

I, Eric Cole Ph.D., have been asked by Acceleration Bay, Inc. (“Acceleration Bay”) to testify as an expert witness in the above referenced action. As part of my work in this action, I have been asked by Acceleration Bay to provide a tutorial of the technology related to U.S. Patent No. 6,701,344 (the “344 Patent”); U.S. Patent No. 6,829,634 (“634 Patent”); U.S. Patent No. 6,732,147 (the “147 Patent”); U.S. Patent No. 6,714,966 (the “966 Patent”); U.S. Patent No. 6,920,497 (the “497 Patent”); U.S. Patent No. 6,910,069 (the “069 Patent”) (collectively, the “Asserted Patents”). I expect to testify at trial on these Asserted Patents consistent with the opinions set forth in this report (the “Report”), as well as on any other issues for which I am qualified and have submitted or will submit an expert report in this action.

I. Summary of Opinions

1. I have been asked by counsel for Acceleration Bay to provide a tutorial on computer networks, network layers, routing algorithms, computer network topologies, overlay networks and the Asserted Patents.

II. Experience and Qualifications

A. Curriculum Vitae

2. The details of my education, work experience, research, and publications (including publications authored in the last 10 years) are summarized in my curriculum vitae (“CV”) attached hereto as Appendix A of this Report.

3. I hold a master's degree in computer science and a doctorate in information security and have worked in the cyber and technical information security industry for over 25 years. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

4. I am the founder of Secure Anchor Consulting where I provide cyber security consulting services and lead research and development initiatives to advance information systems security. I am a Fellow and instructor with The SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses such as SEC401-Security Essentials and SEC501-Enterprise Defender.

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

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

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

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

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

10. As Chief Technical Officer for McAfee I executed the technology strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I worked closely with groups tasked with the development of intellectual property.

11. I am a contributing author of "Securing Cyberspace for the 44th President." and served as a commissioner on cyber security for President Obama. My 8 books on cyber security include "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. I have also written several articles that have been published.

B. Prior Testimony

12. A list of cases in which I have testified at deposition or trial or in written reports during at least the past four years is attached as Appendix A of this Report.

C. Compensation

13. My rate of compensation for my work in this case is \$475 per hour plus any direct expenses incurred. My compensation is based solely on the amount of time that I devote to activity related to this case and is in no way affected by any opinions that I render. I receive no other compensation from work on this action. My compensation is not dependent on the outcome of this matter.

III. Materials Considered

14. My opinions, expressed herein, and preparation of this Report are based on the information I have reviewed to date, including the Asserted Patents and all materials referenced in this Report. My opinions are based on my knowledge and experience in the fields of computer networks and network optimization.

15. In addition to the materials referenced in this Report, a list of the materials that I have considered in forming my opinions is attached as Appendix B to this Report. *See* Appendix B.

16. I reviewed the Court's August 29, 2017 claim construction order, and my summary of the Asserted Patents below is consistent with that order.

IV. Technology Tutorial

17. I plan to present a general tutorial of technology involved in this case, including terms and concepts involved with the technology discussed in the Asserted Patents, and general concepts relating to computer networking, network architecture, and network data flow.

A. Demonstratives

18. In preparation for this tutorial, I may create simulations, graphic depictions and/or tables and charts for exhibits to aid the jury and Court in their understanding of the technology involved. While I intend to use demonstratives at trial, at this time I have not specifically created any demonstratives for this litigation.

B. Computer Networks

19. A computer network is formed when computing devices, such as servers, PCs, Xboxes, PlayStations, laptops, and/or end user devices are linked together in an arrangement that allows them to communicate with each other.

20. Regardless of the arrangement of computing devices, computing devices need to identify each other, and communicate with each other within the bounds of the computer network using a common language. This common language is called a communication protocol, such as Bluetooth, or WiFi. Just as with people, computing devices need to speak the same language in order to engage in a dialogue. To this end, the languages used for communication, both within these computer networks and across the Internet, are standardized to ensure that all devices can speak to each other.

21. The Internet facilitates communication between computing networks by linking these computer networks together using its own network. In this sense, the Internet is actually a network of computer networks.

