PGP blues – a quick review of a computer science malaise.

Camille Akmut

August 7, 2019

Abstract

Bibliography with accompanying material : important debates around PGP, its purported failings as well as newer protocols such as OTR and Signal.

Intro

“– *This is ridiculous. This has gone far enough. (...)*
We’re in the middle of nowhere!
– *There is no ‘middle of nowhere’ any more.*”

Hard to use, hard to understand¹, ‘[horror] museum’ even! –

PGP has no shortage of critics, under continuous assault now for about two decades.

Its detractors emphasize perfect forward secrecy and deniability, among others.

This publication aims to provide an entry point into these discussions.

It makes available a bibliography together with excerpts, notes and a timeline.

In various places, terms such as “*future secrecy*” or “*post-compromise security*” are found instead of forward secrecy, for example²; in others “*backtracking resistance*” is used still instead³!

Elsewhere, we are assured that “*asymmetric cryptography*” has long replaced the outdated category of “*public-key cryptography*”⁴, though doubts remain as to whether this represents a true consensus...

—
These computer scientists seemingly cannot agree on a common terminology, and have yet to do so. Their science, a young one...

These are some of the great debates of our times.

¹The two former points are mentioned by Ian Goldberg for instance, as general challenges of cryptography research, and properties of cryptographic systems, first. Soon the main target however becomes obvious : PGP! (See Goldberg 2007.)

²They refer to the same property, as far as is known to us.

³*Serious Cryptography*.

⁴“Over time terminology has shifted: now public key cryptography is mostly called “asymmetric cryptography” and public keys are more often called “public certificates”” (Hansen 2019).

From PGP to OTRv4 (1991-2019)

*1991 : Introduction of PGP (Phil Zimmermann). Proprietary.

*1997 : Introduction of GPG (Werner Koch). Free software.

— Koch, Werner. 2007. “A Short History of the GNU Privacy Guard”.

“It’s been a decade now that the very first version of the GNU Privacy Guard has been released. This very first version was not yet known under the name of GnuPG but dubbed “g10” as a reference on the German constitution article on freedom of telecommunication (Grundgesetz Artikel 10) and as a pun on the G-10 law which allows the secret services to bypass these constitutional guaranteed freedoms.

Version 0.0.0 released on December 20th 1997, was a barely working replacement of PGP avoiding all patented algorithm by using Elgamal and Blowfish instead of RSA and IDEA.”

*2004 : Introduction of OTR (Nikita Borisov, Eric Brewer, Ian Goldberg).

— Borisov, Nikita, Brewer, Eric and Goldberg, Ian. 2004. “Off-the-Record Communication, or, Why Not To Use PGP”.

“Quite often on the Internet, cryptography is used to protect private, personal communications. However, most commonly, systems such as PGP are used, which use long-lived encryption keys (subject to compromise) for confidentiality, and digital signatures (which provide strong, and in some jurisdictions, legal, proof of authorship) for authenticity.

In this paper, we argue that most social communications online should have just the opposite of the above two properties; namely, they should have *perfect forward secrecy* and *repudiability*. We present a protocol for secure online communication, called “off-the-record messaging”, which has properties better-suited for casual conversation than do systems like PGP or S/MIME. We also present an implementation of off-the-record messaging as a plugin to the Linux GAIM instant messaging client. Finally, we discuss how to achieve similar privacy for high-latency communications such as email.”

— Goldberg, Ian. 2007. “Off-the-Record Messaging: Useful Security and Privacy for IM”.

*2013/14 (?) : Introduction of Signal as TextSecure (Trevor Perrin, Moxie Marlinspike).

“The TextSecure encrypted messaging protocol is derivative of OTR Messaging. The major difference being the use of ECC keys instead of standard DSA (...)”⁵

— Marlinspike, Moxie. 2014. “GPG And Me”.

“There just seems to be something particular about people who try GPG and conclude that its a realistic path to introducing private communication in their lives for casual correspondence with strangers.”

— Green, Matthew. 2014. “What’s the matter with PGP?”.

“a museum of 1990s crypto”

Note : https://en.wikipedia.org/wiki/Matthew_D._Green

*2015 : *ProPublica* article reveals “one guy” is working on GPG, and that person – Werner Koch – is “going broke”. To wide schock.

— Walfield, Neal. 2016. “Op-ed: Why I’m not giving up on PGP”.

“Signal can’t replace PGP.”

⁵Presumably elliptic curve cryptography and Digital Signature Algorithm respectively.

Note : Walfield is a former GPG contributor, currently working on a new OpenPGP implementation called Sequoia (in Rust).

— Cohn-Gordon et al.. 2016. “A Formal Security Analysis of the Signal Messaging Protocol”.

“The Signal protocol is a cryptographic messaging protocol that provides end-to-end encryption for instant messaging in WhatsApp, Wire, and Facebook Messenger among many others, serving well over 1 billion active users. Signal includes several uncommon security properties (such as “future secrecy” or “post-compromise security”), enabled by a novel technique called *ratcheting* in which session keys are updated with every message sent. (...)

We conduct a formal security analysis of Signal’s initial extended triple Diffie-Hellman (X3DH) key agreement and Double Ratchet protocols as a multi-stage authenticated key exchange protocol. (...)

We have found no major flaws in the design (...) of this widely adopted protocol. (...)

In this work we provided the first formal security analysis of the cryptographic core of the Signal protocol.”

— Bini, Ola and Celi, Sofia. 2018. “No evidence of communication: Off-The-Record Protocol version 4”.

“the 4th version of the OTR protocol provides stronger deniability than all current secure messaging protocols in use, such as OTRv3 and Signal. (...)

the purpose of OTRv4 is to provide an up-to-date protocol that provides no convincing cryptographic evidence that a conversation took place. (...) To achieve this property -known as forgeability- we use XSalsa20”

— Gillmor, Daniel. 2019. “OpenPGP Certificate Flooding”.

“My public cryptographic identity has been spammed to the point where it is unusable in standard workflows.”

Note : Debian contributor, ACLU technologist.

— Hansen, Robert. 2019. “SKS Keyserver Network Under Attack”.

“In the last week of June 2019 unknown actors deployed a certificate spamming attack against two high-profile contributors in the OpenPGP community ([self] and Daniel Kahn Gillmor”

Note : GPG contributor.

References

(in order of appearance)

- <https://lists.gnupg.org/pipermail/gnupg-announce/2007q4/000268.html>
- <https://otr.cyberpunks.ca/otr-wpes.pdf>
- [/watch?v=uI1x-z5oafc](#)
- <https://web.archive.org/web/20150107094950/https://github.com/WhisperSystems/TextSecure/wiki/Protocol>
- <https://moxie.org/blog/gpg-and-me/>
- <https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/>
- <https://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-w>
- <https://arstechnica.com/information-technology/2016/12/signal-does-not-replace-pgp/>
- <https://eprint.iacr.org/2016/1013.pdf> ('Extended Version, July 2019')
- <https://petsymposium.org/2018/files/hotpets/7-bini.pdf>
- <https://dkg.fifthhorseman.net/blog/openpgp-certificate-flooding.html>
- <https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f>