

Phil Zimmermann

Philip R. Zimmermann^[2] (born 1954)^[1] is an American computer scientist and cryptographer. He is the creator of Pretty Good Privacy (PGP), the most widely used email encryption software in the world.^[2] He is also known for his work in VoIP encryption protocols, notably ZRTP and Zfone. Zimmermann is co-founder and Chief Scientist of the global encrypted communications firm Silent Circle.

Contents

Background

PGP

Arms Export Control Act investigation

Silent Circle

Dark Mail Alliance

Okuna

Zimmermann's Law

Awards and other recognition

Publications

See also

References

External links

Phil Zimmermann



Born	1954 ^[1] <div><u>Camden, New Jersey, U.S.</u>^[1]</div>
Occupation	<u>Professor</u>
Known for	Creator of <u>Pretty Good Privacy</u>
Website	<u>philzimmermann.com</u> (<u>https://philzimmermann.com/</u>)

Background

He was born in Camden, New Jersey.^[1] Zimmermann received a B.S. degree in computer science from Florida Atlantic University in Boca Raton, Florida in 1978.^[2] In the 1980s, Zimmermann worked in Boulder, Colorado as a software engineer on the Nuclear Weapons Freeze Campaign as a military policy analyst.^[3]

PGP

In 1991, he wrote the popular Pretty Good Privacy (PGP) program, and made it available (together with its source code) through public FTP for download, the first widely available program implementing public-key cryptography. Shortly thereafter, it became available overseas via the Internet, though Zimmermann has said he had no part in its distribution outside the United States.

In 1995, he published a book *"PGP Source Code and Internals"*, as a way to bypass limitation of exporting digital code. The book contains *source code to a software package called PGP*^[4]

The very first version of PGP included an encryption algorithm, BassOmatic, developed by Zimmermann.^[5]

Arms Export Control Act investigation

After a report from RSA Security, who were in a licensing dispute with regard to the use of the RSA algorithm in PGP, the United States Customs Service started a criminal investigation of Zimmermann, for allegedly violating the Arms Export Control Act.^[6] The United States Government had long regarded cryptographic software as a munition, and thus subject to arms trafficking export controls. At that time, PGP was considered to be impermissible ("high-strength") for export from the United States. The maximum strength allowed for legal export has since been raised and now allows PGP to be exported. The investigation lasted three years, but was finally dropped without filing charges.

After the government dropped its case without indictment in early 1996, Zimmermann founded PGP Inc. and released an updated version of PGP and some additional related products. That company was acquired by Network Associates (NAI) in December 1997, and Zimmermann stayed on for three years as a Senior Fellow. NAI decided to drop the product line and in 2002, PGP was acquired from NAI by a new company called PGP Corporation. Zimmermann served as a special advisor and consultant to that firm until Symantec acquired PGP Corporation in 2010.^[2] Zimmermann is also a fellow at the Stanford Law School's Center for Internet and Society. He was a principal designer of the cryptographic key agreement protocol (the "association model") for the Wireless USB standard.

Silent Circle

Along with Mike Janke and Jon Callas, in 2012 he co-founded Silent Circle, a secure hardware and subscription based software security company.^{[3][7]}

Dark Mail Alliance

In October 2013, Zimmermann, along with other key employees from Silent Circle, teamed up with Lavabit founder Ladar Levison to create the Dark Mail Alliance. The goal of the organization is to work on a new protocol to replace PGP that will encrypt email metadata, among other things that PGP is not capable of.

Okuna

Zimmermann is also involved in the social network Okuna, formerly Openbook, which aims to be an ethical and privacy-friendly alternative to existing social networks, especially Facebook.^[8] He sees today's established social media platforms as a threat to democracy and privacy, because of their profit-oriented revenue models that "are all about exploiting our personal information" and "[deepen] the political divides in our culture", and Okuna as the solution to these problems.^[9]

Zimmermann's Law

In 2013, an article on *Zimmermann's Law* quoted Phil Zimmermann as saying *The natural flow of technology tends to move in the direction of making surveillance easier, and the ability of computers to track us doubles every eighteen months*,^[10] in reference to Moore's law.