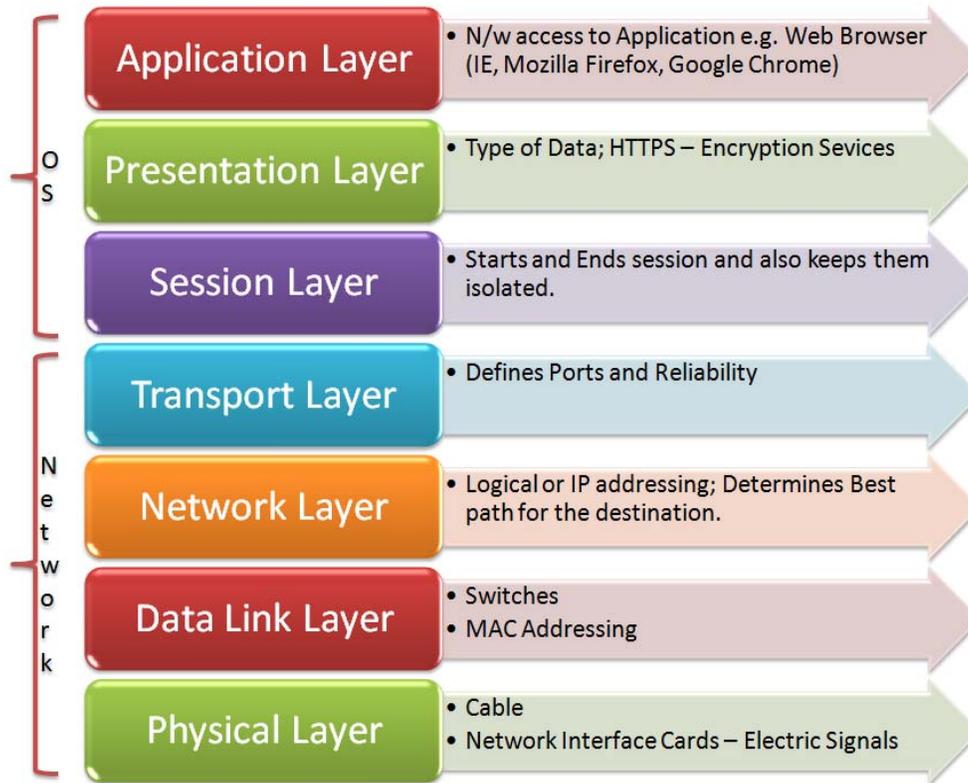
22. An Internet server is a computing device that exists on a computer network yet dialogues with computing devices external to its computer network using links provided by the Internet network. For example, a web site is a software program that runs on an Internet server.

It receives and transmits information accessible over the Internet using a communication language.

C. Network Layers

23. Communication protocols are typically modeled as layers that are partitioned in a vertical arrangement that connotes relative levels of abstraction, and collectively are called the protocol stack. Each layer uses a set of protocols to build on top of the layers below, by providing a set of services and functionality guarantees for higher layers and, to the extent possible, each layer does not depend on details or services from higher levels. To reduce complexity, most networks are designed with a small number of layers, from the physical layer, at the bottom, where computer hardware interfaces with copper wire or wireless radio, to the application layer, at the top, where the user interacts with the software.

24. The well-known Open System Interconnection (OSI) reference model is used to abstract such layers as shown below:



AB-AB 010057-59; *see also* AB-AB 009988-10024, Andrew S. Tanenbaum, Computer Networks (Third Ed.)(1996) (“Tanenbaum”) at AB-AB 009993-94.

25. Other protocol stacks also exist, which have overlapping functionality with the OSI Reference Model. The Internet Protocol stack, for example, groups the top three layers as the application layer, while keeping the bottom four layers as in the OSI Reference Model. In the OSI model, the data link layer is used to transfer data between a pair of network nodes or between nodes in a local-area network and to detect errors that occur at the physical layer, dealing with the logical aspects of sending information across network links, such as in the Ethernet protocol. *See* Tanenbaum at AB-AB 009993-99.

26. The task of the network layer is to provide for the moving of packets between any two hosts, on a best effort basis. It provides a way of individually addressing each host using a numerical label, such an IP address. This layer is concerned with packet transmission and route

searching. The Internet Protocol (“IP”) is an example of a protocol at the network layer. The task of the transport layer is to support communication based on network (e.g., IP) addresses and ports, which are numerical addresses for higher-level protocols to use. For example, the transport layer in the Internet provides a protocol, the Transmission Control Protocol (TCP), which establishes a virtual connection between a client and server and guarantees delivery of all packets in an ordered fashion. The Internet also provides a transport protocol, the User Datagram Protocol (UDP), which assumes no prior setup and delivers packets as quickly as possible but with no delivery or ordering guarantees. The role of the session layer is to manage communication sessions, that is, the exchange of information in the form of multiple back-and-forth related transmissions between two nodes, such as in the HTTP protocol, which uses TCP and supports web browsing sessions. *See* Tanenbaum at AB-AB 009993-99.

27. The presentation layer is dedicated to dealing with the translation of data between a networking service and an application and includes such functions as character encoding, data compression, and encryption and decryption of data, as in the HTTPS protocol that is used to encrypt/decrypt private web sessions. The task of the application layer is to provide protocols that support useful functions for users, based on the services provided by the lower layers. Example application-layer functions include web browsers, web-based collaboration systems, and multi-player online games. Typically, the application layer will use application programming interfaces (“APIs”) that will interact with a variety of underlying networks.

28. Designing network-based communication protocols at the application layer is completely different from designing network-based communication protocols at the network layer. An application can use network-based communication protocols designed at the application layer to provide communications across multiple networks of different types to send

data to other applications. In contrast, a network-based communication protocol that is designed at the network layer does not typically analyze the data payload generated by an application as it is routed through the network, or how the application will process its application data, because its primary function is to deliver packets containing application data in their payload from the source application to the destination application. *See* Tanenbaum at AB-AB 009993-99.

