Hey! I'm **David**, a security engineer at the Blockchain team of **Facebook (https://facebook.com/)**, previously a security consultant for the Cryptography Services of **NCC Group (https://www.nccgroup.com)**. I'm also the author of the **Real World Cryptography book (https://www.manning.com/books/real-world-cryptography?a_aid=Realworldcrypto&a_bid=ad500e09)**. This is my blog about **cryptography** and **security** and other related topics that I find interesting.

A history of end-to-end encryption and the death of PGP

posted January 2020

- **1981 - RFC 788 - Simple Mail Transfer Protocol (https://tools.ietf.org/html/rfc788) (SMTP) is published, the standard for email is born.**

This is were everything starts, we now have an open peer-to-peer protocol that everyone on the internet can use to communicate.

- 1991
  - The US government introduces the 1991 Senate Bill 266, which attempts to allow "the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law" from "providers of electronic communications services and manufacturers of electronic communications service equipment". The bill fails to pass into law.
  - **Pretty Good Privacy (PGP) - released by Phil Zimmermann.**
- 1993 - The US Government launches a criminal investigation against Phil Zimmermann for sharing a cryptographic tool to the world (at the time crypto exporting laws are a thing).

If you don't know **where to start**, you might want to check these popular articles:

- How did length extension attacks made it into SHA-2? (/article/417/how-did-length-extension-attacks-made-it-into-sha-2/)
- Speed and Cryptography (/article/468/speed-and-cryptography/)
- What is the BLS signature scheme? (/article/472/what-is-the-bls-signature-scheme/)
- Zero'ing memory, compiler optimizations and memset_s (/article/419/zeroing-memory-compiler-optimizations-and-memset_s/)
- The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations (/article/461/the-9-lives-of-bleichenbachers-cat-new-cache-attacks-on-tls-implementations/)
- How to Backdoor Diffie-Hellman: quick explanation (/article/360/how-to-backdoor-diffie-hellman-quick-explanation/)
- Tamarin Prover Introduction (/article/404/tamarin-prover-introduction/)

- 1995 - Zimmermann publishes PGP's source code in a book via MIT Press, dodging the criminal investigation by using the first ammendment's protection of books.

That's it, PGP is out there, people now have a weapon to fight government surveillance. As Zimmermann puts it:

> PGP empowers people to take their privacy into their own hands. There's a growing social need for it. That's why I wrote it.

- 1995 - The RSA Data Security company proposes S/MIME as an alternative to PGP.
- 1996
  - criminal investigation against Zimmermann and PGP is dropped.
  - PGP Inc is founded by Zimmermann, PGP becomes licensed-software.
  - RFC 1991 - PGP Message Exchange Formats (https://www.ietf.org/rfc/rfc1991.txt)
- 1997
  - **GNU Privacy Guard (GPG)** - version 0.0.0 released by Werner Koch.
  - PGP 5 is released.

> The original agreement between Viacrypt and the Zimmermann team had been that Viacrypt would have even-numbered versions and Zimmermann odd-numbered versions. Viacrypt, thus, created a new version (based on PGP 2) that they called PGP 4. To remove confusion about how it could be that PGP 3 was the successor to PGP 4, PGP 3 was renamed and released as PGP 5 in May 1997

- 1997 - PGP Inc is acquired by Network Associates
- 1998 - RFC 2440 - OpenPGP Message Format (https://www.ietf.org/rfc/rfc2440.txt)

> OpenPGP - This is a definition for security software that uses PGP 5.x as a basis.

- 1999
  - GPG version 1.0 released
  - **Extensible Messaging and Presence Protocol (XMPP) (https://xmpp.org/)** is developed by the open source community. XMPP is a federated chat protocol (users can run their own servers) that does not have end-to-end encryption and requires communications to be synchronous (both users have to be online).
- 2002 - PGP Corporation is formed by ex-PGP members and the PGP license/assets are bought back from Network Associates
- **2004 - Off-The-Record (OTR) is introduced by Nikita Borisov, Ian Avrum Goldberg, and Eric A. Brewer as an extension of the XMPP chat protocol in "Off-the-Record Communication, or, Why Not To Use PGP (https://otr.cypherpunks.ca/otr-wpes.pdf)"**

> We argue that [...] the encryption must provide perfect forward secrecy to protect from future compromises [...] the authentication mechanism must offer repudiation, so that the communications remain personal and unverifiable to third parties

---

We now have an interesting development: messaging (which is seen as a different way of communication for most people) is getting the same security treatment as email.