Awards and other recognition

Zimmermann has received numerous technical and humanitarian awards for his pioneering work in cryptography:

- In 2018, Zimmermann was inducted into Information Systems Security Association (ISSA) hall of fame by the ISSA International Organization on October 16, 2018.
- In 2012, Zimmermann was inducted into the Internet Hall of Fame by the Internet Society.^[11]
- In 2008, *PC World* named Zimmermann one of the "Top 50 Tech Visionaries" of the last 50 years.^[12]
- In 2006, eWeek ranked PGP 9th in the 25 Most Influential and Innovative Products introduced since the invention of the PC in 1981.^[13]
- In 2003, *Reason* named him a "Hero of Freedom"^[14]
- In 2001, Zimmermann was inducted into the CRN Industry Hall of Fame.^[15]
- In 2000, InfoWorld named him one of the "Top 10 Innovators in E-business".^[16]
- In 1999, he received the Louis Brandeis Award from Privacy International.
- In 1998, he received a Lifetime Achievement Award from *Secure Computing Magazine*.
- In 1996, he received the Norbert Wiener Award for Social and Professional Responsibility for promoting the responsible use of technology.
- In 1996, he received the Thomas S. Szasz Award for Outstanding Contributions to the Cause of Civil Liberties]] from the Center for Independent Thought.^[17]
- In 1995, he received the Chrysler Design Award for Innovation, and the Pioneer Award from the Electronic Frontier Foundation.
- In 1995, *Newsweek* also named Zimmermann one of the "Net 50", the 50 most influential people on the Internet.

Simon Singh's *The Code Book* devotes an entire chapter to Zimmermann and PGP.^[18]

Publications

- *The Official PGP User's Guide*, MIT Press, 1995^[19]
- *PGP Source Code and Internals*, MIT Press, 1995^[20]

See also


- Data privacy
- GNU Privacy Guard
- Information privacy
- Information security
- PGPfone
- PGP word list

References

1. Garfinkel, Simson (1994). *PGP: Pretty Good Privacy* (https://books.google.com/books?id=cSe_0OnZqjAC&q=%22Phil+Zimmermann%22+1954&pg=PA85). O'Reilly & Associates. p. 85. ISBN 0585032211. OCLC 45730291 (<https://www.worldcat.org/oclc/45730291>).
2. "Phil Zimmerman's Homepage: Background" (<http://www.philzimmermann.com/EN/background/index.html>). Retrieved 2012-01-12.
3. Ranger, Steve (23 June 2015). "Defending the last missing pixels: Phil Zimmermann speaks out on encryption, privacy, and avoiding a surveillance state" (<https://www.techrepublic.com/article/defending-the-last-missing-pixels-phil-zimmermann/>). *TechRepublic*.
4. "Author's preface to the book: "PGP Source Code and Internals" " (<https://philzimmermann.com/EN/essays/BookPreface.html>). Retrieved 2020-05-26.

