

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
SAMSUNG ELECTRONICS AMERICA, INC.,
SAMSUNG TELECOMMUNICATIONS AMERICA, LLC,
CISCO SYSTEMS, INC., and AVAYA, INC.,
Petitioner,

v.

STRAIGHT PATH IP GROUP, INC.
Patent Owner

Case No. IPR2014-01366¹
U.S. Patent No. 6,108,704

DECLARATION OF DR. STUART STUBBLEBINE

¹ IPR2015-01011 has been joined with this proceeding.

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background and Qualifications	1
III.	Materials Considered.....	3
IV.	Person of Ordinary Skill in the Art.....	4
V.	Legal Standards	4
VI.	Background of the '704 patent	6
	A. The Challenged Claims of the '704 Patent	12
VII.	Claim Construction.....	14
	A. “process”.....	15
	B. “point-to-point communication link”	16
	C. “connected to the computer network” / “on-line”	18
	D. “transmitting to the server a network protocol address received by the first process following connection to the computer network”	20
	E. “network protocol address”	20
	F. “is” and “status”	21
VIII.	Microsoft Manual	21
IX.	NetBIOS.....	29
X.	PALMER	33

I, Dr. Stuart Stubblebine, being of legal age, hereby declare, affirm, and state the following:

I. Introduction

1. The facts set forth below are known to me personally and I have firsthand knowledge of them.

2. I have been retained as an independent expert witness by Straight Path IP Group, Inc. (“Patent Owner”) to make this declaration in support of Patent Owner’s Response to Petition for Inter Partes Review of U.S. Patent No. 6,108,704. I am being compensated for my time at a rate of \$850 per hour. My compensation is not dependent in any way upon the outcome of this *Inter Partes* Review.

II. Background and Qualifications

3. I received a Bachelor of Science degree in Computer Science and Mathematics from Vanderbilt University in May 1983. Later that year and into 1984, I completed graduate level courses in Teleprocessing Systems (including computer networks and distributed processing) and Radio Systems Design at the US Army Signal Center. In December 1988, I received a Master of Science degree in Electrical Engineering from the University of Arizona; my area of focus was computer engineering with an emphasis in networking and distributed systems. I received my Doctorate in Electrical Engineering in August 1992 from the

University of Maryland; my area of focus was computer engineering, and my dissertation was on Message Integrity in Cryptographic Protocols. My CV is attached as Exhibit 1.

4. I have been working as an independent consultant since March 2000, specializing in computer and network security evaluations, detailed design and formal analysis, applied research, technical due diligence reviews, and in the provision of expert witness services, particularly in patent litigation. My clients range from domestic start-ups to international Fortune 500 companies, and include American Express, AMD, British Telecom, First Data Corporation, IBM, and Microsoft, as well as the New York City Department of Education and the New York City Police Department.

5. Previously, I worked as a research scientist with Stubblebine Research Labs, LLC, where I conduct research in the areas of security and privacy technology. Some of this research has been funded by the National Science Foundation.

6. Between July 2002 and June 2004, I was a Professional Researcher—a position that was the equivalent of a Full Professor—at the University of California at Davis. I was affiliated with the Computer Science Department and my

research was focused in the areas of security, cryptography, and secure software engineering.

III. Materials Considered

7. In forming the opinions set forth in this report, I have considered and relied upon my education, knowledge of the relevant field, and my experience. I have also reviewed and considered U.S. Patent No. 6,108,704, its prosecution history, and documents produced by both Patent Owner and Petitioner.

Specifically, I have considered the following materials:

- U.S. Patent No. 6,108,704 (the “’704 patent”).
- File history for the ’704 patent.
- Reexamination history for the ’704 patent.
- Microsoft Windows NT Server Version 3.5 TCPIP.HLP.
- Technical Standard: Protocols for X/Open PC Interworking: SMB, Version 2.
- Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concept and Methods, RFC 1001 (Mar. 1987).
- Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications, RFC 1002 (Mar. 1987).
- U.S. Patent No. 5,375,068 (“Palmer”).

- “Modifying WINS server defaults”
[https://technet.microsoft.com/en-us/library/cc785736\(d=printer,v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc785736(d=printer,v=ws.10).aspx)
- “Microsoft makes its move with Windows NT SDK”. InfoWorld 14 (28): <http://windows.microsoft.com/en-us/windows/history#T1=era3>.
- http://www.oldcomputermuseum.com/os/windows_nt3.5.html.

I have also reviewed all of the papers filed at the Federal Circuit Court of Appeals in the Straight Path IP Group, Inc. v. Sipnet EU S.R.O appeal.

IV. Person of Ordinary Skill in the Art

8. A person of ordinary skill in the art in the field of the '704 patent in the early 1990s would typically have the knowledge acquired by a person having a Bachelor's degree in computer science or computer engineering or related field. I believe a person of ordinary skill in the art of the '704 patent could also have obtained the requisite knowledge through 1-2 years of professional experience as a software developer designing and constructing distributed applications or systems.

V. Legal Standards

9. It is my understanding that a claim is invalid by anticipation when a single prior art reference (as defined by 35 U.S.C. § 102) existed prior to the claim's priority date and teaches every element of the claim. (*Verizon Servs. Corp.*

v. Cox Fibernet Va., Inc., 602 F.3d 1325, 1336-37 (Fed. Cir. 2010)). I also understand that under 35 U.S.C. § 103, the combined teachings of more than one prior art reference can be used to demonstrate that all of the elements of a claim were known at the time of the invention. I understand this is often referred to as “obviousness,” and such obviousness must be assessed at the time the invention was made. (*Eurand, Inc. v. Mylan Pharms., Inc.*, 676 F.3d 1063, 1073 (Fed. Cir. 2012)). I understand that, under 35 U.S.C. § 103, a patent cannot be obtained “if the differences between the subject matter to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art.” (35 U.S.C. § 103).

10. I understand that, in an *inter partes* review proceeding, claim terms should be given their broadest reasonable construction consistent with the specification. However, I understand that, if a patent has expired, claim terms should be construed according to the standard of a district court, and that under such a standard, a claim term should be construed according to its “ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. It is my further understanding that claim terms are given their ordinary and accustomed meaning as would be understood by

one of ordinary skill in the art, unless the inventor, as a lexicographer, has set forth a special meaning.

VI. Background of the '704 patent

11. The '704 patent discloses a system that enables real-time point-to-point communications between running computer programs or applications that are connected to a computer network. Such programs include programs or applications supporting real-time video teleconferencing and other real-time point-to-point video and voice communications. (Ex. 2013 at 1:9-20; 1:50-56; 7:32-41; 8:18-22.)

12. Applications supporting such point-to-point communication may be installed on a computer, but just because a computer is running does not ensure that a program or application supporting point-to-point communication installed on that computer is also running. Additionally, just because a computer is connected to the Internet (i.e., is “on-line”) it does not mean that a program or application installed on that computer is even running much less that it is actually on-line. In fact a computer that is connected to the Internet may have programs installed on it that are not connected to the Internet, off-line, and not available for communication. Some programs may be running and online, while others may be “closed” (or not running) and offline.

13. Because communication can only be established between computer programs that are on-line at the time the desired communication is sought, it is desirable for a user of a first computer program seeking communication with a user of a second computer program to know when the second user's program is on-line and thus available for communication. (Ex. 2013 at 6:14-16.) The '704 patent discloses a real-time point-to-point Internet communications protocol that enables: (1) a first computer program to query a connection server to determine if a second computer program is currently connected to the network, and (2) if the second computer program is connected, to obtain its existing network address so that the desired point-to-point communication can be established at the time communication is sought. (Ex. 2013 at 1:63-2:10; 3:40-54; 5:15-6:16; 10:4-37; claims 1, 2, 4, 32, 33, 38.)

14. As explained in the '704 patent specification, the prior art made it possible to establish point-to-point communications between devices and programs that had permanent Internet Protocol ("IP") addresses. (Ex. 2013 at 1:48-52.) But, some devices do not have a permanent and stable address on the Internet and instead repeatedly log on and off of the Internet potentially receiving a new dynamically allocated IP address each time they reconnect to the network. (*Id.* 1:35-47; 5:14-29; 6:6-16.)

15. Dynamic assignment of IP addresses made it difficult to establish real-time point-to-point video or voice communications between computer programs that are not permanently connected to the network, because a first user seeking to communicate with a second user would not necessarily know the IP address associated with the second user's computer program as it could be dynamically assigned a different IP address from time to time. (Ex. 2013 at 1:48-56.)

16. The '704 patent solved the problems caused by dynamic allocation of IP addresses to computers continually connecting and disconnect from the Internet by providing a real-time point-to-point Internet communications protocol for: (1) determining whether a particular, computer program is currently running and connected to a network; (2) determining that computer program's address on the network at the time the communication is sought; and (3) establishing a point-to-point communication with that computer program. (Ex. 2013 at 1:63-2:10; 5:15-6:16; 7:32-36; 10:4-37; claims 1, 2, 4, 32, 33, 38.)

