Allan M. Schiffman

45 Bartlett St., #801
San Francisco, CA 94110
+1.775.901.0391
ams@ieee.org

Areas of Specialization

Communications Security and E-commerce Network Protocols.

Secure Distributed Systems.

Object-Oriented Language Implementation.

Engineering Accomplishments

Architected and led development of the *Targeted Therapy Finders*, a set of decision-support web applications for personalized cancer treatment. The underlying platform permits scientists to be their own "knowledge engineers", creating web applications directly from familiar input sources such as spreadsheets and wikis.

Designed the protocol and system architecture of *UsableLogin*, a cloud-based web authentication service that, in contrast to its predecessors, provides compatibility with existing systems and preserves existing user habits while increasing both end-user convenience and security.

Led development of the *SecureWeb Toolkit*, a multi-protocol communications security software library. Terisa System's primary product, it is an integral part of millions of systems that were offered by companies such as WebTV and Novell.

Member of the team that designed the *Secure Electronic Transactions* payment card protocol commissioned by MasterCard and Visa. This protocol included novelties such as dual signatures, use of OAEP, in-band certificate revocation and employment of ASN.1v3 certificate attributes. Led development of the SET reference implementation.

Co-designed the first security protocol for the web, the *Secure HyperText Transfer Protocol*. This protocol pioneered algorithm negotiation, server-only certificates, message pre-enhancement and non-repudiability for the WWW. Considered for standardization by the IETF, it influenced subsequent standards such as TLS, P3P and XML Signatures. Led the development of the first secure web browser, *Secure Mosaic*, which was fielded to CommerceNet members for e-commerce trials in 1994.

Led one of the first website construction consultancies, producing the presence for many of the original e-commerce sites such as Internet Shopping Network and NECX. These systems featured innovations such as DNS-based load balancing, three-tier architecture, URL-rewriting, hit-tracking and user customization.

Developed and deployed the first Internet e-commerce service, *Public Disc*, which used the PEM secure email protocols (later S/MIME) to offer information products over the Internet. This pioneering system provided secure email-based credit-card payment and reliable multi-part bulk file transfer, supplying software products and technical publications to customers for academic publishers such as the AAAI.

Led the development of a family of high-performance Smalltalk systems that gained both academic recognition and commercial success. These systems included many innovations, such as "just-in-time compilation" and "inline caching" (to name two), which have been adopted by most modern programming language implementations.

Architect of the Fairchild 9445 and its family of support chips. The F9445 was a bipolar 16-bit microprocessor first shipped in 1980; it boasted the fastest multiply instruction of any integrated microprocessor of its time. The product line saw broad use in signal-processing systems and military/space applications in the early 1980's.

Work Experience

2005-present President & Executive Director CommerceNet
I lead this entrepreneurial research institute, supervising research fellows and interns, as well as managing seed/incubation investments. Serve as advisor or board-member for most of these investments. The company is not pursuing new investment opportunities as of mid-2016, I remain President.

1998-present Consultant
Engagements included patent analysis and expert testimony for law firms, technical due-diligence for venture capital firms, and security-oriented design reviews for startup companies.

2011-2012 COO & VP Product CollabRx
Conceived, designed and led development of the company's flagship product, the *Targeted Therapy Finder* decision support tool for personalized oncology. A CommerceNet incubated company, now public (CLRX).

2008-2010 Founder & CTO Usable Security Systems
Conceived and designed the company's flagship product, the UsableLogin web authentication service. As co-founder, aided in raising funds, building team, promoting company and product. Webroot Software acquired Usable in 2010.

1997-1998 Chief Technologist SPYRUS
SPYRUS, a provider of high-assurance cryptographic products, merged with Terisa Systems in 1997. As chief technologist, advised the company's CEO on product strategy, new product development and market opportunities.

1995-1997 Founder & CTO Terisa Systems
Founded this company to provide communications security technology to the WWW software industry. Created the SecureWeb Toolkit, a multi-protocol security engine. Created the SET reference implementation. Raised industry awareness of role for security and public key cryptography in e-commerce by giving more than thirty public lectures and tutorials. As acting CEO, raised $8M in investments, negotiated technology licenses, and grew the company to over twenty employees and $3M annual revenue.

1991-1995 CTO Enterprise Integration Tech.
Responsible for engineering operations of this pioneering Internet R&D company. Co-created CommerceNet, an industry consortium dedicated to promoting Internet commerce. Initiated and led several groundbreaking projects in e-commerce, including the first online document distribution service, first retail sales website, and first secure credit card transaction. EIT merged with VeriFone in 1995.

1986-1991 VP Technology ParcPlace Systems
Designed and led development of this archetypal Object-Oriented programming environment and the company's primary product line, the Smalltalk-80 system. The commercial version, derived from work at Xerox PARC, originated dynamic translation ("JIT compilation"), data/application independence ("Model-View-Controller"), and policy-driven automatic storage management, preserving the original system's uniform object-orientation, while providing the best performance of any system of its kind. The product was implemented on dozens of computer systems used by many thousands of programmers in a wide variety of applications. The product line continues to be offered by Cincom, 25 years after its development.