- 2006 - GPG version 2.0 released
- 2007 - RFC 4880 - OpenPGP Message Format (https://www.ietf.org/rfc/rfc4880.txt)
- 2010 - Symantec purchases the rights for PGP for $300 million.
- 2011 - Cryptocat (https://en.wikipedia.org/wiki/Cryptocat) is released.
- **2013 - The TextSecure (now Signal) application is introduced, built on top of the TextSecure protocol with Axolotl (now the Signal protocol with the double ratchet) as an evolution of OTR and SCIMP. It provides asynchronous communication unlike other messaging protocols, closing the gap between messaging and email.**
- 2014
  - Matrix (https://matrix.org/) is introduced as a modern alternative to XMPP.
  - Matthew Green - What's the matter with PGP? (https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/)

PGP becomes increasingly criticized, as Matt Green puts it in 2014:

> It’s time for PGP to die.

- 2015
  - XMPP gets end-to-end encryption with the OMEMO (https://en.wikipedia.org/wiki/OMEMO) extension (which re-uses the Signal protocol)
  - SoK: Secure Messaging (http://cacr.uwaterloo.ca/techreports/2015/cacr2015-02.pdf)
  - Moxie - GPG and me (https://moxie.org/blog/gpg-and-me/)
- 2016
  - Filippo Valsorda - I'm giving up on PGP (https://blog.filippo.io/giving-up-on-long-term-pgp/)

    > All in all, I should be the perfect user for PGP. Competent, enthusiast, embedded in a similar community. But it just didn't work.

  - WhatsApp now uses the Signal protocol, adding end-to-end encryption for its billions of users.

Another unexpected development: security professionals are now giving up on encrypted emails, and are moving to secure messaging. Is messaging going to replace email, even though it feels like a different mean of communication?

Moxie's quotes are quite interesting:

> In the 1990s, I was excited about the future, and I dreamed of a world where everyone would install GPG. Now I'm still excited about the future, but I dream of a world where I can uninstall it.

> In addition to the design philosophy, the technology itself is also a product of that era. As Matthew Green has noted, "poking through an OpenPGP implementation is like visiting a museum of 1990s crypto." The protocol reflects layers of cruft built up over the 20 years that it took for cryptography (and software engineering) to really come of age, and the fundamental architecture of PGP also leaves no room for now critical concepts like forward secrecy.

> In 1997, at the dawn of the internet's potential, the working hypothesis for privacy enhancing technology was simple: we'd develop really flexible power tools for ourselves, and then teach everyone to be like us. Everyone sending messages to each other would just need to understand the basic principles of cryptography. [...]

> The GnuPG man page is over sixteen thousand words long; for comparison, the novel Fahrenheit 451 is only 40k words. [...]

> Worse, it turns out that nobody else found all this stuff to be fascinating. Even though GPG has been around for almost 20 years, there are only ~50,000 keys in the "strong set," and less than 4 million keys have ever been published to the SKS keyserver pool ever. By today's standards, that's a shockingly small user base for a month of activity, much less 20 years.

- 2018
  - the first draft of **Messaging Layer Security (MLS)** is published, a standard for end-to-end encrypted group chat protocols.
  - EFAIL (https://efail.de/) releases damaging vulnerabilities against most popular PGP and S/Mime implementations.

    > In a nutshell, EFAIL abuses active content of HTML emails, for example externally loaded images or styles, to exfiltrate plaintext through requested URLs. To create these exfiltration channels, the attacker first needs access to the encrypted emails, for example, by eavesdropping on network traffic, compromising email accounts, email servers, backup systems or client computers. The emails could even have been collected years ago.

