Filed on behalf of: OpenTV, Inc.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE, INC.
Petitioner

v.

OPENTV, INC.
Patent Owner

Case IPR2015-00969
Patent 5,884,033

DECLARATION OF JUSTIN DOUGLAS TYGAR, Ph.D.

OpenTV Exhibit 2002
Apple v. OpenTV
IPR2015-00969

TABLE OF CONTENTS

I, Justin Douglas Tygar, declare as follows:

I. INTRODUCTION

1. I have been retained by OpenTV, Inc. ("OpenTV" or "Patent Owner") as an independent expert consultant in this proceeding before the United States Patent and Trademark Office. Although I am being compensated at my usual rate of $500.00 per hour for the time I spend on this matter, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding.

2. I understand that this proceeding involves U.S. Patent No. 5,884,033 ("the '033 patent") (attached as Ex. 1001 to the petition). I understand that the '033 patent issued on March 16, 1999 from U.S. application No. 08/645,636 (filed on May 15, 1996) to Spyglass, Inc., the original assignee of the '033 patent. I also understand that Spyglass, Inc. assigned the '033 patent to OpenTV. I understand that the '033 patent will expire on May 15, 2016.

3. I have been asked to provide my opinion as to how one of ordinary skill in the art would have understood claims 1, 2, 9, 15, and 23 of the '033 patent, and to consider whether U.S. Patent No. 5,790,554 to Pitcher et al. discloses the features recited in claims 1, 2, 15, and 23 and renders obvious the features recited in claim 9. My opinions are set forth below.

II. QUALIFICATIONS

4. I am a tenured, full Professor at the University of California, Berkeley, with a joint appointment in the Department of Electrical Engineering and Computer Science (Computer Science Division) and the School of Information. Prior to joining UC Berkeley in 1998, I was a tenured faculty member in the Computer Science Department at Carnegie Mellon University. I was on the computer science faculty at Carnegie Mellon University from 1986 to 1998.

5. In 1982 I earned an A.B. degree in Math/Computer Science from the University of California, Berkeley, and in 1986 I earned a Ph.D. in Computer Science from Harvard University.

6. A copy of my curriculum vitae is attached as Appendix A. My CV includes a list of books, book chapters, papers and other publications that I have authored or co-authored. I am an expert in software engineering, computer networks, computer and network security, and cryptography. I have taught courses in software engineering, computer networking computer security, and cryptography at the undergraduate, masters, and Ph.D. level, at both UC Berkeley and Carnegie Mellon University.

7. I have served in a number of capacities on government, academic, and industrial committees that give advice or set standards in security and electronic commerce.

8. I have co-written three books that address computer security and networking, and one of those books has been translated into Japanese. I am presently completing a fourth book scheduled to be published in 2015 by Cambridge University Press.

9. I have designed cryptographic postage standards for the US Postal Service and have helped build a number of security and electronic commerce systems including: Strongbox, Dyad, Netbill, and Micro-Tesla. “NetBill” (developed in 1995), was an Internet commerce solution to deliver network services. “StrongBox” and “Dyad” are both directed at ensuring data protection in an insecure environment.

10. I have helped design the widely used DETER security networking testbed. DETER is supported by the U. S. National Science Foundation and the U.S. Department of Homeland Security. Further, I led the team that designed the SWOON overlay network used to test mobile networking in that environment.

11. I have also served as chair of the Defense Department’s ISAT Study Group on Security with Privacy, and was a founding board member of ACM's Special Interest Group on Electronic Commerce.

12. I am the UC Berkeley lead of the U.S. National Science Foundation Science and Technology Center TRUST, which studies issues associated with networking and security.

13. The U.S. State Department chose my project at UC Berkeley to examine the security and networking issues for communication protocols and software to support Internet freedom and allow users to bypass national firewalls in countries such as China, Iran, and Syria.

14. Among my awards are the National Science Foundation Presidential Young Investigator Award and the Kyoto Fellowship.

III. MATERIALS REVIEWED

15. In forming my opinions, I have reviewed the ’033 patent, the prosecution history of the ’033 patent, and the following documents:

- Apple Inc.’s Petition for *Inter Partes* Review of U.S. Patent No. 5,884,033 Challenging Claims 1, 2, 9, 15, and 23;
- Declaration of Charles D. Knutson, Ph.D. in Support of Apple Inc.’s Petition for *Inter Partes* Review of U.S. Patent No. 5,884,033 (Ex. 1010);
- Decision, Institution of *Inter Partes* Review, Paper No. 8 in this proceeding;
- U.S. Patent No. 5,790,554 to Pitcher (“Pitcher”) (Ex. 1005);
- Excerpts from Andrew S. Tanenbaum, Computer Networks (3d ed. 1996) (“Tanenbaum”) (Ex. 2004);

- Excerpts from Motorola Codex, The Basics Book of OSI and Network Management (1st ed. 1993) (Ex. 2005); and
- U.S. Patent No. 5,606,668 to Shwed ("Shwed") (Ex. 2006).

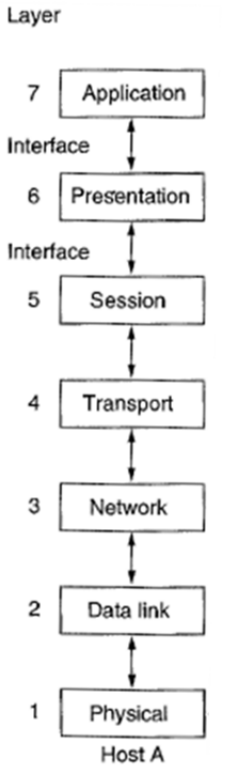
IV. THE PATENTED TECHNOLOGY

A. Overview of sending data over a network using the ISO protocol model

16. Prior to the 1996 filing of the '033 patent, the International Standards Organization (ISO) had created the Open Systems Interconnection (OSI) Reference Model in order to standardize network protocols used for communication among computers on a network. As an initial matter, I disagree with Dr. Knutson's assessment that the term "ISO protocol model" is an "incorrect" name for this reference model created by ISO. *See* Ex. 1010 ¶ 36 n.2. In my opinion, one of ordinary skill in the art would have understood there were various accepted names that referred to the ISO's OSI Reference Model, including, for example: "ISO model" (Ex. 2006 at 6:36-7:10), "ISO OSI reference model" (Ex. 2004 at 31), "OSI Model," (*id.*), "OSI reference model" (*id.*), "OSI basic reference model" (Ex. 2005 at 5), etc. In this declaration, I refer to the ISO's OSI Reference Model as the ISO protocol model, because as I discuss below, that is the name that the '033 patent inventors used during prosecution.

17. One of ordinary skill in the art would have understood that the ISO protocol model specifies seven protocol levels or "layers," each of which performs

a different function. The ISO protocol model is typically described with reference to a protocol stack, such as the one shown below from a textbook by Tanenbaum:



Ex. 2004 at 32 (excerpt of Fig. 1-16). This protocol stack shows all seven protocol levels in the ISO protocol model, from the physical layer (layer 1) to the application layer (layer 7). In my opinion, one of ordinary skill in the art would have been familiar with the ISO protocol model and with the different functions associated with each layer in the model. For example, in 1996 I had been on the Computer Science faculty at Carnegie Mellon University for 10 years, and I regularly taught the ISO protocol model to my undergraduate students. Those functions are described in greater detail in Tanenbaum's text book, *see* Ex. 2004 at

32-37, although a detailed account of each layer is not important for the purposes of this proceeding.

18. One of ordinary skill in the art also would have understood how the different layers interact with each other, as depicted by the dual arrows shown in between each layer in the figure above. For example, data may be received at one layer, processed in accordance with functionality associated with that layer, and then may be passed to an adjacent layer for further processing. *Id.* at 37-38. The figure below, reproduced from another text book, further demonstrates how two computers may pass data from one layer to the next in order to transmit data to each other in accordance with the ISO protocol model.

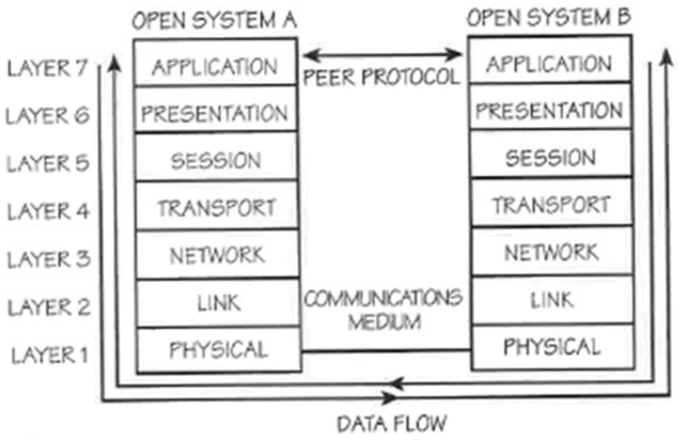


Exhibit 2005 at 5 (Fig. 3). For example, the computer Open System A shown above changes the representation of data originating in the application layer "down" the protocol stack, from the application layer to the physical layer, for transmission over a physical medium, such as a wired or wireless link. *See, e.g., id.* at 5-8. As

the representation of data changes as we move down the protocol stack, each protocol level segments the data into smaller units, sometimes called protocol data units (PDU) or data packets, and adds a corresponding header and/or trailer to encapsulate the PDU. *See, e.g.*, Ex. 2004 at 21-25. Open System B may then receive the transmitted data over the physical medium and change the representation of the data as we move "up" the various levels in the protocol stack until the original data is recovered at its application layer. *See, e.g.*, Ex. 2005 at 5-8. Each level in the ISO protocol model processes the received data using an associated network communication protocol, such that the same protocol is implemented at corresponding levels of the ISO protocol model at both the sender and receiver computer systems. *See, e.g.*, *id.*

19. In my opinion, one of ordinary skill in the art would have understood that data at the application level are often referred to as "messages" that are processed by the lower protocol levels in the ISO protocol model. *See, e.g.*, Ex. 2004 at 22-23. For example, the application level may implement the HyperText Transfer Protocol (HTTP), in which case the data exchanged between the presentation and application levels are HTTP messages, such as an HTTP request or reply. Similarly, the application level may implement an e-mail protocol or file transfer protocol (FTP), such that the data exchanged between the presentation and application levels includes e-mail messages or FTP messages, respectively.

20. In my opinion, one of ordinary skill in the art also would have understood that data at lower levels, such as the data link (layer 2), network (layer 3), and transport (layer 4) levels, are often called "packets." *See, e.g.*, Ex. 2004 at 22-23. In particular, when sending the application level message, data is typically segmented into smaller and smaller data fragments (e.g., PDUs or packets) at each lower protocol level. *See, e.g., id.* at 22-26. The transmitted data consists of data units including all of the header/trailer encapsulations added by the higher levels. During receiving, the physical layer receives the transmitted data units from the physical medium. Then, each protocol level receives a sequence of PDUs or packets from its adjacent lower level, processes the received data units in accordance with the level's associated protocol, which also may include reassembling, error correcting, and/or removing headers in the PDUs or packets, and then passes the processed PDUs or packets to the next higher level in the ISO protocol model.