17. In one embodiment, a first user, who is connected to the Internet and who wishes to communicate with another user over the Internet launches a program on her computer and connects that program to the network. (Ex. 2013 at 3:40-46; 4:26-32; 5:21-24; 10:4-9.) The current IP address of the first user's computer is then transmitted to the claimed connection server which determines

whether a given program is on-line and available for communication and can facilitate communication between different on-line programs. (*Id.* at 5:25-31; 5:55-6:15; 10:4-21.) Upon receiving this transmission, the connection server stores the first user's then-current IP address in a database, thus establishing the first user's computer program as an "active on-line party" in the connection server database. (*Id.* at 5:25-34; 5:55-60; 6:1-16.)

18. The first user's computer program may later disconnect from the network, and thus no longer be an "active on-line party" available for communication. (Ex. 2013 at 6:1-14.) The specification discloses that "[w]hen a user logs off or goes off-line from the Internet 24, the connection server 26 updates the status of the user in the database 34; for example by removing the user's information, or by flagging the user as being off-line." (*Id.*) The user's on-line status is updated when she logs off the network so that the connection server can keep an up to date accounting of which users are connected to the network and available for communication and which are not connected and thus disabled from engaging in point-to-point communication. (*See id.* at 6:6-14.) Like the first user, a second user, or callee, may also start a computer program on his computer and thereby store his then-current IP address in the connection server database and thus establish his computer program as active and on-line. (*Id.* at 5:34-38; 10:4-7.)

19. To initiate a point-to-point communication with a second user, a first user, after connecting her computer program to the Internet and sending her then-current IP address to the connection server, may send a request to the connection server regarding the availability for communication of a second user. (Ex. 2013 at 3:40-43; 5:45-56; 10:7-10, 28-32.) In response to the first user's request, the connection server will search its database to determine if the second user's computer program is on-line. (*Id.* at 5:57-60; 10:28-34.) If it is, the connection server then forwards the IP address of the second user's computer program to the first user's computer program, which then uses that IP address to establish a point-to-point communication between the first and second users' computer programs. (*Id.* at 3:40-42; 5:60-67; 10:12-18, 32-37.) This communication is not intermediated by the connection server. (*See id.*)

20. If the second user's computer program is not on-line at the time the first user's computer program makes its query, the connection server, after checking its database, will determine that the second computer program is not currently on-line and will send back to the first user an "off-line" signal or message. (Ex. 2013 at 6:1-16; 10:14-21.) The connection server will send the first user's computer program an "off-line" signal or message when the second user's program is not currently connected to the network, even if that second program is

still registered with the connection server, i.e., if the second program's name remains stored in the connection server. (*Id.*) Thus, whether a computer program is currently on-line is not and cannot be determined by whether it is registered with a connection server, because the program may be registered but also off-line. (*Id.* at 6:1-14.)

21. During *ex parte* reexamination of the '704 patent, the applicants addressed whether the active on-line status of a process – whether the process is currently connected to the computer network – is the same as the status of having been on-line at some point in the past to establish an active name registration. (Ex. 1003 at 1078-79.). This is the question presented by the NetBIOS reference. The applicants submitted an Office Action Response explaining that the active name registration disclosed in NetBIOS is not the on-line status disclosed in the patent claims because having registered a name with the connection server at some previous time does not indicate that the registered computer is currently on-line:

While NetBIOS uses name entries with 'active' statuses as part of its name management process, an analysis of how that "active" status is used shows that **"an active name" is not synonymous with "an on-line status"** with respect to the computer network. **An active name simply refers to a name that has been registered and that has not yet been de-registered, independent of whether the associated computer is or is not on-line.**

(*Id.* at 1073 (emphasis added).) The PTO subsequently affirmed the patentability of each of the claims at issue in this appeal. (*Id.* at 1928.)

A. The Challenged Claims of the '704 Patent

22. Each of the challenged claims at issue in this appeal concerns a method, apparatus, or “computer program product” for establishing a point-to-point communication between a first (or caller) process and a second (or callee) process. (Ex. 2013 at claims 1, 11, 12, 14, 16, 22, 23, 27, 30, and 31.) Each challenged claim concerns communications between **processes**, not merely computers, and each concerns determining whether those processes are **currently on-line**, not whether they were on-line at some undetermined point in the past. (*See id.*)

23. Each of the challenged claims concerns **processes**—computer programs or applications—not merely the computers on which those processes may (or may not) be running. The preamble of independent claim 1, for example, makes this distinction clear, and shows that the patentees distinctly and deliberately chose to direct their claims towards a “process” not a “computer.” Claim 1 differentiates between the computer (“computer system”) that executes “the first process” and the “first process” itself: “A computer program product for use with a computer system, **the computer system executing a first process**”

(Ex. 2013 at claim 1 (emphasis added).) And the remainder of claim 1, reproduced in its entirety below, pertains to the on-line status of, and communications between, processes, not merely the computers that execute those processes:

1. A computer program product for use with a computer system, **the computer system executing a first process** and operatively **connected to a second process** and a server over a computer network, the computer program product comprising:

a computer usable medium having a program code embodied in the medium, the program code comprising:

program code for transmitting to the server **a network protocol address received by the first process** following connection to the computer network;

program code for transmitting, to the server, a query as to **whether the second process is connected to the computer network;**

program code for receiving **a network protocol address of the second process** from the server, **when the second process is connected to the network;** and

program code, responsive to the network protocol address of the second process, for establishing **a point-to-point communication**

link between the first process and the second process over the computer network.

(Ex. 2013 at claim 1 (emphasis added); *see* claims 11, 12, 14, 16, 22, 23, 27, 30, and 31.)

24. Each of the challenged claims concerns a determination of whether the target process with which the caller wishes to communicate is **currently** connected to the computer network (is currently “on-line”) not whether the process was connected at some previous time. (Ex. 2013, at claims 1, 11, 12, 14, 16, 22, 23, 27, 30, and 31.) For example, claim 1 is directed to a “computer program product” that (1) transmits to the server “a query as to whether the second process **is connected to the computer network,**” and (2) receives the second process’s network protocol address from the server only “when the second process **is connected to the computer network.**” (*Id.* at claim 1.) These claims’ temporal focus on the process’s on-line status **at the time** the desired communication is sought accords with the **realtime** focus of the point-to-point communications protocol disclosed in the ’704 patent. (*Id.* at 1:50-56; 7:32-41, 8:21-22.) One way the patent describes this focus on realtime communications, is by polling the second processing unit every 3-5 seconds. (*Id.* at 6:55-60; Fig. 2.)

VII. Claim Construction

A. “process”

25. I agree with Straight Path’s proposed construction of the claim term “process” as meaning “a running instance of a computer program or application,” because this construction comports with the intrinsic record. Also, I note it has been agreed to by Petitioner in prior proceedings relating to the ’704 patent and by Petitioner’s expert, Dr. Henry Houh, in this proceeding. (Ex. 2022 at 192:21-192:15).

26. As explained above, the claims of the ’704 patent show that the patentees deliberately chose to direct their claims towards a running instance of a computer program, or “process” rather than the machine on which a process runs, i.e., a computer. The specification of the ’704 patent supports this construction. The specification expressly states that the disclosed point-to-point internet protocol can be a “computer program described herein below in conjunction with FIG. 6, which may be implemented from compiled and/or interpreted source code in the C++ programming language, and which may be downloaded.... (Ex. 2013 at 3:40-55.) Further, the specification states that the claimed “process,” also referred to as a “processing unit” in the specification, can be implemented in a PDA, which supports the interpretation of process as a piece of software. (*See id.* at 4:26-32

(“In addition, either of the first processing unit 12 and the second processing unit 22 may be implemented in a personal digital assistant...”).)

27. Additionally, the claim term “process” was construed in several prior lawsuits in which Straight Path asserted the ’704 patent or a related patent. In *Straight Path IP Group, Inc. v. Bandwidth.com, Inc.*, a case involving U.S. Patent No. 6,513,066, a continuation of the ’704 patent application, the United States District Court for the Eastern District of Virginia construed “process” as “a running instance of a computer program or application.” (Ex. 2004 at *13.) Consistent with the *Bandwidth* decision, Samsung, in *Straight Path IP Group, Inc. v. Blackberry, Ltd.*, a case involving the ’704 patent, agreed that the proper construction of the term process is “a running instance of a computer program or application.” (Ex. 2016.)

28. Furthermore, during his deposition, Samsung’s expert, Dr. Houh, agreed that the proper construction of the term “process” is “a running instance of a computer program or application.” (Ex. 2022 at 192:21-193:15.)

B. “point-to-point communication link”

29. Construction of this term is not necessary to my opinions in this declaration, but to the extent the Board construes the term “point-to-point communication link,” I agree with Straight Path that this term should be interpreted

to mean “a connection between two processes over a computer network that is not intermediated by a connection server.”

30. As explained above, the invention provides users with a protocol with which to establish real-time, point-to-point communications over computer networks. During prosecution of the patent, the inventors explained that the claimed point-to-point communication is not intermediated by the connection server disclosed in the invention:

Upon receipt of the network protocol [sic] address of the first process, the second process establishes communications with the first process directly, without any intervention from the address/information server.

Exhibit 1002, Dec. 4, 1997 Amendment, at 350.