- 2019 - Latacora - The PGP Problem (https://latacora.micro.blog/2019/07/16/the-pgp-problem.html)

> Why do people keep telling me to use PGP? The answer is that they shouldn't be telling you that, because PGP is bad and needs to go away.

EFAIL is the straw that broke the camel's back. PGP is officially dead.

- 2019
  - Matrix is out of beta and working on making end-to-end encryption the default.
  - Moxie gives a controversial talk at CCC (https://peertube.co.uk/videos/watch/12be5396-2a25-4ec8-a92a-674b1cb6b270) arguing that advancements in security, privacy, censorship resistance, etc. are incompatible with slow moving decentralized protocols. Today, most serious end-to-end encrypted messaging apps use the Signal protocol (Signal, Facebook Messenger, WhatsApp, Skype, etc.)
  - XMPP's response: Re: the ecosystem is moving (https://blog.jabberhead.tk/2019/12/29/re-the-ecosystem-is-moving/)
  - Matrix's response: On privacy versus freedom (https://matrix.org/blog/2020/01/02/on-privacy-versus-freedom/)

> Well done! You've reached the end of my post. Now you can leave me a comment or read something else.

Here are some random **popular** articles:

- How did length extension attacks made it into SHA-2? (/article/417/how-did-length-extension-attacks-made-it-into-sha-2/)
- Speed and Cryptography (/article/468/speed-and-cryptography/)
- What is the BLS signature scheme? (/article/472/what-is-the-bls-signature-scheme/)
- Zero'ing memory, compiler optimizations and memset_s (/article/419/zeroing-memory-compiler-optimizations-and-memset_s/)
- The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations (/article/461/the-9-lives-of-bleichenbachers-cat-new-cache-attacks-on-tls-implementations/)
- How to Backdoor Diffie-Hellman: quick explanation (/article/360/how-to-backdoor-diffie-hellman-quick-explanation/)
- Tamarin Prover Introduction (/article/404/tamarin-prover-introduction/)

Here are some random **recent** articles:

- Disco: whitepaper (/article/475/disco-whitepaper/)
- Libra: a usable cryptocurrency (/article/480/libra-a-usable-cryptocurrency/)
- Authentication What The Fuck: Part II (/article/494/authentication-what-the-fuck-part-ii/)
- What Are Short Authenticated Strings (SAS)? (/article/493/what-are-short-authenticated-strings-sas/)
- Difference between shamir secret sharing (SSS) vs Multisig vs aggregated signatures (BLS) vs distributed key generation (dkg) vs threshold signatures (/article/486/difference-between-shamir-secret-sharing-sss-vs-multisig-vs-aggregated-signatures-bls-vs-distributed-key-generation-dkg-vs-threshold-signatures/)
- On Doing Research (/article/469/on-doing-research/)
- Hardware Solutions To Highly-Adversarial Environments Part 2: HSM vs TPM vs Secure Enclave (/article/500/hardware-solutions-to-highly-adversarial-environments-part-2-hsm-vs-tpm-vs-secure-enclave/)

Comments

Claudi

Slightly OT but for clarification: PGP may be on the way out for encryption; it's still perfectly fine though to digitally sign files and Git commits.

cicero

Awesome - thank you...

roger

These anti PGP articles keep bewildering me. PGP is used by nation states, corporations, journalists, students, activists, their mum, dad and their dog.

2019 saw the launch of https://keys.openpgp.org a hugely successful new key server giving users much improved control over their data and allowing for verification of email addresses. As only one valid entry per email can exists this also solves a lot of trouble that could arise on the old key servers if users were unable to revoke a secret key of theirs for whatever reasons.

PGP is very alive and interesting things are happening. Sequoia is actively developed. I am pretty sure it will remain an evolving space.

villeneuve

No word on AutoCrypt!?!

david

forgot about the SKS stuff: https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f

Leave a comment

Your name

Enter name

Do you have a homepage?

This information will be displayed

Capital of Italy? (antispam)

Enter antispam

Text

Enter text

Post

Thanks for reading! Need to tell me something? Contact me (/contact)