B. Overview of the '033 patent

21. The '033 Patent, titled "Internet Filtering System for Filtering Data Transferred Over the Internet Utilizing Immediate and Deferred Filtering Actions," was filed on May 15, 1996. One of the objects of the '033 patent was to provide a system and method that allows users to filter the transmission of material sent over the Internet. Ex. 1001 at 1:27-29. For example, an Internet user, such as a parent,

would be able to filter transmissions of Internet messages to protect their children from exposure to objectionable material. *Id*. at 1:18-29.

22. The patented system and method includes a database of filtering information that is used to determine whether to prevent or allow the transmission of a message over the Internet. *See, e.g. id.* at claim 1. The database includes two types of filters: "filters specifying immediate action" and "filters specifying deferred action." *Id.* As the names of these filters indicate, filters specifying immediate action specify whether to allow or block a transmission immediately, while filters specifying deferred action defer the specification of whether to allow or block a transmission until additional conditions are satisfied. *Id.* By comparing information in a message to the claimed filters, the system determines whether to allow or block transmission of the message. *Id.* For example, independent claim 1 of the '033 patent recites:

> 1. A method for communicating with servers over the Internet to prevent or allow access to Internet sites, the method comprising computer-implemented steps of:
>
> (a) opening a data stream to send a message through an interface to an Internet server;
>
> (b) maintaining a database of filtering information comprising a table of filters, said table comprising
>
> (1) filters specifying immediate action, and
>
> (2) filters specifying deferred action;

(c) comparing information in the message to filtering information in at least one of said filters specifying immediate action and said filters specifying deferred action; and

(d) determining whether to prevent or allow the outgoing transmission of the message based on the comparison.

V. PERSON OF ORDINARY SKILL IN THE ART

23. In my opinion, and based on my review of the ’033 patent, one of ordinary skill in the art for the ’033 patent would have a bachelor’s degree or the equivalent in the field of computer science or electrical engineering and one to two years of experience with computer programming or computer networking. This is similar to the level of skill in the art that Dr. Knutson proposes in his definition, which is “someone with a bachelor’s degree or higher in computer science, computer engineering, or the equivalent, plus two or more years of experience in the field of networking and data communications, or a similar field.” Ex. 1010 ¶ 41. I meet both my definition and Dr. Knutson’s definition because in 1996 I held a Ph.D. in Computer Science, I had been working in the field of Computer Science, including computer networking, since 1982, and I had been on the Computer Science faculty at Carnegie Mellon University for 10 years. I have used my definition in my analysis below, but my analysis is unchanged if using Dr. Knutson’s definition.

VI. CLAIM CONSTRUCTION ANALYSIS

24. I have been asked to give my opinion as to how one of ordinary skill in the art would have understood the following terms in the ’033 patent:

- “filters specifying immediate action” (claims 1, 15, and 23); and
- “filters specifying deferred action” (claims 1, 15, and 23).

25. I understand that the ’033 patent will expire prior to an expected Final Decision from the Board in this case. I have been informed that, in this circumstance, the Board construes the claims in accordance with their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the invention, in light of the specification. This is the standard I have applied in my analysis below. When using this standard, I understand that the sources to be consulted in construing the claims include the intrinsic evidence (the patent claims, specification, and file history), which is primarily to be considered, as well as extrinsic evidence (e.g., textbooks, encyclopedias, dictionaries, articles, etc.), which may also be considered. I understand that the file history informs the meaning of the claims and assists in determining whether the inventor limited the scope of the patent claims during the course of prosecution.

26. I understand that OpenTV proposes the following constructions for the terms “filters specifying immediate action” and “filters specifying deferred action”:

Claim Term	OpenTV's Proposed Construction
"filters specifying immediate action"	"filters that, once they are retrieved, specify whether to allow or block a transmission immediately and unconditionally and *operate between the presentation and application levels of the seven-level ISO protocol model*"
"filters specifying deferred action"	"filters that, once they are retrieved, defer the specification of whether to allow or block a transmission until additional conditions are satisfied and *operate between the presentation and application levels of the seven-level ISO protocol model*"

27. I agree with OpenTV's proposed constructions. In my opinion, these constructions are consistent with how one of ordinary skill in the art would have understood the claim terms, when viewed in light of the specification and the prosecution history of the '033 patent.

28. These constructions include two separable parts: (1) the first part (which I show in normal type above) includes a temporal distinction between a filter specifying "immediate" action and a filter specifying "deferred" action, and is required by the plain language of these terms and supported by the specification; and (2) the second part (which I show italicized above) requires these filters to operate at a particular part of the ISO protocol model, and is required based on

statements that the inventors made to the Patent Office during the ’033 patent’s prosecution history. I address each of these requirements in turn.

29. The first part of OpenTV’s proposed constructions are required by the plain language of the claim terms: a filter specifying *immediate* action specifies whether to allow or block a transmission *immediately* after it is retrieved, while a filter specifying a *deferred* action *defers* the specification of whether to allow or block a transmission until another condition is satisfied. The specification of the ’033 patent confirms my understanding of the terms’ plain meanings. It explains that “direct” or “immediate” action filters immediately and unconditionally carry out a filtering action. Ex. 1001 at 1:42-45; 4:15-20, 45-50. It also explains that “deferred” action filters “defer the decision of whether to allow or block” a transmission based on additional conditions. *Id.* at 1:45-52; 4:65-5:29; 6:19-42.

30. The second part of the construction requires both filters to “operate between the presentation and application levels of the seven-level ISO protocol model.” In my opinion, one of ordinary skill in the art would have understood the claimed filters to operate in this manner because that is what the inventors told the Patent Office to obtain the ’033 patent. In response to a rejection from the examiner based on U.S. Patent No. 5,606,668 to Shwed, the inventors stated:

> As discussed during the interview, *the Schwed system and Applicants' methods operate at different layers of the seven-level ISO communication protocol model* [. . .]. As made clear at Fig. 5 and col. 6 ll. 3-7, the packet filters of Schwed operate between the network interface hardware (level 2) and the network software (level 3). *Applicants' filtering methods, by contrast, operate between the presentation and applications levels (layers 6 and 7, respectively) of the seven-level ISO protocol model.* Schwed [. . .] specifically *teaches away* from a system operating on the applications level (layer 7) of the ISO communication protocol model, such as Applicants' filtering methods[.]

Ex. 1007 at 64 (emphases added). Later, in response to the examiner's rejection of the claims based on Shwed and another prior art reference, the inventors reiterated that "Schwed et al. operates at different layers of the seven-level ISO communication protocol model from applicants' inventions." Ex. 1007 at 84. In my opinion, one of ordinary skill in the art would have read these statements by the inventors as requiring the "filters specifying immediate action" and "filters specifying deferred action" to operate between the presentation and application levels of the seven-level ISO protocol model.

31. I have been informed that an inventor's statements made during prosecution can only limit the claims if the statements are clear and unmistakable. In my opinion, the inventors clearly and unmistakably limited their claimed filters to operation between the presentation and application levels of the ISO protocol

model to distinguish a prior art reference, Shwed, which discloses a packet-based filter that operates between the data link and network levels (layers 2 and 3) of the ISO protocol model. *See* Ex. 2006 at Fig. 5, 7:3-7.

32. I disagree with Dr. Knutson's conclusion that this requirement based on the inventors' statements is not supported by the '033 patent specification. Ex. 1010 ¶ 36. Dr. Knutson does not appear to take into account the difference between "messages" and "packets," as I describe above in the discussion of the ISO protocol model. The specification and the original claims disclose and claim filtering "messages" and not "packets." *E.g.*, Ex. 1001 at Abstract, 1:30-52; Ex. 1007 at 26-30 (original claims). As I discussed above, a person of ordinary skill in the art would have understood that a "message" is a higher level construct that would be present at a higher level in the ISO protocol model (such as layer 7) than a "packet," which is a lower level construct that would be present at lower layers in the ISO protocol model (such as layers 2 or 3). The specification also describes filtering messages sent over Hypertext Transfer Protocol (HTTP), Network News Transfer Protocol (NNTP), and Internet Relay Chat (IRC), which are all application layer (layer 7) protocols. *See, e.g.*, Ex. 1001 2:42-50, 5:52-65, 6:10-18; Ex. 2004 at 126-33.

33. I also disagree with Dr. Knutson's conclusion that this construction is inconsistent with dependent claims 3 and 4. Ex. 1010 ¶ 36. In particular, I

disagree with Dr. Knutson's reasoning that because claims 3 and 4 require "an interface port" and "an Internet Protocol (IP) address," and because "[IP] addresses are commonly understood to correspond with layer 3 (network layer) [. . .] and not with layer[s 6 or 7]," then the filters cannot be limited to operate between layers 6 and 7. *Id.* The use of an IP address or a port is not limited to only the network layer (layer 3), as both can be used at higher protocol levels in the ISO protocol model, such as layers 6 or 7. For example, DNS is an application level protocol that uses IP addresses. Ex. 2004 at 108-16. The '033 patent even describes using IP addresses with the DNS protocol. Ex. 1001 3:13-19. Dr. Knutson is not correct that the presence of an IP address or port in the filter somehow requires that filter to operate at the network level, as even the '033 patent itself makes clear.

34. OpenTV's proposed construction is consistent with claims 6, 7, 13, and 14, which require the message to include a uniform resource locator (URL). URLs are typically present at the application layer and used by application layer protocols such as HTTP, FTP, etc. Ex. 2004 at 134-37. The dependent claims support OpenTV's position that the filters recited in the independent claims operate between the presentation and application layers, and on higher level messages in those layers.

VII. PITCHER DOES NOT ANTICIPATE CLAIMS 1, 2, 15, AND 23, OR RENDER OBVIOUS CLAIM 9 OF THE '033 PATENT

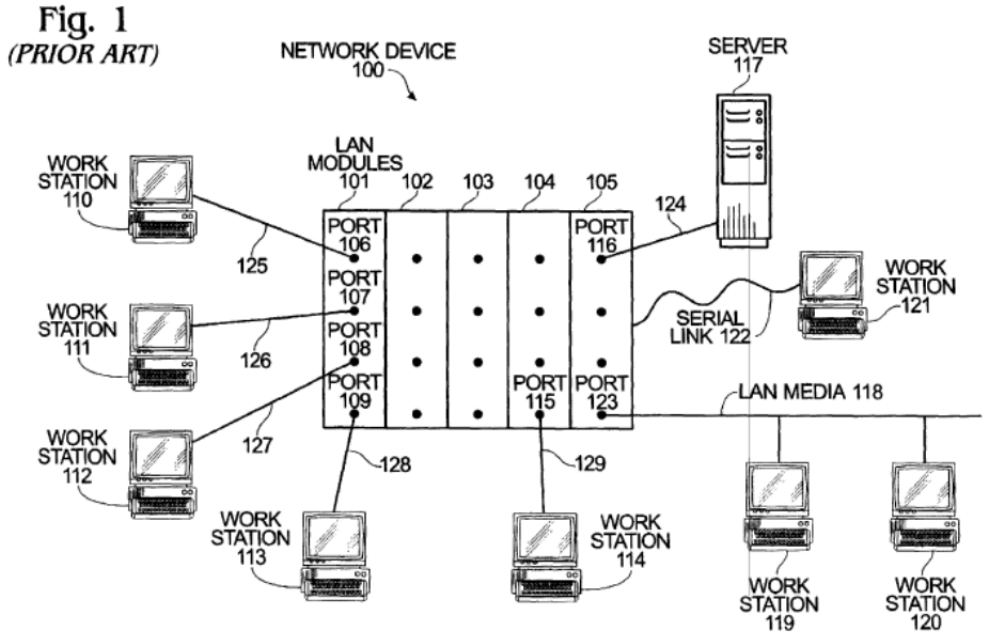
35. I understand that the Board has instituted this proceeding to determine whether claims 1, 2, 15, and 23 are anticipated by Pitcher, and whether claim 9 is obvious based on Pitcher. Below I have included a brief overview of the Pitcher reference, followed by my analysis of why Pitcher does not anticipate claims 1, 2, 15 and 23 and does not render obvious claim 9.