29. There are other network protocols as well, with various advantages and disadvantages. For example, the X.25 network, which was popular in the 1980's and was standardized by the Telecommunications Standardization Sector of the International Telecommunications Union ("ITU-T"). *See* AB-AB 010030 (<https://www.itu.int/rec/T-REC-X.25-199610-I/en>). This standard was created to handle digital public packet-switched networks and interface it with customers. It was designed to provide three conceptual layers, which correspond roughly with the lower three layers in the OSI model. *See* Tanenbaum at AB-AB 010000-01 and AB-AB 010031-41 (<https://en.wikipedia.org/wiki/X.25>).

D. Routing Algorithms

30. At the network level, the concern is about routing packets from a source computer to a destination computer. A routing algorithm is used to determine which line(s) an incoming packet should be transmitted out on. The routing algorithm is agnostic to actual data transferred via the packets. Control packets are used to find the routes to the destination computer. User packets follow the route established by the control packet and the updated routing tables. Examples of routing algorithms include shortest path algorithms, which transmit packets according to a shortest path to the destination in the network, and flooding, which transmits packets to all nodes in a network so as to be sure to reach the destination without knowledge of a

shortest path and even in the presence of node and link failures, as in military applications. *See* Tanenbaum at AB-AB 010002-24.

E. Computer Network Topologies

31. **Peer-to-Peer network** is a network where communication nodes in the network have roughly equal functionality and capability to communicate with each other. These systems typically allow these nodes to dynamically join and leave the system. *See* AB-AB 010025-29, Microsoft Computer Dictionary, Fourth Ed. (1999) at AB-AB 010029.

32. **Client-server network** is a network where client nodes communicate with each other through a central server node, which then forwards the messages to other client nodes. *See* Tanenbaum at AB-AB 009991-92; AB-AB 010025-29, Microsoft Computer Dictionary, Fourth Ed. (1999) at AB-AB 010027.

33. **Full-mesh topology or complete network topology** is a topology where each node is directly connected to all other nodes. AB-AB 010042-49 (https://en.wikipedia.org/wiki/Network_topology); AB-AB 010050-53 (https://en.wikipedia.org/wiki/Complete_graph).

34. **Incomplete network topology** is a topology where less than all of the communication nodes are directly connected through the topology, even if the nodes are directly connected in the underlying network.

35. **Regular network topology** is a topology where each node is connected to the same (non-zero) number of additional nodes through the topology, even if the nodes are directly connected in the underlying network. *See* AB-AB 010054-56 (https://en.wikipedia.org/wiki/Regular_graph).

F. Overlay Networks

36. An overlay network is a computer network that enables the communication nodes in one or more underlying networks to communicate with each other, and may include its own network topology. Network entities in an overlay network form virtual or logical links between them across the network topologies of each underlying network. The topology of the overlay network does not depend on the topology of the underlying network. For example, a full-mesh network or regular network can be overlaid on top of an underlying client-server network.

37. For example, the Internet is an interconnection of multiple networks, each with their own network topology. The backbone networks used to route communications through the core of the Internet may be frame relay or Ethernet networks, each with their own network topologies, whereas the consumer-facing portion of the Internet may utilize the telephone network, which has its own network topology. Further, the underlying network of an overlay network itself can be an overlay network. For example, a VoIP network can function as an overlay network over the Internet, by providing either peer-to-peer or client-server network functionality on top of the underlying Internet, which itself is an overlay network. Typically, a VoIP network can be configured with its own network topology. For example, in a typical conference call, all VoIP nodes may communicate with each other directly over the Internet, or some or all nodes may communicate indirectly through other VoIP nodes.

V. Overview of the Asserted Patents

38. The Asserted Patents are directed to novel computer network technology, developed by named inventors Fred Holt and Virgil Bourassa, working for Boeing, more than sixteen years ago. The Asserted Patents solved critical scalability and reliability problems associated with the real-time sharing of information among multiple widely distributed

computers. This innovative technology enabled large-scale, unlimited online collaborations with numerous participants continually joining and leaving -- with applications ranging from aircraft design development to multi-player online games.

39. Although each of the Asserted Patents focuses on different inventive aspects, the Asserted Patents share and incorporate the same disclosures in the Background of the Invention (the "Background"). The Background of the Asserted Patents provides an overview of point-to-point network protocols, such as UNIX pipes, TCP/IP, and UDP that allow processes on different computers to communicate via point-to-point connections. '344 Patent at 1:44-46. Although the interconnection of all participants to all other participants using point-to-point connections is theoretically possible, it does not scale well as the number of participants grows. *Id.* at 1:46-49. Because each participating process needs to manage its direct connections to all other participating processes, the number of possible participants is limited to the number of direct connections a given machine, or process, can support. *Id.* at 1:49-55.

40. The Asserted Patents are directed to computer network technology overlaying an underlying network connecting participants. The Asserted Patents describe using a broadcast channel that overlays a point-to-point network where each node (participant) is connected to its neighboring network nodes. For example, Fig. 2 of the Asserted Patents shows a network of twenty participants, where each participant is connected to four other participants. Such a network arrangement, where each node in the network is connected to the same number of other nodes, is known as an m-regular network. *Id.* at 4:38-39.

