

Jon Callas

Jon Callas is an American [computer security expert](#),^[1] [software engineer](#), [user experience designer](#), and [technologist](#) who is the co-founder and former CTO of the global encrypted communications service [Silent Circle](#).^[2] He has held major positions at [Digital Equipment Corporation](#), [Apple](#), [PGP](#), and [Entrust](#), and is considered "one of the most respected and well-known names in the mobile security industry."^[3] Callas is credited with creating several Internet Engineering Task Force (IETF) standards, including [OpenPGP](#), [DKIM](#),^[4] and [ZRTP](#), which he wrote.^[3] Prior to his work at [Entrust](#), he was Chief Technical Officer and co-founder of [PGP Corporation](#) and the former Chief Technical Officer of [Entrust](#).

On his website, Callas describes himself as "an entrepreneur and innovator in information and business security, including cryptography, operating system security, public key infrastructure, and intellectual property rights," as well as "an innovator in human-computer interactions, collaboration and social virtual reality."^[5]

He has also worked for [Bruce Schneier's Counterpane Internet Security](#), was one of the primary authors of the DKIM method, and was Chief Scientist of the original PGP, Inc. founded by [Phil Zimmermann](#). Callas is a member of the [Infosec think tank](#) [The Shmoo Group](#).

Early life and education

Callas received a BSc in mathematics from the [University of Maryland at College Park](#), which he attended from 1977 to 1980.^{[2][6]} He minored in philosophy and English literature.^[5]

Career

He was a member of the technical staff at Century Computing from 1980 to 1981, then served as principal software engineer at Digital Equipment from 1981 to 1993.^[2] While working there, he "got to work on a wide variety of things, from graphics to schedulers to memory management to operating system security," and created a [random password generator](#).^[7] At Digital Equipment, he designed the [PATHWORKS](#) network operating system as well as software for Macintosh client systems and server systems running VMS or UNIX, and created cross-platform communications between computers running [Mac OS](#), [VMS](#), [UNIX](#), [Windows](#) and [OS/2](#), using [AppleTalk](#), [DECnet](#), and [TCP/IP](#) networks. He also developed software for 3D, PEX, and DDX for [OpenVMS](#), [OSF/1](#) and [Windows NT](#).^[5]

Jon Callas



Callas at [Kiwicon](#) in [Wellington](#), [New Zealand](#) (2012)

Known for	Internet Security
------------------	-----------------------------------

After Digital Equipment folded, Callas co-founded World Benders, Inc., where he worked from 1993 to 1995.^[2] At World Benders, he "was the lead architect and developer of Meeting Space, a cross-platform group collaboration product" that "allowed people to conduct meetings in real-time on existing networks."^[5]

Callas then held the title of senior scientist II at Apple Computer from 1995 to 1997.^[2] He describes himself as having been the firm's Security Privateer, and as having "designed and built next-generation cryptographic security products for Mac OS X and iOS, including the 'FileVault 2' full-disk encryption product." He also "designed a concurrent programming system for high-performance computing, 'Transforms.'" In addition, he "led the engineering and approvals for a FIPS 140 validation of iOS."^[5] Callas was trusted with the security of Apple's operating system,^[3] and worked on Apple's Whole Disk Encryption. "That was the worst time to be working for Apple, the year before Steve Jobs came back," Callas has said.^[7]

At Apple, he worked for Gursharan Sidhu, the inventor of AppleTalk. Callas "shipped the very first crypto built into an OS, called PowerTalk," which, he has said, "failed for being far too early," although he and his colleague Bruce Gaya managed to hack a piece of it, a password manager called The Keychain, "so that you could run it without the rest of PowerTalk, and thus rescued it from oblivion. The present Keychain on Apple products is completely and utterly rewritten, but I'm proud of saving it."^[7]

He joined PGP, Inc. (developer of Pretty Good Privacy), in January 1997 as chief scientist. Network Associates (NAI) bought PGP in December 1997, and Callas became CTO for the Total Network Security Division of NAI, creating "architecture and direction for the company's network security products" and serving as "the primary author of the IETF's OpenPGP standard."^{[5][8]}

He was director of software engineering at Counterpane from 1999 to 2001, serving as "co-architect of Counterpane's Managed Security Monitoring system – a redundant system with adaptive fail-over that monitors networks on three continents." He also "led the engineering team that built the system, taking it from prototype to operational in four months," and "managed Counterpane's export control process, getting approval for the system, including fifteen new ciphers." As Senior Architect at Wave Systems Corporation from 2001 to 2002, he was the lead architect for Wave's EMBASSY Trust System, on which he performed security analysis and created product security subsystems.