A. Overview of Pitcher

36. Pitcher discloses a method and apparatus for filtering data packets from a network device such as a local area network (LAN) switch. Ex. 1005, Abstract. Pitcher discloses that LANs are strained due to the growing bandwidth demands from increasingly powerful applications and a greater number of connected computers, *id.* at 1:23-27, and that network administrators of these LANs must find ways to increase bandwidth to meet their organization's needs, *id.* at 1:50-60. Pitcher discloses that replacing existing network equipment with LAN switches is "a very effective technology for addressing the problems" discussed above because LAN switches are scalable, fast, and cheap. *Id.* at 2:34-55. Pitcher also explains that "LAN switches operate at the MAC sublayer of the Data Link layer (layer 2)" of the ISO protocol model. *Id.* at 2:39-41. Pitcher's teaching that a LAN switch as operates at the data link level of the ISO protocol model is consistent with how one of ordinary skill in the art would have understood a LAN

switch to operate. Network devices such as bridges and LAN switches operate at the data link level (layer 2).

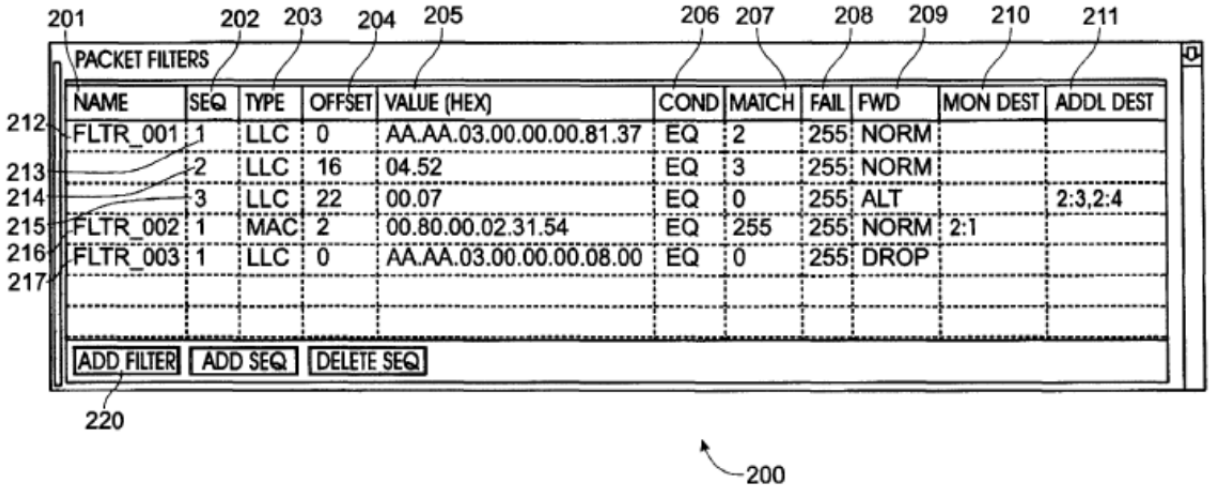
37. Pitcher's data packet filtering techniques are implemented on the LAN switch 100 shown connecting the LAN segments in Fig. 1 below:



Id. at 5:9 ("Network device 100 is a LAN switch"). "LAN switch 100 interconnects multiple LAN segments each via a port on a LAN module," *id.* at 5:12-14, and filters packets transmitted between the segments connected to each port, *id.* at 6:23-33.

38. Fig. 2, shown below, is a graphical user interface that includes "packet filters" used by Pitcher's LAN switch 100 to filter various data packets exchanged over LAN switch 100. I discuss the operation of these filters in greater detail in the sections that follow.

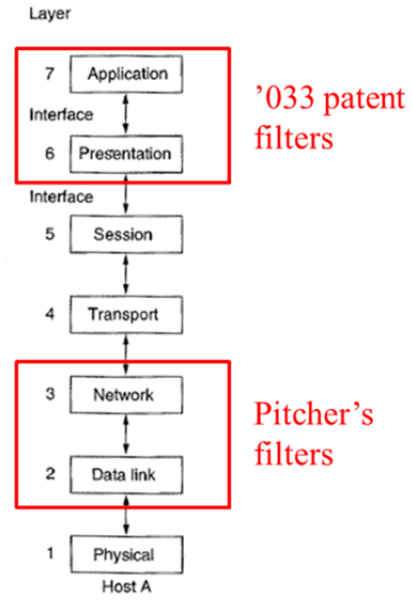
Fig. 2



B. Pitcher does not disclose "filters specifying immediate action" or "filters specifying deferred action"

39. In my opinion, because Pitcher's packet-based filters do not operate between the presentation and application layers of the seven-level ISO protocol model, they are not "filters specifying immediate action" or "filters specifying deferred action." All of Pitcher's disclosed filtering methods are performed "on a network device such as LAN switch 100." Ex. 1005 at 6:21-26. As I have discussed above, a LAN switch is a layer 2 device, as Pitcher makes clear: "network devices such as a LAN switch or bridge operate at the MAC sublayer of the *Data Link* layer [i.e., *layer 2*] of the OSI model." *Id.* at 6:33-37 (emphasis added); *see also id.* at 2:39-42. For example, Pitcher explains that the LAN switch 100 performing the filtering can employ different "modules," such as a Token Ring, Ethernet, FDDI, or ATM module. *Id.* at 5:8-21. These are lower level protocols that operate at layers 2 or 3 of the ISO protocol or their equivalents. *See, e.g.*, Ex.

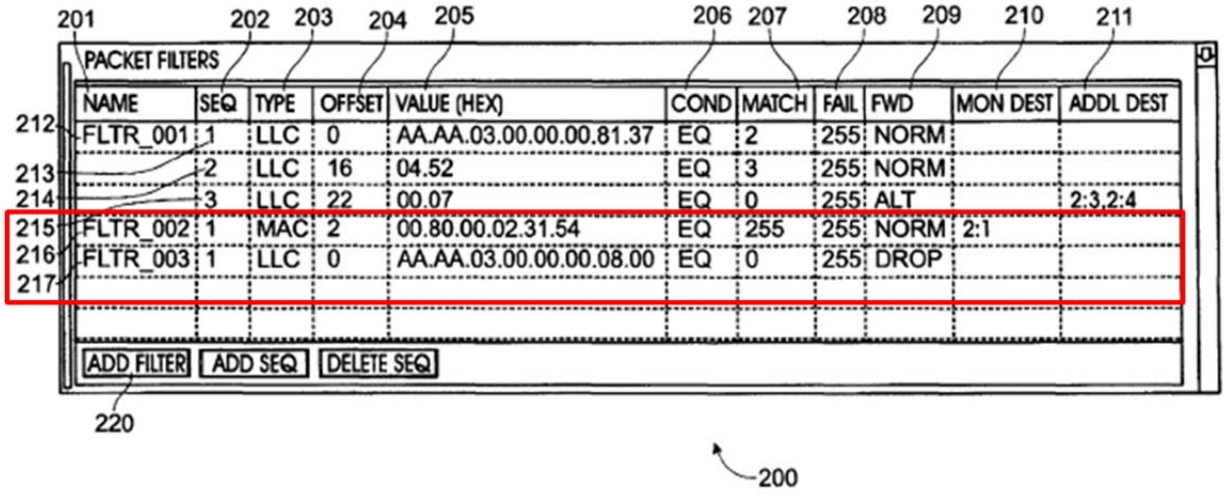
2004 at 57-58 (medium access (MAC) sublayer is a part of the data link layer); 71-78 (Token Ring operates at MAC sublayer), 59-70 (Ethernet operates at MAC sublayer), 79-80 (FDDI operates at MAC sublayer), 51-56 (ATM operates at equivalent to lower levels of ISO protocol model). Moreover, when explaining the "packets" that its system filters, Pitcher uses an IEEE 802.5 Token Ring packet as an example. Ex. 1005 at Fig. 4, 4:54-55, 7:33-8:23. The IEEE 802.5 Token Ring protocol is a layer 2 protocol. For these reasons, and for the additional reasons that I discuss in greater detail below, it is my opinion that one of ordinary skill in the art would have understood that Pitcher's packet filtering techniques operate solely between layers 2 and 3 of the ISO protocol model, and not between layers 6 and 7 like the filters in the '033 patent. The annotated excerpt of figure 1-16 from the Tanenbaum text book, Ex. 2004 at 32, show below, illustrates this distinction:



1. The alleged "filters specifying immediate action" in Pitcher do not operate between the presentation and application layers (claims 1, 2, 9, 15, and 23)

40. Apple and Dr. Knutson argue that Pitcher's filters FLTR_002 and FLTR_003 are "filters specifying immediate action." Pet. at 46, 48; Ex. 1010 ¶¶ 101-02. I disagree. FLTR_002 and FLTR_003 (which are shown in Fig. 2 of Pitcher, reproduced below with a red box highlighting FLTR_002 and FLTR_003) are both packet-based filters and neither operates between the presentation and application levels of the seven-level ISO protocol model.

Fig. 2



Pitcher discloses that the graphical user interface of Fig. 2 is used to enable "packet filtering on a network device such as LAN switch 100." Ex. 1005 at 6:21-26. Network devices such as LAN switches operate at the data link layer (layer 2) of the ISO protocol model, not between the presentation and application layers (layers

6 and 7). *Id.* at 6:33-37. Pitcher also explains in further detail that FLTR_002 and FLTR_003 do not operate at the presentation or application layers because Pitcher discloses that FLTR_002 filters "packets" with a particular media access control (MAC) address and FLTR_003 filters "IP packets." One of ordinary skill in the art would understand that the "packet" filters enabled on Pitcher's layer 2 LAN switch do not operate between the presentation and application levels (layers 6 and 7) of the ISO protocol model.