31. An interpretation of this term to mean not intermediated by any server would be inappropriate because in practice a “point-to-point” communication established over the Internet are often intermediated by a hardware device providing one or more services. These devices could be included in what one of ordinary skill in the art would understand to be a server. For instance, a “point-to-point” communication may be routed as it passes through the Internet, and such routing is often performed by a computer providing services as well.. One example of this is when a computer is acting as a router, but is also running a server process, such as running FTP server program, in addition to its routing functionality. Thus,

interpreting a point-to-point communication not to be intermediated by any server would eliminate from the definition of “point-to-point” common point-to-point communications made over the Internet. Interpreting “point-to-point communication link” as not being intermediated by a connection server takes into account the reality that servers are commonly used to route Internet communications. Routers at the time of the invention were configurable to be servers themselves. The inventors intended use of the internet, which would necessarily have included these routers.

32. Samsung’s construction unnecessarily narrows the scope of the claims, and does so in a way that disregards the prosecution history.

C. “connected to the computer network” / “on-line” ”

33. I agree with Straight Path’s interpretation of “connected to the computer network” and “on-line” as meaning available for communication. I disagree with Petitioner’s proposed construction of these terms as meaning “on-line, e.g., registered with a server.” Petitioner’s proposed construction essentially says that at every moment a given process is registered, it is connected to the computer network, and on-line and available for communication. But, the ’704 patent specification does not support this conclusion. Rather, it clearly states that a

user can still be in the database (“registered”) even when it is not on-line and available for communication:

When a user logs off or goes off-line from the Internet 24, the connection server 26 updates the status of the user in the database 34; for example, by removing the user’s information, or by flagging the user as being off-line. The connection server 26 may be instructed to update the user’s information in the database 34 by an off-line message, such as a data packet, sent automatically from the processing unit of the use prior to being disconnected from the connection server 26. Accordingly, an off-line user is effectively disabled from making and/or receiving point-to-point Internet communications.

(Ex. 2013 at 6:6-16.)

34. The ’704 patent teaches that, once registered, a name of a user will remain in the database regardless of whether the user is actually on-line. The claimed query determines whether the named user is actually on-line and available for communication at the time of the query:

Upon the first user initiating the point-to-point Internet protocol when the first user is logged on to Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server... The first processing unit 12 then sends a query, including the E-mail address of the callee, to the connection server 26. The connection server 26 then searches the database 34 to determine whether the callee is logged-in by finding any stored information corresponding to the callee’s E-mail address indicating that the callee is active and on-line...if the callee is not on-line when the connection server 26 determines the callee’s status, the connection server 26 sends an OFF-LINE signal or message to the first processing unit 12.

(Ex. 2013 at 5:24-6:4.)

D. “transmitting to the server a network protocol address received by the first process following connection to the computer network.”

35. Also Petitioner’s construction of the term “connected to the computer network” / “on-line” to mean “registered with a server” is contradicted by the claims themselves. The claims require a network protocol address received “following connection to the computer network.” (Ex. 2013 at 11:9-11). If a computer is not considered “connected to the network” until it is “registered with a server” then the computer would need to receive its network protocol address after it registered with the server. But in order to register with a server, the computer must already have its network protocol address. Thus, if the term “connected to the computer network” / “on-line” is construed to mean “registered with a server” then neither WINS nor NetBIOS disclose the claim element “a network protocol address received by the first process following connection to the computer network” because neither reference teaches “a network protocol address received by the first process following registration with the server.”

E. “network protocol address”

36. I agree with Straight Path that the term “network protocol address” does not require construction and should be given its plain and ordinary meaning

because the meaning of this term to a person having ordinary skill in the art at the time of the invention is apparent to a lay person upon review of the '704 patent. When construing this very claim term in a prior litigation one court already found that “the ordinary and customary meaning of the claim term ‘network protocol address,’ as understood by a person of skill in the art when read in the context of the entire patent, is readily apparent even to a lay person.” (Ex. 1009 at 17.)

F. “is” and “status” ”

37. I agree with Dr. Houh that in the '704 Patent the inventors did not act as a lexicographer and did not provide a special meaning for any of the claim terms. (Ex. 2022 at 188:24 – 189:15.) Nothing in the claims, specification or prosecution history suggests that the inventors intended to redefine the claim term “is” or the claim term “status.” A person of ordinary skill in the art, in view of the specification, would have understood “is” to mean “the present tense of “be” and “Status” to mean “the current state.” (Ex. 2013 at 8:41-50.)

VIII. Microsoft Manual

38. WINS provides a computer name-to-IP address mapping database. “WINS servers maintain a database that maps computer names to IP addresses.” (Ex. 1012 at 122.) Microsoft Manual explains that the “Windows Internet Name

service (WINS) [is] for dynamically registering and querying computer names on an internetwork” and is a “name resolution service for easy, centralized management of computer name-to-IP address resolution in medium and large internetworks.” (*Id.* at 4.) WINS is implemented using the Transmission Control Protocol/Internet Protocol (TCP/IP) networking protocol and the Microsoft Manual reference “describes how to install, configure, and troubleshoot Microsoft TCP/IP on a computer running the Microsoft Windows NT Workstation or Windows NT Server operating system.” (*Id.* at 3.) Though TCP/IP uses IP addresses to identify and communicate with computers, users typically find it easier to remember specific names assigned to computers (for instance, “Bob’s Computer” is easier to remember than “11.101.10.1”). (*See id.* at 34 (“Although TCP/IP uses IP addresses to identify and reach computers, user typically prefer to use computer names,” because they are easier to remember).) To accommodate this preference, WINS provides a database for keeping track of name-to-IP address mappings. (*See* 1012 at 34.)

39. Microsoft Manual describes the purpose of WINS as the registration and resolution of computer (also known as a “node”) names:

- “Registration is the process used to acquire a unique name for each node (computer system) on the network.” (Ex. 1012 at 62.)
- “Resolution is the process used to determine the specific address for a computer name.” (*Id.*)
- “Name registration ensures that the computer’s name and IP address are unique for each device... A WINS server accepts or rejects a computer name registration depending on the current contents of its database.” (*Id. at 68.*)

40. It does not provide a mechanism for determining whether a computer is on-line and available for communication much less a mechanism for determining whether an individual program on a computer is connected to the network and available for communication.

41. The Microsoft Manual describes WINS as providing “a distributed database for registering and querying dynamic computer name-to-IP address mapping in a routed network environment.” (Ex. 1012 at 65.) “WINS consists of two components: the WINS server, which handles name queries and registrations, and the client software, which queries for computer name resolution.” (*Id.*)

42. Computer name registration concerns transmitting to the WINS server a name-to-IP address mapping of a client computer. (Ex. 1012 at 68.) Microsoft

Manual explains that a “name registration request is sent directly to the WINS server to be added to the database.” (*Id.*) The WINS server will either accept or reject this registration request. (*Id.*) If there is no record of the name in the WINS server database, the WINS server accepts the request and adds the name-to-IP address mapping to its database. (*Id.*) If the WINS server database contains a different address for the name requested, it challenges the current entry to determine if the device already registered under that name still claims the name. (*Id.*) If that device is still using that name, the new name registration request is rejected. (*Id.*)

43. When a computer seeks the name-to-IP address mapping for a second computer with which it seeks to communicate, it first sends a name request query to the WINS server, seeking the IP address of the second computer. (Ex. 1012 at 67.) If there is a record of the queried computer name in the WINS database, the associated IP address is returned and the first computer can use the IP address to initiate communication with the second computer. (*Id.*)

44. The Microsoft Manual reference further explains that when a WINS client is no longer using a particular computer name, such as when the Windows NT Workstation or Windows NT Server service is stopped,² the computer will

² The Windows NT Workstation and Windows NT Server services are distinct from each other. (*See* Ex. 1012 at 3, 65.)

send a release message to the WINS server. A registered name is released if a WINS enabled computer is shut down properly. (Ex. 1012 at 69.) The Microsoft Manual further explains that “[i]f a name is marked released at a WINS server and a new registration arrives using that name but a different address, the WINS server can immediately give that name to the requesting client because it knows that the old client is no longer using that name.” (*Id.*)

45. Once a name-to-IP address mapping in the WINS database is released, it remains released for a certain period of time until the WINS server marks it as extinct. (Ex. 1012 at 69.) “Extinct entries remain in the database for a designated period of time to enable the change to be propagated to all WINS servers.” (*Id.*) Also, a network may rely on multiple WINS servers. Where this is the case, released computer names are not propagated to all WINS servers until after they become extinct. (*Id.* at 134.) A WINS client does not have access to the WINS server database showing that a name has been released, but is not yet extinct. Even when a name is released, it still stays registered in the database for minimum of 24 hours and a maximum of over two months. Before a released entry is removed from the database it must be marked as extinct (minimum 40h, maximum 999 hours), and timed out (min 24 hours, maximum 999 hours). (*See* Ex. 2017 at 2.)

46. Because computers occasionally disconnect from the computer network without properly shutting down, the release process for the WINS server is not perfect. WINS therefore requires computers to periodically “renew” or re-register their name within an allotted period of time. (Ex. 1012 at 69.) The Microsoft Manual describes name renewal as “a timed reregistration of a computer’s name with the WINS server.” (Ex. 1012 at 69.) After registration of a name, the WINS server sets a renewal interval within which the client must re-register, otherwise the WINS server will mark the name as released.

