

Jon Callas

1781 Wema Way
San Jose, CA 95124

T +1 (408) 448-6801

jon@callas.org
<http://www.callas.org/jon/>

PROFILE

I am an innovator in information and business security, including cryptography, operating system security, public key infrastructure, and intellectual property rights. I am also an innovator in human-computer interactions, collaboration and social virtual reality. As a recognized contributor in the security and standards fields, I energetically support industry related issues through written articles, speaking engagements, testimony to Congress, and collaboration with lobbying organizations. I am a frequent commentator to the press on industry issues. A veteran in technical marketing and negotiation, I have a proven track record of delivering complex applications to businesses. I am knowledgeable in the complexities of interoperability, international software design, and modern development techniques.

EXPERIENCE

Cofounder, CTO, and CSO; PGP Corporation, Palo Alto, CA — 2002-present

I designed PGP's next generation products and continue to design and plan new products. I lead internal security for the company and products, and the security response team. I am evangelist to customers, press and partners. I work on business development with the BD team. Set up technical education seminars for engineering. I write white papers, public presentations, and architecture documents. I participate in standards bodies and government interest groups.

Senior Systems Architect; Wave Systems Corporation, Cupertino, CA — 2001-2002

I was Lead Architect for the EMBASSY Trust System. I performed security analysis of Wave's EMBASSY Trust System and created product security subsystems. As part of the project management team I put in place coordinated software development processes for distributed software development. I was a spokesperson for company, presenting at security conferences.

Director of Software Engineering; Counterpane Internet Security, San Jose, CA — 1999-2001

I was co-architect of Counterpane's Managed Security Monitoring system – a redundant system with adaptive fail-over that monitors networks on three continents. I led the engineering team that built the system, taking it from prototype to operational in four months. I managed Counterpane's export control process, getting approval for the system, including fifteen new ciphers. I was secondary spokesperson for the company, writing articles and papers, speaking at conferences, giving lectures, handling media inquiries, and appearing on television.

CTO; Network Associates, Inc., (formerly Pretty Good Privacy, Inc.), Santa Clara, CA — 1997-1999

As CTO for the Total Network Security Division of Network Associates my responsibilities included creating architecture and direction for the company's network security products, evaluating new technologies, and evaluating acquisition candidates. I was NAI's public representative for industry concerns in both the private and government sector including international standards bodies. I helped start and became the primary author of the IETF's OpenPGP standard.

Senior Engineer/Scientist II; Apple Computer, Inc., Cupertino, CA — 1995-1997

I was a software developer and researcher focused on new networking and collaboration products written in C++, Java, on Macintoshes and Win32. I developed systems for electronic commerce and privacy with strong cryptographic systems. I wrote and publicly presented several papers on commerce and cryptographic systems.

Founder, Director of Technology; World Benders, Inc., Nashua, NH — 1992-1995

I was the lead architect and developer of Meeting Space®, a cross-platform group collaboration product for Macintosh, Windows, and UNIX. This product allowed people to conduct meetings in real-time on existing networks. I designed and built a client-server system with common server sources for all platforms, and multiple simultaneous network transports. I was the UI architect and author of the Macintosh client

program. I built a secure network transport using public-key encryption. Along with my technical duties, I planned business strategy, developed proposals, and presented to prospective investors and customers.

Principal Software Engineer; Digital Equipment Corporation — 1990-1992

Architect, author and evangelist of software of PATHWORKS network operating system. Designed and built software for Macintosh client systems and server systems running VMS or UNIX. An active member of the architecture and project management team. Architect for Macintosh file format to VMS. Used object-oriented frameworks in C, C++, and CLOS; created cross-platform communications between computers running MacOS, VMS, UNIX, Windows and OS/2, using AppleTalk, DECnet, and TCP/IP networks. Developed and maintained device drivers for high-performance workstations. Developed software for 3D, PEX, and DDX for OpenVMS, OSF/1 and Windows NT.