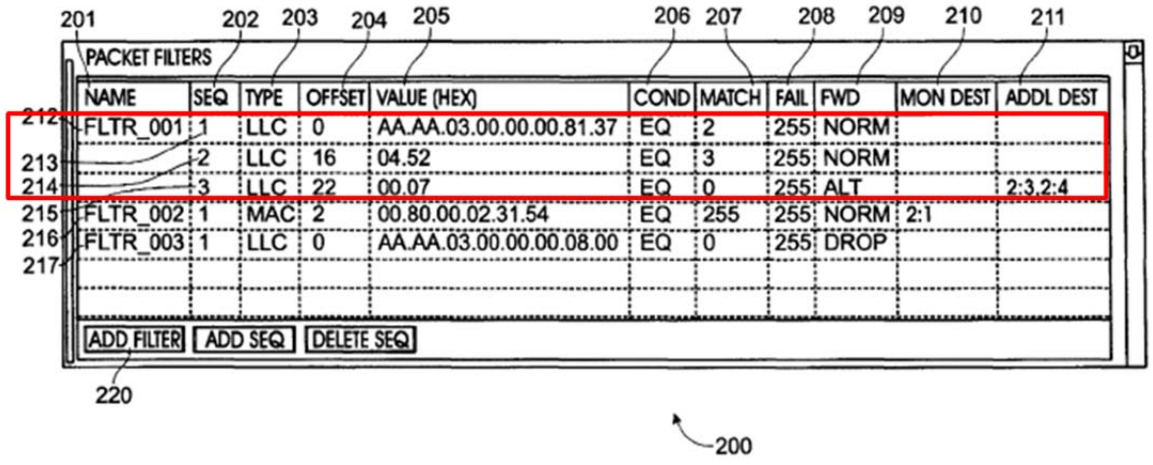
41. When reading Pitcher, one of ordinary skill in the art would have looked to the figures and description of Pitcher as a whole in order to understand the operation of FLTR_002 and FLTR_003. For example, to understand the type field 203 ("MAC" or "LLC" in Fig. 2) and the offset field 204 shown in Fig. 2 in connection with FLTR_002 and FLTR_003, one of ordinary skill in the art would also have looked to Figs. 3 and 4 and the corresponding discussion, which demonstrate that these two fields indicate the location in a particular packet where the filter should start. *Id.* at 7:30-32. In particular, filter type MAC and offset 2 for FLTR_002 indicates that FLTR_002 starts two bytes from the beginning of the MAC field of the data packet, whereas filter type LLC and offset 0 for FLTR_003 indicates that FLTR_003 starts at the beginning of the LLC field. The only embodiment that Pitcher uses to describe these types of fields (MAC and LLC) is the IEEE 802.5 Token Ring packet shown in Fig. 4, which is a level 2 packet. This

confirms my understanding, and the understanding of a person of ordinary skill in the art, that Pitcher's FLTR_002 and FLTR_003 each operates several levels beneath the presentation and application levels of the ISO protocol model, and therefore cannot be the claimed filters specifying immediate action.

2. The alleged "filters specifying deferred action" in Pitcher do not operate between the presentation and application levels (claims 1, 2, 9, 15, and 23)

42. Apple also asserts that Pitcher's FLTR_001, shown in Pitcher's Fig. 2 below (my annotation added in red), discloses "filters specifying deferred action." Pet. at 45. I disagree with this assertion as well, because FLTR_001 does not operate between the presentation and application levels of the seven-level ISO protocol model.

Fig. 2



43. FLTR_001 is also implemented by LAN switch 100, which operates at layer 2 of the ISO protocol model. Ex. 1005 at 6:21-26. Pitcher makes clear

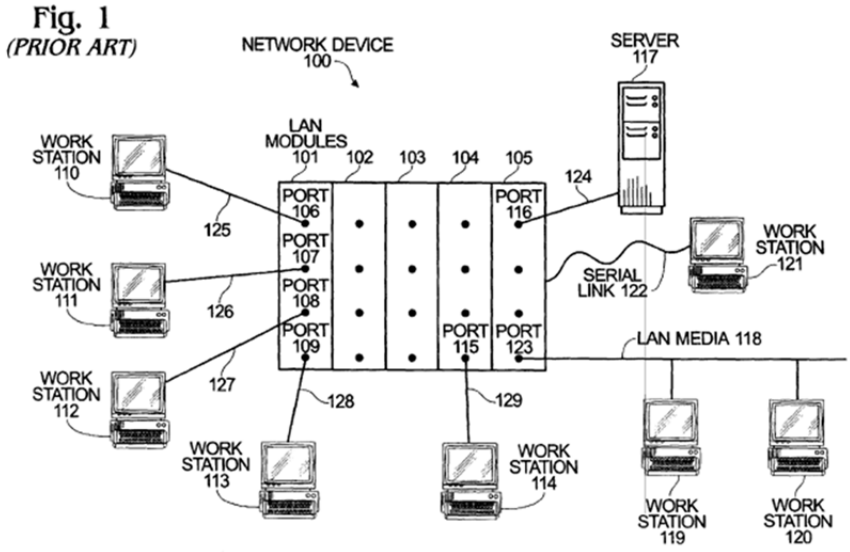
that FLTR_001 is a lower-level packet filter that does not operate between the presentation and application layers. In particular, Pitcher explains that FLTR_001 filters and "redirects all Novell NetWare printer requests." Ex. 1005 at 6:66-7:3. The Novell NetWare network uses the IPX ("internetwork packet exchange") protocol, which is a network level (layer 3) protocol. Ex. 2004 at 48-49. In fact, Pitcher explains that FLTR_001 includes three sequenced filters 213, 214, and 215, each of which "checks for IPX packets" or printer requests within those IPX packets, and are therefore layer 3 filters. Ex. 1005 at 7:7-9. We can see that FLTR_001 does not operate between the presentation and application levels of the ISO protocol stack, and cannot be the claimed "filters specifying deferred action."

44. Dr. Knutson also cites to column 8 of Pitcher as disclosing a deferred action filter. Ex. 1010 ¶ 103. I disagree. This portion of Pitcher describes the exemplary packet in Fig. 4, which as I discussed above in paragraphs 39 and 41, is an IEEE 802.5 token ring packet (a level 2 packet). *See* Ex. 1005 at 7:33-35.

C. Pitcher's LAN is not connected to the Internet and thus Pitcher does not disclose "prevent[ing] or allow[ing] access to Internet sites" (claims 1, 2, 9, 15, and 23)

45. Pitcher does not disclose "prevent[ing] or allow[ing] access to Internet sites" because Pitcher's system is confined to a local area network (LAN) and because Pitcher discloses filtering packets on that LAN using a LAN switch. Pitcher's entire purpose is to route and analyze packets on an internal LAN, such

as one that may be operated by an organization. *See, e.g.*, 1005 at 1:22 ("LAN Management"); 1:50-60 (discussing the challenges of an organization managing its LAN); 2:13-64 (discussing LAN switches and LAN management). In particular, Pitcher's disclosed embodiments are implemented via the system shown in Fig. 1 (reproduced below), which is a LAN, and which does not disclose any connection to the Internet. *See id.* at 5:8-22 ("Network device 100 is a LAN switch.").



46. The LANs disclosed in Pitcher, and LANs in general, are not the same as the Internet. A LAN is a privately-owned network that an organization such as a company or university might use to connect devices such as computers, servers, and printers within the organization. Ex. 2004 at 12-13. The Internet, on the other hand, is a publicly connected, worldwide network used to connect organizations and individuals around the globe. *Id.* at 19.

47. Pitcher's closed LAN system is fundamentally different than the Internet-based system of the '033 patent. For example, the types of content and consequently the types of filtering in an Internet-based system like the '033 patent are different than those in a LAN-based system like Pitcher. One type of concern for Internet-based filtering centers around content control and safety, such as preventing exposure to objectionable material. Ex. 1001 at 1:10-24 ('033 patent describing concerns about preventing children from exposure to objectionable material on the Internet). In contrast, as Pitcher makes clear, internal filtering mechanisms on a closed network such as a LAN commonly have very different goals, such as network performance and scalability. Ex. 1005 at 1:50-59; *see also id.* at 6:45-46 (using LAN switch filtering for traffic analysis on the LAN).

48. Apple and Dr. Knutson cite to several portions of Pitcher, but each portion describes a *LAN*, and does not describe preventing or allowing access to *Internet* sites. *See* Pet. at 46-47. First, Apple cites to a portion that summarizes "the present invention" of Pitcher, and to Pitcher's Abstract. Pet. at 46 (citing Ex. 1005 at 3:48-53, Abstract). These portions disclose only a "network device, such as a LAN switch" coupled to a "network"—they do not disclose the Internet, let alone preventing or allowing access to Internet sites. Ex. 1005 at Abstract, 3:48-53.

49. Second, Apple cites to a portion of Pitcher that discloses filtering based on an "IP address of 129.1.1.1." Pet. at 47 (citing Ex. 1005 at 3:4-9). To the

extent that Apple and Dr. Knutson are asserting that data transmission and filtering over the Internet are disclosed simply because of the disclosure of an IP address, I disagree. This part of Pitcher is in the Background section to describe prior art filtering techniques, and is not actually described as being a part of Pitcher's LAN switch packet filtering embodiments. Ex. 1005 at 2:66-3:9. Further, it possible to create a LAN that uses IP and IP addresses but is not connected to the Internet. In that LAN, data would be sent between computers on the LAN using their internal IP addresses.

50. Third, Dr. Knutson cites to an additional portion of Pitcher that does not disclose preventing or allowing access to Internet sites. Ex. 1010 ¶ 97 (citing Ex. 1005 at 2:49-55). Besides also being in the Background section, this cited portion describes only "workstations and servers [. . .] connected directly to the LAN switch" and multiple LANs connected together. Ex. 1005 at 2:49-55. Nowhere does it disclose connection to the Internet.

D. Pitcher does not disclose "opening a data stream to send/receive a message[. . .] to/from an Internet server" (claims 1, 2, 9, and 23)

51. Independent claim 1 recites "opening a data stream to send a message [. . .] to an *Internet server*," and independent claim 23 recites "opening a data stream to receive a message [. . .] from an Internet server." For reasons similar to those that I discuss in the previous section, Pitcher's closed LAN network does not

disclose sending or receiving messages over the Internet, and therefore does not disclose these claim limitations. *See* paragraphs 45-47, above.

52. Dr. Knutson asserts that this feature is "inherently disclosed by any reference describing TCP/IP communications," Ex. 1010 ¶ 98, and Apple cites to a portion of Pitcher which discloses a network interface card 526 that uses TCP/IP. Pet. at 47 (citing Ex. 1005 at 6:1-7). I disagree with Apple and Dr. Knutson for two reasons.

53. First, sending or receiving a message over the Internet is not inherent in a system using TCP/IP. Two clients can communicate with each other using TCP/IP over a network that is not the Internet, such as the LAN that is disclosed in Pitcher. Therefore, simply disclosing TCP/IP does not inherently disclose sending or receiving messages to or from an Internet server.

54. Second, the network interface card 526 that Apple points to does not send or receive the alleged "message" in Pitcher. Network interface card 526 is a part of a network management station 121 that allows a "network administrator" to "manage[] the configuration and operation of the LAN switch" performing the filtering. Ex. 1005 at 5:23-26; *see also id.* at Fig. 1 (showing workstation 121). In other words, the network interface card 526 is part of a different computer than the one sending or receiving messages filtered by the LAN switch.

55. Independent claims 1 and 23 each require the same "message" that is sent or received in this step to be the filtered message in subsequent steps. *See, e.g.*, Ex. 1001, claim 1 (reproduced in part below, emphases added):

> (a) opening a data stream to send *a message* through an interface to an Internet server; . . .
>
> (c) comparing information *in the message* to filtering information . . .
>
> (d) determining whether to prevent or allow the outgoing transmission *of the message* based on the comparison.

56. Even if Apple were correct that network management station 121 (via network interface card 526) inherently opens a data stream to send "a message" to an Internet server, it is not "the message" being filtered in Pitcher. Moreover, the data from network management station 121 is sent to the LAN switch, which is not an "Internet server."

57. Apple also cites to another portion of Pitcher. Pet. at 47 (citing Ex. 1005 at 6:26-33) This portion does not disclose sending a message to or receiving a message from an Internet server because it simply discloses how the packet filter works inside the LAN switch to forward the packets. Ex. 1005 at 6:26-33. It does not disclose anything about communicating over the Internet.

