Crypto 2019

Bill’s annual crypto rants for 2019

News in review

- HistoCrypt2018/2019 - New historical confeence in europe
- Hill-climbing/annealing cracking more and more classical ciphers.
- FireFox expired! - addon signing key expired
- Debian Buster has LUKS2 (new install only)
- Google Releases Basic Homomorphic Encryption Tool(Schneier)

News 2 – Oopsie

- WhatsApp had horrid vuln, but fixed (Schneier)
- Yubikey recalls keys due to bug (Schneier)
- Two recent Russian Encryption Algorithms have flawed S-box that look like backdoor. (Schneier)
- Gov't proposed mandatory backdoord remain bad idea (Schneier)

Other sources – Security Now!, SANS ISC

Better Practices (1)

- Picking a password store

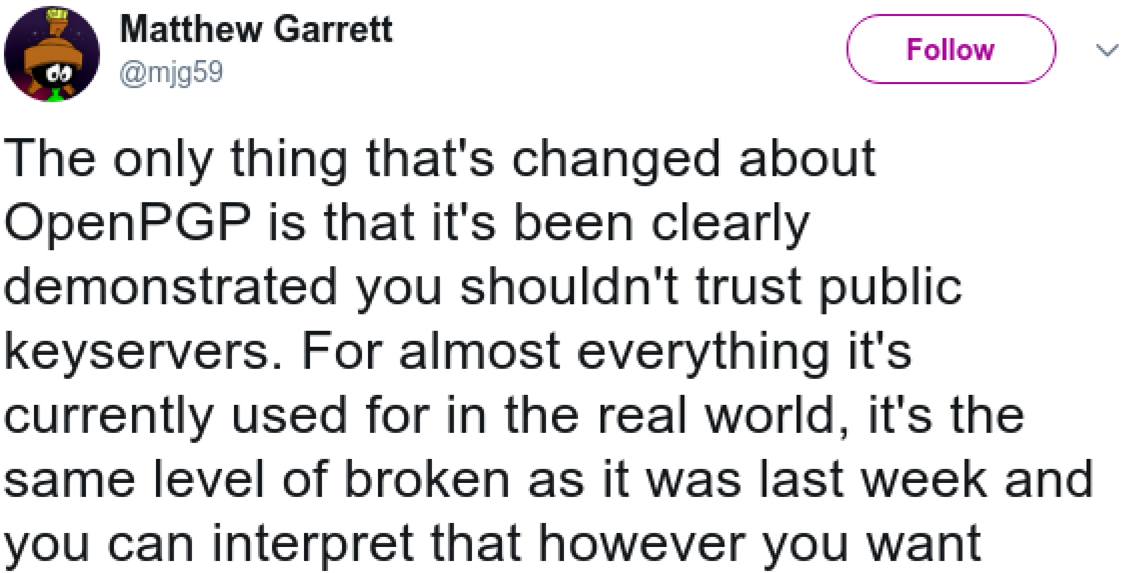
  https://medium.com/@stuartschechter/before-you-use-a-password-manager-9f5949ccf168
-

Better (2): PGP Safety

- "Operational PGP" -- PGP for serious OpSec
  - Not for most people
  - https://gist.github.com/grugq/03167bed45e774551155
- "Using OpenPGP subkeys in Debian development"
  - https://wiki.debian.org/Subkeys
- Deadman switch with web of trust
  - Expiry year, and extended every say 6 months !
- **Don’t use Public Keystores.**

PGP Update

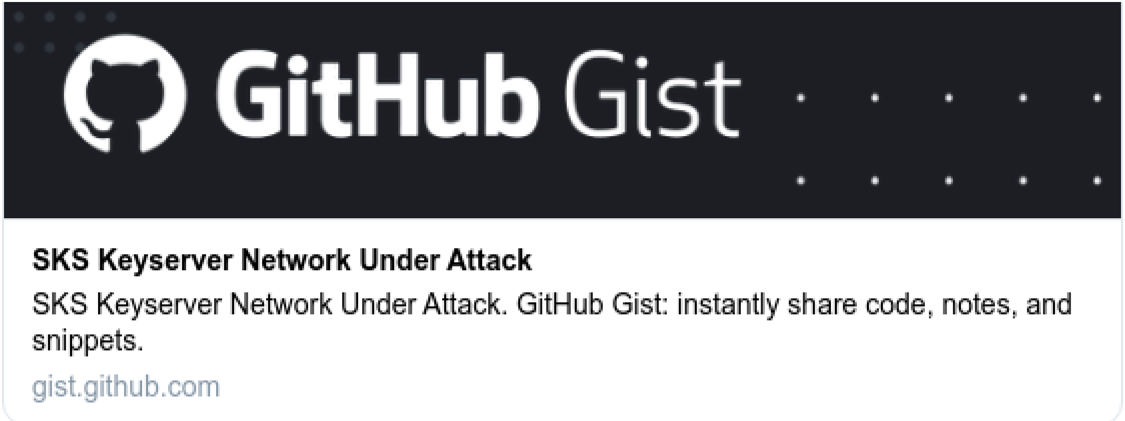
- https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f



