

**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 SSNOLOGY, LLC (Since 2023), Stubblebine Consulting (2000 - 2022)
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 clients include: AgileTCP Inc., Alcatel-Lucent, American Express, AMD, Austin Capital Group, Authentidate, British Telecom, Capital One, Celis Semiconductor, Dickstein Shapiro LLP, DoCoMo USA, Encirq, Gemplus, Global Crypto Systems, ILS Technology, Imagineer Software, Metaswitch Networks, Microsoft, New York City Police Department, New York City Department of Education, Oceana Sensor Technologies, Privada, Quixey, Summit Accelerator Fund, SRD Software / IBM, TantaComm

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

Systems, Wave Systems Corp, Zix Corporation, Zobi Mobile and 3 LP. See also clients in the litigation section.

Also, Dr. Stubblebine was previously affiliated with Stubblebine Research Labs, LLC since Oct, 2001 to 2015 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.

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 advanced 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.

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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 independence properties in a graph-theoretic framework, gave evidence that they are not polynomial-time solvable, and proposed approximation algorithms for these problems. Introduce 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 it's 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

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

Advised graduate students. Was a principal investigator for the 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)
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 tele-conferencing 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

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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
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

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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
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: 2020 Dr. Stubblebine provided expert services for RealTek in a case
To: 2021 brought by Phillips regarding patent infringement in an ITC case the
area of content protection protocols and the HDCP protocol. He
provided a report, was deposed, and testified at trial resulting in a
favorable verdict.

From: 2020 Dr. Stubblebine provides expert services for Qualys in a case
To: Current brought by Finjan regarding patent infringement in the area of code
inspection, protecting web clients against downloading of malicious
code, and enforcing policy restrictions on downloads by gateways.
He has provided a report on invalidity and non-infringement. The
trial is pending.

From: 2015 Dr. Stubblebine provided expert services for Nomadix against
To: 2021 BluePrint RF regarding patent infringement in the area of mobile

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

computer networking and Internet technologies including TCP/IP, DHCP, HTTP, MAC, network protocol stacks, login portals, and access control. He provided multiple declarations. In 2018 he provided two declarations regarding responses to two Guest-Tek PTAB petitions resulting in successfully denying institution. Starting in 2019 with respect to Guest-Tek litigation, he provided declarations on PTAB petitions, and provided two expert reports related to licensed patents, and was deposed. He testified at trial regarding patent validity and use of the patent resulting in a favorable verdict on both issues.

From: 2018 Dr. Stubblebine provided expert services for Metaswitch Networks
To: 2019 LTD in a case brought by Genband US LLC in the area of Voice over IP technology and patents, and various standards including CableLabs/3GPP/IETF in 134th Judicial District, Dallas, Texas. (DC-17-03697). He provided an expert report concerning multiple standard essential patents for various standards and was deposed. The case settled.

From: 2018 Dr. Stubblebine provided expert services for Alarm.com against
To: 2019 IpDatatel patent infringement in the area of a distributed computing system for remote monitoring, alerting, and control. He provided a declaration regarding claim construction. The case settled.

From: 2018 Dr. Stubblebine provided expert services for Ubiquiti Networks
To: 2018 regarding a case brought by Synopsys regarding client-server based software licensing, and associated reporting technology. He provided a declaration, two expert reports, and was deposed.

From: 2015 Dr. Stubblebine provided expert services for RSA regarding a case
To: 2018 brought by Arvest Bank regarding breach of contract related to settlement of an infringement case concerning a patent involving technologies for authentication technology related to SSL/TLS, website authentication, and authentication technologies for protecting against phishing attacks. He provided an expert report and was deposed.

From: 2014 Dr. Stubblebine provided expert services for Symantec regarding a
To: 2018 patent infringement case brought by Finjan regarding multiple patents regarding technologies for endpoint protection including managing remote computers, HTTPS, TCP/IP and appending

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

security information to search engine results. He provided declarations, and expert reports on non-infringement and invalidity and was deposed.

- From: 2017 Dr. Stubblebine provided expert services for PhishMe regarding a
To: 2017 Post Grant Review petition brought by Wombat Security Technologies regarding technologies to counter phishing email attacks. He provided a declaration in support of an initial response. PhishMe prevailed.
- From: 2015 Dr. Stubblebine provided expert services for RSA Security in an
To: 2015 arbitration matter brought by Capital One. Details of the involvement are confidential. (Arbitration involvement only. Not involved in a case before a judge.)
- From: 2014 Dr. Stubblebine provides expert services for Masimo against
To: 2015 Mindray Shenzhen Bio-Medical Electronics regarding patent infringement allegations brought by Mindray in the area of enforcing usage policies in medical devices. He provided invalidity and non-infringement reports, was deposed, and provided one or more declarations.
- From: 2013 Dr. Stubblebine provided expert services for Straight Path in various
To: 2018 venues in the area of establishing a point to point communications link over a network. In the ITC (completed) against LG et al, he provided expert reports on infringement and validity and was deposed. In the PTAB (competed), cases against LG et al and Samsung et al, he provided declarations and was deposed and Straight Path prevailed in IPR defenses. In N.D. Ca, against Apple, Cisco, and Avaya, provided claim construction declarations and was deposed. In EDV against Vizio, Toshiba, LG, Hulu et al and EDT against Blackberry, Huawei, Samsung, ZTE et al.
- From: 2013 Dr. Stubblebine provided expert services for Symantec in a case
To: 2014 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 Dr. Stubblebine provided expert services for Newegg, BB&T,
To: 2013 Expedia/Hotwire, and Orbitz in a case brought by TQP

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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. Newegg prevailed on non-infringement as a matter of law.

From: 2013
To: 2014

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

From: 2012
To: 2014

Dr. Stubblebine provided expert services for Juniper in a case brought by Palo Alto Networks regarding patent infringement in the area of firewall and network security technologies. He provided an expert report on invalidity and addressed issues of assignor estoppel and was deposed. He also provided one or more declarations.

From: 2012
To: 2014

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

From: 2011

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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.

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.

Form: 2010
To: 2013 Dr. Stubblebine provides expert services for 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 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: 2011 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.

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

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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 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

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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, 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 report 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.

Stubblebine Consulting Inc. Consultant Curriculum Vitae

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.

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

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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

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.

Resume of Stuart Stubblebine, Ph.D.

Page 15

Stubblebine Consulting Inc. Consultant Curriculum Vitae

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.

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.

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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.

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.

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

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.

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.

**Stubblebine Consulting Inc.
Consultant Curriculum Vitae**

On Searching for Known and Chosen 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.
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.

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

Stubblebine Consulting Inc. Consultant Curriculum Vitae

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.

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

Awarded the 2019 Lucas Award given to an author of a highly influential paper published in a Formal Methods symposium for the paper "Group Principals and the Formalization of Anonymity", with P. Syverson, World Congress on Formal Methods '99, Toulouse, France, LNCS Series, Springer-Verlag, September, 1999.

Stubblebine Consulting Inc. Consultant Curriculum Vitae

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.

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

Conference panel member for various academic conferences including Financial Cryptography 2005 panel on Phishing.

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).

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**

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.

SSNOLOGY, LLC

Dr. Stuart Stubblebine

Tel: 973-944-0055

Email: stuart@stubblebine.com