalli discloses that encrypted packets must be decrypted in order to determine whether the extracted destination domain name matches the domain associated with the session's URL "in order to detect malware that attempts to fool a hosting site by including false destination domain information." Ex. 1004 at 8:11-24.

101. Petitioner next contends that "a POSITA would have been motivated and found it obvious in view of Buruganahalli to filter the encrypted data of a secure session that was initiated by a handshake message with data corresponding to a network-threat indicator in order to monitor transmission, into or out of a protected network, of data that potentially presents a security risk." Pet. 38-39. I disagree for the following reasons.

102. First, Petitioner's contention that a skilled artisan would be motivated "to monitor transmission, into or out of a protected network, of data that potentially presents a security risk" does not point in the direction of the Challenged Claims. Buruganahalli *already* monitors encrypted traffic.

103. Second, Petitioner's purported motivation ignores the key limitation in the filtering step, which requires the filtering of encrypted packets to be "based on" information specified by the claimed rules. Petitioner does not mention polices at all. A skilled artisan would not apply policies to filter encrypted packets without first decrypting the packets, as Buruganahalli teaches.

104. Third, Petitioner provides no explanation that a skilled artisan would have expected success. As I discuss further below, the problem of detecting threats in encrypted communications session was an considered an "unsolvable" problem, right up to the moment that Cisco copied and incorporated Centripetal's technology into its Stealthwatch product.

B. In My Opinion, Petitioner Has Not Shown that Buruganahalli Teaches the Claimed "Network-Threat Indicators"

105. I understand that all three independent challenged claims recite "network-threat indicators" multiple times. Ex. 1001, claims 1, 24, 25. In my opinion, Petitioner has not shown the prior art discloses "network-threat indicators" because Buruganahalli does not teach that the destination domains on its blacklist indicate network threats.

106. Petitioner relies on the destination domains on Buruganahalli's blacklist for the "network-threat indicators." Pet. 29-30, 32-34. However, a POSITA would recognize that Buruganahalli does not characterize the blacklist as being associated with network threats and is silent as to how the blacklist is formed. Ex. 1004 at 7:39-67. Buruganahalli merely describes that the destination domains on the blacklist are used to decide whether to block or decrypt packets. Ex. 1004 at 5:64-6:38, 7:39-67, 10:54-11:19, cl. 6. As such, it is my opinion that Buruganahalli does not teach that the blacklisted destination domains indicate network threats.

107. Rather than representing the "identity of a resource associated with a network threat" (per Petitioner's construction) or "packets associated with network threats, such as network addresses, ports, domain names, uniform resource locators (URLs), or the like" (per the district court's construction). Buruganahalli's blacklist is simply a list of domains that a network administrator has identified for monitoring or blocking. Ex. 1004 at 5:64-6:38; Ex. 2006 at 1:25-36; Ex. 2007, ¶ 0007 (an access control lists (ACL) "is a list of entries that grant or deny specific access rights to individuals or groups"). In fact, I note that Petitioner's expert characterized Buruganahalli's blacklist as a list of domains that represent ***potential*** threats:

> I think if -- in the full scope of Buru, because one of the potential actions to take on encrypted packets that might relate to HTTP sessions or SSL sessions is to decrypt and look for concerning patterns. To me, then, the domain name, URI, is -- Buru is -- the blacklists in question here are **potential** network threats. Because it's not necessarily blocking every blacklist. Handshake, all right, some are going through and then we do deeper analysis, there is deeper analysis in some cases.

Weissman Tr. at 60:12-22 (emphasis added); *see also id*. at 59:14-22 (testifying that Buruganahalli does not disclose that blacklisted domains are a threat).

108. Petitioner provides another conclusory statement about a skilled artisan's supposed knowledge: "[a] POSITA would have understood that data on the blacklist, as taught in Buruganahalli, comprises network-threat indicators (*e.g.*, whether a destination domain presents a security risk) as the data would be compiled based on 'identification of new, zero-day threats, new vulnerabilities, prevent false positives, and/or provide a feedback loop for any of such activities or trends aggregated and correlated using the security cloud service.'" Pet. 30 (citing Ex. 1004 at 13:43-52). I disagree.

109. The relied upon portion of Buruganahalli merely describes using security device 402 (which includes the firewall) to report destination domains to a security service cloud 410 remote from the firewall. It is the security service cloud 410—not Buruganahalli's firewall having the blacklist—that identifies threats,

vulnerabilities, etc. Buruganahalli does not teach or disclose security service cloud 410 providing the destination domains that it identifies as network threats to Buruganahalli's firewall for inclusion on the blacklist.

C. In My Opinion, the Prior Art Does Not Teach the Claimed Routing Filtered Packets to a Proxy System

110. I understand that each challenged claim recites "[routing/route], by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators" (the "routing step"). Ex. 1001, claims 1, 24, 25. In my opinion, Buruganahalli's firewall does not route filtered packets to a proxy system for the reasons as follows.

1. In My Opinion, Buruganahalli Does Not Disclose the Claimed Routing Filtered Packets to a Proxy System

111. Petitioner asserts that "Buruganahalli discloses that if the filtered packets correspond to a network-threat indicator, *e.g.*, 'if the destination domain is included in the blacklist,' then the encrypted data communications are sent to a 'decrypt engine' of the firewall to be 'decrypted'". Pet. 39 (citing Ex. 1004 at 7:39-51, 7:60-67, 9:61-67). I disagree.

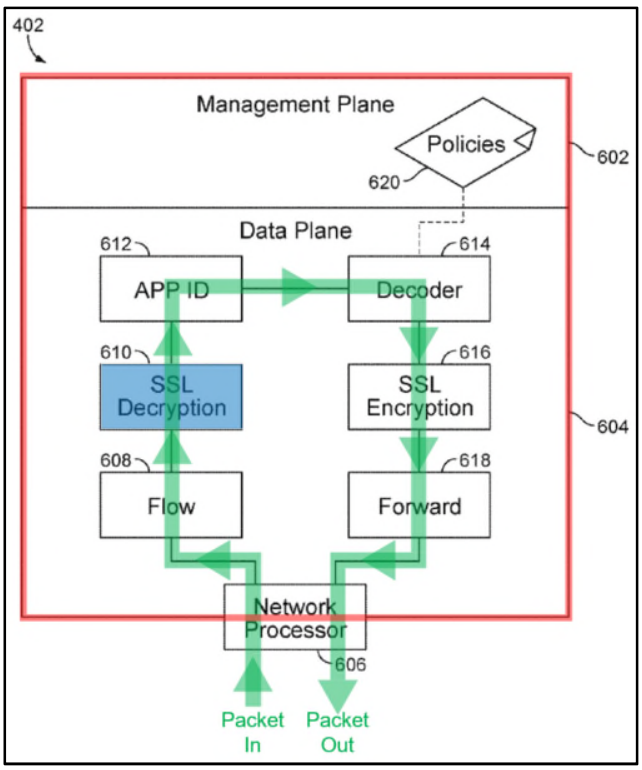
112. As I established above, no filtering of encrypted packets occurs until ***after*** they have been decrypted, so the decrypt engine cannot receive filtered

packets—it decrypts traffic so that the firewall can monitor and filter decrypted packets.

113. I also note that Petitioner equates Buruganahalli's "decrypt engine" with the claimed "proxy system." Pet. 39. This is incorrect.

114. Buruganahalli's decrypt engines 110, 610 are not a proxy, and Petitioner never even attempted to demonstrate that it satisfies the proper construction of the term, which is "a proxy system which intervenes to prevent threats in communications between devices." Ex. 1027 at 39; Ex. 1030 at 33-34, 36

115. Buruganahalli's decrypt engines 110, 610 perform one step (*i.e.*, decryption) of the firewall's own filtering process without "interven[ing] to prevent threats in communications between devices." Ex. 1004 at 14:21-60. This technique is illustrated in the drawing reproduced below showing the **packet flow** through Buruganahalli's **firewall** in which **decrypt engine 610** performs decryption in the middle of the process:



Buruganahalli, Fig. 6 (annotated)

116. In my opinion, the above drawing demonstrates that Buruganahalli's decrypt engines 110, 610 do not meet the proxy system construction I have applied. I understand that on cross-examination Petitioner's expert could not articulate any reason why the firewall's decrypt engine would be considered a proxy system while other functional blocks within the firewall would not be, stating that he had not "really given it a ton of thought" and finally settling on the idea that the proxy has "to carry out certain special functions" that "the normal network… implementation would do." Weissman Tr. at 50:4-5, 51:20-21, 52:2-4. But Buruganahalli's use of decryption to filter encrypted network traffic was the

common solution at the time of Buruganahalli, so its use in this instance does not represent any "certain special functions." *Id.*

117. Petitioner also relies Buruganahalli's Figure 3B as allegedly disclosing proxy-like functionality. *See* Pet. 39-40. This too is wrong.

118. The decrypt engine merely functions to carry out the firewall's own decryption process.

2. In My Opinion, a Skilled Artisan Would Not Have Been Motivated to or Would Reasonably Expect Success Modifying Buruganahalli in View of Baehr

119. I understand that Ground 2 of the Petition relies on Buruganahalli in combination with Baehr. Pet. 42-50. In my opinion, a POSITA would not have had a reasonable expectation of success.

a. In My Opinion, the Proposed Combination Does Not Meet the Claim Elements

120. I understand that Petitioner states that "Buruganahalli's techniques characterizing a transparent proxy function would have been implemented in a proxy system separate from and external to the firewall." Pet. 47. Petitioner never identifies what is meant by "transparent proxy function[s]." And, even then, this vague assertion is not a reason why a skilled artisan would do anything. Petitioner never states what in Buruganahalli would be implemented in Baehr's proxy system and thus it is not clear whether the packets routed to Baehr's proxy would have been filtered first without decryption, particularly because Buruganahalli does not

filter before decrypting. Further, as I mention above, Baehr was filed before the existence of the TLS protocol; hence, a person of ordinary skill in the art would understand that Baehr was not designed to work with TLS.

121. As for Baehr's proxy in general, Petitioner does not indicate whether the purported proxy would be implemented as a physically separate device or merely a logically separate device somewhere in the combination. *Compare* Pet. 44 (handing off filtered traffic "to dedicated proxy servers as an alternative [to] performing the proxy functions internally") *with id.* at 47 (proxy network can merely be a "separate logical entity" internal to the filtering system). The latter "separate logical entity" combination is no different from Buruganahalli's components. Ex. 1004 at 14:8-11, Fig. 6.

122. As for a physically separate proxy, Petitioner has identified no benefit to using a physically separate proxy for encrypting and forwarding packets over Buruganahalli's use of logical components for encryption engine 616 and forwarding module 618 that Petitioner seems to acknowledge already exist in Buruganahalli. Ex. 1004 at 2:24-31, 14:8-12, 14:57-58, Fig. 6. A POSITA would have known that adding a physically separate proxy increases costs due to additional interfaces needed between the firewall and new proxy, increased power consumption from a separate device, and transmission delay in processing. Ex. 1005 at 3:59-64, Fig. 5 (adding interface 420).

b. In My Opinion, Petitioner Does Not Provide Any Persuasive Reason for Why a Skilled Artisan Would Implement its Proposed Combination Using Baehr

123. In my opinion, Petitioner has not shown why a skilled artisan would have been motivated to make the asserted combination to meet the claims—whatever it is.

124. As I explained above, Buruganahalli does not disclose the routing element. Buruganahalli does not disclose a proxy system and the only action left for its firewall after the firewall inspects the decrypted data is to re-encrypt the data and forward it to the client or server. Ex. 1004 at 12:56-61. Baehr's proxy network 430 does not fill this gap. Pet. 45-46.

125. Baehr's proxy network 430 is for mirroring host devices in a private network, not for performing packet-forwarding and encryption. Ex. 1005, Abstract, 4:26-63, 8:13-17, 8:36-46, Fig. 6. For example, Baehr teaches redirecting packets to a mail proxy 440 that can provide the email functionality of the mail host 360 in the private network. *Id.* Baehr describes screen 340 itself performing actions such as encryption, and does not provide a reason for offloading encryption from a firewall to a proxy. *Id.* at 7:8-10, 7:45-54;.

126. As for specific motivations, Petitioner alleges that Baehr teaches the proxy network as "advantageous for various reasons." Pet. 46. The first reason given is to isolate the private network. *Id.*; *see also* Pet. 47-48 (regurgitating this

same reason as though it provides "added advantages"). A POSITA would not have found this as a motivation to combine because Buruganahalli's firewall already isolates the client from the server by creating split sessions. Ex. 1004 at 12:4-55, Fig. 3B. As such, there's no isolation advantage over Buruganahalli.

127. The second reason given (which dovetails with the first) is to provide seamless communication with outsiders. Pet. 46. Again, this is not an advantage over Buruganahalli's firewall, which also provides seamless communication with the server as if the server was communicating with the client. Ex. 1004 at 12:4-55, Fig. 3B.

128. I note that Petitioner also contends that the combination "reduce[s] load on a firewall" by "'hand[ing] off' filtered traffic to dedicated proxy servers as an alternative [to] performing the proxy functions internally." Pet. 44. Petitioner once again does not indicate what it means by internal "proxy functions." Petitioner does not identify any portion of Buruganahalli as teaching a reason to hand off whatever is intended by these internal proxy functions. *See* Pet. 44. Likewise, Petitioner does not identify any portion of Baehr that teaches, for example, its screen 340 handing off functions to its proxy network. Instead, Baehr's proxy network has proxy hosts 435 that perform the functions of the hosts in the private network—not the functions of the screen 340. Ex. 1005 at 4:20-63. Indeed, there is no rationale for modifying Buruganahalli to perform a hand-off

that meets the claims. The only alleged support for this hand-off argument is "NIST, 14" and "Weissman, ¶150." Pet. 44. But, NIST describes a firewall handing off traffic to a proxy server to "perform filtering or logging" (Ex. 1036 at 25). Thus, it is my opinion that it does not teach the routing element.

129. Moreover, a POSITA would have known that there is no net reduced load achieved by somehow adding a proxy to Buruganahalli and that adding such a proxy could introduce additional network delays. The claims require routing "filtered" packets to the proxy system. After Buruganahalli filters packets, the only task left is to encrypt (if necessary) and forward them to the client or server. Whether the forwarding and possible encryption is done by the firewall or a proxy device, the overall computational workload of the system is the same, but the additional routing and transferring could introduce additional network delays, and Petitioner has not alleged there is an actual net reduction in overall workload or network delays in its proposed combination. *Id.* And if Baehr's proxy is implemented as an internal logical entity as Petitioner suggests at one point (Pet. 47), the lack of load reduction is even more apparent as the internal workload would not change at all, but the internal routing required in this alleged combination could nevertheless increase network delays.

130. Petitioner next asserts motivations of "preserving computing resources, achieving load balancing, and maximizing performance." Pet. 47. I disagree with these motivations.

131. Each of these attributes—computing resources, load balancing, and performance—would be unchanged or made worse under Petitioner's theory (Pet. 47) of implementing Baehr's proxy as an internal logical entity. The computing resources, load balancing, and performance would be the same or made worse, as I explain above and below.

132. Petitioner cites Exhibit 1036 ("NIST") for support, but that exhibit does not explain that computing resources are preserved. Ex. 1036 at 14. The overall system would use the same amount of computing resources whether or not a separate proxy system is used—the only difference would be the distribution of those resources together with additional routing and transferring of data. *See* Ex. 1036 at 14 (describing that dedicated proxy servers are used in addition to firewalls).

133. It is also unclear how the proposed combination achieves load balancing. Load balancing in the context of network traffic typically refers to balancing the traffic across multiple similar devices. Ex. 1036 at 17 ("load balancing" is when "two or more firewalls are employed"), 58 (load balancing involving shifting traffic to "backup firewall"). In my opinion, that would not lead

a skilled artisan to modify Buruganahalli to add a proxy system for receiving filtered packets, but rather to add one or more additional firewalls to share the load with Buruganahalli's single firewall.

134. Petitioner also incorrectly assumes Buruganahalli is limited to using the same component (*e.g.*, same processor) for performing the filtering and proxy functions. But there is no need for load balancing where the filtering and proxy functions (*e.g.*, decryption and encryption) are implemented with dedicated logical components, as in Buruganahalli's firewall. Ex. 1004 at 14:8-12, 14:57-58. In that case, the load is already balanced among the different logical components. Moreover, Petitioner's Exhibit 1036 does not describe load balancing that involves relocating decryption functionality from a firewall to proxy servers. *See* Ex. 1036 at 14-16.

135. Finally, the Petition does not explain how adding a proxy maximizes performance or what metric is used for measuring performance here.

136. Given the foregoing, a skilled artisan would not have incurred the additional cost of adding a proxy system to Buruganahalli. Likewise, the added complexity of incorporating a proxy system into Buruganahalli would have discouraged a skilled artisan from such modification. *Id.*; Ex. 1005 at 3:59-64, Fig. 5 (adding interface 420). The increased cost and complexity far outweigh any benefit.

VII. IN MY OPINION, THE OBJECTIVE EVIDENCE OF NONOBVIOUSNESS ALSO DEMONSTRATES THAT THE CLAIMS ARE VALID

A. The ’856 Patent Satisfied a Long-Felt Need in the Industry and Received Substantial Industry Praise

137. The ’856 Patent satisfied a long-felt need and industry praise, contributed to the court’s validity determination and enhanced verdict of willful infringement in the Cisco litigation. Ex. 1027 at 58, 61-65.

138. Petitioner’s Exhibit 1027 twice reproduces a Cisco press release from 2017 called PTX-1135 (Ex. 2013). The Cisco press release is evidence of long-felt need and industry recognition for the technology claimed in the ’856 Patent because it describes the problem of detecting threats in encrypted traffic as “unsolvable” and the ’856 Patent solves that problem with its steps of “determining” and “filtering,” based on rule criteria, “the determined packets comprising the encrypted data….” Ex. 1027 at 64; Ex. 1001, claim 1.

139. Regarding the Cisco press release, I understand that the district court noted “Cisco’s technical and marketing documents which contribute the addition of the infringing functionality as a ‘breakthrough’ in building ‘an intelligent platform with unmatched security.’” Ex. 1027 at 137.

VIII. CONCLUSION

140. For the reasons I explained above, it is my opinion that Petitioner has failed to show that any Challenged Claim is unpatentable over

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

Executed on August 26, 2022, in Toronto, Ontario, Canada.



Michael T. Goodrich, Ph.D.

APPENDIX A

CURRICULUM VITAE

Michael T. Goodrich

Dept. of Computer Science
Bren School of Info. & Computer Sciences
University of California, Irvine
Irvine, CA 92697-3435

E-mail: goodrich (at) acm.org
http://www.ics.uci.edu/~goodrich/
Office Phone: (949)824-9366

CITIZENSHIP: U.S.A.