47. While WINS requires computers to periodically renew or reregister their names, the default renewal period is 5 hours. The minimum renewal period is 40 minutes. (Ex. 1012 at 131; *see also* Ex. 2017.) Thus, the renewal function is a far from perfect mechanism for keeping name-to-address mapping in the WINS server database up to date. Thus, a person of ordinary skill in the art at the time of the invention would have understood that the WINS system was not designed to support real-time applications such as the one described in the patent in suit.

48. Additionally, where there are multiple WINS servers connected to the network, information received at a first server must be propagated to the other WINS servers on the network. For instance, if a WINS client sends a release message to one of the WINS servers, this information is then sent from the first

server receiving the release message to the other WINS servers on the network, so that all servers hold the same registration information. This process is known as replication. The minimum replication interval, the frequency with which a WINS server can replicate itself to other WINS servers on a network, is 40 minutes. (Ex. 1012 at 148.) It was common in 1995 for system administrators to use default settings when configuring servers.

49. WINS does not hold “registration” information in the database when a given computer logs off the system. (*See* Ex. 1012 at 69 (“When a computer finishes with a particular name...it no longer challenges other registration requests for that name. This is referred to releasing a name.... Whenever a computer is shut down properly, it releases its name to the WINS server, which marks the related database entry as released. If the entry remains released for a certain period of time, the WINS server marks it as extinct, and the version number is updated so that the database changed will be propagated among the WINS servers.”).)

50. Compare the above WINS protocol with the ’704 patent which teaches that, once registered, a name of a user will remain in the database, regardless of whether the user is actually on-line – the name does not get released, like in WINS. The claimed query determines whether the named user is actually on-line at the time of the query. (*See* Ex. 2013 at 5:24-6:5 (“Upon the first user

initiating the point-to-point Internet protocol when the first user is logged on to Internet 24, the first processing unit 12 automatically transmits its associated E-mail address and its dynamically allocated IP address to the connection server...The first processing unit 12 then sends a query, including the E-mail address of the callee, to the connection server 26. The connection server 26 then searches the database 34 to determine whether the callee is logged-in by finding any stored information corresponding to the callee's E-mail address indicating that the callee is active and on-line....if the callee is not on-line when the connection server 26 determines the callee's status, the connection server 26 sends an OFF-LINE signal or message to the first processing unit 12.”.)

51. Unlike the claimed invention, the query in WINS is only a name query, it is no guarantee that the queried computer is running. (*See* Ex. 1012 at 68 (“Any name-to-IP address mapping registered with a WINS server can be provided reliably as a response to a name query. However, a mapping in the database does not ensure that the related device is currently running, only that a computer claimed the particular IP address and it is a currently valid mapping.”).)

52. Further, it would not have been uncommon at the time of invention for a computer to disconnect from the computer network without properly shutting down. For instance, it was a common occurrence to have a computer freeze and

need to be manually restarted. In this scenario the computer would not have been shut down properly and thus would not have sent a release message to the WINS server signifying that its name was no longer in use. It also would have been common for laptop users to remove the Ethernet connection and close their laptop. In this case also, the computer would not have sent a release message to the WINS server. In this case, a user's computer could be completely disconnected from the computer network but still retain a name-to-IP address mapping.

IX. NetBIOS

53. The NetBIOS reference, describes a theoretical name server service which is implemented in a Windows NT computer through WINS. (*See* Ex.1012 at 4, 11-12 (“WINS is a NetBIOS over TCP/IP mode of operation defined in RFC 1001/1002 as p-node”); at 65 (“WINS consists of two components: the WINS server, which handles name queries and registering, and the client software, which queries for computer name resolution”); at 66-67; Ex. 1003 at 384-85; *see also Sipnet EU S.R.O v. Straight Path IP Group, Inc.*, IPR2013-00246, Paper No. 62 Final Written Decision at 22 (“WINS, an implementation of NetBIOS”); Ex. 1012 at 34 (“Microsoft Windows networking provides dynamic name resolution for NetBIOS computer names via WINS servers and NetBIOS over TCP/IP”); at 72 (“The LMHOSTS file is a local text file that maps IP addresses to NetBIOS

computer names for Windows-networking computers that you will communicate with outside of the local subnet.”.)

54. The NetBIOS reference explains the NetBIOS name service, which is implemented in WINS. “NetBIOS name service is a collection of procedures through which nodes acquire, defend, and locate the holders of NetBIOS names.” (Ex. 1014 at 395.) In the context of the NetBIOS reference, the terms “node” or “NetBIOS name server node” refer to a computer engaging in computer name registration using the NetBIOS name server. (*See id.* at 384.) The NetBIOS name server, like the WINS server described above, discloses a name server for registering a name associated with a computer, not a name associated with a specific process running on that computer. (*Id.* at 395-98.)

55. NetBIOS discloses a protocol for computer name registration; it does not disclose the ability to register a specific program or application running on a computer with the NetBIOS name server. Further, the 16 byte NetBIOS name does not identify a program or application on a computer registered with the NetBIOS name server. Rather, it simply identifies an address for a computer through mapping a computer name to its related IP address. In the NetBIOS reference, the terms “computer,” “host,” and “station,” are all synonyms for “computer.”

56. The distinction between registration of a computer name and registration of an individual computer program can be shown using an example Dr. Houh used in his declaration in this matter. In his declaration, Dr. Houh explained that the Domain Name System (DNS) translates IP addresses into domain names. (Ex. 1004 at ¶ 38.) Dr. Houh explained that, using DNS, a domain name, such as ftp.symbolics.com could be mapped to an IP address, such as 100.100.200.20, thus implying that an IP address can be mapped to a specific service. Instead, using DNS, a host name is mapped to an IP address. Any number of host names can be mapped to the same IP address. Regardless of what a host name seems to infer regarding a service like “ftp” all that is returned by DNS is a single IP address. DNS has no knowledge what services are running or are not running on a host.

57. In the NetBIOS name service, like in WINS, a computer, or NetBIOS node, may register its computer name and associated IP address. (*See* Ex. 1014 at 395-96.) A user of the NetBIOS name service may use the NetBIOS service to discover an IP address associated with a computer name through a query for the name sent to the NetBIOS name server (“NBNS”). If the name is registered in the NBNS, the NBNS will return to the first user the IP address associated with the NetBIOS name queried. (*Id.* at 396.)

58. Also like WINS, in which the teachings of NetBIOS are implemented, NetBIOS names may be released from the NBNS explicitly or silently through timeout/ expiration. (Ex. 1014 at 396.) Upon explicit release, P nodes, which are NetBIOS nodes that engage in point-to-point communication using directed UDP datagrams and TCP sessions send a notification to the NBNS indicating that they are no longer using the computer name that was previously registered. (*Id.* at 385, 396.) But, upon a silent name release, which can occur when a node is turned-off, the NBNS will not be updated. (*Id.* at 396-97.) Thus, like WINS, the NBNS cannot always consistently tell if a name-to-IP address mapping in its database is current. A NetBIOS node is also unable to access the NBNS database showing whether the status of a name is “released.”

59. Because the name-to-IP address mapping in the NBNS is imperfect, like WINS, the NBNS requires nodes to periodically renew or “refresh” their names in the NBNS. (Ex. 1014 at 397-98; 413-14.) “Names held by an NBNS are given a lifetime during name registration. The NBNS will consider a name to have been silently released if the end-node fails to send a name refresh message to the NBNS before the lifetime expires.” (*Id.* at 397.) An end-node can request a specific lifetime value during registration or can propose an infinite lifetime. (*Id.*)

60. Terminal Emulation Protocol (Telnet) is a protocol allowing a user to connect to remote systems. (Ex. 1012 at 4, 10.) Telnet “allow[s] Windows NT users to interact with and use resources on non-Microsoft hosts, such as UNIX workstations.” (*See id.* at 11.) The “telnet” command “starts terminal emulation with a remote systems running a Telnet service... To provide terminal emulation from a Windows NT computer, the foreign host must be configured with the TCP/IP program, the Telnet server program or daemon, and a user account for the Windows NT computer.” (*Id.* at 249.) The Telnet server daemon is not included with Windows NT. (*Id.*)

61. To initiate a connection using the Telnet function, a user must type the host name “of the remote system [it] want[s] to connect [with]” into the “connect dialog box” and then “choose the Connect button.” (Ex. 1012 at 249.) When using the Telnet function, the “remote system” described in the Microsoft Manual reference is the computer (i.e., a machine) with which communication is sought. (Ex. 1012 at 249.) Telnet runs separate and apart from NetBIOS, and does not transmit any type of “release” message when it is shut down. In other words, if you shut down Telnet (even in the manner intended by the application) Telnet is not able to tell the WINS server or NBNS that it is no longer on-line.

X. PALMER

62. U.S. Patent No. 5,375,068, by Palmer et al. (Ex. 1020, hereinafter “Palmer”) describes n-way video teleconferencing among networked computer workstations using an existing variable bandwidth digital data network for transferring synchronized audio and video teleconferencing data between the workstations. (Ex. 1020 at 1:41-45.)