E. Pitcher does not render claim 9 obvious

58. Claim 9 depends from independent claim 1 and further requires "maintaining the database [of filtering information] in storage residing on the client computer." Ex. 1001, claim 9. In my opinion, Pitcher does not disclose or render obvious this feature. As I discussed above, all of the filtering in Pitcher is performed by "a network device such as a LAN switch." Ex. 1005 at 4:24-26, 5:8-10. While Pitcher explains that the "network device" could be a "hub or bridge," *id.* at 5:10-13, Pitcher does not teach that a client computer performs the filtering or includes a database of filtering information. To the contrary, Pitcher describes several advantages of the filtering functionality being present at a centralized LAN switch. For example, a workstation 121 is connected to the LAN switch 100 to allow a "network administrator [to] manage[] the configuration and operation of the LAN switch," including the filter settings. *Id.* at 5:23-26; *see also id.* at Figs. 2, 3, 6:21-7:29 (describing displays presented on the workstation 121 that allow the network administrator to configure the filter settings of the LAN switch). Similarly, packet filtering at the LAN switch may be used to analyze LAN traffic. *Id.* at 6:45-46.

59. Apple asserts that a portion of Pitcher's background section that discusses segmenting a larger LAN into smaller LAN segments would have rendered obvious storing the database of filtering information at the client

computers in Pitcher's system. Pet. at 51-52. I understand Apple's argument to be as follows:

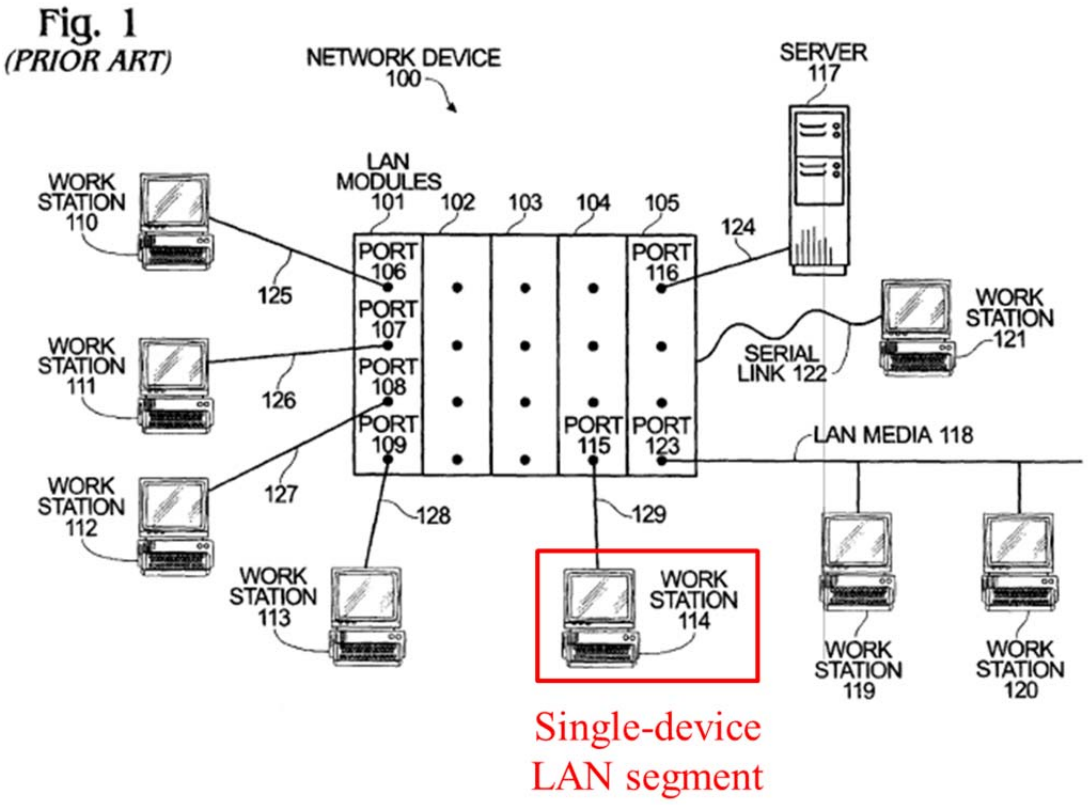
(1) Pitcher discloses that larger LANs can be segmented into smaller LAN segments, and that when carried to its end, this results in each LAN segment having only a single device (server or workstation), *id.* at 51;

(2) In this single-device scenario, there would be a single LAN switch for each LAN segment to control the filtering for the one device in that segment, *id.* at 51 ("the filtering operations carried out on the LAN switch are for the benefit of a single workstation (client)"), *id.* at 52 ("[the LAN switch's] only function [i]s to allow or block network messages to and from a single client computer"); and

(3) It would be more efficient to move the filtering functionality of the LAN switch into the device, to save the hardware costs associated with installing a LAN switch at every segment, *id.* at 52.

60. In my opinion, however, Apple's assertion (2)—that segmentation to the single device level requires a separate LAN switch for each LAN segment—is contradicted by Fig. 1 of Pitcher, which illustrates a single-device LAN segment that shares a LAN switch with other segments. Pitcher explains with reference to Fig. 1 that "LAN switch 100 interconnects *multiple LAN segments* each via a port

on a LAN module," Ex. 1005 5:12-14 (emphasis added). But one of the LAN segments displayed in Fig. 1 is the *single-device LAN segment* of workstation 114, and it shares the LAN switch 100 with the other LAN segments. This directly contradicts Apple's assertion that a single-device LAN segment must include its own LAN switch:



Id. at Fig. 1 (my annotations in red). This is consistent with Pitcher's Background section which explains that LAN switches may be connected directly to single-device LAN segments as bandwidth needs arise. *Id.* at 2:46-55. In my opinion, there is nothing in Pitcher to suggest, and one of ordinary skill in the art would not have been motivated, to move the filtering functionality from the LAN switch to

individual devices on Pitcher's LAN. In addition to there being no reason to make such a modification in the case of single-device LAN segments (because Pitcher already teaches a solution as shown in Fig. 1), the proposed modification would detract from Pitcher's stated advantages of having a centralized filtering system accessible by a network administrator via a single workstation and of enabling traffic analysis on the LAN.

VIII. CONCLUSION

61. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination.

62. I reserve the right to supplement my opinions in the future to respond to any arguments that Apple raises and to take into account new information as it becomes available to me.

63. I declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true, and further that these statements were made with 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.

Dated: 19 December 2015 By: 

Justin Douglas Tygar

Attachments: Curriculum Vitae of Justin Douglas Tygar, Ph.D.

Appendix A

DOUG TYGAR

Address:

University of California.
739 Soda Hall #1776
Berkeley, CA 94720-1776
(510) 643-7855
tygar@cs.berkeley.edu

Personal Information:

Full name: Justin Douglas Tygar
US Citizen

Education:

A.B., 1982 **University of California, Berkeley**, *Math/Computer Science*
Bell Labs University Relations Student (1981)

Ph.D., 1986 **Harvard University**, *Computer Science*
Thesis: *An Integrated Toolkit for Operating System Security*
Advisor: Michael Rabin
NSF Graduate Fellow (1982 – 1985), IBM Graduate Fellow (1985 – 1986)

Academic Appointments:

University of California, Berkeley
Department of Electrical Engineering and Computer Science
& School of Information
1998 – Present *Professor* (tenured, joint appointment)

Carnegie Mellon University
Computer Science Department
2000 – 2005 *Adjunct Professor*
1992 – 2000 *Associate Professor* (tenured 1995, on leave 1998 – 2000)
1986 – 1992 *Assistant Professor*

Major Awards:

NSF Presidential Young Investigator, 1988
Outstanding Professor Award, *Carnegie Magazine*, 1989
Chair, Defense Information Science and Technology Study Group on Security with Privacy
Member, National Research Council Committee on Information Trustworthiness
Member, INFOSEC Science and Technology Study Group
Okawa Foundation Fellow, 2003-4
Wide consulting for both industry and government

Major speeches:

Keynote addresses:

PODC (1995), ASIAN-96 (1996), NGITS (1997), VLDB (1998), CRYPTEC (1999),
CAV (2000), Human Authentication (2001), PDSN (2002), ISM (2005), ISC (2005), ASIACCS (2006),
Croucher ASI (2004, 2006), ISC (2008), AISEC (2010), ISRCS (2013), SERE (2014)

Invited addresses:

Harvard Graduate School of Arts and Science 100th Anniversary,
CMU Computer Science Department 25th Anniversary
More than 260 talks & 20 professional seminars since 1985

External review activities:

Electronic Commerce Program, City University of Hong Kong
Information Systems Management Program, Singapore Management University
Information Technology Program, United Arab Emirates University
Computer Science Program, University of California, Davis

Publications

Books

1. **Adversarial Machine Learning: Computer Security and Statistical Machine Learning.** A. Joseph, B. Nelson, B. Rubinstein, J. D. Tygar. Cambridge University Press, 2015. (To appear).

2. **Computer Security in the 21st Century.** Eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, March 2005. (This book includes item 12 below as well as a technical introduction by me and the other editors.)

3. **Waiyādo/Waiyaresu Nettowōku ni Okeru Burōdokyasuto Tsūshin no Sekyuriti** ワイヤード/ワイヤレスネットワークにおけるブロードキャスト通信のセキュリテ. A. Perrig and J. D. Tygar; translated by Fumio Mizoguchi and the the Science University of Tokyo Information Media Science Research Group with the assistance of J. D. Tygar. Kyoritsu Shuppan, October 2004. (This is a Japanese translation of item 4 which also contains new and additional material written by me in Japanese.)

4. **Secure Broadcast Communication in Wired and Wireless Networks.** A. Perrig and J. D. Tygar. Springer, October 2002. (See also item 3.)

5. **Trust in Cyberspace.** National Research Council Committee on Information Systems Trustworthiness (S. Bellovin, W. E. Boebert, M. Branstad, J. R. Catoe, S. Crocker, C. Kaufman, S. Kent, J. Knight, S. McGeady, R. Nelson, A. Schiffman, F. Schneider [ed.], G. Spix, and J. D. Tygar). National Academy Press, January 1999.

Book Chapters (does not incude items listed above)

6. "Classifier evasion: Models and open problems." B. Nelson, B. Rubinstein, L. Huang, A. Joseph, and J. D. Tygar. In **Privacy and Security Issues in Data Mining and Machine Learning**, eds. C. Dimitrakakis, et al. Springer, July 2011, pp. 92-98.

7. "Misleading learners: Co-opting your spam filter." B. Nelson, M. Barreno, F. Chi, A. Joseph, B. Rubinstein, U. Saini, C. Sutton, J. D. Tygar, and K. Xia. In **Machine Learning in Cyber Trust: Security, Privacy, Reliability**, eds. J. Tsai and P.Yu. Springer, April 2009, pp. 17-51.

8. "Preface." J. D. Tygar. In **從DIGIart@eTaiwan談互動創意 (Interaction and Creation in DIGIart@eTaiwan)**,ed. S. Hsu. Ylib Publisher, July 2007.