EDUCATION

Ph.D.	1987	*Efficient Parallel Techniques for Computational Geometry* Computer Science, Purdue Univ. (M.J. Atallah, advisor)
M.S.	1985	Computer Science, Purdue Univ.
B.A.	1983	Mathematics and Computer Science, Calvin Univ.

PROFESSIONAL EXPERIENCE

July '19 to present	Distinguished Professor, Dept. of Computer Science Univ. of California, Irvine
April '07 to June '19	Chancellor's Professor, Dept. of Computer Science Univ. of California, Irvine
July '12 to June '13	Chair, Dept. of Computer Science Univ. of California, Irvine
October '06 to June '12	Assoc. Dean for Faculty Dev., Bren School of Info. and Comp. Sci. Univ. of California, Irvine
July '01 to March '07	Professor, Dept. of Computer Science Univ. of California, Irvine
Fall '00	Visiting Professor of Computer Science Brown Univ.
July '96 to June '02	Professor of Computer Science (on leave, from July '01) Johns Hopkins Univ.
July '92 to June '96	Associate Professor of Computer Science Johns Hopkins Univ.
Spring '94	Visiting Associate Professor of Computer Science Univ. of Illinois, Urbana-Champaign
July '87 to June '92	Assistant Professor of Computer Science Johns Hopkins Univ.

RESEARCH INTERESTS

Algorithm and data structure design
Information assurance, privacy, and security
Principles of database, machine learning, and typesetting systems
Parallel and distributed computing
Information visualization, computer graphics, and computational geometry

PRIZES, HONORS, AND AWARDS

- *Compere Loveless Fellowship in Computer Sciences*, Purdue Univ., 1985
- *Research Initiation Award*, National Science Foundation, 1988
- *Oraculum Award for Excellence in Teaching*, Johns Hopkins, 1993, 1994, 1995
- *ACM Recognition of Service Award*, 1996
- *Robert B. Pond, Sr. Award for Excellence in Undergraduate Teaching*, Johns Hopkins, 1998
- *Elected Senior Member*, the Institute of Electrical and Electronics Engineers (IEEE), 1999

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 75

- *Spirit of Technology Transition Award*, DARPA Dynamic Coalitions Program, 2002
- *Brown Univ. Award for Technological Innovation* (with R. Tamassia, N. Triandopoulos, D. Yao, and D. Ellis), 2006
- *ACM Distinguished Scientist*, 2006
- *2006 IEEE Computer Society Technical Achievement Award*, "for outstanding contributions to the design of parallel and distributed algorithms for fundamental combinatorial and geometric problems"
- *Fulbright Scholar*, 2007, for senior specialist service to University of Aarhus, Denmark
- *Fellow of the San Diego Supercomputer Center*, 2007
- *Fellow of the American Association for the Advancement of Science (AAAS)*, "for distinguished contributions to parallel and distributed algorithms for combinatorial and geometric problems, and excellence in teaching, academic and professional service, and textbook writing," 2007
- *Named as Chancellor's Professor*, for "demonstrated unusual academic merit and whose continued promise for scholarly achievement is unusually high," Univ. of California, Irvine, 2007
- *Fellow of the Institute of Electrical and Electronics Engineers (IEEE)*, "for contributions to parallel and distributed algorithms for combinatorial and geometric problems," 2009
- *Fellow of the ACM*, "for contributions to data structures and algorithms for combinatorial and geometric problems," 2009
- *ICS Dean's Award for Research*, "for contributions in the area of parallel and distributed algorithms," 2014
- *Chancellor's Award for Excellence in Fostering Undergraduate Research*, Univ. of California, Irvine, 2016
- *Faculty Mentor of the Month*, Undergraduate Research Opportunities Program (UROP), Univ. of California, Irvine, April 2016
- *Elected as a foreign member*, Royal Danish Academy of Sciences and Letters, April 2018
- *Named as Distinguished Professor*, for achieving "the highest levels of scholarship" over the course of a career and having "earned national and international level distinctions and honors of the highest level," Univ. of California, Irvine, 2019

PUBLICATIONS

Google Scholar Citation Statistics:

- Total citations: over 16,300
- H-index (top H publications with at least H citations): 71

Patents and Patent Applications:

P-1. G. Ateniese, B. de Medeiros, and M.T. Goodrich, "Intermediated Delivery Scheme for Asymmetric Fair Exchange of Electronic Items," U.S. Patent Application US 2004/0073790 A1, April 15, 2004.

P-2. M.T. Goodrich and R. Tamassia, "Efficient Authenticated Dictionaries with Skip Lists and Commutative Hashing," U.S. Patent 7,257,711, August 14, 2007.

P-3. J.W. Green, J.L. Schultz, Y. Amir, and M.T. Goodrich, "High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling," U.S. Patent 7,299,219, November 20, 2007.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 76

P-4. R. Tamassia, M.T. Goodrich, N. Triandopoulos, and C. Papamanthou, "Authentication for Operations over an Outsourced File System Stored by an Untrusted Unit," International Patent Application PCT/US2007/024642, WO 2008/147400, filed November 20, 2007, published December 4, 2008.

P-5. R. Tamstorf, M.T. Goodrich, D. Eppstein, "Attribute Transfer Between Computer Models Including Identifying Isomorphic Regions in Polygonal Meshes," U.S. Patent 8,681,145, March 25, 2014. (also Application US 2010/0238166 A1, September 23, 2010).

P-6. N. Triandopoulos, M.T. Goodrich, D. Nguyen, O. Ohrimenko, C. Papamanthou, R. Tamassia, C.V. Lopes, "Techniques for Verifying Search Results Over a Distributed Collection," U.S. Patent, 9,152,716, October 6, 2015.

Books and Monographs:

B-1. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java*, John Wiley and Sons, Inc., 1998.

B-2. M.T. Goodrich and C.C. McGeoch, eds., *Algorithm Engineering and Experimentation*, Lecture Notes in Computer Science (LNCS), Vol. 1619, Springer-Verlag, 1999.

B-3. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Second Edition*, John Wiley and Sons, Inc., 2001.

B-4. M.T. Goodrich and R. Tamassia, *Algorithm Design: Foundations, Analysis, and Internet Examples*, John Wiley and Sons, Inc., 2002.

B-5. M.T. Goodrich and S.G. Kobourov, eds., *10th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science, Vol. 2528, Springer-Verlag, 2002.

B-6. M.T. Goodrich, R. Tamassia, and D. Mount, *Data Structures and Algorithms in C++*, John Wiley and Sons, Inc., 2004.

B-7. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Third Edition*, John Wiley and Sons, Inc., 2004.

B-8. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Fourth Edition*, John Wiley and Sons, Inc., 2006.

B-9. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Fifth Edition*, John Wiley and Sons, Inc., 2011.

B-10. M.T. Goodrich and R. Tamassia, *Introduction to Computer Security*, Addison-Wesley, Inc., 2011.

B-11. M.T. Goodrich, R. Tamassia, and D. Mount, *Data Structures and Algorithms in C++, Second Edition*, John Wiley and Sons, Inc., 2011.

B-12. M.T. Goodrich, R. Tamassia, and M. Goldwasser, *Data Structures and Algorithms in Python*, John Wiley and Sons, Inc., 2013.

B-13. M.T. Goodrich, R. Tamassia, and M. Goldwasser, *Data Structures and Algorithms in Java, Sixth Edition*, John Wiley and Sons, Inc., 2014.

B-14. M.T. Goodrich and R. Tamassia, *Algorithm Design and Applications*, Wiley, 2015.

Book Chapters:

Ch-1. M.J. Atallah and M.T. Goodrich, "Deterministic Parallel Computational Geometry," in *Synthesis of Parallel Algorithms*, J.H. Reif, ed., Morgan Kaufmann, 497–536, 1993.

Ch-2. M.T. Goodrich, "The Grand Challenges of Geometric Computing," in *Developing a Computer Science Agenda for High-Performance Computing*, U. Vishkin, ed., ACM Press, 64–68, 1994.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 77

Ch-3. M.T. Goodrich, "Parallel Algorithms in Geometry," *CRC Handbook of Discrete and Computational Geometry*, J.E. Goodman and J. O'Rourke, eds., CRC Press, Inc., 669–682, 1997.

Ch-4. M.T. Goodrich and K. Ramaiyer, "Geometric Data Structures," *Handbook of Computational Geometry*, J.-R. Sack and J. Urrutia, eds., Elsevier Science Publishing, 463–489, 2000.

Ch-5. M.T. Goodrich and R. Tamassia, "Simplified Analyses of Randomized Algorithms for Searching, Sorting, and Selection," *Handbook of Randomized Computing*, S. Rajasekaran, P.M. Pardalos, J.H. Reif, and J.D.P. Rolim, eds., Kluwer Academic Publishers, Vol. 1, 23–34, 2001.

Ch-6. M.T. Goodrich, "Parallel Algorithms in Geometry," *Handbook of Discrete and Computational Geometry, Second Edition*, J.E. Goodman and J. O'Rourke, eds., Chapman & Hall/CRC Press, Inc., 953–967, 2004. (Revised version of Ch-3.)

Ch-7. C. Duncan and M.T. Goodrich, "Approximate Geometric Query Structures," *Handbook of Data Structures and Applications*, Chapman & Hall/CRC Press, Inc., 26-1–26-17, 2005.

Ch-8. M.T. Goodrich, R. Tamassia, and L. Vismara, "Data Structures in JDSL," *Handbook of Data Structures and Applications*, Chapman & Hall/CRC Press, Inc., 43-1–43-22, 2005.

Ch-9. Y. Cho, L. Bao and M.T. Goodrich, "Secure Location-Based Access Control in WLAN Systems," *From Problem Toward Solution: Wireless and Sensor Networks Security*, Zhen Jiang and Yi Pan, eds., Nova Science Publishers, Inc., Chapter 17, 2007.

Ch-10. M.T. Goodrich and M.J. Nelson, "Distributed Peer-to-Peer Data Structures," *Handbook of Parallel Computing: Models, Algorithms and Applications*, R. Rajasekaran and J. Reif, eds., CRC Press, 17-1–17-17, 2008.

Ch-11. C.A. Duncan and M.T. Goodrich, "Planar Orthogonal and Polyline Drawing Algorithms," *Handbook of Graph Drawing and Visualization*, CRC Press, Inc., 223–246, 2013.

Ch-12. M.T. Goodrich, R. Tamassia, and L. Vismara, "Data Structures in JDSL," *Handbook of Data Structures and Applications*, 2nd edition, Chapman and Hall/CRC, Taylor & Francis, Inc., 43-1–43-22, 2018.

Journal Papers:

J-1. M.J. Atallah and M.T. Goodrich, "Efficient Parallel Solutions to Some Geometric Problems," *Journal of Parallel and Distributed Computing*, **3**(4), 1986, 492–507.

J-2. M.T. Goodrich, "Finding the Convex Hull of a Sorted Point Set in Parallel," *Information Processing Letters*, **26**, 1987, 173–179.

J-3. H. ElGindy and M.T. Goodrich, "Parallel Algorithms for Shortest Path Problems in Polygons," *The Visual Computer*, **3**(6), 1988, 371–378.

J-4. M.J. Atallah and M.T. Goodrich, "Parallel Algorithms For Some Functions of Two Convex Polygons," *Algorithmica*, **3**, 1988, 535–548.

J-5. M.J. Atallah, R. Cole, and M.T. Goodrich, "Cascading Divide-and-Conquer: A Technique for Designing Parallel Algorithms," *SIAM Journal on Computing*, **18**(3), 1989, 499–532.

J-6. M.T. Goodrich, "Triangulating a Polygon in Parallel," *Journal of Algorithms*, **10**, 1989, 327–351.

J-7. M.T. Goodrich and M.J. Atallah, "On Performing Robust Order Statistics in Tree-Structured Dictionary Machines," *Journal of Parallel and Distributed Computing*, **9**(1), 1990, 69–76.

J-8. M.T. Goodrich and J.S. Snoeyink, "Stabbing Parallel Segments with a Convex Polygon," *Computer Vision, Graphics and Image Processing*, **49**, 1990, 152–170.

J-9. J. Johnstone and M.T. Goodrich, "A Localized Method for Intersecting Plane Algebraic Curve Segments," *The Visual Computer*, **7**(2–3), 1991, 60–71.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 78

J-10. M.T. Goodrich, "Intersecting Line Segments in Parallel with an Output-Sensitive Number of Processors," *SIAM Journal on Computing*, **20**(4), 1991, 737–755.

J-11. R. Cole and M.T. Goodrich, "Optimal Parallel Algorithms for Point-Set and Polygon Problems," *Algorithmica*, **7**, 1992, 3–23.

J-12. M.T. Goodrich, "A Polygonal Approach to Hidden-Line and Hidden-Surface Elimination," *Computer Vision, Graphics, and Image Processing: Graphical Models and Image Processing*, **54**(1), 1992, 1–12.

J-13. M.T. Goodrich, S. Shauck, and S. Guha, "Parallel Methods for Visibility and Shortest Path Problems in Simple Polygons," *Algorithmica*, **8**, 1992, 461–486, with addendum in *Algorithmica*, **9**, 1993, 515–516.

J-14. M.T. Goodrich, C. Ó'Dúnlaing, and C. Yap "Constructing the Voronoi Diagram of a Set of Line Segments in Parallel," *Algorithmica*, **9**, 1993, 128–141.

J-15. M.T. Goodrich, "Constructing the Convex Hull of a Partially Sorted Set of Points," *Computational Geometry: Theory and Applications*, **2**, 1993, 267–278.

J-16. M.T. Goodrich, "Constructing Arrangements Optimally in Parallel," *Discrete and Computational Geometry*, **9**, 1993, 371–385.

J-17. M.T. Goodrich, M.J. Atallah, and M. Overmars, "Output-Sensitive Methods for Rectilinear Hidden Surface Removal," *Information and Computation*, **107**(1), 1993, 1–24.

J-18. M.J. Atallah, P. Callahan, and M.T. Goodrich, "P-Complete Geometric Problems," *Int. Journal of Computational Geometry & Applications*, **3**(4), 1993, 443–462.

J-19. M.J. Atallah, M.T. Goodrich, and S.R. Kosaraju, "Parallel Algorithms for Evaluating Sequences of Set-Manipulation Operations," *Journal of the ACM*, **41**(6), 1994, 1049–1088.

J-20. M.T. Goodrich, "Efficient Piecewise-Linear Function Approximation Using the Uniform Metric," *Discrete and Computational Geometry*, **14**, 1995, 445–462.

J-21. H. Brönnimann and M.T. Goodrich, "Almost Optimal Set Covers in Finite VC-Dimension," *Discrete and Computational Geometry*, **14**, 1995, 463–479.

J-22. M.T. Goodrich, "Planar Separators and Parallel Polygon Triangulation," *J. Computer and System Sciences*, **51**(3), 1995, 374–389.

J-23. M.T. Goodrich, M. Ghouse, and J. Bright, "Sweep Methods for Parallel Computational Geometry," *Algorithmica*, **15**(2), 1996, 126–153.

J-24. M.T. Goodrich and S.R. Kosaraju, "Sorting on a Parallel Pointer Machine with Applications to Set Expression Evaluation," *Journal of the ACM*, **43**(2), 1996, 331–361.

J-25. A. Garg, M.T. Goodrich, and R. Tamassia, "Planar Upward Tree Drawings with Optimal Area," *International Journal of Computational Geometry & Applications*, **6**(3), 1996, 333–356.

J-26. M.H. Nodine, M.T. Goodrich, and J.S. Vitter, "Blocking for External Graph Searching," *Algorithmica*, **16**(2), 1996, 181–214.

J-27. R. Cole, M.T. Goodrich, C. Ó Dúnlaing, "A Nearly Optimal Deterministic Parallel Voronoi Diagram Algorithm," *Algorithmica*, **16**, 1996, 569–617.

J-28. G. Das and M.T. Goodrich, "On the Complexity of Optimization Problems for 3-Dimensional Convex Polyhedra and Decision Trees," *Computational Geometry: Theory and Applications*, **8**, 1997, 123–137.

J-29. M.T. Goodrich and R. Tamassia, "Dynamic Ray Shooting and Shortest Paths in Planar Subdivisions via Balanced Geodesic Triangulations," *J. Algorithms*, **23**, 1997, 51–73.

J-30. M. Ghouse and M.T. Goodrich, "Fast Randomized Parallel Methods for Planar Convex Hull Construction," *Computational Geometry: Theory and Applications*, **7**, 1997, 219–235.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 79

J-31. L.P. Chew, M.T. Goodrich, D.P. Huttenlocher, K. Kedem, J.M. Kleinberg, and D. Kravets, "Geometric Pattern Matching under Euclidean Motion," *Computational Geometry: Theory and Applications*, **7**, 1997, 113-124.

J-32. M.T. Goodrich and E.A. Ramos, "Bounded-Independence Derandomization of Geometric Partitioning with Applications to Parallel Fixed-Dimensional Linear Programming," *Discrete & Computational Geometry*, **18**(4), 1997, 397–420.

J-33. M.T. Goodrich, "An Improved Ray Shooting Method for Constructive Solid Geometry Models via Tree Contraction," *International Journal of Computational Geometry & Applications*, **8**(1), 1998, 1–23.

J-34. G. Barequet, A.J. Briggs, M.T. Dickerson, and M.T. Goodrich, "Offset-Polygon Annulus Placement Problems," *Computational Geometry: Theory and Applications*, **11**(3–4), 1998–99, 125–141.

J-35. M.T. Goodrich and R. Tamassia, "Dynamic Trees and Dynamic Point Location," *SIAM J. Comput.*, **28**(2), 1999, 612–636.

J-36. G. Barequet, S.S. Bridgeman, C.A. Duncan, M.T. Goodrich, and R. Tamassia, "GeomNet: Geometric Computing Over the Internet," *IEEE Internet Computing*, **3**(2), 1999, 21–29.

J-37. M.T. Goodrich, J.S.B. Mitchell, and M.W. Orletsky, "Approximate Geometric Pattern Matching Under Rigid Motion," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, **21**(4), 1999, 371–379.

J-38. M.T. Goodrich, "Communication-Efficient Parallel Sorting," *SIAM Journal on Computing*, **29**(2), 1999, 416–432.

J-39. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees and Their Use for Drawing Very Large Graphs," *Journal of Graph Algorithms and Applications*, **4**(3), 2000, 19–46. Also available at www.cs.brown.edu/publications/jgaa/.

J-40. M.T. Goodrich and C.G. Wagner, "A Framework for Drawing Planar Graphs with Curves and Polylines," *Journal of Algorithms*, **37**, 2000, 399–421.