63. Palmer was filed on June 3, 1992, and discloses that workstation should be compatible of running in the Microsoft WindowsTM or Windows NTTM graphical operating systems environments. (Ex. 1020 at [22] and 7:9-11.) A person of ordinary skill in the art at the time would not have understood the reference to Windows NT to mean Windows NT Server. 3.5. They would have understood this reference to be to Windows NT Workstation, a separate and distinct operating system from Windows NT Server.

64. At around the time Palmer’s application was filed, a beta version of Windows NT 3.1 (“Windows NT Workstation”) was made available, and was commercially released on July 27, 1993. (*See* Ex. 2020 Strehlo, Kevin (1992-07-13). "Microsoft makes its move with Windows NT SDK". InfoWorld 14 (28): 1, 92; and, <http://windows.microsoft.com/en-us/windows/history#T1=era3>.) A person of ordinary skill in the art at the time of the invention would not have been

motivated to combined Palmer, which expressly states it is for “workstations” with a server.

65. The Microsoft Manual reference is a manual associated with Windows NT 3.5 Server (“Windows NT Server”) and was released on September 21, 1994. (*See* Ex. 2019.)

http://www.oldcomputermuseum.com/os/windows_nt3.5.html.) The Workstation NT Workstation is a separate and distinct software product from the Windows NT Server. (Ex. 2022 at 32:10-33:3; *see also* Ex. 2022 at 17:2-18, (acknowledging that Windows NT Workstation is different product from Windows NT Server).)

66. A person of skill in the art would have understood Palmer’s Windows NT reference to be to Windows NT Workstation; not to Windows NT Server since it did not exist at the time. The Microsoft Manual, NetBIOS, and Palmer combination teaches away from the ’704 patent. While Palmer states that it can be used with Windows NT, a person of ordinary skill in the art at the time would have understood this to mean Windows NT Workstation, not Windows NT Server. 3.5.

67. Windows NT Workstation is not before the Board and is not included in the grounds of institution for the present inter partes review. Because Palmer does not refer to Windows NT Server, it cannot be said to provide a motivation to

combine Palmer with the Microsoft Manual. Samsung has not provided a motivation to combine Palmer with Microsoft Manual and NetBIOS.

I understand and have been warned that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001). 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 § 1001 of title 18 of the United States Code.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on **June 8, 2015** in **Miami, FL**.



Stuart Stubblebine, Ph.D.

EXHIBIT 1

**Stubblebine Consulting, Inc.
Consultant Curriculum Vitae**

Stuart G. Stubblebine, Ph.D.

Expertise

- Computer and Network Systems
 - Distributed systems and applications of distributed computing
 - Internet Protocols
 - Security and Cryptographic Evaluation & Design
 - Network Security Protocols
 - Firewalls, VPNs
 - Authentication, Authorization, and Audit
 - Conditional Access, Content Protection, Piracy Countermeasures, Digital Rights Management
 - Best Security Practices
 - Electronic Payment and Credit Card Processing
 - Privacy Technology, Anonymity Techniques, and HIPAA
 - Identity Theft
 - Secure Software Engineering
 - Public Key Management
 - Specialized Protocols and Systems
 - Smart Card Technology
 - Cryptographic Protocols
 - Encryption, Authentication Codes, Digital Signatures
-
-

Employment History

From: Various Stubblebine Consulting (since March, 2000)
To: Present
Position: Consultant

Independent consultant specializing in computer and network security evaluations, detailed design and formal analysis, applied research, technical due diligence reviews, intellectual property, and expert witness services. Clients range from individuals and domestic startups to international Fortune 100 companies. Consulting services have included topic areas listed in the expertise section above.

A list of past clients include: AgileTCP Inc., Alcatel-Lucent, American Express, AMD, Austin Capital Group, Authentidate, British Telecom, Celis Semiconductor, Dickstein Shapiro LLP, DoCoMo USA, Encirq, Gemplus, Global Crypto Systems, ILS Technology, Imagineer Software, Acatel-Lucent, Microsoft, New York City Police Department, New York City Department of Education, Oceana Sensor Technologies, Privada, EMC/RSA, Summit Accelerator Fund, SRD Software / IBM, TantaComm Systems, Wave Systems Corp, Zix Corporation, Zobi Mobile. See also clients in the

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

litigation section.

Also, Dr. Stubblebine is affiliated with Stubblebine Research Labs, LLC since Oct, 2001 as a research scientist. Previously he conducted basic research under the sponsorship of the National Science Foundation. His projects focus on security and privacy technology. There has been no ongoing activity with this affiliation for many years.

From: 07/ 2002 University of California – Davis
To: 06/ 2004

Position: Professional Researcher, (Full Professor Level)

Affiliated with the computer science department regarding research in the area of security, cryptography, and secure software engineering.

From: 1998 CertCo, Inc
To: 07/ 2001

Position: Vice President & Cryptographer

Research, design, and analysis of public key infrastructure protocols and related risk management services. Advised engineering on product/service design and advance technology. Technology includes Public key cryptography, smart cards, authentication and authorization protocols.

From: 1996 AT&T Labs –Research (formerly Bell Labs)
To: 1998

Position: Principal Member of Technical Staff

Basic research in computer and network security technology.

On the business front, consulted extensively with product managers and their developers on electronic commerce and public key infrastructure issues. Spearheaded efforts to establish trusted-third party revocation services. Participated in countless security designs and reviews including digital rights management associated with AT&T's a2b music. Participated in many business-consulting activities. Some larger projects include a) Secure Internet Telephony: analysis and design of provisioning phone service using set top boxes (i.e., protecting against service fraud, providing authenticity, authorization, numerous privacy issues, etc.), and b) Internet Security: establishing the security components for the next generation IP network architecture (joint project with British Telecom).

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

On more of the research front (but largely integral to the business needs), worked on a scalable design and system for trusted third-party revocation services. The theory and system enables countless numbers of clients to subscribe to freshness evidence concerning the validity of credentials (e.g., the validity of identity and attributed certificates). Also, worked on “Delaying Functions” which are functions that take a provably long time to compute and preserve randomness on the inputs. Delaying functions are important since they can minimize the need to trust a third party (e.g., we eliminate trust in a lottery agent to pick a random number to determine a lottery winner). Worked on methods to check the validity of information returned from a stack and queue stored on a hostile environment. Our method improves on the efficiency over other known methods. Worked on protocols for Unlinkable Serial Transactions. These protocols prevent a networked service from tracking the behavior of its customers on a per transaction basis. Previously, granularity of protection was at the level of protecting the identity of customers (e.g., using pseudonyms). Show the service vendor can be protected from abuse due to simultaneous or “cloned” usage from a single subscription (e.g., password sharing). Worked on methods to check properties of code without requiring software vendors to releasing code to trusted third parties. The approach assumes content providers are provided with physically secure computing devices. Also, worked on techniques for using trusted software certification authorities to secure software-module configuration management. Worked on techniques for automatically detecting known and chosen plaintext pairs in cryptographic protocols. Discovered new (but related) attacks on IPSEC protocols.

From: 07/1994 AT&T Bell Labs
To: 1996 Murray Hill, N.J
Position: Member Technical Staff

Basic research in computer security technology.

On the business front, provided technical and strategic guidance particularly to AT&T Worldnet. Consulting in the areas of electronic commerce services, and key management infrastructure. Senior technology consultant to various business units in various areas of Internet protocols, security, and electronic commerce. This included design and analysis of new internet-based credit card processing technology involving the consumer, merchant, and credit card processor. Other work included design and analysis of protocols for electronic document notarization and archiving services.

Research related activities included developing a theory and system for authenticating trust assertions in large-scale systems based on independence of trusted paths established through trusted intermediaries. Formalize the problems of locating maximum sets of paths using

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

independence properties in a graph-theoretic framework, gave evidence that they are not polynomial-time solvable, and proposed approximation algorithms for these problems. Introduced PathServer, a service for finding sets of such paths to support authentication in PGP-based applications. Worked on acceptable metrics for authentication. This work gives a set of guiding principles for the design of authentication metrics, illustrates our principles by demonstrating the limitations of previous approaches, and defines a new metric. The new metric establishes the amount for which a transaction may be insured. It is computed as the min-cut of a trust graph where the labels of the graph represent insurance amounts. Worked on an analysis method to reason about synchronization, recency, and revocation in distributed systems. The approach helps designers learn hidden assumptions necessary to establish recent-secure authentication. Recent-secure authentication requires that all assumptions necessary for the transaction satisfy designated freshness policies. Worked on public-key methods for establishing trusted third-party revocation services. The technique adds recentness verification policies to identification/ authorization/ delegation/ policy certificates. By adjusting freshness constraints, the delay for certain revocation can be arbitrarily bounded. Using this technique, design a general architecture for a secure and highly available trusted-third party revocation service. This service enables a trusted-third party to be a revocation authority (e.g., authority for issuing revocation statements) while the customer retains authority on issuing its own identification/ authorization/ delegation certificates. The practical significance of this theory is that the customer can delegate revocation authority (i.e., the difficult task of making revocation lists highly available and fresh) to a less trusted principal. Gave a general method for formally specifying and reasoning about revocation in distributed systems with any desired degree of immediacy for revoking authentication.

From: 07/1994 Computer Science Department, University of Southern California
To: 12/1998
Position: Adjunct Faculty
Advised graduate students. Was a principal investigator for National Security Agency University Research Program contract on Traffic Flow Confidentiality.

