25 Jahre später verschlüsselt Johnny immer noch nicht

Jens Kubieziel
<jens@kubieziel.de>

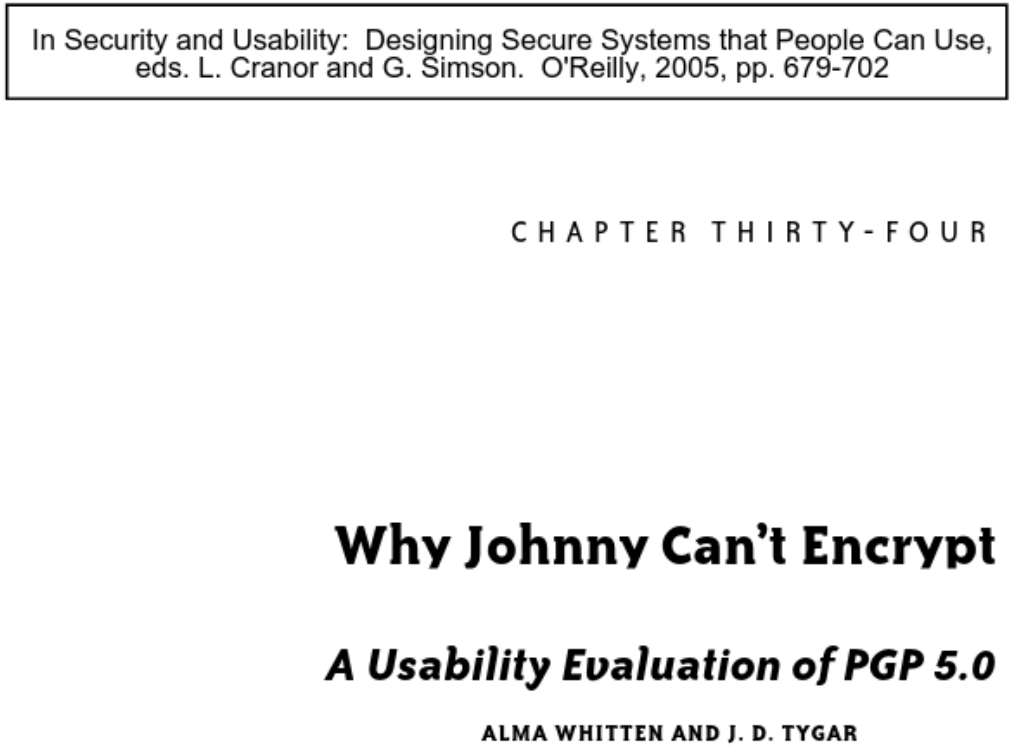
23. März 2025

Wer?

- Jens Kubieziel
- Anonymität, IT-Sicherheit, Netzpolitik
- Kontakt:
  - Mastodon: @qbi@freie-re.de
  - Matrix: @qbi:matrix.kraut.space
  - Anderes über die aufgelisteten Kommunikationswerkzeuge

Outline

Why Johnny can't encrypt


In Security and Usability: Designing Secure Systems that People Can Use, eds. L. Cranor and G. Simson. O'Reilly, 2005, pp. 679-702

CHAPTER THIRTY-FOUR

Why Johnny Can't Encrypt

A Usability Evaluation of PGP 5.0

ALMA WHITTEN AND J. D. TYGAR

https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/index.html

Why Johnny still, still can't encrypt

Why Johnny Still, Still Can't Encrypt:
Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isrl.byu.edu, {zappala, seamons} @ cs.byu.edu

https://arxiv.org/abs/1510.08555

PGP vs. OpenPGP vs. GnuPG

Pretty Good Privacy (PGP) wurde von Phil Zimmermann geschaffen und irgendwie nach Europa exportiert. Später entstand aufgrund einer Förderung der Bundesregierung GnuPG. Dazu gibt es den OpenPGP als Standard (RFC 4880).

Was wird mit GnuPG alles gemacht?

- Verschlüsseln und Signieren von E-Mails
- Verschlüsseln von Dateien
- Signieren von Software
- Signieren von git-Commits

Das Problem E-Mail

Das Medium E-Mail bietet vielfältige Probl~~Probl~~ Herausforderungen.

- Versand und Empfang (aka Spamhandling)
- Text- vs. HTML-Mails
- Verschlüsselung von Anhängen
- Was ist eigentlich mit dem Betreff einer E-Mail?
- Metadaten
- »Unendlich« lange Speicherung von E-Mails

Das Problem E-Mail

Wie kann man die Probleme mit E-Mails lösen?

Gar nicht

Use Signal!

GnuPG in der Praxis

- Wer hat mal `man gpg` durchgelesen? (ca. 40 Seiten Text)
- Wer hat mal versucht, OpenPGP in Software zu gießen? (Paketlänge, Kompressionsformate etc.)
- Verfallsdatum der Schlüssel
- usw.

Moderne Werkzeuge zum Ersatz

Wenn euch obige Argumente zum Nachdenken gebracht haben, ist die Frage:
Was nutzt man stattdessen?

Doing one thing, well.

Signieren von Softwarepaketen

1. `minisign`
   - `minisign -G`
   - `minisign -Sm datei`
   - `minisign -Vm datei`
2. Sigstore
3. SSH-Signaturen

Signieren von git-Commits

Man kann seine git-Commits auch mittels SSH signieren. Dabei solltet ihr Ed25519-Signaturen verwenden.

- `git config --global gpg.format ssh`
- `git commit`

Gitlab hat eine gute Doku zu SSH-Signaturen.

Software über das Netz übertragen

https://magic-wormhole.readthedocs.io/en/latest/ecosystem.html

Dateien verschlüsseln

- `age-keygen -o datei`
- `age -e rein > raus`
- https://github.com/FiloSottile/age
- https://github.com/FiloSottile/awesome-age

GnuPG?

Mit den obigen Anwendungen lässt sich der Anwendungsbereich durch moderne, einfach zu benutzende und sichere Werkzeuge ersetzen.

Ende

Vielen Dank fürs Zuhören.
Gibt es Fragen?