J-41. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees: Combining the Benefits of k-D Trees and Octrees," *J. Algorithms*, **38**, 2001, 303–333.

J-42. G. Barequet, M. Dickerson, and M.T. Goodrich, "Voronoi Diagrams for Polygon-Offset Distance Functions," *Discrete and Computational Geometry*, **25**(2), 2001, 271–291.

J-43. C.C. Cheng, C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Drawing Planar Graphs with Circular Arcs," *Discrete and Computational Geometry*, **25**(3), 2001, 405–418.

J-44. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "A Randomized Algorithm for Triangulating a Simple Polygon in Linear Time," *Discrete and Computational Geometry*, **26**(2), 2001, 245–265.

J-45. R. Tamassia, M.T. Goodrich, L. Vismara, M. Handy, G. Shubina, R. Cohen, B. Hudson, R.S. Baker, N. Gelfand, and U. Brandes, "JDSL: The Data Structures Library in Java," *Dr. Dobbs Journal*, **323**, 2001, 21–31.

J-46. G. Barequet, D.Z. Chen, O. Daescu, M.T. Goodrich, and J.S. Snoeyink, "Efficiently Approximating Polygonal Paths in Three and Higher Dimensions," *Algorithmica*, **33**(2), 2002, 150–167.

J-47. T. Chan, M.T. Goodrich, S.R. Kosaraju, and R. Tamassia, "Optimizing Area and Aspect Ratio in Straight-Line Orthogonal Tree Drawings," *Computational Geometry: Theory and Applications*, **23**(2), 2002, 153–162.

J-48. C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Planarity-Preserving Clustering and Embedding for Large Planar Graphs," *Computational Geometry: Theory and Applications*,

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 80

24(2), 2003, 95–114.

J-49. A.L. Buchsbaum and M.T. Goodrich, "Three-Dimensional Layers of Maxima," *Algorithmica*, **39**, 2004, 275–286.

J-50. G. Barequet, M.T. Goodrich, and C. Riley, "Drawing Graphs with Large Vertices and Thick Edges," *J. of Graph Algorithms and Applications* (JGAA), **8**(1), 2004, 3–20.

J-51. G. Barequet, M.T. Goodrich, A. Levi-Steiner, and D. Steiner, "Contour Interpolation by Straight Skeletons," *Graphical Models* (GM), **66**(4), 2004, 245–260.

J-52. P. Gajer, M.T. Goodrich, and S.G. Kobourov, "A Multi-Dimensional Approach to Force-Directed Layouts of Large Graphs," *Computational Geometry: Theory and Applications*, **29**(1), 3–18, 2004.

J-53. G. Barequet, P. Bose, M.T. Dickerson, and M.T. Goodrich, "Optimizing a Constrained Convex Polygonal Annulus," *J. of Discrete Algorithms* (JDA), **3**(1), 1–26, 2005.

J-54. A. Bagchi, A.L. Buchsbaum, and M.T. Goodrich, "Biased Skip Lists," *Algorithmica*, **42**(1), 31–48, 2005.

J-55. M. Dickerson, D. Eppstein, M.T. Goodrich, J.Y. Meng, "Confluent Drawings: Visualizing Non-planar Diagrams in a Planar Way," *J. of Graph Algorithms and Applications* (JGAA), **9**(1), 31–52, 2005.

J-56. A. Bagchi, A. Chaudhary, M.T. Goodrich, C. Li, and M. Shmueli-Scheuer, "Achieving Communication Efficiency through Push-Pull Partitioning of Semantic Spaces to Disseminate Dynamic Information," *IEEE Trans. on Knowledge and Data Engineering* (TKDE), **18**(10), 1352–1367, 2006.

J-57. D. Eppstein, M.T. Goodrich, and J.Y. Meng, "Confluent Layered Drawings," *Algorithmica*, **47**(4), 439–452, 2007.

J-58. A. Bagchi, A. Chaudhary, D. Eppstein, and M.T. Goodrich, "Deterministic Sampling and Range Counting in Geometric Data Streams," *ACM Transactions on Algorithms*, **3**(2), Article 16, 2007, 18 pages.

J-59. D. Eppstein, M.T. Goodrich, and D. Hirschberg, "Improved Combinatorial Group Testing Algorithms for Real-World Problem Sizes," *SIAM Journal on Computing*, **36**(5), 1360–1375, 2007.

J-60. D. Eppstein, M.T. Goodrich, and J.Z. Sun, "Skip Quadtrees: Dynamic Data Structures for Multidimensional Point Sets," *Int. Journal on Computational Geometry and Applications*, **18**(1/2), 131–160, 2008.

J-61. M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," *IEEE/ACM Transactions on Networking*, **16**(1), 15–24, 2008.

J-62. M.T. Goodrich and D.S. Hirschberg, "Improved Adaptive Group Testing Algorithms with Applications to Multiple Access Channels and Dead Sensor Diagnosis," *Journal of Combinatorial Optimization*, **15**(1), 95–121, 2008.

J-63. M.T. Goodrich, R. Tamassia, and D. Yao, "Notarized Federated ID Management and Authentication," *Journal of Computer Security*, **16**(4), 399–418, 2008.

J-64. M.T. Goodrich, "Pipelined Algorithms to Detect Cheating in Long-Term Grid Computations," *Theoretical Computer Science*, **408**, 199–207, 2008.

J-65. D. Eppstein, M.T. Goodrich, E. Kim, and R. Tamstorf, "Motorcycle Graphs: Canonical Quad Mesh Partitioning," *Computer Graphics Forum*, special issue on papers from 6th European Symp. on Geometry Processing (SGP), **27**(6), 1477–1486, 2008.

J-66. M.T. Goodrich, M. Sirivianos, J. Solis, C. Soriente, G. Tsudik, E. Uzun, "Using Audio in Secure Device Pairing," *Int. J. Security and Networks*, **4**(1/2), 57–68, 2009.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 81

J-67. M.T. Goodrich, "On the Algorithmic Complexity of the Mastermind Game with Black-Peg Results," *Information Processing Letters*, **109**, 675–678, 2009.

J-68. D. Eppstein, M.T. Goodrich, E. Kim, and R. Tamstorf, "Approximate Topological Matching of Quad Meshes," *The Visual Computer*, **25**(8), 771–783, 2009.

J-69. D. Eppstein and M.T. Goodrich, "Succinct Greedy Geometric Routing Using Hyperbolic Geometry," *IEEE Transactions on Computers*, **60**(11), 1571–1580, 2011. Posted online Dec. 2010, IEEE Computer Society Digital Library.

J-70. D. Eppstein, M.T. Goodrich, and D. Strash, "Linear-Time Algorithms for Geometric Graphs with Sublinearly Many Edge Crossings," *SIAM Journal on Computing*, **39**(8), 3814–3829. 2010.

J-71. M.T. Goodrich, R. Tamassia, and N. Triandopoulos, "Efficient Authenticated Data Structures for Graph Connectivity and Geometric Search Problems," *Algorithmica*, **60**(3), 505–552, 2011.

J-72. D. Eppstein and M.T. Goodrich, "Straggler Identification in Round-Trip Data Streams via Newton's Identities and Invertible Bloom Filters," *IEEE Transactions on Knowledge and Data Engineering* (TKDE), **23**(2), 297–306, 2011.

J-73. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Planar Drawings of Higher-Genus Graphs," *Journal of Graph Algorithms and Applications*, **15**(1), 7–32, 2011.

J-74. M.T. Dickerson, M.T. Goodrich, T.D. Dickerson, and Y.D. Zhuo "Round-Trip Voronoi Diagrams and Doubling Density in Geographic Networks," *Transactions on Computational Science*, M.L. Gavrilova et al. (Eds.), Vol. 14, LNCS 6970, 211–238, 2011.

J-75. M.T. Goodrich, "Randomized Shellsort: A Simple Data-Oblivious Sorting Algorithm," *Journal of the ACM*, **58**(6), Article No. 27, 2011.

J-76. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Lombardi Drawings of Graphs," *Journal of Graph Algorithms and Applications (JGAA)*, **16**(1), 85–108, 2012.

J-77. E. Wolf-Chambers, D. Eppstein, M.T. Goodrich, and M. Löffler, "Drawing Graphs in the Plane with a Prescribed Outer Face and Polynomial Area," *Journal of Graph Algorithms and Applications (JGAA)*, **16**(2), 243–259, 2012.

J-78. M.T. Goodrich, D. Nguyen, O. Ohrimenko, C. Papamanthou, R. Tamassia, N. Triandopoulos, and C.V. Lopes, "Efficient Verification of Web-Content Searching Through Authenticated Web Crawlers," *Proc. VLDB*, **5**(10):920-931, 2012.

J-79. D. Eppstein, M.T. Goodrich, D. Strash, and L. Trott, "Extended Dynamic Subgraph Statistics Using h-Index Parameterized Data Structures," *Theoretical Computer Science*, **447**, 44–52, 2012.

J-80. M.T. Goodrich, "Learning Character Strings via Mastermind Queries, With a Case Study Involving mtDNA," *IEEE Transactions on Information Theory*, **58**(11), 6726–6736, 2012.

J-81. A.U. Asuncion and M.T. Goodrich, "Nonadaptive Mastermind Algorithms for String and Vector Databases, with Case Studies," *IEEE Transactions on Knowledge and Data Engineering* (TKDE), **25**(1), 131–144, 2013.

J-82. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Drawing Trees with Perfect Angular Resolution and Polynomial Area," *Discrete & Computational Geometry*, **49**(2), 157–182, 2013.

J-83. E. Angelino, M.T. Goodrich, M. Mitzenmacher and J. Thaler, "External Memory Multimaps," *Algorithmica*, **67**(1), 23–48, 2013.

J-84. D. Eppstein, M.T. Goodrich, M. Löffler, D. Strash and L. Trott, "Category-Based Routing

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 82

in Social Networks: Membership Dimension and the Small-World Phenomenon," *Theoretical Computer Science*, **514**, 96–104, 2013.

J-85. M.T. Goodrich, "Spin-the-bottle Sort and Annealing Sort: Oblivious Sorting via Round-robin Random Comparisons," *Algorithmica*, **68**(4), 835–858, 2014.

J-86. Michael J. Bannister, William E. Devanny, David Eppstein, and M.T. Goodrich, "The Galois Complexity of Graph Drawing: Why Numerical Solutions are Ubiquitous for Force-Directed, Spectral, and Circle Packing Drawings," *Journal of Graph Algorithms and Applications*, **19**(2), 619–656, 2015.

J-87. C. Duncan, D. Eppstein, M.T. Goodrich, S.G. Kobourov and M. Löffler, "Planar and Poly-Arc Lombardi Drawings," *Journal of Computational Geometry* (JoCG), **9**(1), 328–355, 2018.

J-88. G. Barequet, D. Eppstein, M.T. Goodrich, and N. Mamano, "Stable-Matching Voronoi Diagrams: Combinatorial Complexity and Algorithms," *Journal of Computational Geometry* (JoCG), **11**(1), 26–59, 2020.

J-89. W.E. Devanny, M.T. Goodrich, S. Irani, "A Competitive Analysis for the Start-Gap Algorithm for Online Memory Wear Leveling," *Information Processing Letters*, **116**, 106042, 2021.

J-90. G. Barequet, M. De, and M.T. Goodrich, "Convex-Straight-Skeleton Voronoi Diagrams for Segments and Convex Polygons," *Algorithmica*, **83**(7), 2245–2272, 2021.

J-91. G. Da Lozzo, D. Eppstein, M.T. Goodrich, and S. Gupta, "C-Planarity Testing of Embedded Clustered Graphs with Bounded Dual Carving-Width," *Algorithmica*, **83**(8), 2471–2502, 2021.

J-92. M.T. Goodrich, M. Shinder, O. Gila, M. Dillencourt, "Beyond Big O: Teaching Experimental Algorithmics," *Journal of Computing Sciences in Colleges*, **37**(10), 23–36, 2022.

Papers in Peer-Reviewed Proceedings:

C-1. M.J. Atallah and M.T. Goodrich, "Efficient Parallel Solutions to Geometric Problems," *1985 IEEE Int. Conf. on Parallel Processing (ICPP)*, 411–417. (Preliminary version of J-1.)

C-2. F. Berman, M.T. Goodrich, C. Koelbel, W. Robison, and K. Showell, "Prep-P: A Mapping Preprocessor for CHiP Computers," *1985 IEEE Int. Conf. on Parallel Processing*, 731–733.

C-3. M.J. Atallah and M.T. Goodrich, "Parallel Algorithms For Some Functions of Two Convex Polygons," *24th Allerton Conf. on Communication, Control and Computing*, 1986, 758–767. (Preliminary version of J-4.)

C-4. M.J. Atallah and M.T. Goodrich, "Efficient Plane Sweeping in Parallel," *2nd ACM Symp. on Computational Geometry* (SoCG), 1986, 216–225.

C-5. M.T. Goodrich, "A Polygonal Approach to Hidden-Line Elimination," *25th Allerton Conf. on Communication, Control, and Computing*, 1987, 849–858. (Preliminary version of J-12.)

C-6. M.J. Atallah, R. Cole, and M.T. Goodrich, "Cascading Divide-and-Conquer: A Technique for Designing Parallel Algorithms," *28th IEEE Symp. on Foundations of Computer Science* (FOCS), 1987, 151-160. (Preliminary version of J-5.)

C-7. M.J. Atallah, M.T. Goodrich, and S.R. Kosaraju, "Parallel Algorithms for Evaluating Sequences of Set-Manipulation Operations," *3rd Aegean Workshop on Computing* (AWOC), *Lecture Notes in Computer Science* (LNCS): 319, Springer-Verlag, 1988, 1–10. (Preliminary version of J-19.)

C-8. R. Cole and M.T. Goodrich, "Optimal Parallel Algorithms for Polygon and Point-Set Problems," *4th ACM Symp. on Computational Geometry* (SoCG), 1988, 201–210. (Preliminary version of J-11.)

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 83

C-9. M.T. Goodrich, "Intersecting Line Segments in Parallel with an Output-Sensitive Number of Processors," *1989 ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 127–137. (Preliminary version of J-10.)

C-10. M.T. Goodrich and S.R. Kosaraju, "Sorting on a Parallel Pointer Machine with Applications to Set Expression Evaluation," *30th IEEE Symp. on Foundations of Computer Science* (FOCS), 1989, 190–195. (Preliminary version of J-24.)

C-11. M.T. Goodrich, C. Ó'Dúnlaing, and C. Yap "Constructing the Voronoi Diagram of a Set of Line Segments in Parallel," *Lecture Notes in Computer Science 382, Algorithms and Data Structures* (WADS), Springer-Verlag, 1989, 12–23. (Preliminary version of J-14.)

C-12. M.T. Goodrich and J.S. Snoeyink, "Stabbing Parallel Segments with a Convex Polygon," *Lecture Notes in Computer Science 382, Algorithms and Data Structures* (WADS), Springer-Verlag, 1989, 231–242. (Preliminary version of J-8.)

C-13. J. Johnstone and M.T. Goodrich, "A Localized Method for Intersecting Plane Algebraic Curve Segments," *New Advances in Computer Graphics: Proc. of Computer Graphics International '89*, R.A. Earnshaw, B. Wyvel, eds., Springer-Verlag, 1989, 165–181. (Preliminary version of J-9.)

C-14. M.J. Atallah, P. Callahan, and M.T. Goodrich, "P-Complete Geometric Problems," *2nd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1990, 317–326. (Preliminary version of J-18.)

C-15. R. Cole, M.T. Goodrich, C. Ó Dúnlaing, "Merging Free Trees in Parallel for Efficient Voronoi Diagram Construction", *17th Int. Conf. on Automata, Languages, and Programming* (ICALP), 1990, 432–445. (Preliminary version of J-27.)

C-16. M.T. Goodrich, M.J. Atallah, and M. Overmars, "An Input-Size/Output-Size Trade-Off in the Time-Complexity of Rectilinear Hidden-Surface Removal", *17th Int. Conf. on Automata, Languages, and Programming* (ICALP), 1990, 689–702. (Preliminary version of J-17.)

C-17. M.T. Goodrich, M. Ghouse, and J. Bright, "Generalized Sweep Methods for Parallel Computational Geometry," *2nd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1990, 280–289. (Preliminary version of J-23.)

C-18. M.T. Goodrich, "Applying Parallel Processing Techniques to Classification Problems in Constructive Solid Geometry," *1st ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1990, 118–128. (Preliminary version of J-33.)

C-19. M.T. Goodrich, S. Shauck, and S. Guha, "Parallel Methods for Visibility and Shortest Path Problems in Simple Polygons," *6th ACM Symp. on Computational Geometry* (SoCG), 1990, 73–82. (Preliminary version of J-13.)

C-20. M. Ghouse and M.T. Goodrich, "In-Place Techniques for Parallel Convex Hull Algorithms," *3rd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1991, 192–203. (Preliminary version of J-30.)

C-21. M.T. Goodrich, "Constructing Arrangements Optimally in Parallel," *3rd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1991, 169–179. (Preliminary version of J-16.)

C-22. M.T. Goodrich and R. Tamassia, "Dynamic Trees and Dynamic Point Location," *23rd ACM Symp. on Theory of Computing* (STOC), 1991, 523–533. (Preliminary version of J-35.)

C-23. M.T. Goodrich, "Using Approximation Algorithms to Design Parallel Algorithms that May Ignore Processor Allocation," *32nd IEEE Symp. on Foundations of Computer Science* (FOCS), 1991, 711–722.

C-24. M.T. Goodrich, "Planar Separators and Parallel Polygon Triangulation," *24th ACM Symp. on Theory of Computing* (STOC), 1992, 507–516. (Preliminary version of J-22.)

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 84

C-25. M.T. Goodrich, Y. Matias, U. Vishkin, "Approximate Parallel Prefix Computation and Its Applications," *7th IEEE Int. Parallel Processing Symp* (IPPS), 1993, 318–325.

C-26. M. Ghouse and M.T. Goodrich, "Experimental Evidence for the Power of Random Sampling in Practical Parallel Algorithms," *7th IEEE Int. Parallel Processing Symp* (IPPS), 1993, 549–556.

C-27. L.P. Chew, M.T. Goodrich, D.P. Huttenlocher, K. Kedem, J.M. Kleinberg, and D. Kravets, "Geometric Pattern Matching under Euclidean Motion," *5th Canadian Conf. on Computational Geometry* (CCCG), 1993, 151–156. (Preliminary version of J-31.)

C-28. M.T. Goodrich, "Geometric Partitioning Made Easier, Even in Parallel," *9th ACM Symp. on Computational Geometry* (SoCG), 1993, 73–82.