From: 08/1992 Computer Science Department, University of Southern California
To: 07/1994
Position: Research Assistant Professor, Computer Science Department, and Computer Scientist, Information Sciences Institute (joint appointment)

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Advised computer science and computer engineering students on academic programs, on directed research classes, and on Ph.D. dissertation research in the areas of security, networking, distributed systems, and software engineering. Taught and was active in service to the department. Developed (and taught) the course curriculum for Software Analysis and Formal Methods for a new M.S. program in Software Engineering.

Develop research programs in security, networking, distributed systems, real-time systems, and software engineering. Researched the use of interconnection networks for minimizing the delay and bandwidth for protecting traffic flow confidentiality. Designed a formal methodology for design configuration/formal specification and specification analysis/verification of protocols for secure networking and distributed systems. Participated in the research and design of all layers of ISI's multimedia teleconferencing architecture. Helped design Internet's Real-Time Transport Protocol. Research proposal on the availability of integrated network services, and distributed systems selected for funding. Designed directory service infrastructure support for distributed systems. Active in the development of both Internet engineering standards, IEEE, and NIST standards. Reviewed papers for SIGCOMM, IEEE Transactions on Software Engineering, and others.

From: 01/1991 IBM Federal Systems Division

To: 08/1992

Position: Computer Scientist (Consultant – External to IBM)

Conducted Internal Research and Development (IRAD) in the areas of distributed computing systems and networking architecture for secure systems. Discovered weaknesses in existing analysis methods for protocols for distributed processing, developed a theory and method for protocol analysis. Applied the method and thus exposed significant vulnerabilities in Open Software Foundation's (OSF's) Distributed Computing Environment (DCE), Internet's Privacy Enhanced Electronic Mail, and Kerberos Network Authentication Service. Used the theory to recommend secure message structures and protocols which have since been adopted

From: 08/1990 University of Maryland

To: 05/1991

Position: Teaching Assistant

Taught two semesters of digital computer laboratory for undergraduate seniors in computer engineering.

From: 01/1989 Commcrypt

To: 01/1990

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Position: Director of Secure Systems Engineering
Directed R&D in the design of network and file server architectures, automated key management, secure electronic mail, piracy countermeasures, single chip computer (smart card) based systems for trusted applications and associated distributed computing applications. Participated in establishing national standards for programming (NIST).

From: 01/1988 University of Arizona

To: 12/1988

Position: Research Assistant

Designed a video, telecommunication, and distributed computer system architecture for conferencing. Created performance models for the distributed processing elements and communication channels, and optimized the communication protocols and network design using simulation.

From: 07/1986 US Army

To: 06/1987 Location

Position: Director of Information Management

Created a staff organization from scratch that was responsible for the design and engineering of all Army telecommunications and automation projects for the United Kingdom and Southwest Germany. Supervised an engineering staff of eight. Awarded medal for best organization of its type.

From: 08/1985 City Colleges of Chicago

To: 05/1987

Position: Instructor

Taught various undergraduate computer science courses including: System Analysis and Design, Programming Logic, and Programming Languages.

From: 01/1985 US Army

To: 07/1986

Position: Communications Engineer

Directed the restorations of low and high frequency radio, microwave, satellite and cable transmission circuits, including the associated cryptographic, conditioning, and end equipment. Responsible for all communications systems from the Headquarters European Command (EUCOM) to the Joint Chiefs of Staff and all theater nuclear communication to subordinate units. Developed policies for high-speed intelligence computer circuits which reduced outage times by 75%. Promoted and placed into above position.

From: 01/1984 US Army

Stubblebine Consulting, Inc.
Consultant Curriculum Vitae

To: 01/1985
Position: Manager
Managed 56 persons in a multi-functional automated telecommunications facility. Discovered, documented, and proved system deficiencies in a major Army automated message processing project. Awarded medal for accomplishments.

Litigation Support Experience

From: 2015

To: Current Dr. Stubblebine provided expert services for RSA Security in an arbitration matter brought by Capital One, N. A. Details of the involvement are confidential.

To: Current Dr. Stubblebine provided expert services for T-Mobile regarding patent in a patent infringement cases brought by Prism Technologies in the area of controlling access to protected computer resources. He provided an expert report on invalidity.

From: 2013

To: Current Dr. Stubblebine provided expert services for Straight Path in ITC against Sony et. al, and EDT/EVA cases brought against Blackberry et al. in the area of establishing a point to point communications links over a network. He provided expert reports on infringement and validity and was deposed. The ITC case has completed. The EDT/EVA cases have been stayed.

From: 2013

To: 2014 Dr. Stubblebine provided expert services for Symantec in a case brought by Dig Reg of Texas in the area of access control and software activation. He provided an expert report on non-infringement and was deposed.

From: 2013

To: 2013 Dr. Stubblebine provided expert services for Newegg, BB&T, Expedia/Hotwire, and Orbitz in a case brought by TQP Development in the area of SSL, key management, TLS, SSL offloading, RC4 cipher, symmetric ciphers, and web servers. He provided an expert report on non-infringement and testified at trial.

From: 2013

To: 2014 Dr. Stubblebine provided expert services for PNC, Vanguard, Groupon, and numerous other defendants (MDL No. 2354) in a case

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

brought by Maxim Integrated Products in the area of secure transactions including hardware circuits/systems and methods for performing digital signatures to authorize monetary transactions. He provided a declaration on claim construction and was deposed.

From: 2013
To: 2015

Dr. Stubblebine provided expert services for Monec in a case brought against Motorola Mobility LLC, et al regarding a patent infringement in the area of electronic books. He provided an declaration concerning claim construction. He has provided expert reports on infringement and validity and was deposed.

From: 2013
To: 2013

Dr. Stubblebine provided expert services for Electronic Arts, Symantec, Solarwinds in a case brought by Achates Reference Publishing regarding a patent infringement in the area of technology for software installation, licensing, and activation. He provided an expert report on non-infringement on behalf of Symantec and was deposed. The case has settled.

From: 2012
To: 2014

Dr. Stubblebine provided expert services for Juniper against Palo Alto Networks regarding patent infringement in the area of packet processing, firewall technology, and packet processing in a multiple processor system. He provided an expert report on validity on behalf of Juniper and was deposed.

From: 2011
To: 2013

Dr. Stubblebine provides expert services for Avaya, Siemens, and Mitel in a case brought by Virnetx regarding VoIP signaling protocols focusing on SIP-enabled IP telephony and security. He provided an expert report on invalidity and was deposed. The case has settled.

From: 2011
To: 2012

Dr. Stubblebine provides expert services for Internet Brands in a case brought by Versata Software regarding a patent infringement and trade secrets regarding software for automatic configuration and comparison. He provided multiple expert reports, deposed, and testified at trial. Favorable verdict for client on all aspects of case including non-infringement, invalidity, and theft of trade secrets. Also, provided a declaration on behalf of Internet Brands in a related matter against Versata in 2013 regarding civil action 12-CV-704-JRG.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

- Form: 2010
To: 2013 Dr. Stubblebine provides expert services for Docomo/Nomadix against AT&T, HP, et al. regarding a patent infringement in the area of mobile computer networking and Internet technologies including TCP/IP, DHCP, HTTP, MAC, NAT, ARP, Ethernet, Login Portals, AAA, RADIUS, and access control. He provided a multiple expert reports and was deposed. The case has settled for all defendants except for IBAHN which filed for bankruptcy.
- From: 2011
To: 2011 Dr. Stubblebine provided expert services for Microsoft in a trade secret case with Datel regarding reverse engineering and trade secrets with respect to authentication and key exchange protocols within the Xbox 360. He provided an expert report and was deposed. The case settled.
- From: 2011
To: Current Dr. Stubblebine provided expert services for Microsoft in a patent infringement case brought by Motorola (now Google) in the areas of email (e.g., Microsoft Exchange) and instant messaging. He provided multiple expert reports and was deposed. The case has changed venue, and was stayed.
- From: 2011
To: 2011 Dr. Stubblebine provided expert services for Nokia in a patent infringement case against Apple in the areas of 3G, encryption and integrity protection, and authentication of cell handoff protocols. He provided a declaration. No deposition or expert reports provided. The case settled.
- From: 2010
To: 2011 Dr. Stubblebine provides expert services for PMC in a patent infringement case against Motorola, and Echostar/Dishnetwork in the areas of communication systems, security and encryption for secure video distribution, conditional access, anti-piracy, and digital rights management. He provided multiple declarations and was deposed.
- From: 2009
To: 2012 Dr. Stubblebine provided expert services for TecSec a patent infringement case against IBM, in the areas of encrypted objects and XML encryption related to web application server and database products. He provided expert reports on infringement and validity and was deposed.
- From: 2010
To: 2010 Dr. Stubblebine provided expert services for Digital-Vending Services International, LLC regarding a patent infringement case against The University of Phoenix, Inc et al., in the area of

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

preventing unauthorized use of courseware and other content related to access to online courses. He provided multiple declarations, depositions, expert reports, and gave a tutorial at a claims construction hearing.