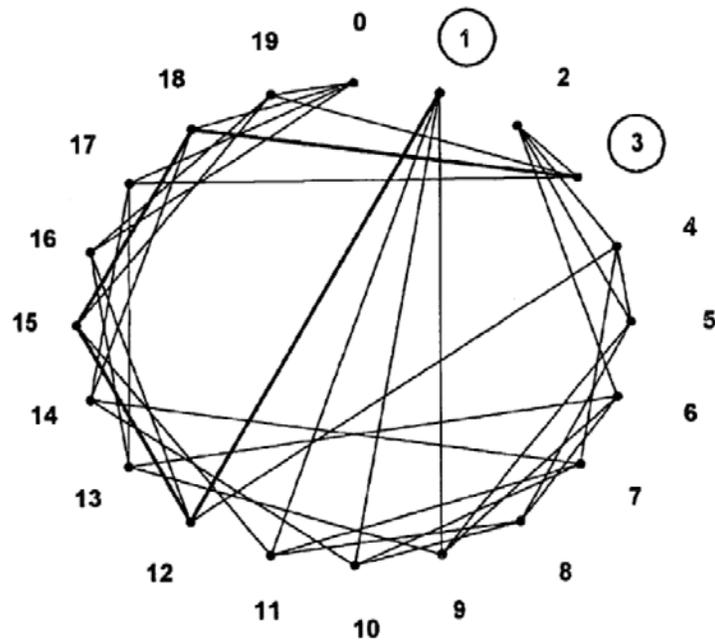


Fig. 2

41. Because the specifications of the Asserted Patents are similar, much of my discussion below applies to each of the patents, but is not repeated for purposes of brevity.

A. '344 Patent

42. The '344 Patent focuses on “a game environment” which “is provided by a game application program executing on each player’s computer.” '344 Patent at 16:30–34. In order to participate in the game environment, “[e]ach player joins a game (e.g., a first shooter game) by connecting to the broadcast channel on which the game is played.” *Id.* at 16:34–36. The gaming application programs connected to the broadcast channel form an m-regular, incomplete network in order to ensure reliability and scalability of the network. *See id.* at Claim 12, 2:38–41.

43. The broadcast channel is implemented through connections that overlay the underlying network. *Id.* at 4:19–26. The broadcast technique disclosed and claimed in the '344 Patent establishes a gaming environment that uses the broadcast channel for participants, or

gaming applications, to communicate and participate in a game. *Id.* at 16:30-34. As a result of implementing the gaming environment using a broadcast channel, each participant is connected to some—but not all—neighboring participants. *Id.* at Fig. 2, 5:65–66.

44. The ability of players to send information and game updates to all the other players is facilitated by the broadcast channel. The broadcast channel described in the ‘344 Patent (and the other Asserted Patents) can be used to distribute a wide variety of data. For example, each time a player takes an action, a message representing that action is broadcast on the game's broadcast channel. The broadcast channel also allows a player to send messages (e.g., strategy information) to one or more other players by broadcasting a message. The broadcast channel can also be used to support voice over IP-based chat (VoIP), quality of service (QoS) messaging, membership data, game control data, game updates, synchronizations and heartbeat data, indicate changes in players’ location, the arrival and departure of players, score reporting, and any other data used by the game. *Id.* at 16:30-56. The ‘344 Patent specifically describes how its technology can be applied to first-person shooter type games, as well as other types of games. *Id.* at 16:30-17:11.

45. The broadcast technique disclosed and claimed in the ‘344 Patent contemplates a gaming environment as an overlay network that utilizes an application level network communication protocol (of the OSI layering model). This network communication protocol may incorporate Presentation Layer and Session Layer abstractions of the protocol stack as well, to communicate across the Internet. ‘344 Patent at 4:15-19. This ensures that gaming applications are able to achieve a reliable, scalable network that is agnostic to the underlying network on which they are run. *Id.* at 4:1-18.

46. Each participant application process maintains the connections to its neighbors as edges in the overlay network. That is, pairs of participants share a connection established in the application layer overlay, while an underlying network (which can have a different topology) handles the actual transfer of data between the physical network components. *See* ‘344 Patent at 4:23–26. The gaming application processes, that is, the game participants, are connected to the broadcast channel so as to form an m-regular, incomplete overlay network.

B. ‘966 Patent

47. The ‘966 Patent focuses on “an information delivery service application” which “allows participants to monitor messages as they are broadcast on the broadcast channel.” ‘966 Patent at 16:25-28. The information delivery service application “may be downloaded to the user’s computer if not already available on the user’s computer.” *Id.* at 16:45-49.