C-29. M.T. Goodrich and R. Tamassia, "Dynamic Ray Shooting and Shortest Paths via Balanced Geodesic Triangulations," *9th ACM Symp. on Computational Geometry* (SoCG), 1993, 318–327. (Preliminary version of J-29.)

C-30. A. Garg, M.T. Goodrich, and R. Tamassia, "Area-Efficient Upward Tree Drawings," *9th ACM Symp. on Computational Geometry* (SoCG), 1993, 359–368. (Preliminary version of J-25.)

C-31. M.H. Nodine, M.T. Goodrich, and J.S. Vitter, "Blocking for External Graph Searching," *12th ACM Symp. on Principles of Database Systems* (PODS), 1993, 222–232. (Preliminary version of J-26.)

C-32. E.M. Arkin, M.T. Goodrich, J.S.B. Mitchell, D. Mount, and S.S. Skiena, "Point Probe Decision Trees for Geometric Concept Classes," *Lecture Notes in Computer Science 709: Algorithms and Data Structures* (WADS), Springer-Verlag, 1993, 95–106.

C-33. M.T. Goodrich, J.J. Tsay, D.E. Vengroff, and J.S. Vitter, "External-Memory Computational Geometry," *34th IEEE Symp. on Foundations of Computer Science* (FOCS), 1993, 714–723.

C-34. M.T. Goodrich, Y. Matias, and U. Vishkin, "Optimal Parallel Approximation Algorithms for Prefix Sums and Integer Sorting," *5th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1994, 241–250.

C-35. H. Brönnimann and M.T. Goodrich, "Almost Optimal Set Covers in Finite VC-Dimension," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 293–302. (Preliminary version of J-21.)

C-36. M.T. Goodrich, "Efficient Piecewise-Linear Function Approximation Using the Uniform Metric," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 322–331. (Preliminary version of J-20.)

C-37. M.J. Atallah, M.T. Goodrich, and K. Ramaiyer, "Biased Finger Trees and Three-Dimensional Layers of Maxima," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 150–159.

C-38. M.T. Goodrich, J.S.B. Mitchell, and M.W. Orletsky, "Practical Methods for Approximate Geometric Pattern Matching under Rigid Motions," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 103–112. (Preliminary version of J-37.)

C-39. N.M. Amato, M.T. Goodrich, E.A. Ramos, "Parallel Algorithms for Higher-Dimensional Convex Hulls," *35th IEEE Symp. on Foundations of Computer Science* (FOCS), 1994, 683–694.

C-40. P.J. Tanenbaum, M.T. Goodrich, and E.R. Scheinerman, "Characterization and Recognition of Point-Halfspace and Related Orders," *2nd Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 894, Springer-Verlag, 1994, 234–245.

C-41. Y.J. Chiang, M.T. Goodrich, E.F. Grove, R. Tamassia, D.E. Vengroff, and J.S. Vitter, "External-Memory Graph Algorithms," *6th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1995, 139–149.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 85

C-42. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "Computing Faces in Segment and Simplex Arrangements," *27th ACM Symp. on Theory of Computing* (STOC), 1995, 672–682.

C-43. P. Callahan, M.T. Goodrich, and K. Ramaiyer, "Topology B-Trees and Their Applications," *1995 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 955, Springer-Verlag, 381–392.

C-44. G. Das and M.T. Goodrich, "On the Complexity of Approximating and Illuminating Three-Dimensional Convex Polyhedra," *1995 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 955, Springer-Verlag, 74–85. (Preliminary version of J-28.)

C-45. M.T. Goodrich, "Fixed-Dimensional Parallel Linear Programming via Relative ϵ-Approximations," *7th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1996, 132–141. (Preliminary version of J-32.)

C-46. M. Chrobak, M.T. Goodrich, and R. Tamassia, "Convex Drawings of Graphs in Two and Three Dimensions," *12th ACM Symp. on Computational Geometry* (SoCG), 1996, 319–328.

C-47. M.T. Goodrich, "Communication-Efficient Parallel Sorting," *28th ACM Symp. on Theory of Computing* (STOC), 1996, 247–256. (Preliminary version of J-38.)

C-48. T. Chan, M.T. Goodrich, S.R. Kosaraju, and R. Tamassia, "Optimizing Area and Aspect Ratio in Straight-Line Orthogonal Tree Drawings," *4th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1190, Springer-Verlag, 1996, 63–75. (Preliminary version of J-47.)

C-49. M.T. Goodrich, "Randomized Fully-Scalable BSP Techniques for Multi-Searching and Convex Hull Construction," *8th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1997, 767–776.

C-50. C.A. Duncan, M.T. Goodrich, and E.A. Ramos, "Efficient Approximation and Optimization Algorithms for Computational Metrology," *8th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1997, 121–130.

C-51. M.T. Goodrich, M. Orletsky, and K. Ramaiyer, "Methods for Achieving Fast Query Times in Point Location Data Structures," *8th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1997, 757–766.

C-52. M.T. Goodrich, L.J. Guibas, J. Hershberger, P.J. Tanenbaum, "Snap Rounding Line Segments Efficiently in Two and Three Dimensions," *13th ACM Symp. on Computational Geometry* (SoCG), 1997, 284–293.

C-53. G. Barequet, S.S. Bridgeman, C.A. Duncan, M.T. Goodrich, and R. Tamassia, "Classical Computational Geometry in GeomNet," *13th ACM Symp. on Computational Geometry* (SoCG), 1997, 412–414.

C-54. G. Barequet, A. Briggs, M. Dickerson, C. Dima, and M.T. Goodrich, "Animating the Polygon-Offset Distance Function," *13th ACM Symp. on Computational Geometry* (SoCG), 1997, 479–480, and the *Video Review for the 13th ACM Symp. on Computational Geometry* (SoCG).

C-55. G. Barequet, A. Briggs, M. Dickerson, and M.T. Goodrich, "Offset-Polygon Annulus Placement Problems," *1997 Workshop on Algorithms and Data Structures* (WADS), 1997, 378–391. (Preliminary version of J-34.)

C-56. G. Barequet, M. Dickerson, and M.T. Goodrich, "Voronoi Diagrams for Polygon-Offset Distance Functions," *1997 Workshop on Algorithms and Data Structures* (WADS), 1997, 200–209. (Preliminary version of J-42.)

C-57. N. Gelfand, M.T. Goodrich, and R. Tamassia, "Teaching Data Structure Design Patterns,"

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 86

29th ACM SIGCSE Technical Symp. on Computer Science Education, 1998, 331–335.

C-58. M.T. Goodrich and R. Tamassia, "Teaching the Analysis of Algorithms with Visual Proofs," *29th ACM SIGCSE Technical Symp. on Computer Science Education*, 1998, 207–211.

C-59. G. Barequet, D.Z. Chen, O. Daescu, M.T. Goodrich, and J.S. Snoeyink, "Efficiently Approximating Polygonal Paths in Three and Higher Dimensions," *1998 ACM Symp. on Computational Geometry* (SoCG), 1998, 317–326. (Preliminary version of J-46.)

C-60. M.T. Goodrich and C.G. Wagner, "A Framework for Drawing Planar Graphs with Curves and Polylines," *6th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1547, Springer-Verlag, 1998, 153–166. (Preliminary version of J-40.)

C-61. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees and Their Use for Drawing Very Large Graphs," *6th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1547, Springer-Verlag, 1998, 111–124. (Preliminary version of J-39.)

C-62. M.T. Goodrich, M. Handy, B. Hudson, and R. Tamassia, "Abstracting Positional Information in Data Structures: Locators and Positions in JDSL," *Object-Oriented Programming, Systems, Languages & Applications (OOPSLA) '98 Technical Notes*, 1998.

C-63. M.T. Goodrich and J.G. Kloss II, "Tiered Vector: An Efficient Dynamic Array for JDSL," *Object-Oriented Programming, Systems, Languages & Applications (OOPSLA) '98 Technical Notes*, 1998.

C-64. M.T. Goodrich, M. Handy, B. Hudson, and R. Tamassia, "Accessing the Internal Organization of Data Structures in the JDSL Library," *Int. Workshop on Algorithm Engineering and Experimentation* (ALENEX), Springer-Verlag, Lecture Notes in Computer Science, Vol. 1619, 1999, 124–139.

C-65. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees: Combining the Benefits of k-D Trees and Octrees," *10th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1999, 300–309. (Preliminary version of J-41.)

C-66. R.S. Baker, M. Boilen, M.T. Goodrich, R. Tamassia, and B.A. Stibel, "Testers and Visualizers for Teaching Data Structures," *30th ACM SIGCSE Technical Symp. on Computer Science Education*, 1999, 261–265.

C-67. M.T. Goodrich and R. Tamassia, "Using Randomization in the Teaching of Data Structures and Algorithms," *30th ACM SIGCSE Technical Symp. on Computer Science Education*, 1999, 53–57. (Preliminary version of Ch-5.)

C-68. G. Barequet, C. Duncan, M.T. Goodrich, S. Kumar, M. Pop, "Efficient Perspective-Accurate Silhouette Computation," *15th ACM Symp. on Computational Geometry* (SoCG), 1999, 417–418, and the *Video Review for the 15th ACM Symp. on Computational Geometry* (SoCG).

C-69. C.C. Cheng, C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Drawing Planar Graphs with Circular Arcs," *7th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1731, Springer-Verlag, 1999, 117–126. (Preliminary version of J-43.)

C-70. C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Planarity-Preserving Clustering and Embedding for Large Planar Graphs," *7th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1731, Springer-Verlag, 1999, 186–196. (Preliminary version of J-48.)

C-71. M.T. Goodrich and J.G. Kloss II, "Tiered Vectors: Efficient Dynamic Arrays for Rank-Based Sequences," *1999 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 1663, Springer-Verlag, 1999, 205–216.

C-72. M.T. Goodrich, "Competitive Tree-Structured Dictionaries," *11th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2000, 494–495.

C-73. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "Computing the Arrangement of Curve

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 87

Segments: Divide-and-Conquer Algorithms via Sampling," *11th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2000, 705–706.

C-74. S. Bridgeman, M.T. Goodrich, S.G. Kobourov, and R. Tamassia, "PILOT: An Interactive Tool for Learning and Grading," *31st ACM SIGCSE Technical Symp. on Computer Science Education*, 2000, 139–143.

C-75. S. Bridgeman, M.T. Goodrich, S.G. Kobourov, and R. Tamassia, "SAIL: A System for Generating, Archiving, and Retrieving Specialized Assignments in LaTeX," *31st ACM SIGCSE Technical Symp. on Computer Science Education*, 2000, 300–304.

C-76. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "Linear-Time Triangulation of a Simple Polygon Made Easier Via Randomization," *16th ACM Symp. on Computational Geometry* (SoCG), 2000, 201-212. (Preliminary version of J-44.)

C-77. A.L. Buchsbaum, M.T. Goodrich, and J.R. Westbrook, "Range Searching Over Tree Cross Products," *8th European Symp. on Algorithms* (ESA), Lecture Notes in Computer Science 1879, Springer-Verlag, 2000, 120–131.

C-78. C.A. Duncan, M.T. Dickerson, and M.T. Goodrich, "k-D Trees are Better When Cut on the Longest Side," *8th European Symp. on Algorithms* (ESA), Lecture Notes in Computer Science 1879, Springer-Verlag, 2000, 179–190.

C-79. P. Gajer, M.T. Goodrich, and S.G. Kobourov, "A Fast Multi-Dimensional Algorithm for Drawing Large Graphs," *8th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1984, Springer-Verlag, 2001, 211–221. (Preliminary version of J-52.)

C-80. G. Ateniese, B. de Medeiros, and M.T. Goodrich, "TRICERT: A Distributed Certified E-mail Scheme," *Network and Distributed Systems Security Symp.* (NDSS), 2001, 47–56.

C-81. M.T. Goodrich and R. Tamassia, "Teaching Internet Algorithmics," *32nd ACM SIGCSE Technical Symp. on Computer Science Education*, 2001, 129–133.

C-82. M. Pop, G. Barequet, C.A. Duncan, M.T. Goodrich, W. Hwang, and S. Kumar, "Efficient Perspective-Accurate Silhouette Computation and Applications," *17th ACM Symp. on Computational Geometry* (SoCG), 2001, 60–68.

C-83. M.T. Goodrich and R. Tamassia, "Implementation of an Authenticated Dictionary with Skip Lists and Commutative Hashing," *DARPA Information Survivability Conf. & Exposition II* (DISCEX), IEEE Press, 2001, 68–82.

C-84. A. Bagchi, A. Chaudhary, R. Garg, M.T. Goodrich, and V. Kumar, "Seller-Focused Algorithms for Online Auctioning," *2001 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 2125, Springer-Verlag, 2001, 135–147.

C-85. A. Anagnostopoulos, M.T. Goodrich, R. Tamassia, "Persistent Authenticated Dictionaries and Their Applications," *Information Security Conf.* (ISC), Lecture Notes in Computer Science 2200, Springer-Verlag, 2001, 379–393.

C-86. M.T. Goodrich, R. Tamassia, and J. Hasic, "An Efficient Dynamic and Distributed Cryptographic Accumulator," *5th Information Security Conf.* (ISC), Lecture Notes in Computer Science 2433, Springer-Verlag, 2002, 372–388.

C-87. A.L. Buchsbaum and M.T. Goodrich, "Three-Dimensional Layers of Maxima," *10th European Symp. on Algorithms* (ESA), Lecture Notes in Computer Science 2461, Springer-Verlag, 2002, 257–267. (Preliminary version of J-49.)

C-88. A. Bagchi, A.L. Buchsbaum, and M.T. Goodrich, "Biased Skip Lists," *13th Int. Symp. on Algorithms and Computation* (ISAAC), Lecture Notes in Computer Science 2518, Springer-Verlag, 2002, 1–13. (Preliminary version of J-54.)

C-89. M.T. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback," *9th ACM Conf.*

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 88

on Computer and Communications Security (CCS), 2002, 117–126. (Preliminary version of J-61.)

C-90. M.T. Goodrich, R. Tamassia, N. Triandopoulos, and R. Cohen, "Authenticated Data Structures for Graph and Geometric Searching," *RSA Conf.—Cryptographers' Track* (CT-RSA), Lecture Notes in Computer Science 2612, Springer-Verlag, 2003, 295–313. (Preliminary version of J-71.)

C-91. M.T. Goodrich, M. Shin, R. Tamassia, and W.H. Winsborough, "Authenticated Dictionaries for Fresh Attribute Credentials," *1st Int. Conf. on Trust Management* (iTrust), Lecture Notes in Computer Science 2692, Springer-Verlag, 2003, 332–347.

C-92. G. Barequet, M.T. Goodrich, A. Levi-Steiner, and D. Steiner, "Straight-Skeleton Based Contour Interpolation," *14th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2003, 119–127. (Preliminary version of J-51.)

C-93. G. Barequet, M.T. Goodrich, and C. Riley, "Drawing Graphs with Large Vertices and Thick Edges," *2003 Workshop and Data Structures and Algorithms* (WADS), Lecture Notes in Computer Science 2748, Springer-Verlag, 2003, 281–293. (Preliminary version of J-50.)

C-94. A. Bagchi, A. Chaudhary, M.T. Goodrich, and S. Xu, "Constructing Disjoint Paths for Secure Communication," *17th Int. Symp. on Distributed Computing* (DISC), Lecture Notes in Computer Science 2848, Springer-Verlag, 2003, 181–195.

C-95. M. Dickerson, D. Eppstein, M.T. Goodrich, J.Y. Meng, "Confluent Drawings: Visualizing Non-planar Diagrams in a Planar Way," *11th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 2912, Springer-Verlag, 2003, 1–12. (Preliminary version of J-55.)

C-96. F. Brandenberg, D. Eppstein, M.T. Goodrich, S. Kobourov, G. Liotta, P. Mutzel, "Selected Open Problems in Graph Drawing," *11th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 2912, Springer-Verlag, 2003, 515–539.

C-97. A. Bagchi, A. Chaudhary, D. Eppstein, and M.T. Goodrich, "Deterministic Sampling and Range Counting in Geometric Data Streams," *20th ACM Symp. on Computational Geometry* (SoCG), 144–151, 2004. (Preliminary version of J-58.)

C-98. M.T. Goodrich, J.Z. Sun, and R. Tamassia, "Efficient Tree-Based Revocation in Groups of Low-State Devices," *Advances in Cryptology* (CRYPTO), Springer, Lecture Notes in Computer Science 3152, 511–527, 2004.

C-99. D. Eppstein, M.T. Goodrich, and J.Y. Meng, "Confluent Layered Drawings," *12th Int. Symp. on Graph Drawing* (GD), Springer, Lecture Notes in Computer Science 3383, 184–194, 2004. (Preliminary version of J-57.)

C-100. M.J. Atallah, K.B. Frikken, M.T. Goodrich, and R. Tamassia, "Secure Biometric Authentication for Weak Computational Devices," *9th Int. Conf. on Financial Cryptograpy and Data Security*, Springer, Lecture Notes in Computer Science 3570, 357–371, 2005.

C-101. M.T. Goodrich, "Leap-Frog Packet Linking and Diverse Key Distributions for Improved Integrity in Network Broadcasts," *IEEE Symp. on Security and Privacy* (S&P), 196–207, 2005.

C-102. D. Eppstein, M.T. Goodrich, and J.Z. Sun, "The Skip Quadtree: A Simple Dynamic Data Structure for Multidimensional Data," *21st ACM Symp. on Computational Geometry* (SoCG), 296–305, 2005. (Preliminary version of J-60.)

C-103. M.J. Atallah, M.T. Goodrich, and R. Tamassia, "Indexing Information for Data Forensics," *3rd Applied Cryptography and Network Security Conf.* (ACNS), Lecture Notes in Computer Science 3531, Springer, 206–221, 2005.

C-104. W. Du and M.T. Goodrich, "Searching for High-Value Rare Events with Uncheatable Grid Computing," *3rd Applied Cryptography and Network Security Conf.* (ACNS), Lecture Notes

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 89

in Computer Science 3531, Springer, 122–137, 2005.

C-105. L. Arge, D. Eppstein, and M.T. Goodrich, "Skip-Webs: Efficient Distributed Data Structures for Multi-Dimensional Data Sets," *24th ACM Symp. on Principles of Distributed Computing* (PODC), 2005.

C-106. D. Eppstein, M.T. Goodrich, and D. Hirschberg, "Improved Combinatorial Group Testing for Real-World Problem Sizes," *Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 3608, Springer, 86–98, 2005. (Preliminary version of J-59.)

C-107. A. Chaudhary and M.T. Goodrich, "Balanced Aspect Ratio Trees Revisited," *Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 3608, Springer, 73–85, 2005.