From: 2009
To: 2010

Dr. Stubblebine provided expert services for Research In Motion Corp. regarding patent infringement cases brought by Prism Technologies in the area of controlling access to protected computer resources in a network related to access to BlackBerry Enterprise Server. He provided a declaration.

From: 2009
To: 2009

Dr. Stubblebine provided expert services for Microsoft regarding a patent infringement case brought by Digital Reg of Texas, in the area of digital rights management for digital content related to Windows DRM. He provided multiple expert reports and was deposed regarding invalidity and non-infringement. The case settled.

From: 2009
To: 2010

Dr. Stubblebine provided expert services for Monec against Apple regarding a patent infringement case in the area of electronic books. He provided an affidavit and declaration. No deposition or expert reports provided.

From: 2008
To: 2009

Dr. Stubblebine provided expert services for Docomo/Nomadix against Second Rule regarding a patent infringement case in the area of mobile computer networking and Internet protocols and technologies including NAT, VLANs, ARP, Ethernet, DNS, DHCP, authentication and authorization. He provided multiple expert reports regarding infringement. My client won a permanent injunction and an award for damages.

From: 2007
To: 2008

Dr. Stubblebine provided expert services for Microsoft regarding a patent infringement case with Alcatel – Lucent in the area of network security, 802.1x port based authentication, VLANs, Radius, MS IAS (Internet Authentication Service), MS Active Directory, wireless security, and user authentication. He provided multiple expert reports on non-infringement and invalidity and was deposed by the plaintiff Alcatel. The case settled.

From: 2007
To: 2008

Dr. Stubblebine provided expert services for DeepNines regarding a patent infringement case with McAfee in the area of network based intrusion detection systems (IDS) for various networking protocols (IP, TCP, UDP, SNMP, SMB, etc.), firewalls, and network based security. He gave multiple expert reports, multiple depositions,

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

answered technical questions of the judge at the claims construction hearing, and testified at trial resulting in a favorable verdict for my client on all issues.

From: 2006
To: 2006

Dr. Stubblebine provided expert services for a patent infringement case in the area of digital time-stamping services for Authentidate on a case brought by TimeCertain. He gave a tutorial on digital time-stamping at a Markman hearing and responded to questions from the judge. No deposition or expert reports provided.

From: 2006
To: 2007

Dr. Stubblebine provided expert witness services in the area of Secure Socket Layer protocol (SSL) and public key certificates for class action certification regarding SETMA v. Verisign. SETMA alleged that VeriSign overstated the security differences between its Secure Site and Secure Site Pro certificate He provided an expert report that assisted in gaining class action certification for the case. The case has since settled for approximately \$40 million.

From: 2005
To: 2006

Dr. Stubblebine provided expert witness services for a patent infringement case in the area of security certification and accreditation for Telos Corporation on a case brought by SecureInfo. He provided an expert report.

From: 2004
To: 2005

Dr. Stubblebine provided expert witness services for SurfControl regarding website filtering products in a case between Grendysa and Evesham Township Board of Education. He provided an expert report.

From: 2003
To: 2011

Dr. Stubblebine testified at a claims construction hearing concerning patent infringement litigation relating to security and encryption for secure video distribution, conditional access, anti-piracy, and digital rights management for Personalized Media Corporation against Scientific Atlanta. He wrote multiple expert reports and was deposed.

From: 2003
To: 2008

Dr. Stubblebine provided expert services concerning patent infringement litigation concerning secure transaction-processing technology for First Data Corporation on a case brought by DataTreasury. He provided a declaration.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Patents

<u>Patent Number</u>	<u>Date Issued</u>	<u>Title</u>
US07184988	02/27/2007	Methods for operating infrastructure and applications for cryptographically-supported services
US06405313	06/11/2002	Method for providing assurance in a key-binding system
US07644284; US06216231; US06256741	Various	Specifying security protocols and policy constraints in distributed systems
US06148401; US06381698	Various	System and method for providing assurance to a host that a piece of software possesses a particular property
US06108644	08/22/2000	System and method for electronic transactions
US06101603; US06249871	Various	System and method for using a second resource to store a data element from a first resource in a first-in last-out stack
US06098170; US06237094	Various	System and method for using a second resource to store a data element from a first resource in a first-in first-out queue
US06049872	04/11/2000	Method for authenticating a channel in large-scale distributed systems

The above does not include international patents.

Education

08/1992	University of Maryland, Electrical Engineering. Area: Computer Engineering. Dissertation: Message Integrity in Cryptographic Protocols. Advisor: Virgil Gligor	Ph.D. (E.E.)
12/1988	University of Arizona, Electrical Engineering. Area: Computer Engineering emphasis in Networking and Distributed Systems. Thesis: Analysis, Design, and Performance Evaluation of a Video and Computer Teleconference System for Distance Learning.	M.S. (E.E.)
05/1983	Vanderbilt University, Computer Science & Mathematics (double major).	B.S.

Other Education

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Teleprocessing Systems Course. Graduate level courses in computer networks, distributed processing, computer performance measurement and evaluation. US Army Signal Center. Honor Graduate, 10/83 - 01/84.

Radio Systems Design Course. Radio design, multichannel, microwave and troposcatter system engineering. US Army Signal Center. Honor Graduate, 07/83 - 10/83.

Signal Officer's Basic Course. Courses in military communication systems. US Army Signal Center, 05/83-07/83.

Publications

Temporarily Hidden Bit Commitment and Lottery Applications with D. Goldschlag and P. Syverson, *International Journal of Information Security*, Springer, Vol. 9, No. 1, February, 2010.

On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop, with P.C. van Oorschot, *ACM Transactions on Information and System Security*, vol.9 issue 3 (Aug. 2006), 235-258.

Reducing the dependence of SPKI/SDSI on PKI, with H. Wang, S. Jha, T. Reps, and S. Schwoon, Proceedings of 11th European Symposium on Research in Computer Security (ESORICS), September, 2006.

Secure Distributed Human Computation, with C. Gentry, and Zulfikar Ramzan, Fourteenth International Workshop on Security Protocols, Cambridge, England, Lecture Notes in Computer Science, Springer-Verlag, March 2006.

Secure Distributed Human Computation, with C. Gentry, and Zulfikar Ramzan, ACM Conference on Electronic Commerce, Montreal, Canada, June 2005.

Countering Identity Theft through Digital Uniqueness, Location Cross-Checking, and Funneling, with P.C. van Oorschot. *Financial Cryptography and Data Security 2005*, Springer Verlag LNCS 3570, February 2005.

Secure Distributed Human Computation (extended abstract), with Craig Gentry, and Zulfikar Ramzan. *Financial Cryptography 2005: 328-332*, LNCS 3570, Springer Verlag, 2005.

A Formal Privacy System and its Application to Location based Services. In 4th Workshop on Privacy Enhancing Technologies, with Carl A. Gunter, and Michael May, Springer-Verlag LNCS 3424, May 2004.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Michael Gertz, April Kwong, Charles U. Martel, Glen Nuckolls, Premkumar T. Devanbu, Stuart S. Stubblebine: Databases that tell the Truth: Authentic Data Publication. In Bulletin of the Technical Committee on Data Engineering, March 2004, Vol 7, No 1.

Addressing Online Dictionary Attacks with Login Histories and Humans-in-the-Loop. Financial Cryptography 2004, with Paul van Oorschot, Springer-Verlag LNCS 3110, February 2004.

A General Model for Authentic Data Publication, with Martel, C., Nuckolls, G., Devanbu, P., Gertz, M., and Kwong, A., *Algorithmica* (Springer), Volume 39, January 2004.

Flexible Authentication of XML Documents with Prem Devanbu, Michael Gertz, April Kwong, and Chip Martel. *Journal of Computer Security*, Vol. 12, No 6, 2004.

Protecting the Privacy of Observable Behavior in Distributed Recommender Systems, with Douglas W. Oard, Anton Leuski, ACM SIGIR Workshop on Implicit Methods, Toronto, Canada, 2003.

Certifying Data from Multiple Sources, 17th Annual IFIP WG 11.3 Working Conference on Database and Applications Security, with G. Nuckolls, and C. Martel, Aug. 2003.

Authentic Data Publication over the Internet, with Premkumar Devanbu, Michael Gertz, and Charles Martel. *Journal of Computer Security*, vol. 11, Issue 3, 2003.

On Generalized Authorization Problems with Somesh Jha, Tom Reps, and Stefan Schwoon. 16th IEEE Computer Security Foundations Workshop, June 2003.

An Authentication Logic Supporting Synchronization, Revocation, and Recency, with R. Wright, *IEEE Transactions on Software Engineering*, March 2002, (Vol. 28, No. 3).

Stack and Queue Integrity on Hostile Platforms, with P. Devanbu, *IEEE Transactions on Software Engineering*, January 2002 (Vol. 28, No.1).

Flexible authentication of XML documents with Prem Devanbu, Michael Gertz, April Kwong, Chip Martel, and Glen Nuckolls. Eighth ACM Conference on Computer and Communications Security, Philadelphia, PA, USA, November, 2001.

Secure Distributed Computing in a Commercial Environment, with Philippe Golle, Financial Cryptography 2001, LNCS Series, Springer-Verlag, February, 2001.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Authentic Third-party Data Publication, with Prem Devanbu, Michael Gertz, and Chip Martel, 14th IFIP 11.3 Working Conference in Database Security, Scoorl, The Netherlands, August, 2000, (Publisher: Kluwer).