Matthew Garrett
@mjg59

The only thing that's changed about OpenPGP is that it's been clearly demonstrated you shouldn't trust public keyservers. For almost everything it's currently used for in the real world, it's the same level of broken as it was last week and you can interpret that however you want

2:16 PM - 29 Jun 2019



SKS Keyserver Network Under Attack

SKS Keyserver Network Under Attack. GitHub Gist: instantly share code, notes, and snippets.

gist.github.com

Why all the PGP h8?

- The Math is fine. (At least for now.)
- The support-all-use-cases UX is terrible.
  - Why don’t HR, Banker, Contracts office have PGP?
  - Which can result in crypto fails as well as just fail fails.
  - Normal people need fit-for-purpose tools not Legos™
- Can’t replace a flawed magic hammer with another single magic hammer

Alternatives

- https://blog.gtank.cc/modern-alternatives-to-pgp/
- Everything depends on threat model
  - Threat Model is (partly) different per mode
  - Is your opponent
    - The auditor / avoiding data breach
    - A hostile nation-state with massive intel budget
    - A police-state with unrestained ethics
    - Nosy journalists
    - Your sister/boss/sysop

Alternatives - Email

- Modern email supports point-to-point secure delivery
  - secures meta-data better than PGP;
  - encrypted in transit, but not at rest, may be good enough depending on threat model/regulatory
- Put sensitive content in an encrypted attachment
- Or, specialized vendor – often for Corp use, where Audit access to secured emails required and/or easy interface needed for support staff

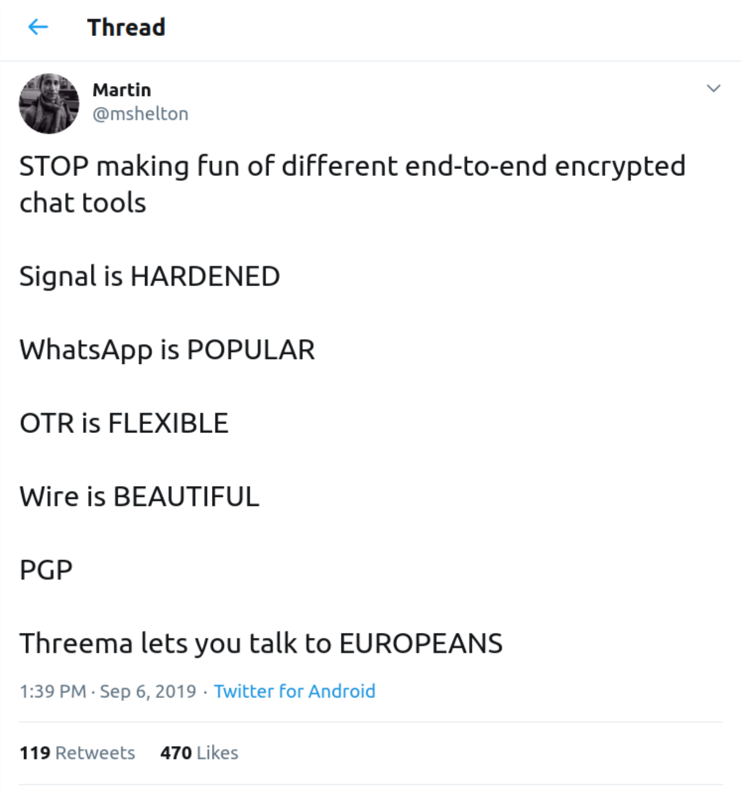
Alternatives – files/attachments

- Password on a ZIP
  - usually weak encryption,
  - sometimes good enough (check threat model)
  - most people have the software already
- Cloud
  - Keybase Filesystem

- Magic-wormhole - send file interactively (like chat)
  - Weak password + interaction = strong; live > store’n’forward
  - Uses Rendezvous, PAKE
    - Password
Authenticated
Key
Excange
=> out-of-band horse-stapler passphrase
  - http://www.lothar.com/~warner/MagicWormhole-PyCon2016.pdf

Alternatives - Chat

- Secure chat E2E easier to automate key management securely than eMail
- Stream (vs store’n’forward) avoids issues
- Choices
  - Add “keybase chat”