C-108. M.T. Goodrich, R. Tamassia, and D. Yao, "Accredited DomainKeys: A Service Architecture for Improved Email Validation," *2nd Conf. on Email and Anti-Spam* (CEAS), 1–8, 2005.

C-109. M.T. Goodrich, G.S. Lueker, and J.Z. Sun, "C-Planarity of Extrovert Clustered Graphs," *13th Int. Symp. Graph Drawing* (GD), 211–222, 2005.

C-110. D. Eppstein, M.T. Goodrich, J.Y. Meng, "Delta-Confluent Drawings," *13th Int. Symp. Graph Drawing* (GD), 165–176, 2005.

C-111. M.T. Goodrich, M.J. Nelson, and J.Z. Sun, "The Rainbow Skip Graph: A Fault-Tolerant Constant-Degree Distributed Data Structure," *17th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 384–393, 2006.

C-112. M.T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, E. Uzun, "Loud And Clear: Human-Verifiable Authentication Based on Audio," *26th IEEE Int. Conf. on Distributed Computing Systems* (ICDCS), 1–8, 2006. (Preliminary version of J-66.)

C-113. M.T. Goodrich, R. Tamassia, and D. Yao, "Notarized Federated Identity Management for Web Services," *20th IFIP WG Working Conf. on Data and Application Security* (DBSec), Springer, Lecture Notes in Computer Science, Vol. 4127, 133–147, 2006. (Preliminary version of J-63.)

C-114. M.T. Goodrich and D.S. Hirschberg, "Efficient Parallel Algorithms for Dead Sensor Diagnosis and Multiple Access Channels," *18th ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 118–127, 2006. (Preliminary version of J-62.)

C-115. Y. Cho, L. Bao, and M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol," *2006 3rd Annual Int. Conf. on Mobile and Ubiquitous Systems - Workshop on Ubiquitous Access Control* (IWUAC), 1–7, 2006.

C-116. M.B. Dillencourt, D. Eppstein, and M.T. Goodrich, "Choosing Colors for Geometric Graphs via Color Space Embeddings," *14th Int. Symp. Graph Drawing* (GD), Lecture Notes in Computer Science, Vol. 4372, Springer, 294–305, 2006.

C-117. D. Eppstein, M.T. Goodrich, and N. Sitchinava, "Guard Placement for Wireless Localization," *23rd ACM Symp. on Computational Geometry* (SoCG), 27–36, 2007.

C-118. M.T. Goodrich, C. Papamanthou, and R. Tamassia, "On the Cost of Persistence and Authentication in Skip Lists," *6th Workshop on Experimental Algorithms* (WEA), LNCS 4525, 94–107, 2007.

C-119. M.J. Atallah, M. Blanton, M.T. Goodrich, and S. Polu, "Discrepancy-Sensitive Dynamic Fractional Cascading, Dominated Maxima Searching, and 2-d Nearest Neighbors in Any Minkowski Metric," *Workshop on Algorithms and Data Structures* (WADS), LNCS, Vol. 4619, Springer, 114–126, 2007.

C-120. D. Eppstein and M.T. Goodrich, "Space-Efficient Straggler Identification in Round-Trip Data Streams via Newton's Identities and Invertible Bloom Filters," *Workshop on Algorithms*

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 90

and Data Structures (WADS), LNCS, Vol. 4619, Springer, 2007, 638–649. (Preliminary version of J-72.)

C-121. M.T. Goodrich and J.Z. Sun, "Checking Value-Sensitive Data Structures in Sublinear Space," *18th Int. Symp. on Algorithms and Computation* (ISAAC), LNCS, vol. 4835, Springer, 2007, 353–364.

C-122. M.T. Goodrich, R. Tamassia, and N. Triandopoulos, "Super-Efficient Verification of Dynamic Outsourced Databases," *RSA Conf.—Cryptographers' Track* (CT-RSA), LNCS, vol. 4964, Springer, 2008, 407–424.

C-123. D. Eppstein, M.T. Goodrich, E. Kim, and R. Tamstorf, "Approximate Topological Matching of Quadrilateral Meshes," *IEEE Int. Conf. on Shape Modeling and Applications* (SMI), 2008, 83–92. (Preliminary version of J-68.)

C-124. G. Barequet, D. Eppstein, M.T. Goodrich, and A. Waxman, "Straight Skeletons of Three-Dimensional Polyhedra," *16th European Symp. on Algorithms* (ESA), LNCS, vol. 5193, 2008, 148–160.

C-125. M.T. Goodrich, C. Papamanthou, R. Tamassia, and N. Triandopoulos, "Athos: Efficient Authentication of Outsourced File Systems," *11th Information Security Conf.* (ISC), LNCS, vol. 5222, 2008, 80–96.

C-126. L. Arge, M.T. Goodrich, M. Nelson, and N. Sitchinava, "Fundamental Parallel Algorithms for Private-Cache Chip Multiprocessors," *20th ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 2008, 197–206.

C-127. D. Eppstein and M.T. Goodrich, "Succinct Greedy Graph Drawing in the Hyperbolic Plane," *16th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 5417, Springer, 2008, 14–25. (Preliminary version of J-69.)

C-128. D. Eppstein and M.T. Goodrich, "Studying (Non-Planar) Road Networks Through an Algorithmic Lens," *16th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2008, 125–134. **Best Paper Award**.

C-129. M. Dickerson and M.T. Goodrich, "Two-Site Voronoi Diagrams in Geographic Networks," *16th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2008, 439–442.

C-130. D. Eppstein, M.T. Goodrich, and D. Strash, "Linear-Time Algorithms for Geometric Graphs with Sublinearly Many Crossings," *20th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2009, 150–159. (Preliminary version of J-70.)

C-131. M.T. Goodrich, "The Mastermind Attack on Genomic Data," *30th IEEE Symp. on Security and Privacy* (S&P), 2009, 204–218. (Preliminary version of J-80.)

C-132. W. Du, D. Eppstein, M.T. Goodrich, and G.S. Lueker, "On the Approximability of Geometric and Geographic Generalization and the Min-Max Bin Covering Problem," *Algorithms and Data Structures Symp.* (WADS), LNCS, vol. 5664, Springer, 2009, 242–253.

C-133. M.T. Goodrich, R. Tamassia, and N. Triandopoulos, J.Z. Sun, "Reliable Resource Searching in P2P Networks," *5th Int. ICST Conf. on Security and Privacy in Communication Networks* (SecureComm), Lecture Notes of ICST, vol. 19, Springer, 2009, 437–447.

C-134. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Planar Drawings of Higher-Genus Graphs," *17th Int. Symp. on Graph Drawing* (GD), LNCS, Springer, vol. 5849, 2009, 45–56. (Preliminary version of J-73.)

C-135. D. Eppstein, M.T. Goodrich, L. Trott, "Going Off-road: Transversal Complexity in Road Networks," *17th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2009, 23–32.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 91

C-136. M.T. Goodrich and Darren Strash, "Succinct Greedy Geometric Routing in the Euclidean Plane," *20th Int. Symp. on Algorithms and Computation* (ISAAC), LNCS, vol. 5878, Springer, 2009, 781–791.

C-137. M.T. Goodrich, "Randomized Shellsort: A Simple Oblivious Sorting Algorithm," *21st ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2010, 1262–1277. (Preliminary version of J-75.)

C-138. L. Arge, M.T. Goodrich, and N. Sitchinava, "Parallel External Memory Graph Algorithms," *24th IEEE Int. Parallel & Distributed Processing Symp.* (IPDPS), 2010, 1–11.

C-139. G. Wang, T. Luo, M.T. Goodrich, W. Du, and Z. Zhu, "Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting," *5th ACM Symp. on Information, Computer and Communications Security*, 2010, 226–237.

C-140. M.T. Dickerson, M.T. Goodrich, and T.D. Dickerson, "Round-Trip Voronoi Diagrams and Doubling Density in Geographic Networks," *7th Int. Symp. on Voronoi Diagrams in Science and Engineering* (ISVD), IEEE Press, 132–141, 2010. (Preliminary version of J-74.)

C-141. M.T. Dickerson, D. Eppstein, and M.T. Goodrich, "Cloning Voronoi Diagrams via Retroactive Data Structures," *18th European Symp. on Algorithms* (ESA), LNCS, vol. 6346, 2010, 362–373.

C-142. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Lombardi Drawings of Graphs," *18th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 6502, 2010, 195–207. (Preliminary version of J-76.)

C-143. E. Wolf-Chambers, D. Eppstein, M.T. Goodrich, and M. Löffler, "Drawing Graphs in the Plane with a Prescribed Outer Face and Polynomial Area," *18th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 6502, 2010, 129–140. (Preliminary version of J-77.)

C-144. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Drawing Trees with Perfect Angular Resolution and Polynomial Area," *18th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 6502, 2010, 183–194. (Preliminary version of J-82.)

C-145. A.U. Asuncion and M.T. Goodrich, "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitive Binary Attribute Vectors," *Workshop on Privacy in the Electronic Society* (WPES), held in conjunction with the 17th ACM Conf. on Computer and Communications Security (CCS), 2010, 21–30. (Preliminary version of J-81.)

C-146. D. Eppstein, M.T. Goodrich, D. Strash, and L. Trott, "Extended Dynamic Subgraph Statistics Using h-Index Parameterized Data Structures," *4th Annual Int. Conf. on Combinatorial Optimization and Applications* (COCOA), LNCS, vol. 6508, 2010, 128–141. (Preliminary version of J-79.)

C-147. M.T. Goodrich and D. Strash, "Priority Range Trees," *21st Int. Symp. on Algorithms and Computation* (ISAAC), LNCS, vol. 6506, 2010, 97–108.

C-148. D. Eppstein, M.T. Goodrich, R. Tamassia, "Privacy-Preserving Data-Oblivious Geometric Algorithms for Geographic Data," *18th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2010, 13–22.

C-149. M.T. Goodrich, "Spin-the-bottle Sort and Annealing Sort: Oblivious Sorting via Round-robin Random Comparisons," *8th Workshop on Analytic Algorithmics and Combinatorics* (ANALCO), in conjunction with the ACM-SIAM Symp. on Discrete Algorithms (SODA), 2011. (Preliminary version of J-85.)

C-150. M.T. Goodrich and F. Kerschbaum, "Privacy-Enhanced Reputation-Feedback Methods to Reduce Feedback Extortion in Online Auctions," *ACM Conf. on Data and Application*

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 92

Security and Privacy (CODASPY), 2011, 273–282.

C-151. M.T. Goodrich, "Data-Oblivious External-Memory Algorithms for the Compaction, Selection, and Sorting of Outsourced Data," *23rd ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 2011, 379–388.

C-152. M.T. Goodrich and M. Mitzenmacher, "Large-Scale Multimaps," *23rd ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 2011, 259–260.

C-153. D. Eppstein, M.T. Goodrich, F. Uyeda, and G. Varghese, "What's the Difference? Efficient Set Synchronization without Prior Context," *SIGCOMM* 218–229, 2011.

C-154. D. Eppstein, M.T. Goodrich, and M. Löffler, "Tracking Moving Objects with Few Handovers," *Algorithms and Data Structures Symp.* (WADS), 362–373, LNCS, vol. 6844, 2011.

C-155. M.T. Goodrich and M. Mitzenmacher, "Privacy-Preserving Access of Outsourced Data via Oblivious RAM Simulation," *38th Int. Colloquium on Automata, Languages and Programming (ICALP)*, LNCS, vol. 6756, 2011, 576–587.

C-156. M.T. Goodrich and P. Pszona, "External-Memory Network Analysis Algorithms for Naturally Sparse Graphs," *European Symp. on Algorithms (ESA)*, LNCS, vol. 6942, 664–676, 2011.

C-157. C. Duncan, D. Eppstein, M.T. Goodrich, S.G. Kobourov and M. Löffler, "Planar and Poly-Arc Lombardi Drawings," *Int. Symp. Graph Drawing (GD)*, LNCS, vol. 7034, 308–319, 2011. (Preliminary version of J-87.)

C-158. R. Chernobelskiy, K. Cunningham, M.T. Goodrich, S.G. Kobourov and L. Trott, "Force-Directed Lombardi-Style Graph Drawing," *Int. Symp. Graph Drawing (GD)*, LNCS, vol. 7034, 320–331, 2011.

C-159. M.T. Goodrich and M. Mitzenmacher, "Invertible Bloom Lookup Tables," *49th Allerton Conf. on Communication, Control, and Computing*, IEEE Press, **invited paper**, 2011.

C-160. M.T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, "Oblivious RAM Simulation with Efficient Worst-Case Access Overhead," *ACM Cloud Computing Security Workshop (CCSW)*, in conjunction with the 17th ACM Conf. on Computer and Communications Security (CCS), 95–100, 2011.

C-161. M.T. Goodrich and J.A. Simons, "Fully Retroactive Approximate Range and Nearest Neighbor Searching," *22nd Int. Symp. on Algorithms and Computation (ISAAC)*, Springer, LNCS, vol. 7074, 292–301, 2011.

C-162. E. Angelino, M.T. Goodrich, M. Mitzenmacher and J. Thaler, "External Memory Multimaps," *22nd Int. Symp. on Algorithms and Computation (ISAAC)*, Springer, LNCS, vol. 7074, 384–394, 2011. (Preliminary version of J-83.)

C-163. M.T. Goodrich, N. Sitchinava, and Q. Zhang, "Sorting, Searching, and Simulation in the MapReduce Framework," *22nd Int. Symp. on Algorithms and Computation (ISAAC)*, Springer, LNCS, vol. 7074, 374–383, 2011.

C-164. D. Eppstein, M.T. Goodrich, M. Löffler, D. Strash and L. Trott, "Category-Based Routing in Social Networks: Membership Dimension and the Small-World Phenomenon," *IEEE Int. Conf. on Computational Aspects of Social Networks* (CASoN), 102–107, 2011. (Preliminary version of J-84.)

C-165. M.T. Goodrich, O. Ohrimenko, M. Mitzenmacher, and R. Tamassia, "Privacy-Preserving Group Data Access via Stateless Oblivious RAM Simulation," *23rd ACM-SIAM Symp. on Discrete Algorithms* (SODA), 157–167, 2012.

C-166. M.T. Goodrich, O. Ohrimenko, M. Mitzenmacher, and R. Tamassia, "Practical Oblivious

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 93

Storage," *2nd ACM Conf. on Data and Application Security and Privacy* (CODASPY). 13–24, 2012.

C-167. M.T. Goodrich and M. Mitzenmacher, "Anonymous Card Shuffling and its Applications to Parallel Mixnets," *39th Int. Colloquium on Automata, Languages and Programming* (ICALP), Springer, LNCS, vol. 6756, 576–587, 2012.

C-168. M.T. Goodrich, O. Ohrimenko, and R. Tamassia, "Graph Drawing in the Cloud: Privately Visualizing Relational Data using Small Working Storage," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 43–54, 2012.

C-169. F.J. Brandenburg, D. Eppstein, A. Gleissner, M.T. Goodrich, K. Hanauer, and J. Reislhuber, "On the Density of Maximal 1-Planar Graphs," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 327–338, 2012.

C-170. M.J. Bannister, D. Eppstein, M.T. Goodrich, and L. Trott, "Force-Directed Graph Drawing Using Social Gravity and Scaling," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 414–425, 2012.

C-171. M.T. Goodrich and J.A. Simons, "More Graph Drawing in the Cloud: Data-Oblivious st-Numbering, Visibility Representations, and Orthogonal Drawing of Biconnected Planar Graphs," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 569–570, 2012.

C-172. M.T. Goodrich, D.S. Hirschberg, M. Mitzenmacher, and J. Thaler, "Cache-Oblivious Dictionaries and Multimaps with Negligible Failure Probability," *Mediterranean Conf. on Algorithms* (MedAlg), Springer, LNCS, vol. 7659, 203–218, 2012.

C-173. D. Eppstein, M.T. Goodrich, and D.S. Hirschberg, "Combinatorial Pair Testing: Distinguishing Workers from Slackers," *Algorithms and Data Structures Symp.* (WADS), Springer, LNCS, vol. 8037, 316–327, 2013.

C-174. D. Eppstein, M.T. Goodrich, and J.A. Simons, "Set-Difference Range Queries," *25th Canadian Conf. on Computational Geometry* (CCCG), 2013, http://www.cccg.ca/proceedings/2013/.

C-175. M.T. Goodrich and P. Pszona, "Cole's Parametric Search Technique Made Practical," *25th Canadian Conf. on Computational Geometry* (CCCG), 2013, http://www.cccg.ca/proceedings/2013/.

C-176. L. Arge, M.T. Goodrich, F. van Walderveen, "Computing Betweenness Centrality in External Memory," *IEEE Int. Conf. on Big Data* (BigData), 368–375, 2013.

C-177. M.T. Goodrich and P. Pszona, "Achieving Good Angular Resolution in 3D Arc Diagrams," *21st Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8242, 161–172, 2013.

C-178. M.T. Goodrich and P. Pszona, "Streamed Graph Drawing and the File Maintenance Problem," *21st Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8242, 256–267, 2013.

C-179. M.T. Goodrich, "Zig-zag Sort: A Simple Deterministic Data-Oblivious Sorting Algorithm Running in $O(n \log n)$ Time," *46th ACM Symp. on Theory of Computing* (STOC), 684–693, 2014.

C-180. D. Eppstein, M.T. Goodrich, M. Mitzenmacher, and P. Pszona, "Wear Minimization for Cuckoo Hashing: How Not to Throw a Lot of Eggs into One Basket," *Symp. on Experimental Algorithms* (SEA), Springer, LNCS, vol. 8504, 162–173, 2014.

C-181. O. Ohrimenko, M.T. Goodrich, and R. Tamassia, an E. Upfal, "The Melbourne Shuffle: Improving Oblivious Storage in the Cloud," *41st Int. Colloq. on Automata, Languages, and Programming* (ICALP), Springer, LNCS, vol. 8573, 556–567, 2014.

C-182. M.J. Bannister, W.E. Devanny, M.T. Goodrich, J.A. Simons, and Lowell Trott, "Windows

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 94

into Geometric Events: Data Structures for Time-Windowed Querying of Temporal Point Sets," *26th Canadian Conf. on Computational Geometry* (CCCG), 2014.

C-183. M.J. Bannister, W.E. Devanny, D. Eppstein and M.T. Goodrich, "The Galois Complexity of Graph Drawing: Why Numerical Solutions are Ubiquitous for Force-Directed, Spectral, and Circle Packing Drawings," *22nd Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8871, 149–161, 2014. (Preliminary version of J-86.)