48. As with the ‘344 Patent’s game environment, the information delivery service application connected to the broadcast channel forms an m-regular, incomplete network. *See* ‘966 Patent at Claims 13, 2:38–41. In one example, “a graph that is 4-regular and 4-connected which represents the broadcast channel.” *Id.* at 4:48–49. The broadcast technique disclosed and claimed in the ‘966 Patent uses the broadcast channel for participants, such as application programs, to communicate. *Id.* at 16:25-30. As a result of the service using a broadcast channel, each participant is connected to some—but not all—neighboring participants. *See id.* at Fig. 2, 5:63–6:7.

C. ‘634 Patent

49. The ‘634 Patent is directed to a novel, non-routing table based computer network and broadcast channel where participants are updated as to data broadcast on the network without the use of routing tables and without a complete graph topology. ‘634 Patent at 2:46-53.

A routing table is a table which lists and keeps track of specific routing information regarding intended routes between nodes. For example, with hop-by-hop routing, a routing table would keep the address of the next device on the path to that destination for all reachable destinations.

50. The '634 Patent focuses on a process for adding nodes, or participants, to an existing m-regular network. In order to join an existing network, a seeking computer (*e.g.* node *Z* in Fig. 3B) locates and contacts a portal computer that is fully connected to the network. *Id.* at 6:19–25. The portal computer then identifies computers to which the seeking computer will connect. *Id.* at 12:64–66.

D. '147 Patent

51. The '147 Patent focuses on the manner in which a node or participant is removed from a network, which involves a first computer sending a disconnect message to a second computer, which includes a list of the departing computer's neighbors, and the second computer broadcasting a connection port search message to find one of the first computer's neighbors to which it can connect in order to maintain an m-regular graph. '147 Patent at Abstract, 8:66-9:26.

E. '069 Patent

52. The '069 Patent focuses on a process for adding nodes, or participants, to an existing network. In order to join an existing network, a seeking computer locates and contacts a portal computer that is fully connected to the network. '069 Patent at 5:20–24. The portal computer then identifies computers to which the seeking computer will connect. *Id.* at 5:42–45. Once identified, the seeking computer joins the network by connecting to the identified computers. *Id.* at 5:20-7:6.

53. The '069 Patent describes a problem that arises when a seeking computer connects to computers directly connected to the portal computer or directly connected to one of

its neighbors: the diameter of the network increases as it “becomes elongated in the direction of where the new nodes are added.” *See id.* at 6:63–7:6, Figs. 4A-4C. In order to minimize the diameter of the graph as new nodes are added, the ‘069 Patent describes a “random selection technique to identify” neighbors for a seeking computer to connect to in joining the network. *Id.* at 7:20–28, 13:36-48.

F. ‘497 Patent

54. The ‘497 Patent focuses on methods and systems for locating and connecting to a broadcast channel. *See generally*, ‘497 Patent at 1:30-2:45. Each computer is aware of one or more “portal computers” through which that given computer may locate the broadcast channel. *Id.* at 5:37–39. Each computer connected to the broadcast channel contains communications ports for communicating with other computers. *Id.* at 6:10–12. The “user ports cannot be statically allocated to an application program because other applications programs executing on the same computer may use conflicting port numbers.” *Id.* at 11:36-39. The ‘497 Patent teaches that the ports selected may be reordered if too many computers are seeking to connect at the same time. *Id.* at 12:12-32.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on September 20, 2017 in Ashburn, Virginia.



Eric Cole, Ph.D.

APPENDIX A

Dr. Eric B. Cole
Cyber Security Expert

43605 Edison Club Court
Ashburn, VA 20147
703-675-2055



A computer and cyber security expert with over 20 years of hands-on experience, Dr. Cole consults in information technology with a focus on information technology and cyber security. He is an invited speaker for and a member of many key organizations including the Commission on Cyber Security for the 44th President and the Purdue University Executive Advisory Board, and is a senior fellow with SANS. He is the author of several books and inducted into the InfoSec European Hall of Fame in 2014.

Professional Experience

Secure Anchor Consulting Services: 2005-Present

Consulting services to Fortune 500, Fortune 50, financial institutions, international organizations and the federal government. One assignment has included a major system design and assessment for an international financial institution in Hong Kong. Employs cutting edge technology and technical components (network security, network architecture, and incident response, NOC/SOC design) to provide security solutions. Serves as an expert witness for a variety of litigation involving government and commercial companies.

SANS (SysAdmin Audit Network Security): 1999-Present

Director of Research-Computer Network Attack-Enterprise Security Architecture
Director of the Cyber Defense Initiative

Lead instructor and course developer for several security courses, including the top selling courses. One of the highest rated instructors and one of the few instructors teaching a variety of courses. Executed and contributed to the development of several of the GIAC certifications including GIAC Certified Security Essentials (GSEC), GIAC Certified Advanced Incident Handling Analysts (GCIH) and GIAC Certified Firewall Analysts (GCFW). Responsible for staying up on technology and developing new course material that teaches students the state of the art in networking, information technology, and security. Created and led several key efforts including the Levelone Notebook, top 10/20 vulnerability list and the Cyber defense initiative, including the author of the Critical Controls for Effective Cyber Defense. Developed business plans for and created new technological initiatives. Constantly researched, tested and evaluated new security products and research efforts.