9. "Case study: Acoustic keyboard emanations." L. Zhuang, F. Zhou, and J. D. Tygar. In **Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft**, eds. M. Jakobsson and S. Myers. Wiley-Interscience, December 2006, pp. 221-240. (This is a popularized version of item 30.)

10. "Dynamic security skins." R. Dhamija and J. D. Tygar. In **Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft**, eds. M. Jakobsson and S. Myers. Wiley-Interscience, December 2006, pp. 339-351. (This is a popularized version of item 76.)

11. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." A. Whitten and J. D. Tygar. In **Security and Usability: Designing Secure Systems that People Can Use**, eds. L. Cranor and G. Simson. O'Reilly, September 2005, pp. 679-702. (An earlier version of this paper was published in **Proceedings of the 8th USENIX Security Symposium**, August 1999, pp. 169-183. See also item 125.)

12. "Private matching." Y. Li, J. D. Tygar, J. Hellerstein. In **Computer Security in the 21st Century**, eds. D. Lee, S. Shieh, and J. D. Tygar. Springer, March 2005, pp. 25-50. (See item 2.) (An early version of this paper appeared as Intel Research Laboratory Berkeley technical report IRB-TR-04-005, February 2004.)

13. "Digital cash." J. D. Tygar. In **Berkshire Encyclopedia of Human Computer Interaction,** ed. W. Bainbridge. Berkshire Publishing, October 2004, pp. 167-170.

14. "Spamming." J. D. Tygar. In **Berkshire Encyclopedia of Human Computer Interaction**, ed. W. Bainbridge. Berkshire Publishing, October 2004, pp. 673-675.

15. "Viruses." J. D. Tygar. In **Berkshire Encyclopedia of Human Computer Interaction**, ed. W. Bainbridge. Berkshire Publishing, October 2004, pp. 788-791.

16. "Privacy in sensor webs and distributed information systems." J. D. Tygar. In **Software Security: Theories and Systems,** eds. M. Okada, B. Pierce, A. Scedrov, H. Tokuda, and A. Yonezawa. Springer, 2003, pp. 84-95.

17. "Atomicity in electronic commerce." J. D. Tygar. In **Internet Besieged**, eds. D. Denning and P. Denning. ACM Press and Addison-Wesley, October 1997, pp. 389-405. (An expanded earlier version of this paper was published in **Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing**, *Keynote paper*, May 1996, pp. 8-26; and as Carnegie Mellon University Computer Science technical report CMU-CS-96-112, January 1996. See also item 40.)

18. "Cryptographic postage indicia." J. D. Tygar, B. Yee, and N. Heintze. In **Concurrency and Parallelism, Programming, Networking, and Security**, eds. J. Jaffar and R. Yap. Springer, 1996, pp. 378-391. (Preprint also available. Early versions appeared as Carnegie Mellon University Computer Science technical reports CMU-CS-96-113, January 1996, UC San Diego Computer Science technical report UCSD-TR-CS96-485, and in the 1996 **Securicom Proceedings,** Paris, June 1996. See also item 127.)

19. "Dyad: A system for using physically secure coprocessors." J. D. Tygar and B. Yee. In **Technological Strategies for the Protection of Intellectual Property in the Networked Multimedia Environment**. Interactive Multimedia Association, 1994, pp. 121-152. (An early version appeared as Carnegie Mellon University Computer Science technical report CMU-CS-91-140R, May 1991.)

20. "A system for self-securing programs." J. D. Tygar and B. Yee. In **Carnegie Mellon Computer Science: A 25-Year Commemorative**, ed. R. Rashid. ACM Press and Addison-

Wesley, 1991, pp. 163-197. (Note: The first printing of this volume had incorrect text due to a production error.)

21. "Implementing capabilities without a trusted kernel." M. Herlihy and J. D. Tygar. In **Dependable Computing for Critical Applications**, eds. A. Avizienis and J. Laprie. Springer, January 1991, pp. 283-300. (Note: An early version appeared in the **(IFIP) Proceedings of the International Working Conference on Dependable Computing for Critical Applications**, August 1989.)

22. "Strongbox." J. D. Tygar and B. Yee. In **Camelot and Avalon: A Distributed Transaction Facility**, eds. J. Eppinger, L. Mummert, and A. Spector. Morgan-Kaufmann, February 1991, pp. 381-400.

23. "ITOSS: An Integrated Toolkit for Operating System Security." M. Rabin and J. D. Tygar. In **Foundations of Data Organization**, eds. W. Litwin and H.-J. Shek. Springer, June 1989, pp. 2-15. (Preprint also available.) (Note: Earlier, longer versions appeared as Harvard University Aiken Computation Laboratory technical report TR-05-87R and my Ph.D. dissertation.)

24. "Formal semantics for visual specification of security." M. Maimone, J. D. Tygar, and J. Wing. In **Visual Languages and Visual Programming**, ed. S. K. Chang. Plenum, 1990, pp. 97-116. (An early version was published in **Proceedings of the 1988 IEEE Workshop on Visual Programming**, pp. 45-51, and as Carnegie Mellon University Computer Science technical report CMU-CS-88-173r, December 1988.)

Journal Articles (does not include items listed above)

25. "Machine Learning Methods for Computer Security." A. Joseph, P. Laskov, F. Roli, J. D. Tygar, B. Nelson. ***Dagstuhl*** *Manifestos* 3:1, December 2013, pp. 1-30.

26. "A low-bandwidth camera sensor platform with applications in smart camera networks." P. Chen, K. Hong, N. Naikal, S. Sastry, J. D. Tygar, P. Yan, A. Yan, L. Chang, L. Lin, Leon S. Wang, E. Lobaton, S. Oh, and P. Ahammad. *ACM Transactions on Sensor Networks*, 9:2, March 2013, pp. 21:1-21:23.

27. "Query strategies for evading convex-inducing classifiers." B. Nelson, B. Rubinstein, L. Huang, A. Joseph, S. Lee, S. Rao, and J. D. Tygar. *Journal of Machine Learning Research*, May 2012 (volume 13) pp. 1293-1332. (Also available as arXiv report 1007.0484v1, July 2010.)

28. "The security of machine learning." M. Barreno, B. Nelson, A. Joseph, and J. D. Tygar. *Machine Learning*, 81:2, November 2010, pp. 121-148. (An earlier version appeared as UC Berkeley EECS technical report UCB/EECS-2008-43, April 2008.)

29. "Secure encrypted-data aggregation for wireless sensor networks." S. Huang, S. Shieh and J. D. Tygar. *Wireless Networks*, 16:4, May 2010, pp. 915-927.

30. "Keyboard acoustic emanations revisited." L. Zhuang, F. Zhou, and J. D. Tygar. *ACM Transactions on Information and Systems Security*, 13:1, October 2009, pp 3:1-3:26. (An

earlier version appeared in **Proceedings of the 12th ACM Conference on Computer and Communications Security**, November 2005, pp. 373-382.) (See also item 9.)

31. "Stealthy poisoning attacks on PCA-based anomaly detectors." B. Rubinstein, B. Nelson, L. Huang, A. Joseph, S. Lau, S. Rao, N. Taft, and J. D. Tygar. *ACM SIGMETRICS Performance Evaluation Review*, 37:2, October 2009, pp. 73-74.

32. "Injecting heterogeneity through protocol randomization." L. Zhuang, J. D. Tygar, R. Dhamija. In *International Journal of Network Security*, 4:1, January 2007, pp. 45-58.

33. "Cyber defense technology networking and evaluation." Members of the DETER and EMIST Projects (R. Bajcsy, T. Benzel, M. Bishop, B. Braden, C. Brodley, S. Fahmy, S. Floyd, W. Hardaker, A. Joseph, G. Kesidis, K. Levitt, B. Lindell, P. Liu, D. Miller, R. Mundy, C. Neuman, R. Ostrenga, V. Paxson, P. Porras, C. Rosenberg, S. Sastry, D. Sterne, J. D. Tygar, and S. Wu). In *Communications of the ACM*, 47:3, March 2004, pp. 58-61.

34. "Technological dimensions of privacy in Asia." J. D. Tygar. In *Asia-Pacific Review*, 10:2, November 2003, pp. 120-145.

35. "SPINS: Security protocols for sensor networks." A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler. In *[ACM Journal of] Wireless Networks*, 8:5, September 2002, pp. 521-534. (An early version of this paper appears in **Proceedings of the 7th Annual International Conference on Mobile Computing and Networks (MOBICOM),** July 2001, pp. 189-199.)

36. "The TESLA broadcast authentication protocol." A. Perrig, R. Canneti, J. D. Tygar, and D. Song. In *CryptoBytes*, 5:2, Summer/Fall 2002, pp. 2-13.

37. "SAM: A flexible and secure auction architecture using trusted hardware." A. Perrig, S. Smith, D. Song, and J. D. Tygar. In *Electronic Journal on E-commerce Tools and Applications*, 1:1, January 2002 (online journal). (An early version of this paper appeared in **Proceedings of the 1st IEEE International Workshop on Internet Computing and Electronic Commerce**, April 2001, pp. 1764-1773.)

38. "Why isn't the Internet secure yet?" J. D. Tygar and A. Whitten. In *ASLIB Proceedings*, 52:3, March 2000, pp. 93-97.

39. "Multi-round anonymous auction protocols." H. Kikuchi, M. Harkavy, and J. D. Tygar. In *Institute of Electronics, Information, and Communication Engineers Transactions on Information and Systems*, E82-D:4, April 1999, pp. 769-777. (An early version appeared in **Proceedings of of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems (DARE '98)**, June 1998, pp. 62-69.)

40. "Atomicity in electronic commerce." J. D. Tygar. In *ACM NetWorker*, 2:2, April/May 1998, pp. 32-43. (Note: this is a revision of item 17 published together with a new article: "An update on electronic commerce." In *ACM NetWorker*, Volume 2, Number 2, April/May 1998, pp. 40-41.)

41. "A model for secure protocols and their compositions." N. Heintze and J. D. Tygar. In *IEEE Transactions on Software Engineering*, 22:1, January 1996, pp. 16-30. (An extended abstract appeared in **Proceedings of the 1994 IEEE Symposium on Security and Privacy**, May

1994, pp. 2-13. Another early version appeared as Carnegie Mellon University Computer Science technical report CMU-CS-92-100, January 1992.)

42. "NetBill: An Internet commerce system optimized for network-delivered services." M. Sirbu and J. D. Tygar. In *IEEE Personal Communications*, 2:4, August 1995, pp. 34-39. (An early version appeared in **Proceedings of Uniforum '96**, February 1996, pp. 203-226. Another early version appeared in **Proceedings of the 40th IEEE Computer Society International Conference**, March 1995, pp. 20-25.)

43. "Optimal sampling strategies for quicksort." C. C. McGeoch and J. D. Tygar. In *Random Structures and Algorithms*, 7:4, December 1995, pp. 287-300. (An early version appeared in **Proceedings of the 28th Annual Allerton Conference on Communication, Control, and Computing**, October 1990, pp. 62-71.)

44. "Geometric characterization of series-parallel variable resistor networks." R. Bryant, J. D. Tygar, and L. Huang. In *IEEE Transactions on Circuits and Systems 1: Fundamental Theory and Applications*, 41:11, November 1994, pp. 686-698. (Preprint also available.) (An early version appeared in **Proceedings of the 1993 IEEE International Symposium on Circuits and Systems**, May 1993, pp. 2678-2681.)