C-184. M.J. Alam, D. Eppstein, M.T. Goodrich, S. Kobourov and S. Pupyrev, "Balanced Circle Packings for Planar Graphs," *22nd Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8871, 125–136, 2014.

C-185. M. Bannister, M.T. Goodrich, and P. Sampson, "Force-Directed 3D Arc Diagrams," *22nd Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8871, 521–522, 2014.

C-186. M.T. Goodrich and P. Pszona, "Two-Phase Bicriterion Search for Finding Fast and Efficient Electric Vehicle Routes," *22nd ACM SIGSPATIAL Int. Conf. on Adv. Geographic Information Systems* (GIS), 193–202, 2014.

C-187. M.T. Goodrich and J. Simons, "Data-Oblivious Graph Algorithms in Outsourced External Memory," *8th Int. Conf. on Combinatorial Optimization and Applications* (COCOA), LNCS, Vol. 8881, 241–257, 2014.

C-188. M.T. Goodrich, T. Johnson, M. Torres, "Knuthian Drawings of Series-Parallel Flowcharts," *23rd Int. Symp. on Graph Drawing and Network Visualization* (GD), Springer, LNCS, vol. 9411, 556–557, 2015. (See also http://arxiv.org/abs/1508.03931.)

C-189. M.T. Goodrich and A. Eldawy, "Parallel Algorithms for Summing Floating-Point Numbers," *28th ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 13–22, 2016.

C-190. W.E. Devanny, M.T. Goodrich, and K. Jetviroj, "Parallel Equivalence Class Sorting: Algorithms, Lower Bounds, and Distribution-Based Analysis," *28th ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 265–274, 2016.

C-191. D. Eppstein, M.T. Goodrich, J. Lam, N. Mamano, M. Mitzenmacher, and M. Torres, "Models and Algorithms for Graph Watermarking," *19th Information Security Conf.* (ISC), 283–301, 2016. **Best Student Paper Award**.

C-192. E. Ghosh, M.T. Goodrich, O. Ohrimenko, R. Tamassia, "Verifiable Zero-Knowledge Order Queries and Updates for Fully Dynamic Lists and Trees," *10th Conf. on Security and Cryptography for Networks* (SCN), 216–236, 2016.

C-193. M.T. Goodrich, E. Kornaropoulos, M. Mitzenmacher, R. Tamassia, "More Practical and Secure History-Independent Hash Tables," *21st European Symp. on Research in Computer Security* (ESORICS), 20-38, 2016.

C-194. J.J. Besa Vial, W.E. Devanny, D. Eppstein, and M.T. Goodrich, "Scheduling Autonomous Vehicle Platoons Through an Unregulated Intersection," *2016 Workshop on Algorithmic Approaches for Transportation Modeling, Optimization, and Systems* (ATMOS), 5:1–5:14.

C-195. M.J. Alam, M.B. Dillencourt, and M.T. Goodrich, "Capturing Lombardi Flow in Orthogonal Drawings by Minimizing the Number of Segments," *24th Int. Symp. on Graph Drawing and Network Visualization* (GD), LNCS, Vol. 9801, 608–610, 2016.

C-196. M.J. Alam, M.T. Goodrich, and T. Johnson, "Sibling-First Recursive Graph Drawing for Java Bytecode," *24th Int. Symp. on Graph Drawing and Network Visualization* (GD), LNCS, Vol. 9801, 611–612, 2016.

C-197. M.T. Goodrich, S. Gupta, and M. Torres, "A Topological Algorithm for Determining How Road Networks Evolve Over Time," *24th ACM SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems* (GIS), 31:1–31:10, 2016.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 95

C-198. M.J. Alam, M.T. Goodrich, and T. Johnson, "J-Viz: Finding Algorithmic Complexity Attacks via Graph Visualization of Java Bytecode," *13th IEEE Symp. on Visualization for Cyber Security* (VizSec), 1–8, 2016.

C-199. M.T. Goodrich, E. Kornaropoulos, M. Mitzenmacher, and R. Tamassia, "Auditable Data Structures," *2nd IEEE European Symp. on Security and Privacy* (EuroS&P), 285–300, 2017.

C-200. D. Eppstein, M.T. Goodrich, M. Mitzenmacher, and M. Torres, "2-3 Cuckoo Filters for Faster Triangle Listing and Set Intersection," *36th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems* (PODS), 247–260, 2017.

C-201. D. Eppstein, M.T. Goodrich, and N. Mamano, "Algorithms for Stable Matching and Clustering in a Grid," *18th International Workshop on Combinatorial Image Analysis* (IWCIA), 117–131, 2017.

C-202. G. Ateniese, M.T. Goodrich, V. Lekakis, C. Papamanthou, E. Paraskevas, and R. Tamassia, "Accountable Storage," *15th International Conference on Applied Cryptography and Network Security* (ACNS), 623–644, 2017.

C-203. D. Eppstein and M.T. Goodrich, "Using Multi-Level Parallelism and 2-3 Cuckoo Filters for Faster Set Intersection Queries and Sparse Boolean Matrix Multiplication," *29th ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 137–139, 2017.

C-204. W.E. Devanny, J. Fineman, M.T. Goodrich, and T. Kopelowitz, "The Online House Numbering Problem: Min-Max Online List Labeling," *25th European Symposium on Algorithms* (ESA), 33:1–33:15, 2017.

C-205. M.T. Goodrich, "Answering Spatial Multiple-Set Intersection Queries Using 2-3 Cuckoo Hash-Filters," *25th ACM SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems* (GIS), 65:1–65:4, 2017.

C-206. D. Eppstein, M.T. Goodrich, D. Korkmaz, and N. Mamano, "Defining Equitable Geographic Districts in Road Networks via Stable Matching," *25th ACM SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems* (GIS), 52:1–52:4, 2017.

C-207. M.T. Goodrich, "BIOS ORAM: Improved Privacy-Preserving Data Access for Parameterized Outsourced Storage,' *ACM Workshop on Privacy in the Electronic Society* (WPES), 41–50, 2017.

C-208. J.J. Besa Vial, W.E. Devanny, D. Eppstein, M.T. Goodrich, and T. Johnson, "Quadratic Time Algorithms Appear to be Optimal for Sorting Evolving Data," *Algorithm Engineering & Experiments* (ALENEX), 87–96, 2018.

C-209. D. Eppstein, M.T. Goodrich, N. Mamano, "Reactive Proximity Data Structures for Graphs," *13th Latin American Theoretical Informatics Symposium* (LATIN), LNCS, Vol. 10807, Springer, 777–789, 2018.

C-210. M.T. Goodrich, "Isogrammic-Fusion ORAM: Improved Statistically Secure Privacy-Preserving Cloud Data Access for Thin Clients," *13th ACM ASIA Conf. on Information, Computer and Communications Security* (ASIACCS), 699–706, 2018.

C-211. J.J. Besa Vial, W.E. Devanny, D. Eppstein, M.T. Goodrich, and T. Johnson, "Optimally Sorting Evolving Data," *45th Int. Colloq. on Automata, Languages, and Programming* (ICALP), 81:1–81:13, 2018.

C-212. G. Barequet, D. Eppstein, M.T. Goodrich, and N. Mamano, "Stable-Matching Voronoi Diagrams: Combinatorial Complexity and Algorithms," *45th Int. Colloq. on Automata, Languages, and Programming* (ICALP), 89:1–89:14, 2018.

C-213. G. Da Lozzo, D. Eppstein, M.T. Goodrich, and S. Gupta, "Subexponential-Time and FPT Algorithms for Embedded Flat Clustered Planarity," *44th Int. Workshop on Graph-Theoretic*

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 96

Concepts in Computer Science (WG), 111–124, 2018.

C-214. G. Barequet, M. De, and M.T. Goodrich, "Computing Convex-Straight-Skeleton Voronoi Diagrams for Segments and Convex Polygons," *24th International Computing and Combinatorics Conference* (COCOON), 130–142, 2018. (Preliminary version of J-90.)

C-215. M.T. Goodrich and T. Johnson, "Low Ply Drawings of Trees and 2-Trees," *30th Canadian Conference on Computational Geometry* (CCCG), 1–9, 2018.

C-216. D. Eppstein, M.T. Goodrich, J. Jorgensen, and M.R. Torres, "Geometric Fingerprint Recognition via Oriented Point-Set Pattern Matching," *30th Canadian Conference on Computational Geometry* (CCCG), 1–16, 2018.

C-217. G. Da Lozzo, D. Eppstein, M.T. Goodrich, and S. Gupta, "C-Planarity Testing of Embedded Clustered Graphs with Bounded Dual Carving-Width," *14th Int. Symp. on Parameterized and Exact Computation* (IPEC), LIPIcs, vol. 148, 9:1–9:17, 2019. **Best Paper Award**.

C-218. J.J. Besa, G. Da Lozzo, and M.T. Goodrich, "Computing k-Modal Embeddings of Planar Digraphs," *European Symposium on Algorithms* (ESA), 19:1–19:16, 2019.

C-219. N. Mamano, A. Efrat, D. Eppstein, D. Frishberg, M.T. Goodrich, S. Kobourov, P. Matias, and V. Polishchuk, "New Applications of Nearest-Neighbor Chains: Euclidean TSP and Motorcycle Graphs," *30th Int. Symp. on Algorithms and Computation* (ISAAC), 51:1–51:21, 2019.

C-220. D. Eppstein, M.T. Goodrich, J.A. Liu, and P.A. Matias, "Tracking Paths in Planar Graphs," *30th Int. Symp. on Algorithms and Computation* (ISAAC), 54:1–54:17, 2019.

C-221. J.J. Besa, M.T. Goodrich, T. Johnson, and M.C. Osegueda, "Minimum-Width Drawings of Phylogenetic Trees," *13th Int. Conf. on Combinatorial Optimization and Applications* (COCOA), LNCS, vol. 11949, 39–55, 2019.

C-222. M.T. Goodrich, Z.M. Liang, and S. Zhao, "Inverse-Rendering Based Analysis of the Fine Illumination Effects in the Salvator Mundi," *ACM SIGGRAPH Art Papers Program, 47th International Conference and Exhibition on Computer Graphics and Interactive Techniques*, 2020.

C-223. R. Afshar, M.T. Goodrich, P. Matias, and M.C. Osegueda, "Reconstructing Binary Trees in Parallel," *32nd ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 491–492, 2020.

C-224. R. Afshar, M.T. Goodrich, P. Matias, and M.C. Osegueda, "Reconstructing Biological and Digital Phylogenetic Trees in Parallel," *European Symposium on Algorithms* (ESA), 3:1–3:24, 2020.

C-225. R. Afshar, A. Amir, M.T. Goodrich, and P. Matias, "Adaptive Exact Learning in a Mixed-Up World: Dealing with Periodicity, Errors, and Jumbled-Index Queries in String Reconstruction," *27th International Symposium on String Processing and Information Retrieval* (SPIRE), 155–174, 2020.

C-226. M.T. Goodrich, R. Jacob, N. Sitchinava, "Atomic Power in Forks: A Super-Logarithmic Lower Bound for Implementing Butterfly Networks in the Nonatomic Binary Fork-Join Model," *ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2141–2153, 2021.

C-227. R. Afshar, M.T. Goodrich, P. Matias, and M.C. Osegueda, "Parallel Network Mapping Algorithms," *33rd ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 410–413, 2021.

C-228. M.T. Goodrich, S. Gupta, H. Khodabandeh, and P. Matias, "How to Catch Marathon Cheaters: New Approximation Algorithms for Tracking Paths," *17th Algorithms and Data Structures Symposium* (WADS), 442–456, 2021.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 97

C-229. R. Afshar, M.T. Goodrich, P. Matias, and M.C. Osegueda, "Mapping Networks via Parallel kth-Hop Traceroute Queries," *39th Int. Symp. on Theoretical Aspects of Computer Science* (STACS), LIPIcs, Vol. 219, 4:1–4:21, 2022.

C-230. R. Afshar, M.T. Goodrich, and E. Ozel, "Efficient Exact Learning Algorithms for Road Networks and Other Graphs with Bounded Clustering Degrees," *20th Int. Symp. on Experimental Algorithms* (SEA), 2022.

C-231. G. Barequet, S. Fukuzawa, M.T. Goodrich, D. Mount, M. Osegueda, and E. Ozel, "Diamonds are Forever in the Blockchain: Geometric Polyhedral Point-Set Pattern Matching," *34th Canadian Conf. on Computational Geometry* (CCCG), 2022.

Other Publications:

O-1. M.T. Goodrich, "Guest Editor's Introduction," *International Journal of Computational Geometry & Applications*, **2**(2), 1992, 113–116.

O-2. M.T. Goodrich, "Parallel Algorithms Column 1: Models of Computation," *SIGACT News*, **24**(4), 1993, 16–21.

O-3. M.T. Goodrich, V. Mirelli, M. Orletsky, and J. Salowe, "Decision tree construction in fixed dimensions: Being global is hard but local greed is good," Technical Report TR-95-1, Johns Hopkins University, Department of Computer Science, Baltimore, MD 21218, May 1995.

O-4. R. Tamassia, P.K. Agarwal, N. Amato, D.Z. Chen, D. Dobkin, R.L.S. Drysdale, S. Fortune, M.T. Goodrich, J. Hershberger, J. O'Rourke, F.P. Preparata, J.-R. Sack, S. Suri, I.G. Tollis, J.S. Vitter, and S. Whitesides, "Strategic Directions in Computational Geometry Working Group Report," *ACM Computing Surveys*, **28A**(4), December 1996.

O-5. G.A. Gibson, J.S. Vitter, and J. Wilkes, A. Choudhary, P. Corbett, T.H. Cormen, C.S. Ellis, M.T. Goodrich, P. Highnam, D. Kotz, K. Li, R. Muntz, J. Pasquale, M. Satyanarayanan, D.E. Vengroff, "Report of the Working Group on Storage I/O Issues in Large-Scale Computing," *ACM Computing Surveys*, **28A**(4), December 1996.

O-6. T.H. Cormen and M.T. Goodrich, "A Bridging Model for Parallel Computation, Communication, and I/O," *ACM Computing Surveys*, **28A**(4), December 1996.

O-7. M.T. Goodrich, "Computer Science Issues in the National Virtual Observatory," in *Virtual Observatories of the Future*, ASP Conf. Series, vol. 225, R.J. Brunner, S.G. Djorgovski, and A.S. Szalay, eds., 329–332, 2001.

O-8. M.T. Dickerson and M.T. Goodrich, "Matching Points to a Convex Polygonal Boundary," Proceedings of the 13th Canadian Conf. on Computational Geometry (CCCG'01), 89–92, 2001.

O-9. M.T. Goodrich, "Guest Editor's Foreword," *Algorithmica*, **33**(3), 271, 2002.

O-10. M.T. Goodrich, M. Shin, C.D. Straub, and R. Tamassia, "Distributed Data Authentication (System Demonstration)," *DARPA Information Survivability Conf. and Exposition*, IEEE Press, Volume 2, 58–59, 2003.

O-11. M.T. Goodrich and R. Tamassia, "Efficient and Scalable Infrastructure Support for Dynamic Coalitions," *DARPA Information Survivability Conf. and Exposition*, IEEE Press, Volume 2, 246–251, 2003.

O-12. E. Ghosh, M.T. Goodrich, O. Ohrimenko, and R. Tamassia, "Poster: Zero-Knowledge Authenticated Order Queries and Applications," *IEEE Symp. on Security and Privacy*, 2015. (See also https://eprint.iacr.org/2015/283.)

O-13. F. Bayatbabolghani, M. Blanton, M. Aliasgari, and M.T. Goodrich, "Poster: Secure Computations of Trigonometric and Inverse Trigonometric Functions," *IEEE Symposium on Security and Privacy*, 2017.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 98

PROFESSIONAL SERVICE

Guest Editor:

Int. Journal of Computational Geometry & Applications, **2**(2), 1992
Journal of Computer & System Sciences, **52**(1), 1996
Computational Geometry: Theory and Applications, **12(1–2)**, 1999.
Algorithmica, **33**(3), 2002.