STI (SANS Technology Institute): 1999-2015

Dean of Faculty

Member of a five-person team tasked with creating a degree granting institution and receiving certification from the state of Maryland. Offered two Master's degree programs focused on technical people needing managerial skills and managers needing technical skills. Designed and implemented curriculum and provided leadership to faculty to successfully deliver the degrees. Successfully achieved accreditation.

McAfee: 2009-2010**SVP, CTO of the Americas**

McAfee's visionary and evangelist responsible for strongly influencing the company's technical direction in alignment with the CEO, EVP, Product Operations and other key product executives and technologists across the world. Played an integral role in the company's strategic direction, development, and future growth as the global leader in digital security solutions. Key leader in the execution of technology strategy for technology platforms, partnerships, and external relationships. Worked closely with the CEO, EVP of Product Operations and other key stakeholders to establish a product vision and road map to achieve McAfee's goals and business strategies. Focused on identifying and capturing intellectual property and driving new innovation across the company.

Lockheed Martin: 2005-2009**IS&GS Chief Scientist****LM Senior Fellow**

The Sytex Group, Inc. (TSGI) was acquired by Lockheed Martin with a key component being the intellectual property created under the CTO leadership. I was selected by Lockheed Martin into its prestigious fellowship program, an award it makes to less than 1% of its 130,000 employees. As a Lockheed Martin Senior Fellow (the first Fellow within Lockheed Martin's Information Technology Division), I was a frequently invited speaker at a variety of conferences and security events. As Lockheed Martin Chief Scientist, performed research and development to advance the state-of-the art in information systems security. Specialized in: secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. Played a lead technical advisory role in many high-profile, security-focused projects for Federal clients to include civil, Intel and Department of Defense, including the FBI Sentinel, DHS Eagle, JPL, Hanford and FBI IATI programs.

The Sytex Group, Inc. (TSGI): 2001-2005**Chief Technology Officer (CTO)**

Positioned company to accomplish corporate growth and meet financial targets by utilizing and enhancing technology. Worked as an executive team member to determine and implement technical direction and focus of company. Extensive experience with running projects including managing development efforts to exceed client requirements. Successfully created an intellectual property base (to include patents, journals, books and white papers) – this effort resulted in an overall increase in market value. The efforts of the research team's intellectual property increased advertising, market share and customer satisfaction through conferences, proposal and magazine articles. Maintained full accountability for revenue of \$55 million and indirectly involved in revenue of over \$80 million. Provided continuous leadership to research team of over 20 people that created intellectual property that competed and surpassed teams 20 times their size. Yearly patents were in line with the top 1000 producing patent companies in the United States. Developed and executed on creative techniques for infusing technology into non-technical business units to drive revenue and profit. Interfaced with government officials, including the Pentagon, White House and Capitol Hill, and corporate executives to identify critical network security problems that needed to be addressed and researched.

GraceIC: 2000-2001**Chief Security Officer (CSO)**

Designed and executed in establishing GraceIC as a leader in the network security arena. Developed the product line and executed on the expertise to build the services. Provided management and gave direction to successful delivery on technical skills of security employees. Provided leadership and implemented the proper internal security infrastructure within Grace such as secure email, proper protection of data and security policies. Presented at several national and international conferences and wrote several articles. Performed and documented research

into the area of future applications and solutions to the network security problem existing in the current market. Trained sales people, program managers and engineers on how to sell, manage and deliver security services. Maintained a pulse on technology in the market place to produce trending and markets plans.

American Institutes for Research: 1999-2000

Chief Information Officer (CIO)

Brought in to fix and revamp the entire IT infrastructure based on the organization having several security breaches, virus outbreaks and unreliable performance on the network. Within three months stabilized the entire IT infrastructure and within nine months rebuilt the entire infrastructure. Network designed to achieve a balance between functionality and security while minimizing the monetary impact to the organization. After one year, there were no severe security breaches and all attempted breaches were contained prior to causing any significant monetary loss. Virus problems were contained and controlled and network uptime was 99.999%. Security and performance were greatly increased while overall IT costs were reduced by 15%. In addition, provided technical support for DARPA sponsored research projects. Helped invent technology and innovation that lead to a spin off company, Pynapse, which created a state of the art intrusion detection system known as Checkmate that was later sold to SAIC.

Vista Information Technologies: 1998-1999

VP of Enterprise Security Services

Developed and executed the Enterprise Security Services Group and responsible for all internal and external security issues. Tracked and managed separate profit and loss center for security. Grew the team from one person to over 12 people and executed on several million in annual revenue in less than a year. Set up the security and other monitoring services for the NOC/SOC. Created all of the security services offerings and generated all necessary marketing and sales material. Followed and assured compliance with business plan and financial tracking of security group. Performed security assessments and consulted on all areas of security. Designed, implemented and monitored security solutions including firewall design, intrusion detection, vulnerability assessment and penetration testing. Performed evaluation and analysis of security tools and provided technical recommendations and product improvements for VC funded startups. Key presenter at Cisco sponsored security seminars around the country and performed partnership activities with Fortune 500 organizations.