Principal Software Engineer; Digital Equipment Corporation — 1984-1990

Architect, designer, author, and maintainer for portions of the VAX/VMS executive. Provided solutions in security, CPU scheduling, memory management, process management, and extensions to the VAX/VMS for VMS Integrated POSIX, extended memory, and vector processing. Designed, implemented, and maintained software for VMS-based workstations including single and multiple-plane raster graphics, font management, memory management, and windowing primitives. Member of the scheduling, project leadership, and ready-to-ship team for VMS V5.0, V4.7, and V4.0. Architect of a direct-manipulation human interface for workstations and member of the committees for the DEC windows/OSF Human Interface Style Guide and the Digital sub committee or the ISO-Latin 1 character set

EDUCATION

University of Maryland, College Park, MD — B.Sc. Mathematics, minors in philosophy and English literature

PATENTS

Eight patents granted and pending:

- System and Method for Secure and Transparent Electronic Communications
- System and Method for Dynamic Security Operations
- System and Method for Secure Electronic Communications in a Partially Keyless Environment
- Apparatus for Partial Authentication of Messages
- Apparatus and Method for Facilitating Encryption and Decryption Operations Over an Email Server Using an Unsupported Protocol
- Identity-based Encryption With Conventional Public-key Cryptography
- Method and Apparatus for Dynamic Network Intrusion Monitoring, Detection, and Response
- Cryptographic System and Methodology for Creating and Managing Crypto Policy on a Certificate Server

PUBLICATIONS, ETC.

Frequent commentator to the press, quoted and interviewed on BBC Digital Planet; The New Scientist; The Wall Street Journal, Network World, others.

Profile in Self-Exposure, *hakin9* magazine, 2007

RFC 4880, *OpenPGP Message Format*, with L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer

RFC 4871, *DomainKeys Identified Mail (DKIM) Signatures*, with E. Allman, M. Delany, J. Fenton, M. Libbey, M. Thomas

Virtual Economies: Threats and Risks, with Christopher Thorpe, Jessica Hammer, Jean Camp, and Mike Bond, Financial Cryptography 2007, < <http://www.eecs.harvard.edu/~cat/cs/fc07/vetr.pdf>>

Co-author for IETF RFCs for SYSLOG-SIGN and ZRTP (in process).

Numerous articles in PGP Corporation's *CTO Corner*, www.pgp.com, 2004-2007

Email Security, article in Handbook of Information Security, Hossein Bidgolli ed., Wiley, 2006

An Introduction to Cryptography, 77pp, PGP Corporation, 2006

The Future of Cryptography, "Information Systems Security," The (ISC)² Journal, Vol. 16, No. 1, PP 15-22. Jan-Feb 2007

EntagsFliegen, "<kes>," Die Zeitschrift für Informations-Sicherheit; Issue #1, März 2006

Personal profile in *PC Plus Magazine*, 2006

Identity-Based Encryption with Conventional Public-Key Infrastructure, Fourth Annual PKI Research Workshop, 2005

Improving Message Security With a Self-Assembling PKI, Second Annual PKI Research Workshop, 2003

Expert on the TechTarget *Ask the Experts* panel in network security, intellectual property, and PKI, 2001-2004

Why Digital Signatures Are Not Signatures with Bruce Schneier, Industry Standard, 2000.

Fair Use, Intellectual Property, and the Information Economy, Proceedings of the Financial Cryptography 1999 conference, Springer-Verlag.

The WIPO Copyright Treaties Implementation Act, Hearing Before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce, House of Representatives, One-Hundred-Fifth Congress, Second Session on H.R. 2281, June 5, 1998; Serial No. 105-102. US Government Printing Office, Washington D.C., ISBN 0-16-057421-8.

RFC2440, *OpenPGP Message Format*, with L. Donnerhacke, H. Finney, and R. Thayer

The State of the World of Cryptography, MacTech Magazine, September 1999.

Using Cryptographic-Quality Random Numbers, Proceedings of the 1996 MacHack conference.

Real World Cyberspace, by Jon Callas and Susan Giusto, proceedings of the 1994 Boston Computer Society

Real Work in Virtual Space, by Jon Callas and Margaret Russell-Gonzalez, pp685-692 in the book *Tricks of the Internet Gurus*, SAMS publishing, ISBN 0-672-30599-2 (1994)

Technical reviewer for *Develop Magazine* (1994)

PROFESSIONAL ORGANIZATIONS & ACTIVITIES

Member of the ACM, IACR, IFCA, and IEEE

Member of ENISA virtual group on security of Reputation Systems and Social Networking

Speaker at professional conferences sponsored by SANS, CSI, ISACA, DIMACS, Gartner Group, ISSA, MacCrypto, Silicon Valley Linux Users Group, and others.

Guest lecturer at Indiana University, Carnegie-Mellon University, Stanford Business School, and University of Waterloo

Program committee member for Financial Cryptography 2007; NDSS 2007-2008; ShmooCon 2007-2008.

Program co-chair, ShmooCon 2008