5. Mollin, Richard A. (2007). *An introduction to cryptography* (<https://books.google.com/books?id=Vje8TRcLlycC&pg=PA227>). CRC Press. p. 227. ISBN 9781420011241.
6. Sussman, Vic (March 26, 1995). "Lost in Kafka Territory" (https://web.archive.org/web/20130616165334/http://www.usnews.com/usnews/news/articles/950403/archive_010975.htm). *US News & World Report*. Archived from the original (https://www.usnews.com/usnews/news/articles/950403/archive_010975.htm) on 16 June 2013. Retrieved 27 May 2012.
7. "Silent Circle" (<https://web.archive.org/web/20150611211029/https://home.silentcircle.com/>). Silent Circle. Private By Design. Archived from the original (<https://home.silentcircle.com/>) on 11 June 2015. Retrieved 25 June 2015.
8. "Okuna | Ethical social network" (<https://about.okuna.io/en/about-us>). *about.okuna.io*. Retrieved 2021-01-21.
9. "Phil Zimmermann on Openbook" (<https://www.youtube.com/watch?v=n99xXlbGFjw>). *YouTube*. Retrieved 2021-01-21.
10. Om Malik (2013-08-11). "Zimmermann's Law: PGP inventor and Silent Circle co-founder Phil Zimmermann on the surveillance society — Tech News and Analysis" (<https://web.archive.org/web/20130815064716/http://gigaom.com/2013/08/11/zimmermanns-law-pgp-inventor-and-silent-circle-co-founder-phil-zimmermann-on-the-surveillance-society/>). *GigaOM*. Archived from the original (<http://gigaom.com/2013/08/11/zimmermanns-law-pgp-inventor-and-silent-circle-co-founder-phil-zimmermann-on-the-surveillance-society/>) on 2013-08-15. Retrieved 2013-08-20.
11. 2012 Inductees (<http://www.internethalloffame.org/inductees/year/2012>), Internet Hall of Fame website. Last accessed April 24, 2012
12. "Top 50 Tech Visionaries" (<https://web.archive.org/web/20080528110152/http://www.pcworld.com/article/id,145290-page,1-c,technology/article.html>). Archived from the original (<http://www.pcworld.com/article/id,145290-page,1-c,technology/article.html>) on 2008-05-28. Retrieved 2008-05-21.
13. "25 Most Influential and Innovative Products introduced since the invention of the PC in 1981" (<http://www.eweek.com/c/a/Past-News/The-25-Most-Influential-Products-of-the-Past-25-Years/>).
14. *35 Heroes of Freedom* (<http://www.reason.com/news/show/28959.html>) Archived (<https://web.archive.org/web/20070912015047/http://www.reason.com/news/show/28959.html>) 2007-09-12 at the Wayback Machine *Reason*, December 2003 Retrieved April 10, 2007
15. "CRN Industry Hall of Fame" (<https://web.archive.org/web/20040405065312/http://www.crn.com/sections/special/hof/hof01.asp?ArticleID=31279>). Archived from the original (<http://www.crn.com/sections/special/hof/hof01.asp?ArticleID=31279>) on April 5, 2004.
16. "Top 10 Innovators in E-business" (<http://www.infoworld.com/articles/hn/xml/00/10/09/001009hnpz.xml>) Archived (<https://web.archive.org/web/20080724053221/http://www.infoworld.com/articles/hn/xml/00/10/09/001009hnpz.xml>) 2008-07-24 at the Wayback Machine.
17. "Past Szasz Award Recipients" (http://www.centerforindependentthought.org/past_szasz_award_recipients.html). *Center for Independent Thought*.
18. Singh, Simon (2000). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (US paperback ed.). Doubleday. ISBN 0-385-49532-3.
19. Zimmermann, Philip (1995). *The Official PGP User's Guide*. MIT Press. ISBN 0-262-74017-6.
20. Zimmermann, Philip (1995). *PGP Source Code and Internals*. MIT Press. ISBN 0-262-24039-4.

External links

- Official website (<https://philzimmermann.com/>) 
- Why I wrote PGP (<https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html>)
- Conversation With Phil Zimmermann (<https://web.archive.org/web/20030812140828/http://grep.la.w.harvard.edu/article.pl?sid=03%2F06%2F06%2F1441247&mode=nested>), Mikael Pawlo, GrepLaw, June 6, 2003.
- E-mail security hero takes on VoIP (<https://www.cnet.com/news/e-mail-security-hero-takes-on-voip/>), Declan McCullagh, C|net, 15 August 2006.
- VON Pioneers: Philip Zimmermann Encrypts VoIP (<https://web.archive.org/web/20070403214130/http://www.vonmag-digital.com/vonmag/200701/>), VON Magazine, Jan 2007.

- **Silent Circle – Global Encrypted Communications Service** (<https://web.archive.org/web/20200514214241/https://www.silentcircle.com/>)
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Phil_Zimmermann&oldid=1001866550"

This page was last edited on 21 January 2021, at 19:23 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.