1984-1986 Senior Staff Engineer Schlumberger Palo Alto Rsch.
Schlumberger's liaison to Stanford's Center for Integrated Systems as a Stanford "Industrial Visitor." Led design reviews for several products.

1981-1984 Manager, Systems Fairchild Lab for AI Rsch.
Created a world-class computing environment for forty AI researchers, including several custom-built systems. Implemented the Smalltalk-80 system on the prototype SUN workstation.

1978-1981 Microprocessor Engineer Fairchild Semiconductor
Developed the architecture of the F9445 microprocessor product line and led implementation of a companion software development system.

Litigations

DE Technologies, Inc. v. Dell, Inc.
Civil Action No. 7:04-CV-00628
United States District Court, W. D. of VA; Date filed: 10/27/2004
Vinson & Elkins LLP representing Dell, Inc., 2005-2007
Served as the testifying expert for Dell:
Submitted an expert report and was deposed.
Subject matter:
Patent described an international transaction system operating over the Internet that included a pre-transactional calculation of all charges, automatic credit authorization, generation of an electronic title or commercial invoice, arrangement/payment of shipping charges, taxes, and import/export duties.
Case dismissed in favor of client

Sun Microsystems, Inc. v. Microsoft Corporation
Civil Action No. JFM-O2-2739
United States District Court, N. D. of CA; Pretrial proceedings transferred: Aug. 2002
Civil Action No. C-02-01150 RMW (PVT)
District of Maryland (MDL-1332); Date filed: 2002
Day Casebeer Madrid & Batchelder LLP representing Sun Microsystems, Inc., 2002-2004
Private antitrust case
Consulted re object-oriented software
Case decided in favor of client

Sun Microsystems, Inc. v. Microsoft Corporation
Civil Action No. C 97-20884 RMW (PVT)
United States District Court, N. D. of CA; Date filed: 1997
Day Casebeer Madrid & Batchelder LLP representing Sun Microsystems, Inc., 1998-2000
Case re software-license violations, copyrights, and unfair competition
Consulted re object-oriented software
Case decided in favor of client

Eastman Kodak, Inc. v. Sun Microsystems, Inc.
Civil Action No. 02-CV-6074
United States District Court, W. D. of NY; Date filed: 1997
Day Casebeer Madrid & Batchelder LLP representing Sun Microsystems, Inc., 2002-2004
Patent case
Expert consultant re object-oriented software
Case settled

PI-Net International, Inc. v. Focus Business Bank
Civil Action No. 5:12-cv-04958-PSG
United States District Court, N. D. of CA; Date filed: 09/24/2012
Finnegan LLP representing Dell, Inc., 2013
Performed invalidity research for patents involving Web-based portals and a system for enabling real-time, bidirectional transactions on a network
Case was dismissed in favor of client

Backflip Software, Inc. v. Cisco Systems, Inc. et al
Case No. 113CV242234
Superior Court of the State of California, Santa Clara County
Hosie Rice LLP representing Backflip Software, Inc., 2015-1016
Briefly involved with source-code review issues

Education

M.S. Computer Science, Stanford University (1986)

Selected Publications

A Aleyasen, O Starov, AP Au, AM Schiffman, J Shrager, *On the Privacy Practices of Just Plain Sites*, Workshop on Privacy in the Electronic Society, October 2015.

Y Kang, AM Schiffman, J Shrager, *RAPPD: A language and prototype for recipient-accountable private personal data*, IEEE Security and Privacy Workshops (SPW), May 2014.

A Baquero, AM Schiffman, J Shrager, *Blend me in: Privacy-preserving input generalization for personalized online services,* International Conference on Privacy, Security and Trust, July 2013.

E Rescorla, AM Schiffman, *The Secure Hypertext Transfer Protocol*. Internet Engineering Task Force RFC-2660 & RFC-2658, August 1999.

AM Schiffman, *Security on the Web*, invited talk and tutorial, Second International WWW Conference, Chicago, October 1994.

FR Jackson, LP Deutsch, AM Schiffman, D Ungar, *Automatic storage-reclamation postmortem finalization process*. US Patent #5,274,804

LP Deutsch, AM Schiffman*, An Efficient Implementation of the Smalltalk-80 System*. 11th Annual ACM Symposium on Principles of Programming Languages, Salt Lake City, Utah, January 1984

Y Mor, AM Schiffman*, Microprocessor with improved arithmetic logic unit data path*. US Patent #4,396,979

Professional Activities

National Research Council Committee on Information Systems Trustworthiness

Netscape Security Advisory Board

World Wide Web Consortium Security Advisory Board

IEEE Compcon Program Committee

Asilomar Microprocessor Workshop Organizing Committee

Top 25 Technology Drivers*, Network Computing Magazine*

Stanford University "Distinguished Lecturer"