Authentic Re-Publication by Untrusted Servers: A Novel Approach to Database Survivability, with Prem Devanbu, Michael Gertz, Chip Martel, and Philip Rogaway. In Third Information Survivability Workshop (ISW-2000), 2000.

The Next Revolution: Free, Full, Open Person-2-Person (P2P) E-commerce, with Prem Devanbu, and Michael Uschold. TWIST 2000 Conference, July 2000.

Engineering Secure Software Systems: Issues and Challenges, with P. Devanbu, invited paper, International Conference on Software Engineering, ICSE 2000, June, 2000.

Formal Characterization and Automated Analysis of Known-Pair and Chosen-Text Attacks, with C. Meadows, In IEEE Journal on Selected Areas in Communications, Special issue on Network Security, Vol. 18, No. 4, April, 2000.

Authentic Attributes with Fine-Grained Anonymity Protection, with P. Syverson, Financial Cryptography 2000, LNCS Series, Springer-Verlag, February, 2000.

Cryptographic Verification of Test Coverage Claims, with P. Devanbu, In *IEEE Transactions on Software Engineering*, February, 2000, vol. 26, no. 2.

Unlinkable Serial Transactions: Protocols and Applications, with P. Syverson, and D. Goldschlag., ACM Transactions on Information and System Security, Vol. 2, No. 4, Nov.1999.

Group Principals and the Formalization of Anonymity, with P. Syverson, World Congress on Formal Methods '99, Toulouse, France, LNCS Series, Springer-Verlag, September, 1999.

Security for Automated, Distributed Configuration Management, with P. Devanbu, and M. Gertz., Proceedings, ICSE 99 Workshop on Software Engineering over the Internet, 1999.

Authentication metric analysis and design, with M. Reiter, ACM Transactions on Information and System Security, Vol. 1, No. 3, May 1999.

Fair On-line Auctions Without Special Trusted Parties, with P. Syverson, Financial Cryptography 1999, LNCS Series, Springer-Verlag, February, 1999.

Stubblebine Consulting, Inc.
Consultant Curriculum Vitae

Resilient Authentication using Path Independence, with M. Reiter, *IEEE Transactions on Computers*, Vol. 47, No. 12, December 1998.

Stack and Queue Integrity on Hostile Platforms, with P. Devanbu, *IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, CA, May, 1998, pp. 198-206.

Techniques for trusted software engineering, with P. Devanbu, and P. Fong, *Proceedings of the 20th International Conference on Software Engineering*, Kyoto, Japan, April, 1998, pp. 126-135.

Publicly Verifiable Lotteries: Applications of Delaying Functions, with D. Goldschlag, *Financial Cryptography*, LNCS Series, Springer-Verlag, February, 1998.

Research directions for automated software verification: Using trusted hardware, with P. Devanbu, *12th IEEE International Conference on Automated Software Engineering - ASE'97*, IEEE Computer Society, Incline Village, Nevada, USA, Nov. 3-5, 1997, pp. 274-279.

On Searching for Known and Chosen Cipher Pairs Using the NRL Protocol Analyzer, with C. Meadows, *DIMACS Workshop on Design and Formal Verification of Security Protocols*, Sep., 1997.

Cryptographic verification of test coverage claims, with P. Devanbu, In *Proceedings, Fifth ACM/SIGSOFT Conference on Foundations of Software Engineering*, Zurich, Switzerland, Sept., 1997, pp.395-413.

Towards Acceptable Metrics of Authentication, with M. Reiter, *IEEE Computer Society Symposium on Security and Privacy*, Oakland, CA, May, 1997, pp. 10-20.

Unlinkable Serial Transactions, with P. Syverson and D. Goldschlag. *Financial Cryptography 1997*, (Lecture Notes in Computer Science Vol. 1318), Springer-Verlag, February, 1997, pp. 39-55.

Path Independence for Authentication in Large-Scale Systems, with M. Reiter, *Fourth ACM Conference on Computer and Communications Security*, Zurich, Switzerland, April, 1997, pp. 57-66.

Path Independence for Authentication in Large-Scale Systems, with M. Reiter, *AT&T Labs -- Research Technical Report, TR 96.8.1*, 1996.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

An Authentication Logic Supporting Synchronization, Recency, and Revocation, with R. Wright, Third ACM Conference on Computer and Communications Security, New Delhi, India, March, 1996, pp. 95-105.

An Authentication Logic Supporting Synchronization, Revocation, and Recency, with R. Wright, Technical Memorandum, AT&T Bell Laboratories, January, 1996.

Recent-Secure Authentication: Enforcing Revocation in Distributed Systems, IEEE Computer Society Symposium on Security and Privacy, Oakland, CA, May, 1995, pp. 224-234.

Reasoning About Message Integrity, with R. Kailar and V. Gligor, Proc. Fourth IFIP Working Conference on Dependable Computing for Critical Applications, San Diego, CA, January, 1994. Also, complete version in Tech Report Number 93-065, Electrical Engineering Department, University of Maryland, College Park, MD 20742

Security Services for Multimedia Conferencing, Proc. 16th National Computer Security Conference, Baltimore, MD, September, 1993, pp. 391-395.

Protocol Design for Integrity Protection, with V. Gligor, IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May, 1993, pp. 41-53.

A Note on the Use of Timestamps as Nonces, with B. Clifford Neuman, ACM Operating Systems Review, Vol. 27, No. (2), April 1993, pp.10-14.

Protecting the Integrity of Privacy-enhanced Electronic Mail with DES-based Authentication Codes, with V. Gligor, Proceedings PSRG Workshop on Network and Distributed System Security, San Diego, CA, February, 11-12, 1993, pp. 75-80.

Message Integrity in Cryptographic Protocols, Ph.D. Dissertation, University of Maryland, August 1992.

On Message Integrity in Cryptographic Protocols, with V. Gligor, IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May, 1992, pp. 85-104.

On Message Integrity in Cryptographic Protocols, with V. Gligor, Computer Science Technical Report #2843, University of Maryland, College Park, MD., February, 1992.

Virtue and Limitations of Logics for Cryptographic Protocols, with V. Gligor, R. Kailar, and L. Gong, IEEE Proc. of the Computer Security Foundations Workshop IV, June 1991, pp. 219-226.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Analysis, Design, and Performance Evaluation of a Video and Computer Teleconference System for Distance Learning, M.S. Thesis, Electrical and Computer Engineering Department, University of Arizona, December, 1988.

Professional Associations and Achievements

Professional Memberships: Association of Computing Machinery (ACM), and International Association for Cryptologic Research (IACR).

Associate Editor, ACM Transactions on Information and System Security¹, January 2000-April, 2007.

Invited Editor, Special issue on Software Engineering and Security for ACM Transactions on Software Engineering and Methodology, 2000.

Program Committee, International Workshop on Software Engineering for Secure Systems: 2008.

Program Committee, ACM Conference on Computer and Communications Security: 1996, 1997, 2002, and 2003.

Program Committee Formal Methods in Security Engineering (FMSE): 2003, 2004.

Program Committee for Financial Cryptography: 2001, 2006.

Program Committee for Software Engineering for Secure Systems: 2006

Program Committee for International Conference on Emerging Trends in Information and Communication Security: 2006.

Tutorial Chair, ACM Conference on Computer and Communications Security: 2000.

Session Chair, ACM Conference on Computer and Communications Security: 2000, 2003.

Program Committee for IEEE Computer Security Symposium on Research in Security and Privacy: 1994, 1996, 1997, and 1998.

Session Chair, IEEE Computer Security Symposium on Research in Security and Privacy: 1994, 1998.

Program Committee, European Symposium on Research in Computer Security: 1998.

Publications Chair, ACM Conference on Computer and Communications Security: 1998.

¹ ACM TISSEC is the premier academic journal in the area of network and computer security. It is sponsored by the Association for Computing Machinery (ACM). The ACM is the primary academic professional organization for computer scientists.

Stubblebine Consulting, Inc. Consultant Curriculum Vitae

Session Chair, 1997 DIMACS Workshop on Design and Formal Verification of Security Protocols.

Program Committee, National Computer Security Conference: 1993, 1994.

Best Paper selection for “Techniques for trusted software engineering”, Proceedings of the 20th International Conference on Software Engineering, Kyoto, Japan, 1998 (with P. Devanbu).

Invited paper and talk at International Conference on Software Engineering. “Software Engineering for Security: A Roadmap”, with P. Devanbu. International Conference on Software Engineering, ICSE 2000, June 2000.

Tutorial speaker, "Security and Software Engineering", Eighth ACM Conference on Computer and Communications Security Tutorials, Monday, November 5, 2001, Philadelphia, Pennsylvania, USA.

Awarded grant from National Science Foundation, Trusted Computing Program to study Privacy as it relates to identification, authentication, and authorization. 2002-2005.

Awarded grant from National Science Foundation, to study tools and techniques for protecting against online password guessing attacks. 2004.

Stubblebine Consulting, Inc

Dr. Stuart Stubblebine

Tel: 973-944-0055

Email: stuart@stubblebine.com