Teligent: 1996-1998

Director of Security

Created and in charge of IT Corporate Security Department. Central point of contact for all security concerns. Evaluated strategic plans and operational activities by performing risk assessment and determining how it might impact corporate security. Designed security solutions to meet operational needs. Integrated security and help create NOC to provide for proper monitoring of network. Developed the company's security policy and all required security guidelines across the company. Set up security lab to properly test and enhance the security features of the network. Performed and executed on several computer investigations. Assisted and advised the legal department on researching laws, regulations, and policies relating to computer and information security. Evaluated several secure email solutions and installed PGP company-wide. Established and set up web traffic monitoring and password tracking systems.

Central Intelligence Agency: 1991-1996

Received Six Exceptional Performance Awards.

Program Manager / Technical Director for the Internet Program Team with Office of Technical Services

A Senior Officer of the agency that implemented the Internet Program Team that specializes in rapid development and in exploiting the latest Internet technologies that meet customer's

requirements. The team designs, develops, tests, and deploys products in three to six month intervals. Designed and developed several secure communication systems. Responsible for providing technical direction, technical design, security assessment, and programming modules. Secured internal servers, continually perform intrusion detection, and reviewed audit logs. Performed independent security reviews and penetration testing of (World Wide Web) servers for other offices. Identified several weaknesses and devised ways to fix those problems and secure the system. Received letter of appreciation from the DCI (Director of Central Intelligence) and several Exceptional Performance Awards for this project.

Computer Engineer with Office of Security

Member of the information security assessment team. Evaluated and performed security assessment of network operating systems. Identified potential vulnerabilities and ways to secure the holes. Designed a large scale auditing system with automated review capability. Worked on several virus investigations.

Education

Doctorate degree (now PhD) in Network Security, Pace University - 2003

M.S., New York Institute of Technology - 1993

Major: Computer Science
GPA: 4.0/4.0
Honors: Harry Schure Graduate Memorial Award (awarded to one graduating senior)

B.S., New York Institute of Technology - 1992

Major: Computer Science
Minor: Business
GPA: 3.7/4.0
Honors: Graduated Magna Cum Laude, Dorothy Schure Memorial Award, Jules Singer Award, Grace Hopper Award from Computer Associates, Presidential Academic Award (4.0 all semesters), Presidential Service Award, Dean's List, Member of Who's Who Among Students in American Universities, and Member of Nu Ypsilon Tau Honor Society.

Certifications

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

Organizations / Memberships

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

Publications

Books

Eric Cole. *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*. Syngress, 2012.

Eric Cole. *Network Security Bible. 2nd Edition*, Wiley, 2009.

Eric Cole, Ronald L. Krutz, James Conley, Brian Reisman, Mitch Ruebush, Dieter Gollman, and Rachelle Reese. *Wiley Pathways Network Security Fundamentals Project Manual*. Wiley, 2007.

Eric Cole and Sandra Ring. *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. Syngress, 2006.

Eric Cole. *Hiding in Plain Sight: Steganography and the Art of Covert Communication*. Wiley, 2003.

Eric Cole. *Hackers Beware: The Ultimate Guide to Network Security*, New Riders/Sams Publishing, 2001.

Monthly Column on TechTarget - <http://www.techtarget.com/contributor/Eric-Cole>

- Supply chain security: Controlling third-party risks
- Cyberhunting: Why enterprises need to hunt for signs of compromise
- Six ways to improve endpoint device security
- Why security operations centers are the key to the future
- Offensive countermeasures: How they can slow down adversaries
- Accidental insider threats and four ways to prevent them

Selected White Papers - <https://www.sans.org/reading-room/analysts-program>

- Decision Criteria and Analysis for Hardware-Based Encryption
- Threat Hunting: Open Season on the Adversary
- Automating the Hunt for Hidden Threats

Selected Journal Publications

Eric Cole, Sandy Ring, "Taking a Lesson from Stealthy Rootkits," *IEEE Security and Privacy*, Vol 2 (4), pp. 38-45, Aug 2004

Eric Cole, Sandy Ring, "Volatile Memory Computer Forensics to Detect Kernel Level Compromise," *Lecture Notes in Computer Science, Information and Communications Security*, Springer Press, Vol 3269, ICICS Sep 2004, Malaga, Spain

Eric Cole, David Esler, and Sandy Ring, "Self-healing Mechanisms for Kernel System Compromises," Proceedings of ACM Workshop on Self-managed Systems (WOSS) 04, Oct 2004, Newport Beach, CA, USA

Eric Cole, Vignesh Kumar and Sandy Ring, "Ant colony based optimization based model for network zero-configuration," Proceedings of SPCOM 04, Dec 2004, Bangalore India

Eric Cole, Vignesh Kumar, Sandy Ring, "Transform Domain Steganography Detection using Fuzzy Inference Systems," IEEE International Symposium on Multimedia Software Engineering, 2004