Editorial Board Membership:

Computational Geometry: Theory and Applications, 2006–2015
Journal of Computer & System Sciences, 1994–2011
Journal of Graph Algorithms and Applications, 1996–2011
Int. Journal of Computational Geometry & Applications, 1993–2010
Information Processing Letters, 1995–1997

Journal Advisory Board Membership:

Int. Journal of Computational Geometry & Applications, 2010–
Journal of Graph Algorithms and Applications, 2011–

Program Committee Service:

7th ACM Symp. on Computational Geometry (SoCG), 1991
1991 Workshop on Algorithms and Data Structures (WADS)
8th ACM Symp. on Computational Geometry (SoCG), 1992
25th ACM Symp. on Theory of Computing (STOC), 1993
Chair, 26th ACM Symp. on Theory of Computing (STOC), 1994
11th ACM Symp. on Computational Geometry (SoCG), 1995
DAGS '95 Conf. on Electronic Publishing and the Information Superhighway
1996 SIAM Discrete Mathematics Conference
1997 Workshop on Algorithms and Data Structures (WADS)
International Symposium on Graph Drawing (GD), 1997
1999 Workshop on Algorithms and Data Structures (WADS)
Co-chair, Workshop on Algorithm Engineering and Experimentation (ALENEX), 1999
International Symposium on Graph Drawing (GD), 2000
2000 Workshop on Algorithm Engineering (WAE)
41st IEEE Symp. on Foundations of Computer Science (FOCS), 2000
2001 Workshop on Algorithms and Data Structures (WADS)
International Symposium on Graph Drawing (GD), 2001
Workshop on Algorithm Engineering and Experimentation (ALENEX), 2002
18th ACM Symp. on Computational Geometry (SoCG), 2002
13th ACM-SIAM Symp. on Discrete Algorithms (SODA), 2002
Co-Chair, Graph Drawing 2002
International Symposium on Graph Drawing (GD), 2003
16th ACM-SIAM Symp. on Discrete Algorithms (SODA), 2005
32nd Int. Colloq. on Automata, Languages and Programming (ICALP), 2005
12th Int. Computing and Combinatorics Conference (COCOON), 2006
13th ACM Conf. on Computer and Communication Security (CCS), 2006
15th Annual European Symposium on Algorithms (ESA), 2007
5th International Conference on Applied Cryptography and Network Security (ACNS), 2007
21st IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2007
19th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2007
5th Workshop on Algorithms and Models for the Web-Graph (WAW), 2007

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 99

7th International Workshop on Experimental Algorithms (WEA), 2008
Second International Frontiers of Algorithmics Workshop (FAW), 2008
16th ACM SIGSPATIAL Int. Symp. on Adv. in Geographic Information Systems (GIS), 2008
17th ACM SIGSPATIAL Int. Symp. on Adv. in Geographic Information Systems (GIS), 2009
31st IEEE Symposium on Security and Privacy (S&P), 2010
18th Int. Symp. on Graph Drawing (GD), 2010
2011 Workshop on Analytic Algorithmics and Combinatorics (ANALCO)
8th Workshop on Algorithms and Models for the Web Graph (WAW), 2011
19th International Symposium on Graph Drawing (GD), 2011
24th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2012
20th European Symposium on Algorithms (ESA), 2012
2013 IEEE Int. Conf. on Big Data (BigData), 2013
30th IEEE Int. Conf. on Data Engineering (ICDE), 2014
21st ACM Conf. on Computer and Communication Security (CCS), 2014
Sympoisum on Algorithms and Data Structures (WADS), 2015
ACM Cloud Computing Security Workshop (CCSW), 2015
International Symposium on Graph Drawing (GD), 2015
co-chair, 2016 Workshop on Algorithm Engineering and Experiments (ALENEX)
2016 Workshop on Massive Data Algorithmics (MASSIVE)
2016 Int. Symposium on Algorithms and Computation (ISAAC)
29th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2017
25th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems (GIS), 2017
26th European Symposium on Algorithms (ESA), 2018
26th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems (GIS), 2018
2nd Symposium on Simplicity in Algorithms (SOSA), 2019
1st ACM SIGSPATIAL Int. Workshop on Spatial Gems, 2019
2021 SIAM Applied Computational & Discrete Algorithms (ACDA)

Conference/Workshop Committee Service:

Conference chair, 12th ACM Symposium on Computational Geometry, 1996
Organizer, 1st CGC Workshop on Computational Geometry, 1996
Co-chair, 1999 Dagstuhl Workshop on Computational Geometry, 1999
Conference chair, Graph Drawing, 2002
Co-organizer, Hawaiian Workshop on Parallel Algorithms, 2017, 2019

Steering Committee and Executive Committee Service:

Member at large, ACM SIG on Algorithms & Comp. Theory (SIGACT) Exec. Comm., 1993–97
Member, Exec. comm. for 1996 Federated Computing Research Conference (FCRC)
co-Founder and member, Steering Comm. for Workshop on Algorithm Engineering and Experimentation (ALENEX), 1999–2017 (chair, 2014–16)
co-Chair, Steering Comm. for ACM Symposium on Computational Geometry, 1999–2001
Member, Steering Comm. for Graph Drawing Conference, 2000–03, 2014–16
Conference Chair, ACM SIG on Algorithms & Comp. Theory (SIGACT), 2005–09

Center and Institute Affiliations:

Algorithms, Combinatorics and Optimization Center, UCI
Center for Algorithms and Theory of Computation, UCI
Center for Embedded and Cyber-physical Systems, UCI
Center for Machine Learning and Intelligent Systems, UCI
The Institute for Virtual Environments and Computer Games (IVECG), UCI
Secure Computing & Networking Center, UCI

Postdoctoral Fellows:

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 100

1. Timothy Chan, Johns Hopkins, 1996. (Now at Univ. of Illinois)
2. Gill Barequet, Johns Hopkins, 1996-98. (Now at Technion)
3. Pawel Gajer, Johns Hopkins, 2000. (Now at Univ. of Maryland)
4. Amitabh Chaudhary, UC-Irvine, 2002-2004. (Now at U. Chicago)
5. Amitabha Bagchi, UC-Irvine, 2002-2004. (Now at IIT-Dehli)
6. Martin Nollenburg, UC-Irvine, 2010, mentored jointly with David Eppstein. (Now at TU Wien)
7. Maarten Loffler, UC-Irvine, 2010-2011, mentored jointly with David Eppstein. (Now at Utrecht University)
8. Md. Jawaherul Alam, UC-Irvine, 2015-16. (Now at Amazon)
9. Giordano Da Lozzo, UC-Irvine, 2016-2017, mentored jointly with David Eppstein. (Now at "Roma Tre" University)

Ph.D. Students:

1. Mujtaba Ghouse, "Randomized Parallel Computational Geometry in Theory and Practice," Johns Hopkins Univ., May 1993.
2. Paul Tanenbaum, "On Geometric Representations of Partially Ordered Sets," Johns Hopkins Univ., May 1995 (co-advised with Edward Scheinerman).
3. Mark Orletsky, "Practical Methods for Geometric Searching Problems with Experimental Validation," Johns Hopkins Univ., May 1996.
4. Kumar Ramaiyer, "Geometric Data Structures and Applications," Johns Hopkins Univ., Aug. 1996.
5. Christian Duncan, "Balanced Aspect Ratio Trees," Johns Hopkins Univ., Aug. 1999.
6. Christopher Wagner, "Graph Visualization and Network Routing," Johns Hopkins Univ., Oct. 1999 (co-advised with Prof. Lenore Cowen).
7. Stephen Kobourov, "Algorithms for Drawing Large Graphs," Johns Hopkins Univ., May 2000.
8. Amitabha Bagchi, "Efficient Strategies for Topics in Internet Algorithmics," Johns Hopkins Univ., Oct. 2002.
9. Amitabh Chaudhary, "Applied Spatial Data Structures for Large Data Sets," Johns Hopkins Univ., Oct. 2002.
10. Breno De Medeiros, "New Cryptographic Primitives with Applications to Information Privacy and Corporate Confidentiality," Johns Hopkins Univ., May 2004 (co-advised with Giuseppe Ateniese).
11. "Jeremy" Yu Meng, "Confluent Graph Drawing," UC-Irvine, June 2006.
12. Jonathan Zheng Sun, "Algorithms for Hierarchical Structures, with Applications to Security and Geometry," UC-Irvine, Aug. 2006.
13. Nodari Sitchinava, "Parallel External Memory Model—A Parallel Model for Multi-core Architectures," UC-Irvine, Sep. 2009.
14. Darren Strash, "Algorithms for Sparse Geometric Graphs and Social Networks," UC-Irvine, May 2011 (co-advised with with David Eppstein).
15. Lowell Trott, "Geometric Algorithms for Social Network Analysis," UC-Irvine, May 2013.
16. Joseph Simons, "New Dynamics in Geometric Data Structures," UC-Irvine, May 2014.
17. Pawel Pszona, "Practical Algorithms for Sparse Graphs," UC-Irvine, May 2014.
18. William E. Devanny, "An Assortment of Sorts: Three Modern Variations on the Classic Sorting Problem," UC-Irvine, July 2017 (co-advised with David Eppstein).
19. Siddharth Gupta, "Topological Algorithms for Geographic and Geometric Graphs," UC-

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 101

Irvine, Aug. 2018 (co-advised with with David Eppstein).

20. Timothy Johnson, "Graph Drawing Representations and Metrics with Applications," UC-Irvine, Aug. 2018.
21. Juan Besa, "Optimization Problems in Directed Graph Visualization," UC-Irvine, Aug. 2019.
22. Nil Mamano Grande, "New Applications of the Nearest-Neighbor Chain Algorithm," UC-Irvine, Sep. 2019 (co-advised with David Eppstein).
23. Pedro Matias, "Exact Learning of Sequences from Queries and Trackers," UC-Irvine, May 2021
24. Martha Osegueda, "Constructing, Counting and Matching Combinatorial and Geometric Shapes," UC-Irvine, May 2022

Ph.D. Committee Service:

John Augustine	UC-Irvine	Advancement to candidacy, September 2003
Nikos Triandopoulos	Brown U.	Thesis prelim., February 2004
Einar Mykletun	UC-Irvine	Advancement to candidacy, March 2004
Kartic Subr	UC-Irvine	Advancement to candidacy, September 2004
S. Joshua Swamidass	UC-Irvine	Advancement to candidacy, April 2005
Jeong Hyun Yi	UC-Irvine	Thesis defense, August, 2005
Nodari Sitchinava	UC-Irvine	Advancement to candidacy, chair, December 2005
John Augustine	UC-Irvine	Thesis defense, July 2006
Maithili Narasimha	UC-Irvine	Thesis defense, August, 2006
Josiah Carlson	UC-Irvine	Advancement to candidacy, August 2006
Xiaomin Liu	UC-Irvine	Advancement to candidacy, September 2006
Gabor Madl	UC-Irvine	Advancement to candidacy, September 2006
Nikos Triandopoulos	Brown U.	Thesis defense, September 2006
Rabia Nuray-Turan	UC-Irvine	Advancement to candidacy, May 2007
S. Joshua Swamidass	UC-Irvine	Thesis defense, June 2007
Michael Sirivianos	UC-Irvine	Advancement to candidacy, June 2007
Kevin Wortman	UC-Irvine	Advancement to candidacy, August 2007
Di Ma	UC-Irvine	Advancement to candidacy, December 2007
Josiah Carlson	UC-Irvine	Thesis defense, December 2007
Michael Nelson	UC-Irvine	Advancement to candidacy, chair, March 2008
Minas Gjoka	UC-Irvine	Advancement to candidacy, June 2008
Sara Javanmardi	UC-Irvine	Advancement to candidacy, June 2008
Ali Zandi	UC-Irvine	Advancement to candidacy, September 2008
Jihye Kim	UC-Irvine	Thesis defense, September 2008
Darren Strash	UC-Irvine	Advancement to candidacy, December 2008
Kevin Wortman	UC-Irvine	Topic defense, January 2009
Nodari Sitchinava	UC-Irvine	Topic defense, chair, June 2009
Fabio Soldo	UC-Irvine	Advancement to candidacy, July 2009
Emil De Cristofaro	UC-Irvine	Advancement to candidacy, July 2009
Di Ma	UC-Irvine	Thesis defense, August 2009
Yanbin Lu	UC-Irvine	Advancement to candidacy, December 2009
Anh Le	UC-Irvine	Advancement to candidacy, April 2010
Lowell Trott	UC-Irvine	Advancement to candidacy, June 2010
Xiaomin Liu	UC-Irvine	Thesis defense, August 2010
Josh Olsen	UC-Irvine	Advancement to candidacy, September 2010
Yasser Altowim	UC-Irvine	Advancement to candidacy, December 2010

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 102

Angela Wong	UC-Irvine	Advancement to candidacy, May 2011
Joshua Hill	UC-Irvine	Advancement to candidacy, September 2011
Alex Abatzoglou	UC-Irvine	Advancement to candidacy, September 2011
Michael Wolfe	UC-Irvine	Masters Thesis defense, October 2011
Olya Ohrimenko	Brown Univ.	PhD Thesis proposal, October 2011
Yanbin Lu	UC-Irvine	PhD Thesis defense, November 2011
Chun Meng	UC-Irvine	Advancement to candidacy, December 2011
Abinesh Ramakrishnan	UC-Irvine	Advancement to candidacy, March 2012
Pegah Sattari	UC-Irvine	PhD Thesis defense, April 2012
Michael Bannister	UC-Irvine	PhD Thesis defense, May 2015
Yingyi Bu	UC-Irvine	PhD Thesis defense, August 2015
Jenny Lam	UC-Irvine	PhD Thesis defense, November 2015
Timothy Johnson	UC-Irvine	Advancement to candidacy, chair, June 2016
Jiayu Xu	UC-Irvine	Advancement to candidacy, November 2016
Sky Faber	UC-Irvine	PhD Thesis defense, November 2016
Juan Jose Besa Vial	UC-Irvine	Advancement to candidacy, chair, March 2017
William Devanny	UC-Irvine	PhD Thesis defense, co-chair, July 2017
Ingo van Duijn	Aarhus Univ.	PhD Thesis defense, September 2017
Siddharth Gupta	UC-Irvine	Advancement to candidacy, January 2018
Boyang Wei	UC-Irvine	PhD Thesis defense, August 2018
Timothy Johnson	UC-Irvine	PhD Thesis defense, chair, August 2018
Siddharth Gupta	UC-Irvine	PhD Thesis defense, August 2018
Pedro Matias	UC-Irvine	Advancement to candidacy, chair, May 2019
Juan Jose Besa Vial	UC-Irvine	PhD Thesis defense, chair, August 2019
Sameera Chayyur	UC-Irvine	Advancement to candidacy, September 2019
Nil Mamano Grande	UC-Irvine	PhD Thesis defense, co-chair, September 2019
Yihan Sun	CMU	PhD Thesis defense, October 2019
Martha Osegueda	UC-Irvine	Advancement to candidacy, chair, June 2020
Tatiana Bradley	UC-Irvine	PhD Thesis defense, December 2020
Julius Ceasar Aguma	UC-Irvine	Advancement to candidacy, December 2020
Ramtin Afshar	UC-Irvine	Advancement to candidacy, chair, March 2021
Pedro Matias	UC-Irvine	PhD Thesis defense, chair, May 2021
Elham Havvaei	UC-Irvine	PhD Thesis defense, May 2021
Daniel Frishberg	UC-Irvine	Advancement to candidacy, May 2021
Hadi Khodabandeh	UC-Irvine	Advancement to candidacy, July 2021
Sameera Ghayyur	UC-Irvine	PhD topic defense, February 2022
Rohith Gangam	UC-Irvine	Advancement to candidacy, May 2022
Martha Osegueda	UC-Irvine	PhD Thesis defense, chair, May 2022
Yanqi Gu	UC-Irvine	Advancement to candidacy, June 2022

University Service:

Ph.D. Requirements Committee, Dept. of Computer Science, chair: 1987–89
Graduate Admissions Committee, Dept. of Computer Science, 1991–1993 (chair: 1992)
Faculty Recruiting Committee, Dept. of Computer Science, 1993,95,96 (chair: 1996)
Steering Committee, Whiting School of Engineering, 1990–93 (chair, 1993)
Johns Hopkins Homewood Academic Computing Oversight Committee, 1990–93
Curriculum Committee, Whiting School of Engineering, 1994–96
Strategic Planning Committee, Whiting School of Engineering, 1999–00

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 103

Graduate Policy Committee, UCI Dept. of Information & Computer Science (ICS), 2001–02
Faculty Search Committee in Cryptography, UCI Dept. of ICS, 2001–03
School of Info. and Computer Science Executive Committee, 2002–04
UCI Committee on Educational Policy (CEP), 2002–03, 2004–06
UCI Change of Major Criteria Committee, 2002–03
UCI CEP Policy Subcommittee, 2002–2003
Distinguished Faculty Search Committee, Bren School of ICS, 2004–11 (chair, 2007–08)
Equity Advisor, Bren School of ICS, 2005–09
Dean's Advisory Council, Bren School of ICS, 2007–13
Associate Dean for Faculty Development, Bren School of ICS, 2006–12
Chair, Department of Computer Science, Bren School of ICS, 2012–13
Master of Computer Science Development Committee, Bren School of ICS, 2013–2016
Stragic Planning Committee, Dept. of Computer Science, Bren School of ICS, 2015–16
Master of Computer Science Steering/Admissions Comm., Bren School of ICS, 2016–
Executive Committee, Bren School of ICS, 2017–18
UC-Irvine Senate Committee on Scholarly Honors & Awards, 2017–20
UC-Irvine Special Research Program Review Committee for CalIT2, 2018–19

Courses Taught and Developed:

Advanced Parallel Computing (developed and taught at Johns Hopkins)
Cyber-Puzzlers (designed and taught at UCI)
Computer Literacy (taught at Purdue, developed at Johns Hopkins)
Computer Programming for Scientists and Engineers (taught at Purdue)
Computer Security Algorithms (developed and taught at UCI)
Computational Models (revised and taught at Johns Hopkins)
Computational Geometry (revised and taught at Johns Hopkins and UCI)
Compiler Theory and Design (revised and taught at Johns Hopkins)
Computer Graphics (taught at Johns Hopkins)
Cyber-Fraud Detection and Prevention (designed and taught at UCI)
Data Structures (revised and taught at Johns Hopkins and UCI)
Graph Algorithms (revised and taught at UCI)
Formal Languages and Automata Theory (revised and taught at UCI)
Fundamentals of Algorithms with Applications (revised and taught at UCI)
Introduction to Algorithms (developed and taught at Johns Hopkins and UCI)
Internet Algorithmics (developed and taught at Johns Hopkins, Brown, and UCI)
Design and Analysis of Algorithms (revised and taught at Johns Hopkins and UCI)
Parallel Algorithms (developed and taught at Johns Hopkins and Univ. of Illinois)
Project in Algorithms and Data Structures (revised and taught at UCI)
Text Processing and Pattern Matching (developed and taught at UCI)

Consulting:

APAC Security, Inc., 2005
Algomagic Technologies, Inc., 2000–2005
Army Research Laboratory, Fort Belvior, 1995
AT&T, 1998
Battelle Research Triangle, Columbus Division, 1996
Brown University, 2000–2007
3M, 2015
Purdue University, 2002

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 104

The National Science Foundation, 1990–2016
Univ. of Miami, 1999
Walt Disney Animation Studios, 2009
Technical expert and expert witness, retained for IP litigations, 2012–

GRANTS AND CONTRACTS

1. PI, "Research Initiation Award: Parallel and Sequential Computational Geometry," National Science Foundation (NSF Grant CCR-8810568), $32,914, 1988–90.
2. co-PI, "Paradigms for Parallel Algorithm Design," NSF and DARPA (as NSF Grant CCR-8908092), $523,837, 1989–93 (with S.R. Kosaraju (PI), S. Kasif, and G. Sullivan).
3. PI, "Parallel Computation and Computational Geometry," NSF (Grant CCR-9003299), $67,436, 1990–93.
4. co-PI, "A Facility for Experimental Validation," NSF (Grant CDA-9015667), $1,476,147, 1991–96 (with G. Masson (PI), J. Johnstone, S. Kasif, S.R. Kosaraju, S. Salzberg, S. Smith, G. Sullivan, L. Wolff, and A. Zwarico).
5. PI, "Parallel Network Algorithms for Cell Suppression," The Bureau of the Census (JSA 91-23), $14,998 1991–92.
6. PI, "A Geometric Framework for the Exploration & Analysis of Astrophysical Data," NSF (Grant IRI-9116843), $535,553, 1991–96 (with S. Salzberg and H. Ford (from Physics and Astronomy Dept.)).
7. PI, "Research Experiences for Undergraduates supplement to IRI-9116843," NSF, $4,000, 1993–94 (with S. Salzberg and H. Ford).
8. PI, "Constructing, Maintaining, and Searching Geometric Structures," NSF (Grant CCR-9300079), $134,976, 1993–96.
9. co-PI, "Robust and Applicable Geometric Computing," Army Research Office (ARO MURI Grant DAAH04-96-1-0013), $4,500,000, 1996–2000 (with F. Preparata (PI, Brown U.), R. Tamassia (Brown U.), S. Rao Kosaraju, J. Vitter (Duke U.), and P. Agarwal (Duke U.)). Subaward size: $1,466,640.
10. PI, "Application-Motivated Geometric Algorithm Design," NSF (Grant CCR-9625289), $107,389, 1996-98.
11. co-PI, "vBNS Connectivity for the Johns Hopkins University," NSF, $350,000, 1997–99 (with T.O. Poehler (PI), D.J. Binko, J.G. Neal, and A.S. Szalay).
12. co-PI, "Product Donation, Technology for Education Program," Intel Corporation, $480,071, 1997–2001 (with T.O. Poehler (PI), J.H. Anderson, A.S. Szalay, and M. Robbins).
13. co-PI, "A Networked Computing Environment for the Manipulation & Visualization of Geometric Data" (Research Infrastructure), NSF, $1,638,785, 1997–2003 (with L.B. Wolff (PI), Y. Amir, S.R. Kosaraju, S. Kumar, R. Tamassia (Brown U.), R.H. Taylor, and D. Yarowsky).
14. PI, "Geometric Algorithm Design and Implementation," NSF, Grant CCR-9732300, $224,982, 1998–2002.
15. PI, "Certification Management Infrastructure – Certificate Revocation," $52,023, 1998, NSA LUCITE grant.
16. PI, "Software Engineering Data Loading, Analysis, and Reporting," $41,614, 1998, NSA LUCITE grant.
17. PI, "Establishing a LUCITE Collaboration Environment," $10,018, 1998, NSA LUCITE grant.
18. PI, "In Support of a Secure Multilingual Collabortive Computing Environment," $51,471, 1999-2000, NSA LUCITE grant.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 105