45. "Computability and complexity of ray tracing." J. Reif, J. D. Tygar, and A. Yoshida. In *Discrete and Computational Geometry*, 11:3, April 1994, pp. 265-287. (An early version appeared in **Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science**, October 1990, pp. 106-114.)

46. "Specifying and checking Unix security constraints." A. Heydon and J. D. Tygar. In *Computing Systems*, 7:1, Winter 1994, pp. 91-112. (An early version appeared in **Proceedings of the 3rd USENIX Security Symposium**, September 1992, pp. 211-226, preprint also available.)

47. "Protecting privacy while preserving access to data." L. J. Camp and J. D. Tygar. In *The Information Society*, 10:1, January 1994, pp. 59-71.

48. "Miro: visual specification of security." A. Heydon, M. Maimone, J. D. Tygar, J. Wing, and A. Zaremski. In *IEEE Transactions on Software Engineering*, 16:10, October 1990, pp. 1185-1197. (An early version appeared as Carnegie Mellon University Computer Science Department technical report CMU-CS-89-199, December 1989.)

49. "Efficient parallel pseudo-random number generation." J. Reif and J. D. Tygar. In *SIAM Journal of Computation*, 17:2, April 1988, pp. 404-411. (An early version appeared in **Proceedings of CRYPTO-85,** eds. E. Brickell and H. Williams, Springer, 1986, pp. 433-446.)

50. "Review of **Abstraction and Specification in Program Development**." J. D. Tygar. In *ACM Computing Reviews*, 28:9, September 1987, pp. 454-455.

Refereed Conference Papers (does not include items listed above)

51. "Censorship Arms Race: Research vs. Practice." S. Afroz, D. Fifield, M. Tschantz, V. Paxson, J. D. Tygar. In **HotPETs 2015 Proceedings**. June 2015. (To appear.)

52. "Large-Margin Convex Polytope Machine." A. Kantchelian, M. Tschantz, L. Huang, P. Bartlett, A. Joseph, J. D. Tygar. In **Advances in Neural Information Process Systems 27**. December 2014, pp. 3248-3256.

53. "Adversarial Active Learning." B. Miller, A. Kantchelian, S. Afroz, R. Bachwani, E. Dauber, L. Huang, M. Tschantz, A. Joseph, J. D. Tygar. In **AISec '14: Proceedings of the 2014 Workshop on Artificial Intelligence and Security**. November 2014, pp. 3-14.

54. "I know why you went to the clinic: Risks and Realization of HTTPS traffic analysis." B. Miller, L. Huang, A. Joseph, J. D. Tygar. In **Proceedings of the 14th International Symposium on Privacy Enhancing Technologies (PETS 2104)**, July 2014, pp. 143-163.

55. "Managing employee security behaviour in organisations: The role of cultural factors and individual values." L. Connolly, M. Lang, and J. D. Tygar In **Proceedings of the 29th IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection (SEC 2014)**, June 2014, pp. 417-430.

56. "Approaches to adversarial drift." A. Kantchelian, S. Afroz, L. Huang, A. Islam, B. Miller, M. Tschantz, R. Greenstadt, A. Joseph, J. D. Tygar. In **Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security**, November 2013, pp. 99-109.

57. "Systematic analysis and evaluation of Web privacy policies and implementations." B. Miller, K. Buck, and J. D. Tygar. In **Proceedings of the 7th International Conference for Internet Technology and Secure Transactions**, December 2012, pp. 534-540.

58. "Robust detection of comment spam using entropy rate." A. Kantchelian, J. Ma, L. Huang, S. Afroz, A. Jospeh, and J. D. Tygar. In **Proceedings of 5th ACM Workshop on Artificial Intelligence and Security**, October 2012, pp. 59-70.

59. "Adversarial machine learning." L. Huang, A. Joseph, B. Nelson, B. Rubenstein, and J. D. Tygar. In **Proceedings of 4th ACM Workshop on Artificial Intelligence and Security**, October 2011, pp. 43-58.

60. "Near-optimal evasion of convex-inducing classifiers." B. Nelson, B. Rubinstein, L. Huang, A. Joseph, S. Lau, S. Lee, S. Rao, A. Tran, and J. D. Tygar. In **Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics,** May 2010, pp. 549-556.

61. "CAPTCHA: Using strangeness in machine translation." T. Yamamoto, J. D. Tygar, and M. Nishigaki. In **Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications**, April 2010, pp.430-437. (See also item 123.)

62. "ANTIDOTE: Understanding and defending against poisoning of anomaly detectors." B. Rubinstein, B. Nelson, L. Huang, A. Joseph, S. Lau, S. Rao, N. Taft, and J. D. Tygar. In **Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement**, November 2009, pp. 1-14.

63. "Conditioned-safe ceremonies and a user study of an application to web authentication." C. Karlof, J. D. Tygar, and D. Wagner. In **Proceedings of the 16th Annual Network & Distributed System Security Symposium**, February 2009.

64. "Optimal ROC curve for a combination of classifiers." M. Barreno, A. Cardenas and J.D. Tygar. In **Advances in Neural Information Processing Systems (NIPS)**, December 2008, pp. 57-64.

65. "Open problems in the security of learning." M. Barreno, P. Bartlett, F. Chi, A. Joseph, B. Nelson, B. Rubinstein, U. Saini, and J. D. Tygar. In **Proceedings of the First ACM Workshop on AISec**, October 2008, pp. 19-26.

66. "Evading anomaly detection through variance injection attacks on PCA." (Extended abstract). B. Rubinstein, B. Nelson, L. Huang, A. Joseph, S. Lau, N. Taft, and J. D. Tygar. In **Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection**, September 2008, pp. 394-395.

67. "CITRIC: A low-bandwidth wireless camera network platform." P. Chen, P. Ahammad, C. Boyer, S. Huang, L. Lin, E. Lobaton, M. Meingast, S. Oh, S. Wang, P. Yan, A. Yang, C. Yeo, L. Chang, J. D. Tygar, and S. Sastry. In **Proceedings of the 2nd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC-08)**, September 2008, pp. 1-10.

68. "A power-preserving broadcast protocol for WSNs with DoS resistance." C. Ni, T. Hsiang, J. D. Tygar. In **Proceedings of 17th International IEEE Conference on Computer Communications and Networks**, August 2008, pp. 1 – 6.

69. "SWOON: A testbed for secure wireless overlay networks." Y. Huang, J. D. Tygar, H. Lin, L. Yeh, H. Tsai, K. Sklower, S. Shieh, C. Wu, P. Lu, S. Chien, Z. Lin, L. Hsu, C. Hsu, C. Hsu, Y. Wu, and M. Leong. In **Proceedings USENIX Workshop on Cyber Security and Test**, July 2008.

70. "Characterizing botnets from email spam records." L. Zhuang, J. Dunagan, D. Simon, H. Wang, I. Osipkov, G. Hulten and J. D. Tygar. In **Proceedings of First USENIX Workshop on Large Scale Exploits and Emergent Threats (LEET 2008)**, April 2008.

71. "Exploiting machine learning to subvert your spam filter. " B. Nelson, M. Barreno, F. Chi, A. D. Joseph, B. Rubinstein, U. Saini, C. Sutton, J. D. Tygar, and K. Xia. In **Proceedings of the First USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 2008)**, April 2008.

72. "Dynamic pharming attacks and locked same-origin policies for web browsers." C. Karlof, U. Shankar, J.D. Tygar, and D. Wagner. In **Proceedings of the Fourteenth ACM Conference on Computer and Communications Security (CCS 2007)**, November 2007, pp. 58-71.

73. "Coexistence proof using chain of timestamps for multiple RFID tags." C. Lin, Y. Lai, J. D. Tygar, C. Yang, and C. Chiang. In **Proceedings of Advances in Web and Network Technologies and Information Management,** June 2007, pp. 634-643.

74. "Why phishing works." R. Dhamija, J. D. Tygar, and M. Hearst. In **Proceedings of CHI-2006: Conference on Human Factors in Computing Systems**, April 2006, pp. 581-590.

75. "Can machine learning be secure?" M. Barreno, B. Nelson, R. Sears, A. Joseph, and J. D. Tygar. *Invited paper*. In **Proceedings of the ACM Symposium on Information, Computer, and Communication Security,** March 2006, pp. 16-25.

76. "The battle against phishing: Dynamic security skins." R. Dhamija and J. D. Tygar. In **SOUPS 2005: Proceedings of the 2005 ACM Symposium on Usable Security and Privacy**, *ACM International Conference Proceedings Series*, ACM Press, July 2005, pp. 77-88. (See also item 10.)

77. "Collaborative filtering CAPTCHAs." M. Chew and J. D. Tygar. In **Human Interactive Proofs: Second International Workshop (HIP 2005)**, eds. H. Baird and D. Lopresti, Springer, May 2005, pp. 66-81.

78. "Phish and HIPs: Human interactive proofs to detect phishing attacks." R. Dhamija and J. D. Tygar. In **Human Interactive Proofs: Second International Workshop (HIP 2005)**, eds. H. Baird and D. Lopresti, Springer, May 2005, pp. 127-141.

79. "Image recognition CAPTCHAs." M. Chew and J. D. Tygar. In **Proceedings of the 7th International Information Security Conference (ISC 2004)**, Springer, September 2004, pp. 268-279. (A longer version appeared as UC Berkeley Computer Science Division technical report UCB/CSD-04-1333, June 2004.)

80. "Side effects are not sufficient to authenticate software." U. Shankar, M. Chew, and J. D. Tygar. In **Proceedings of the 13th USENIX Security Symposium**, August 2004, pp. 89-101. (A version with an additional appendix appeared as UC Berkeley Computer Science Division technical report UCB/CSD-04-1363, September 2004.)

81. "Statistical monitoring + predictable recovery = Self-*." A Fox, E. Kiciman, D. Patterson, R. Katz, M. Jordan, I. Stoica and J. D. Tygar. In **Proceedings of the 2nd Bertinoro Workshop on Future Directions in Distributed Computing (FuDiCo II)**, June 2004 (online proceedings).

82. "Distillation codes and their application to DoS resistant multicast authentication." C. Karlof, N. Sastry, Y. Li, A. Perrig, and J. D. Tygar. In **Proceedings of the Network and Distributed System Security Conference (NDSS 2004),** February 2004, pp. 37-56.

83. "Privacy and security in the location-enhanced World Wide Web." J. Hong, G. Boriello, J. Landay, D. McDonald, B. Schilit, and J. D. Tygar. In **Proceedings of the Workshop on Privacy at Ubicomp 2003,** October 2003 (online proceedings).

84. "The problem with privacy." J. D. Tygar. *Keynote paper*. In **Proceedings of the 2003 IEEE Workshop on Internet Applications,** June 2003, pp. 2-8.

85. "Safe staging for computer security." A. Whitten and J. D. Tygar. In **Proceedings of the 2003 Workshop on Human-Computer Interaction and Security Systems,** April 2003.

86. "Expander graphs for digital stream authentication and robust overlay networks." D. Song, D. Zuckerman, and J. D. Tygar. In **Proceedings of the 2002 IEEE Symposium on Security and Privacy,** May 2002, pp. 258-270.

87. "ELK: A new protocol for efficient large-group key distribution." A. Perrig, D. Song, and J. D. Tygar. In **Proceedings of the 2001 IEEE Symposium on Security and Privacy**, May 2001, pp. 247-262.