Eric Cole, Vignesh Kumar and Sandy Ring, "Least Significant Bit-Spatial Domain Steganography Detection using Least Significant Bit Plane Smoothness," The 6th IASTED International Conference on SIGNAL AND IMAGE PROCESSING, 2004

Eric Cole, Sandy Ring, "Detecting Kernel Rootkits," *Sys Admin Magazine*, Vol. 12 (9), pp. 28-33, Sept 2003

Eric Cole, Ron Krutz, "The Computer Forensics CMM," Proceedings of the SPIE Defense & Security Symposium, 28 March-1 April 2005

Eric Cole and Angela Orebaugh, "Intrusion Prevention and Active Response: Implementing an Open Source Defense," *SysAdmin Magazine*, 2005

Presentations

Numerous keynotes and presentations given to corporations and government entities as well as classes and courses taught on the subjects of cyber threats, information security, and technology innovation.

Expert Witness Testimony in the Last 5 Years

Activision Blizzard, Inc. et al. v. Acceleration Bay, LLC, Case Nos. IPR 2015-01951, 2015-01953, 2015-01964, 2015-01970, 2015-01972, 2015-01996, 2016-00724, 2016-00747 – Expert declarations and deposition

Finjan, Inc. v. Blue Coat Systems, Inc., Case No. 15-cv-03295-BLF – Expert report and deposition

YLD Ltd. v. The Node Firm, LLC, Case No. 16-CV-00399-VC – Expert report and deposition

Finjan, Inc. v. ESET SPOL. S.R.O. and ESET DEUTSCHLAND GMBH, District Court - 4th Civil Chamber Werdener Str. 1, 40227 Düsseldorf - Expert report

Finjan, Inc. v. Symantec Corp., Case No. 14-CV-02998-HSG – Expert report, deposition

Finjan, Inc. v. Sophos, Inc., Case No. 14-CV-01197-WHO – Expert report, deposition and testimony – Client awarded \$15 million verdict September 2016

Finjan v. ProofPoint, Inc. and Armorize Technologies, Inc., Case No. 3:13-cv-05808-HSG – Expert report and deposition – Case settled May 2016

National Union Fire Insurance Company of Pittsburgh, Pennsylvania v. Tyco Integrated Security, LLC et al., Case No. 13-080371-CIV-BLOOM/HUNT – Expert report, deposition and testimony – April 2016

FTC v. LifeLock, Case No. CV-10-00530-PHX-MHM – Expert report – Case settled and client awarded a \$100 million settlement based on analysis in expert report August 2015

Finjan, Inc. v. Blue Coat Systems, Inc., Case No. 13-cv-03999-BLF – Expert report, deposition and testimony – Client awarded \$40 million verdict July 2015

The Trustees of Columbia University in the City of New York v. Symantec Corporation, Civil Action No. 3:13-cv-00808 – Expert report and deposition – Case settled September 2014

APPENDIX B

APPENDIX B: LIST OF MATERIALS REVIEWED

In addition to the materials set forth in my Expert Report, I have considered also the below listed documents.

Documents Produced by Acceleration Bay LLC:

Bates Numbers
AB-AB 009988-10024
AB-AB 010025-29
AB-AB 010030
AB-AB 010031-41
AB-AB 010042-49
AB-AB 010050-53
AB-AB 010054-56
AB-AB 010057-59

Other Documents

U.S. Patent No. 6,701,344
U.S. Patent No. 6,714,966
U.S. Patent No. 6,732,147
U.S. Patent No. 6,829,634
U.S. Patent No. 6,910,069
U.S. Patent No. 6,920,497

File History for U.S. Patent No. 6,701,344
File History for U.S. Patent No. 6,714,966
File History for U.S. Patent No. 6,732,147
File History for U.S. Patent No. 6,829,634
File History for U.S. Patent No. 6,910,069
File History for U.S. Patent No. 6,920,497

Memorandum Opinion, *Acceleration Bay LLC, v. Activision Blizzard, Inc.*, Civil Action No. 16-453-RGA, *Acceleration Bay LLC, v. Electronic Arts, Inc.*, Civil Action No. 16-454-RGA, *Acceleration Bay LLC v. Take-Two Interactive Software et al.*, Civil Action No. 16-455-RGA, Docket No. 275, filed on August 29, 2017

Memorandum Order, *Acceleration Bay LLC, v. Activision Blizzard, Inc.*, Civil Action No. 16-453-RGA, *Acceleration Bay LLC, v. Electronic Arts, Inc.*, Civil Action No. 16-454-RGA, *Acceleration Bay LLC v. Take-Two Interactive Software et al.*, Civil Action No. 16-455-RGA, Docket No. 276, filed on August 29, 2017

Claim Construction Order, *Acceleration Bay LLC, v. Activision Blizzard, Inc.*, Civil Action No. 16-453-RGA, *Acceleration Bay LLC, v. Electronic Arts, Inc.*, Civil Action No. 16-454-RGA, *Acceleration Bay LLC v. Take-Two Interactive Software et al.*, Civil Action No. 16-455-RGA, Docket No. 287, filed on September 6, 2017