19. PI, "Accessing Large Distributed Archives in Astronomy and Particle Physics," $199,981. subcontract to UCI from Johns Hopkins Univ. on NSF Grant PHY-9980044 (total budget, $2,500,000), 1999–2004.
20. PI, "Efficient and Scalable Infrastructure Support for Dynamic Coalitions," $1,495,000, DARPA Grant F30602-00-2-0509, 2000-2003 (with Robert Cohen and Roberto Tamassia), including $227,893 subaward to UCI (with Gene Tsudik).
21. PI, "Graph Visualization and Geometric Algorithm Design," $400,000, NSF Grant CCR-0098068, 2001-2004 (with Roberto Tamssia).
22. PI, "Collaborative Research: Teaching Data Structures to the Millennium Generation," $125,00, NSF Grant DUE-0231467, 2003–2005.
23. PI, "Collaborative Research: An Algorithmic Approach to Cyber-Security," $100,000, NSF Grant CCR-0311720, 2003–2006.
24. PI, "The OptIPuter," $900,000, subcontract from UCSD on NSF ITR grant CCR-0225642 (total budget, $13.5 million), 2002–2007 (with Padhraic Smyth and Kane Kim).
25. PI, "ITR: Algorithms for the Technology of Trust," $300,000, NSF Grant CCR-0312760, 2003–2009.
26. co-PI, "SDCI Data New: Trust Management for Open Collaborative Information Repositories: The CalSWIM Cyberinfrastructure," NSF grant OCI-0724806, $1,103,590, 2007–2012.
27. co-PI, "Support for Machine Learning Techniques for Cyber-Fraud Detection," Experian Corporation, $200,000 gift, 2008.
28. PI, "IPS: Collaborative Research: Privacy Management, Measurement, and Visualization in Distributed Environments," NSF Grant IIS-0713046, $224,851, 2007–2009.
29. PI, "Collaborative Research: Algorithms for Graphs on Surfaces," $400,000, NSF Grant CCR-0830403, 2008–2011.
30. PI, "ROA Supplement: IPS: Collaborative Research: Privacy Management, Measurement, and Visualization in Distributed Environments," NSF Grant IIS-0847968, $25,000, 2008–2009.
31. co-investigator, "Scalable Methods for the Analysis of Network-Based Data," Office of Naval Research: Multidisciplinary University Research Initiative (MURI) Award, number N00014-08-1-1015, $529,152, 2008–2014.
32. PI, "EAGER: Usable Location Privacy for Mobile Devices," NSF Grant 0953071, $300,000, 2009–2011.
33. PI, "TC:Large:Collaborative Research: Towards Trustworthy Interactions in the Cloud," NSF Grant 1011840, $500,000, 2010-2015.
34. PI, "TWC: Medium: Collaborative: Privacy-Preserving Distributed Storage and Computation," NSF Grant 1228639, $390,738, 2012-2018.
35. PI, "Support for Research on Geometric Motion Planning," 3M Corporation, $40,000 gift, 2014.
36. PI, "A4V: Automated Analysis of Algorithm Attack Vulnerabilities," subcontract 10036982-UCI from University of Utah for DARPA agreement no. AFRL FA8750-15-2-0092, $980,000, 2015–2019.
37. PI, "TWC: Small: Collaborative: Practical Security Protocols via Advanced Data Structures," NSF Grant 1526631, $166,638, 2015–2018.
38. PI, "NSF-BSF: AF: Small: Geometric Realizations and Evolving Data," NSF Grant 1815073, $474,392, 2018–2022.
39. PI, "Collaborative Research: AF: Medium: Algorithms for Geometric Graphs," NSF Grant 2212129, $799,800, 2022–2026.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 106

SELECTED INVITED TALKS (RECENT YEARS ONLY)

- "Probabilistic Packet Marking for Large-Scale IP Traceback," Purdue Univ., 2003
- "Algorithms for Data Authentication," Harvey Mudd College, 2003
- "Efficient Tree-Based Revocation in Groups of Low-State Devices," Univ. of Arizona, 2004
- "Leap-Frog Packet Linking and Diverse Key Distributions for Improved Integrity in Network Broadcasts," Southern California Security and Cryptography Workshop, 2005
- "Is Your Business Privacy Protected?," NEXT Connections, 2005
- "Distributed Peer-to-peer Data Structures," Harvard Univ., 2006
- "Balancing Life with an Academic Research Career," Grace Hopper Conference, 2006
- "Computer Security in the Large," Univ. Texas, San Antonio, 2006
- "Inspirations in Parallelism and Computational Geometry," Brown Univ., 2006
- "Efficiency and Security Issues for Distributed Data Structures," Computer Science Distinguished Lecture Series, Johns Hopkins Univ., 2006
- "Efficiency and Security Issues for Distributed Data Structures," UCLA, 2006
- "Efficiency and Security Issues for Distributed Data Structures," Edison Distinguished Lecturer Series, Univ. of Notre Dame, 2006
- "Efficiency and Security Issues for Distributed Data Structures," Computer Science Distinguished Lecturer Series, Texas A & M Univ., 2006
- "Algorithms for Secure Computing and Searching with Applications to Medical Informatics," Purdue Univ., 2006
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be Used for DNA Sequencing, Wireless Broadcasting, and Network Security," Univ. of Southern California, 2007
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be Used for DNA Sequencing, Wireless Broadcasting, and Network Security," Univ. California, San Diego, 2007
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be Used for DNA Sequencing, Wireless Broadcasting, and Network Security," Univ. Minnesota, 2007
- "Blood on the Database: How Algorithms for Testing Blood Samples can be Used for Database Integrity," Invited Keynote, 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec), 2007
- "Space-Efficient Straggler Identification," ALCOM Seminar, Univ. of Aarhus, 2007
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be used in Modern Applications," ALCOM Seminar, Univ. of Aarhus, 2007
- "Studying Road Networks Through an Algorithmic Lens," ALCOM Seminar, Univ. of Aarhus, 2008
- "Studying Geometric Graph Properties of Road Networks Through an Algorithmic Lens," International Workshop on Computing: from Theory to Practice, 2009
- "Randomized Shellsort: A Simple Oblivious Sorting Algorithm," Distinguished Lecture Series, Department of Computer Science, Brown University, 2009
- "Simulating Parallel Algorithms in the MapReduce Framework with Applications to Parallel Computational Geometry," MASSIVE 2010
- "Data Cloning Attacks for Nearest-Neighbor Searching based on Retroactive Data Structures," Department of Computer Science, UCSB, 2011
- "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitve Binary Attribute Vectors," Department of Computer Science Distin-

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 107

guished Lecturer Series, Univ. of Illinois, Chicago, 2011

- "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitve Binary Attribute Vectors," Department of Computer Science, Purdue Univ., 2011
- "Spin-the-bottle Sort and Annealing Sort: Oblivious Sorting via Round-robin Random Comparisons," Department of Computer Science, Brown Univ., 2012
- "Using Data-Oblivious Algorithms for Private Cloud Storage Access," Qatar University, 2013
- "Using Data-Oblivious Algorithms for Private Cloud Storage Access," Department of Computer Science and Engineering Distinguished Speaker Series, University of Buffalo, 2013
- "Force-Directed Graph Drawing Using Social Gravity and Scaling," invited talk, ICERM Workshop on Stochastic Graph Models, Providence, RI, 2014
- "Invertible Bloom Lookup Tables and Their Applications in Large-Scale Data Analysis," invited key-note speaker, Algorithms for Big Data, Frankfurt, Germany, 2014
- "Invertible Bloom Lookup Tables and Their Applications in Large-Scale Data Analysis," Brown University, Providence, RI, 2014
- "Studying Road Networks Through an Algorithmic Lens," Bold Aspirations Visitor and Lecture, University of Kansas, 2015
- "Learning Character Strings via Mastermind Queries, with Case Studies," Invited Lecture, Workshop on Pattern Matching, Data Structures and Compression, Bar-Ilan University, Tel Aviv, Israel, 2016
- "Invertible Bloom Lookup Tables and Their Applications in Data Analysis," University of Hawaii, 2016
- "Invertible Bloom Lookup Tables," Purdue University, 2016
- "Combinatorial Pair Testing: Distinguishing Workers from Slackers," Calvin Univ., 2016
- "Invertible Bloom Lookup Tables," University of California, Riverside, 2016
- "2-3 Cuckoo Filters for Faster Triangle Listing and Set Intersection," Technion, Israel Institute of Technology, Haifa, Israel, 2017
- "2-3 Cuckoo Filters for Faster Triangle Listing and Set Intersection," University of Arizona, 2017
- "Parallel Computational Geometry," First Hawaii Workshop on Parallel Algorithms and Data Structures, University of Hawaii, 2017
- "Fighting Gerrymandering with Algorithmic Fairness," Calvin University, 2019
- "Fighting Gerrymandering with Algorithmic Fairness," Carnegie Mellon University, 2019
- "Sorting Evolving Data in Parallel," Second Hawaii Workshop on Parallel Algorithms and Data Structures, University of Hawaii, 2019
- "Dealing with Big Data via External Memory Algorithms and Data Structures," Aarhus University, Denmark, 2021
- "Dealing with Big Data via External Memory Algorithms and Data Structures," Royal Danish Academy of Sciences and Letters, 2021

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 108

TECHNICAL EXPERT CONSULTING SUMMARY
(LAST FOUR YEARS)

Michael T. Goodrich, PhD



Dept. of Computer Science
Bren School of Info. & Computer Sciences
University of California, Irvine
Irvine, CA 92697-3435

Office Phone: (949)824-9366
http://www.ics.uci.edu/~goodrich/
E-mail: goodrich (at) acm.org

TECHNICAL EXPERT CONSULTING

The following is a listing of prior and current expert consulting work for Michael T. Goodrich, PhD, for the last four years, where I have testified as an expert, but it may not include confidential information, as per written agreements.

1. Apr. 2016 to present, Technical expert and deponent, retained through Kramer Levin LLP on behalf of Acceleration Bay LLC, in IPR proceedings and patent litigation, Acceleration Bay LLC v. Activision Bizzard, Inc., Electronic Arts Inc., Take-Two Interactive Software, Inc., Rockstar Games, Inc., and 2K Sports, Inc. Civil Actions No. 1:16-cv-00453-RGA, No. 1:16-cv-00454-RGA, No. 1:16-cv-00455-RGA (D. Del.).

2. May 2016 to present, Technical expert and deponent, retained through Kramer Levin LLP (transferred to Fish & Richardson) on behalf of Finjan, Inc., in PTO proceedings and patent litigations, Finjan, Inc. v. Blue Coat, Finjan, Inc. v. ESET, LLC, Finjan, Inc. v. Juniper Networks, Inc., Finjan, Inc. v. Palo Alto Networks, Inc., Finjan, Inc. v. Cisco Systems, Inc., Finjan, Inc. v. Qualys, Inc., Finjan, Inc. v. Rapid7, Inc., and Finjan, Inc. v. SonicWall, Inc., Civil Actions 5:15-cv-03295-BLF-PSG (N.D. Cal.), 3:17-cv-05659-WHA (N.D. Cal.), 3:17-cv-0183-CAB-BGS (S.D. Cal.), 17-cv-0072-BLF-SVK (N.D. Cal.), 4:18-cv-07229-YGR (N.D. Cal.), 1:18cv-01519-MN (Del.), and 5:17-cv-04467-BLF (N.D. Cal.).

3. Jan. 2017 to Jan. 2021, Technical expert and deponent, retained by Fitzpatrick, Cella, Harper & Scinto, Venable LLP, on behalf of Koninklijke Philips N.V. and U.S. Philips Corp., in patent litigation, Philips v. Acer Inc., ASUSTeK Computer, Double Power Tech., HTC, Southern Telecom, Visual Land, Zowee Marketing Co., Ltd., Shenzen Zowee Technology Co., Ltd., YiFang USA, Inc. d/b/a EFun, Inc., and Intervenor/Counterclaim Defendant Microsoft Corporation. Civil Actions No. 15-1125-GMS, No. 15-1126-GMS, No. 15-1127-GMS, No. 15-1128-GMS, No. 15-1130-GMS, No. 15-1131-GMS, No. 15-1170-GMS (D. Del.), and 4:18-cv-01885-HSG (N.D. Cal., Oakland Div.).

4. Jul. 2017 to Dec. 2018, Technical expert and deponent, retained by Haynes and Boone, LLP, on behalf of mSIGNIA, in patent litigation, mSIGNIA v. InAuth. Civil Action No. 8:17-cv-01289-AG-KES (C.D. Cal.).

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 109

5. Nov. 2017 to Jun. 2019, Technical expert, declarant, and deponent, retained by Thompson & Knight LLP on behalf of SEVEN Networks LLC, in patent litigation, SEVEN Networks LLC v. Google, Samsung, and ZTE. Civil Actions No. 2:17-CV-441-JRG, No. 2:17-CV-442-JRG (E.D. Texas), and 3:17-cv-1495-M (N.D. Texas).

6. Jun. 2018 to present, Technical expert, deponent, and trial expert witness, retained through Kramer Levin LLP on behalf of Centripetal Networks, Inc., in IPRs and patent litigation, Centripetal Networks, Inc. v. Keysight Technologies, Inc. and Ixia, and Cisco. Civil Actions No. 2:17-cv-00383/HCM-LRL and 2:18-cv-00094-HCM-LRL (E.D. Virginia, Norfolk Div.), IPR2018-01386, IPR2018-01443, IPR2018-01444, IPR2018-01512, and IPR2018-01513 (PTAB).

7. Feb. 2019 to present, Technical expert, declarant, and deponent, retained through Reichman Jorgensen LLP on behalf of Kove IO, Inc., in patent litigation, Kove IO, Inc. v. Amazon Web Services, Inc., Civil Action No. 1:18-cv-08175 (N.D. Illinois, Eastern Div.).

8. Apr. 2019 to Sep. 2020, Technical expert and deponent, retained by McKool Smith on behalf of SEVEN Networks LLC in patent litigation, SEVEN Networks LLC v. Apple, Inc. Civil Action No. 2:19-cv-115 (E.D. Texas).

9. Jun. 2019 to present, Technical expert, declarant, and deponent, retained through Kramer Levin LLP on behalf of CUPP Cybersecurity LLC, in patent litigation, CUPP Cybersecurity LLC, et al., v. Trend Micro, Inc. IPR2021-00813, IPR2021-01236, IPR2021-01237 (PTAB), Civil Action no. 3:18-cv-01251-M, 3:20-cv-03206-M (N.D. Texas).

10. Jul. 2020 to Feb. 2021, Technical expert and declarant, retained through Goodwin Procter LLP on behalf of MobileIron, Inc., in patent litigation, MobileIron, Inc. v. BlackBerry Corp. IPR2020-01741 (PTAB).

11. Aug. 2020 to present, Technical expert, retained through Thompson & Knight LLP (now Holland & Knight) on behalf of Broadcom Corp., in patent litigation, Broadcom Corp. and Avago Technologies International Sales PTE. Limited v. Netflix, Inc. Civil actions no. 8:20-cv-529 (C.D. Cal.), 3:20-cv-04677-JD (N.D. Cal.).

12. Nov. 2020 to present, Technical expert and deponent, retained through Kramer Levin LLP on behalf of Midwest Athletics and Sports Alliance LLC (MASA), in patent litigation, Midwest Athletics and Sports Alliance LLC v. RICOH USA, Inc., and Midwest Athletics and Sports Alliance LLC v. Xerox Corp. Civil Action Nos. 19-CV-00514 (E.D. Penn.) and 6:19-CV-06036-EAW-JFW (W.D. New York).

13. Mar. 2021 to present, Technical expert and deponent, retained through Nix Patterson LLP on behalf of Ikorongo Technology LLC, in patent litigation, Ikorongo v. Samsung, LG, Lyft, Uber, and Bumble Trading, Civil Action Nos. 6:20-cv-00256-ADA, 6:20-cv-00257-ADA, 6:20-cv-00258-ADA, 6:20-cv-00259-ADA, 6:20-cv-00843-ADA (W.D. Texas, Waco).

14. May 2021 to present, Technical expert and declarant, retained by McKool Smith on behalf of SEVEN Networks LLC in patent litigation, SEVEN Networks, LLC v. LG Electronics, Inc. and SEVEN Networks, LLC v. Motorola Mobility LLC. Civil Action Nos. 2:21-cv-88 (E.D. Texas) and 3:21-cv-1036 (N.D. Texas).

15. Aug. 2021 to present, Technical expert, deponent, and declarant, retained through Holland & Knight LLP on behalf of CA, Inc., in patent litigation, CA, Inc. and Avago Technologies International Sales PTE. Limited v. Netflix, Inc. Civil action no. 2:21-cv-00080-JRG-RSP (E.D. Texas).

16. Aug. 2021 to present, Technical expert, declarant, and deponent, retained through Kramer Levin LLP on behalf of Centripetal Networks, Inc., in patent litigation and IPRs, Centripetal Networks, Inc. v. Palo Alto Networks, Inc. Civil Action No. 2:21-cv-00137-RCY (E.D. Virginia, Norfolk Div.), IPR2021-01150, IPR2021-01152, and IPR2021-01157.

Patent Owner, Centripetal Networks, Inc. - Ex. 2026, p. 111