He then co-founded the new PGP Corporation in 2002. He worked as a server architect at PGP from July 2002 to October 2009, and during his time at the company was the principal author of the IETF OpenPGP standard, now RFC2440,^{[2][5][8][9]} and developed the PGP (Pretty Good Privacy) Universal Server.^[7] He was security privateer at I Could Tell You But Then I'd Have To Kill You and Associates from October 2009 to July 2011. He was chief technical officer at Entrust, a provider of identity-based security software, from July 2011 to January 2013.^[3]

He co-founded Silent Circle in 2012 and Blackphone in 2013, and continued to serve as CTO of Silent Circle until April 2016,^{[2][3]} where he led the development and operations groups, the former of which "produces the apps that manifest Silent Circle's services to its subscribers" and the latter of which "runs the actual services themselves."^[5]

Callas holds patents, or has patents pending, on several systems and methods for erasing media, facilitating secure media access, for secure and transparent electronic communications, for dynamic security operations, for partial message authentication, and for facilitating encryption and decryption operations over an email server.^[5]

Callas's security product designs have won major innovation awards from The Wall Street Journal and others.^[7] He is one of the primary authors of the DKIM method and a member of the Infosec think tank The Shmoo Group. He has served as Adjunct Professor at Indiana University since 2012.^[2]

Callas lectured widely about computers and Internet security, and was scheduled to be a speaker at the Oslo Freedom Forum in 2014.^[9] Callas was selected to be one of two keynote speakers at the 2015 PDF Technical Conference in San Jose, California.^[10]

By May 2016 Callas rejoined Apple.^[11]

Callas appeared on the January 11, 2018 episode of John Wants Answers.^[12]

Views

Callas has stated that tech companies are a bigger threat to privacy than the government. His views stem from big tech's mass pooling of personal data for advertising and the polarization within Silicon Valley. While some companies are committed to privacy, many more earn their revenues from selling user data. Callas has stated that if the advertising market takes a downturn, companies that protect their users' data are the most insulated from harm.^[13]

Personal life

He lives in San Jose, California.^{[2][5]}

References

1. Interview with Jon Callas, CTO of PGP Corporation. (<http://www.net-security.org/article.php?id=195>) Help Net Security, 2011. Retrieved 17 July 2011.
2. <http://www.linkedin.com/in/joncallas>
3. Trutta, Filip (Jul 26, 2011). "Former Apple Security Expert Jon Callas Joins Entrust" (<http://news.softpedia.com/news/Former-Apple-Security-Expert-Jon-Callas-Joins-Entrust-213530.shtml>). *softpedia*.
4. Mimoso, Michael (May 23, 2016). "Apple has hired cryptography pioneer Jon Callas for a third time. Callas, who previously at Apple helped design and implement encryption systems for Macs, was most recently at Silent Circle" (<https://threatpost.com/crypto-innovator-entrepreneur-jon-callas-rejoins-apple/118283/>). *Threatpost*.
5. "Jon Callas" (<https://www.merrymeet.com/jon/JDCC-Resume.pdf>) (PDF). *Merry Meet*.
6. "Jon Callas, Entrust Inc: Profile and Biography" (<http://investing.businessweek.com/research/stock/s/private/person.asp?personId=2911318&privcapId=28140&previousCapId=25604096&previousTitle=Vimo,%20Inc.>).
7. Risner, Erin (June 5, 2013). "AMA: Interview with Cryptographer, Computer Security Expert Jon Callas" (<https://blog.spideroak.com/20130605095553-ama-interview-with-cryptographer-computer-security-expert-jon-callas>). *Spideroak Blog*.
8. Kucan, Berislav (4 October 2002). "Interview with Jon Callas, CTO of PGP Corporation" (<http://www.net-security.org/article.php?id=195>). *Net Security*.
9. "Speakers" (<https://web.archive.org/web/20140421115035/http://www.oslofreedomforum.com/pdfs/OFF14Speakers.pdf>) (PDF). *Oslo Freedom Foundation*. Archived from the original (<http://www.oslofreedomforum.com/pdfs/OFF14Speakers.pdf>) (PDF) on 2014-04-21.

10. "Phil Ydens and Jon Callas to keynote at the PDF Technical Conference 2015" (<http://www.pdfa.org/news/phil-ydens-and-jon-callas-to-keynote-at-the-pdf-technical-conference-2015/>). *PDF Association*. 21 September 2015. Retrieved September 24, 2015.
11. Apple rehires prominent security pro as encryption fight boils (<https://www.reuters.com/article/us-apple-encryption-callas-idUSKCN0YF2J1>), *Reuters*, May 24, 2016
12. "Home" (<http://johnwantsanswers.com/>). *johnwantsanswers.com*.
13. Whittaker, Zack (Feb 4, 2016). "PGP co-founder: Ad companies are the biggest privacy problem today, not governments" (<https://www.zdnet.com/article/pgp-co-founder-the-biggest-privacy-issue-today-are-online-ads/>). *ZDNet*.

External links

- Jon Callas on Twitter (<https://twitter.com/joncallas>)
 - Résumé to 2008 (<http://www.merrymeet.com/jon/JDCC-Resume.pdf>)
 - silentcircle.com (<https://silentcircle.com/>)
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Jon_Callas&oldid=1150276263"

▪