Thread

Martin
@mshelton

STOP making fun of different end-to-end encrypted chat tools

Signal is HARDENED

WhatsApp is POPULAR

OTR is FLEXIBLE

Wire is BEAUTIFUL

PGP

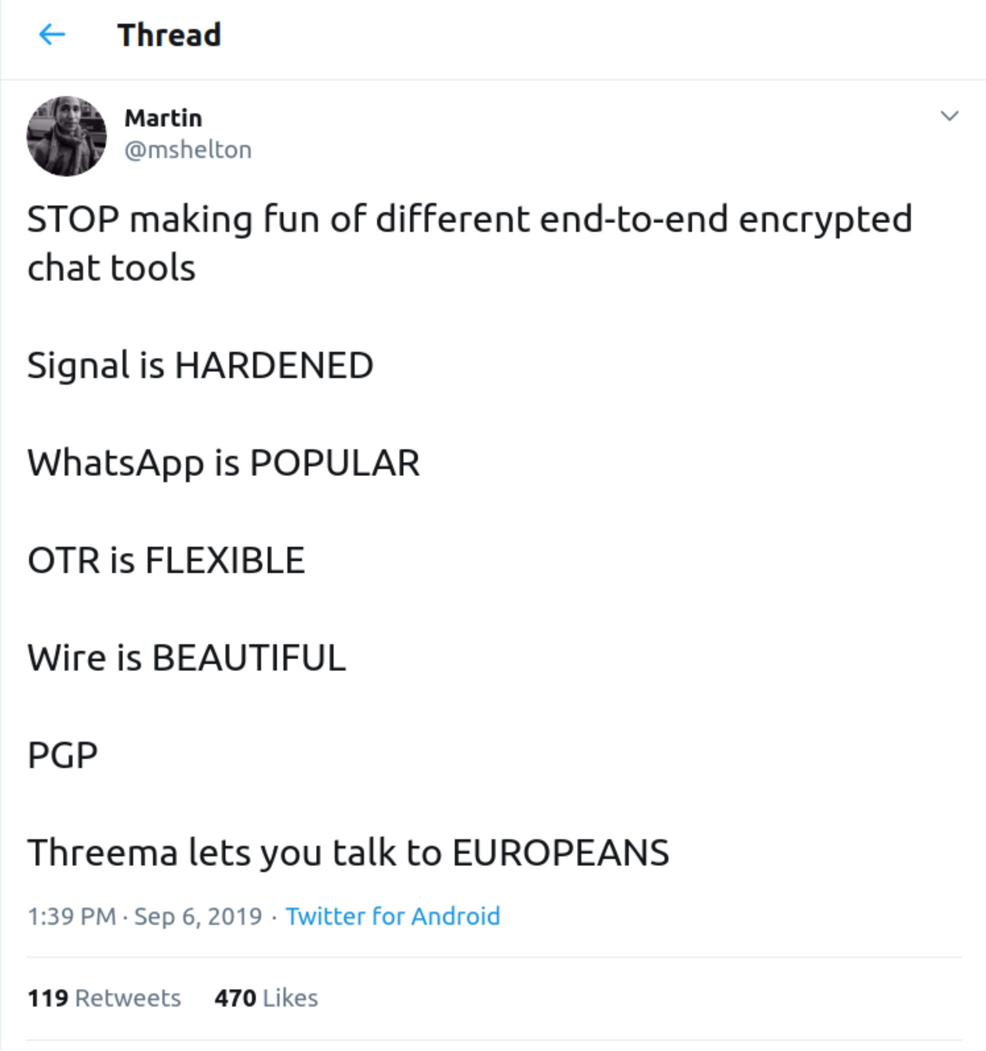
Threema lets you talk to EUROPEANS

1:39 PM · Sep 6, 2019 · Twitter for Android

119 Retweets 470 Likes

(chat)

- https://twitter.com/mshelton/status/1170028705378263041



Martin
@mshelton

STOP making fun of different end-to-end encrypted chat tools

Signal is HARDENED

WhatsApp is POPULAR

OTR is FLEXIBLE

Wire is BEAUTIFUL

PGP

Threema lets you talk to EUROPEANS

1:39 PM · Sep 6, 2019 · Twitter for Android

119 Retweets **470** Likes

Alternatives: Blobs

- Secured Data blobs on disk or in cloud
  - nacl/box
  - nacl/secretbox.
  - Keybase saltpack (NACL usecase packaging)

Alternatives: Key Server

- Keybase.io
- Put key hash in .sig and key on personal site

Alternatives: Signed software

- e.g. Debian packages
- Last use to get alternatives; largest de facto use of PGP; but no longer alternate free.
- OpenBSD has signify & minisign (uses ED25519
- The Update Framework (TUF) provides Notary service

Now for Irony

- Having told you why not to use PGP and what to switch to, now we’ll sign some PGP keys :-D