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 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

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 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).

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 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
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)

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/verificatior 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 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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.