88. "Efficient and secure source authentication for multicast." A. Perrig, R. Canetti, D. Song, and J. D. Tygar. In **Proceedings of the Internet Society Network and Distributed System Security Symposium (NDSS 2001)**, February 2001, pp. 35-46.

89. "Efficient authentication and signing of multicast streams over lossy channels." A. Perrig, R. Canetti, J. D. Tygar, and D. Song. In **Proceedings of the 2000 IEEE Symposium on Security and Privacy**, May 2000, pp. 56-73.

90. "Flexible and scalable credential structures: NetBill implementation and experience." Y. Kawakura, M. Sirbu., I. Simpson, and J. D. Tygar. In **Proceedings of the International Workshop on Cryptographic Techniques and E-Commerce**, July 1999, pp. 231-245.

91. "Open problems in electronic commerce." J. D. Tygar. *Invited address.* In **Proceedings of the 18th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 1999)**, May 1999, p. 101.

92. "Electronic auctions with private bids." M. Harkavy, J. D. Tygar, and H. Kikuchi. In **Proceedings of the 3rd USENIX Workshop on Electronic Commerce,** September 1998, pp. 61-73.

93. "Atomicity versus anonymity: Distributed transactions for electronic commerce." J. D. Tygar. In **Proceedings of the 24th International Conference on Very Large Data Bases,** August 1998, pp. 1-12.

94. "Smart cards in hostile environments." H. Gobioff, S. Smith, J. D. Tygar, and B. Yee. In **Proceedings of the 2nd USENIX Workshop on Electronic Commerce**, November 1996, pp. 23-28. (An early version appeared as Carnegie Mellon University Computer Science technical report CMU-CS-95-188, September 1995.)

95. "Anonymous atomic transactions." L. J. Camp, M. Harkavy, and B. Yee. In **Proceedings of the 2nd USENIX Workshop on Electronic Commerce**, November 1996, pp. 123-133. (Preprint also available.) (An early version appeared as Carnegie Mellon University Computer Science technical report CMU-CS-96-156, July 1996.)

96. "Model checking electronic commerce protocols." N. Heintze, J. D. Tygar, J. Wing, and H. Wong. In **Proceedings of the 2nd USENIX Workshop on Electronic Commerce**, November 1996, pp. 147-164.

97. "WWW electronic commerce and Java Trojan horses." J. D. Tygar and A. Whitten. In **Proceedings of the 2nd USENIX Workshop on Electronic Commerce**, November 1996, pp. 243-250.

98. "Building blocks for atomicity in electronic commerce." J. Su and J. D. Tygar. In **Proceedings of the 6th USENIX Security Symposium**, July 1996, pp. 97-102.

99. "Token and notational money in electronic commerce." L. J. Camp, M. Sirbu, and J. D. Tygar. In **Proceedings of the 1st USENIX Workshop on Electronic Commerce**, July

1995, pp. 1-12. (An early version was presented at the Telecommunications Policy Research Conference, October 1994.)

100. "NetBill security and transaction protocol." B. Cox, J. D. Tygar, and M. Sirbu. In **Proceedings of the 1st USENIX Workshop on Electronic Commerce**, July 1995, pp. 77-88.

101. "Secure coprocessors in electronic commerce applications." B. Yee and J. D. Tygar. In **Proceedings of the 1st USENIX Workshop on Electronic Commerce**, July 1995, pp. 155-170.

102. "Completely asynchronous optimistic recovery with minimal rollbacks." S. Smith, D. Johnson, and J. D. Tygar. In **Proceedings of the 25th IEEE Symposium on Fault-Tolerant Computing**, June 1995, pp. 361-370. (An early version appears as Carnegie Mellon University Computer Science technical report CMU-CS-94-130, March 1994.)

103. "A fast off-line electronic currency protocol." L. Tang and J. D. Tygar. In **CARDIS 94: Proceedings of the First IFIP Smart Card Research and Advanced Application Conference**, October 1994, pp. 89-100.

104. "Security and privacy for partial order time." S. Smith and J. D. Tygar. In **Proceedings 1994 Parallel and Distributed Computing Systems Conference**, October 1994, pp. 70-79. (Early versions appeared as Carnegie Mellon University Computer Science technical reports CMU-CS-93-116, October 1991 and February 1993, and CMU-CS-94-135, April 1994.)

105. "Certified electronic mail." A. Bahreman and J. D. Tygar. In **Proceedings of the 1994 Network and Distributed Systems Security Conference**, February 1994, pp. 3-19.

106. "Miro tools." A. Heydon, M. Maimone, A. Moormann, J. D. Tygar and J. Wing. In **Proceedings of the 3rd IEEE Workshop on Visual Languages**, October 1989, pp. 86-91. (A preprint appeared as Carnegie Mellon University Computer Science technical report CMU-CS-89-159, July 1989.)

107. "Constraining pictures with pictures." A. Heydon, M. Maimone, A. Moormann, J. D. Tygar, and J. Wing. In **Information Processing 89: Proceedings of the 11th World Computer Congress**, August 1989, pp. 157-162. (An early version appeared as Carnegie Mellon University Computer Science technical report CMU-CS-88-185, November 1988.)

108. "How to make replicated data secure." M. Herlihy and J. D. Tygar. In **Proceedings of CRYPTO-87**, ed. C. Pomerance, 1988, pp. 379-391. (An early version appeared as Carnegie Mellon University Computer Science Technical Report CMU-CS-87-143, August 1987.

109. "Visual specification of security constraints." J. D. Tygar and J. Wing. In **Proceedings of the 1987 (First IEEE) Workshop on Visual Languages**, August 1987, pp. 288-301. (A preprint appeared as Carnegie Mellon University Computer Science Technical Report CMU-CS-87-122, May 1987.)

110. "Efficient netlist comparison using hierarchy and randomization." J. D. Tygar and R. Ellickson. In **Proceedings of the 22nd ACM/IEEE Design Automation Conference**, Las Vegas, NV, July 1985, pp. 702-708.

111. "Hierarchical logic comparison." R. Ellickson and J. D. Tygar. In **Proceedings of MIDCON '84**, 1984.

Other Conference Publications (does not include items listed above)

112. "Keynote speech: Adversarial Machine Learning." J. D. Tygar. In **Companion to the 2014 IEEE Eighth International Conference on Software Security and Reliability**, June 2014, pp. xviii-xxi.

113. "Panel: Authentication in constrained environments." M. Burmester, V. Gligor, E. Kranakis, J. D. Tygar and Y. Zheng . Transcribed by B. de Medeiros. In **Proceedings First International Workshop: MADNES 2005,** September 2005**,** pp. 186-191.

114. "When computer security crashes with multimedia." [Abstract] J. D. Tygar. In **Proceedings of the 7th International IEEE Symposium on Multimedia,** December 2005, p. 2.

115. "Notes from the **Second USENIX Workshop on Electronic Commerce**." M. Harkavy, A. Meyers, J. D. Tygar, A. Whitten, and H. Wong. In **Proceedings of the 3rd USENIX Workshop on Electronic Commerce,** September 1998, pp. 225-242.

116. "How are we going to pay for this? Fee-for-service in distributed systems - research and policy issues." C. Clifton, P. Gemmel, E. Means, M. Merges, J. D. Tygar. In **Proceedings of the 15th International Conference on Distributed Computing Systems**, May 1995, pp. 344-348.

117. "Miro: A visual language for specifying security." [Abstract] M. Maimone, A. Moorman, J. D. Tygar, J. Wing. In **Proceedings of the (First) USENIX UNIX Security Workshop**, August 1988, p. 49.

118. "StrongBox: Support for self-securing programs." [Abstract] J. D. Tygar, B. Yee, and A. Spector. In **Proceedings of the (First) USENIX UNIX Security Workshop**, August 1988, p. 50.

Standards Documents (does not include items listed above)

119. **TESLA: Multicast Source Authentication Transform Introduction.** A. Perrig, D. Song, R. Canetti, J. D. Tygar, B. Briscoe. IETF RFC 4082. June 2005. (Early drafts of this RFC were published in October 2002, and in May, August, and December 2004.)

120. **Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C) (Draft)**. United States Postal Service. January 1999. (Note: I was a major contributor to this document.)

121. **Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidence Systems (PCIBI-O) (Draft)**. United States Postal Service. February 2000. (Note: I was a major contributor to this document.)

122. **Production, Distribution, and Use of Postal Security Devices and Information Based Indicia**." United States Postal Service. *Federal Register* 65:191, October 2, 2000, pp. 58682-58698. (Note: I was a major contributor to this document.)

Technical Reports (does not include items listed above)

123. **機械翻訳の違和感を用いた CAPTCHA の提案 (A Proposal of CAPTCHA Using Strangeness in Machine Translation)**. T. Yamamoto, J. D. Tygar, and M. Nishigaki. IPSJ SIG Technical Report 2009-CSEC-46 No.38, June 2009. (See also item 61.)

124. **Compromising PCA-based anomaly detectors for network-wide traffic.** B. Rubinstein, B. Nelson, L. Huang, A. Joseph, S. Lau, N. Taft, and J. D. Tygar. UC Berkeley, EECS technical report UCB/EECS-2008-73, May 2008.

125. **Usability of Security: A Case Study**. A. Whitten and J. D. Tygar. Carnegie Mellon University Computer Science technical report CMU-CS-98-155, December 1998. (Note: this report partly overlaps item 11, but also includes substantial additional material.)

126. **Security for Network Attached Storage Devices**. H. Gobioff, G. Gibson and J. D. Tygar. Carnegie Mellon University Computer Science technical report CMU-CS-97-185, October 1997.

127. **Cryptography: It's Not Just for *Electronic* Mail Anymore**. J. D. Tygar and B. Yee. Carnegie Mellon University Computer Science technical report CMU-CS-93-107, March 1993. (See also item 18 above.)

128. **Median Separators in *d* Dimensions**. J. Sipelstein, S. Smith, and J. D. Tygar . Carnegie Mellon University Computer Science technical report CMU-CS-88-206, December 1988.

129. **When are Best Fit and First Fit Optimal?** C. McGeoch and J. D. Tygar. Carnegie Mellon University Computer Science technical report CMU-CS-87-168, October 1987.

130. **Display Manager User's Guide.** J. D. Tygar. Valid Logic Systems engineering memorandum, VED-050682-1-JDT, May 1982.

131. **Performance analysis of the DANTE Network**. Bell Telephone Laboratories technical memorandum, August 1981.

Patents (does not include items listed above)

132. **Anonymous certified delivery**. L. J. Camp, J. D. Tygar, and M. Harkavy. US Patent 6,076,078, June 13, 2000.

133. **Method and apparatus for purchasing and delivering digital goods over a network**. M. Sirbu, J. D. Tygar, B. Cox, T. Wagner. US Patent 5,809,144, September 1998.

Miscellaneous Technical (does not include items listed above)

134. **Security with Privacy**. Briefing from the Information Science and Technology Study Group on Security and Privacy (chair: J. D. Tygar). December 2002.

135. **Expert Report of J. D. Tygar ... A&M Records et al v. Napster....** J. D. Tygar. (For Hearing) July 2000.

Miscellaneous Non-Technical (does not include items listed above)

136. "Welcome multiculturalism (Letter to the editor)." J. D. Tygar. *Taipei Times*, November 12, 2004, p. 8.