

GNU Privacy Guard

Funktionsweise und Nutzung

A. Kaiser T. Diebelt

Hochschule für Technik, Wirtschaft und Kultur

15.01.2021

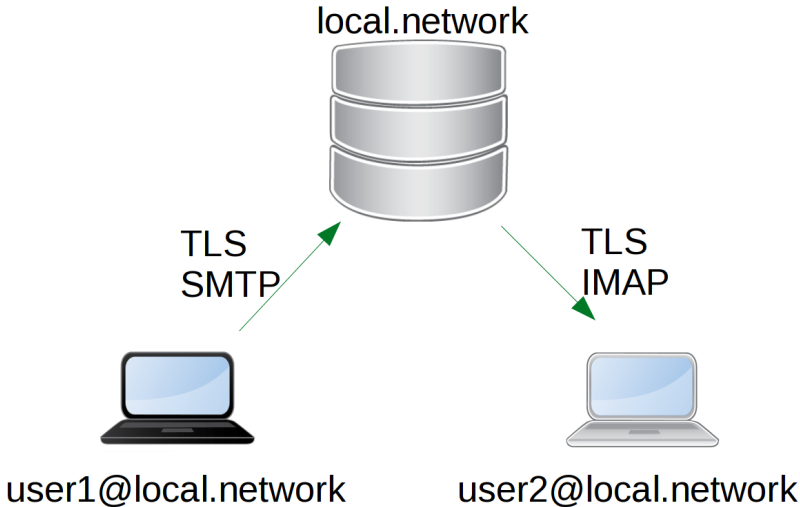
GNU Privacy Guard

- 1 Einleitung
- 2 Funktionsweise
- 3 Betrieblicher Aspekt
- 4 Beispielhafte Verwendung
- 5 Sicherheitsrisiken
- 6 Fazit

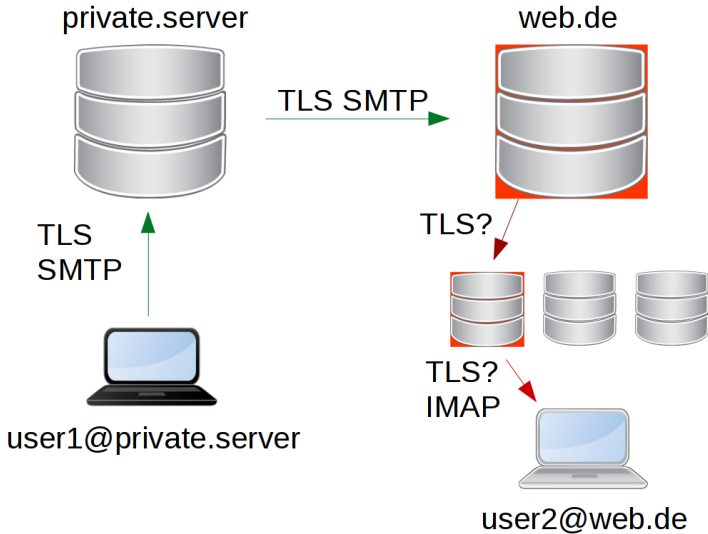
Motivation:

- abhörsichere Kommunikation (gegen Spionage)
- Privatsphäre

Mail-Verkehr im Privaten Netzwerk



Mail-Verkehr mit fremden Servern



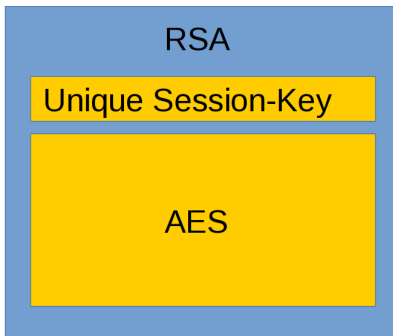
eMail-Versand mit Ende-zu-Ende-Verschlüsselung

- Pretty Good Privacy (PGP)
 - Symantec, 1991
 - Lizenz: Commercial proprietary software
 - OpenPGP standard
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
 - RSA Data Security, 1996
 - Erweiterung des Mail-Standards ('application/pkcs7-mime')

Laut Electronic Frontier Foundation (EFF), Mai 2018:
Kritische Sicherheitslücken, schwer zu beheben ('EFAIL')

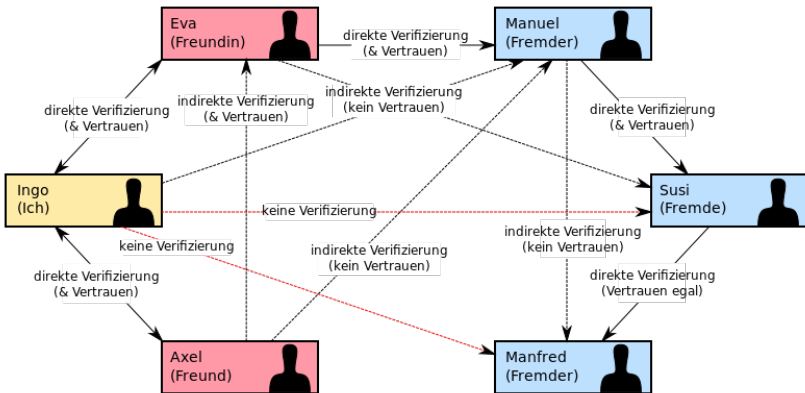
GNU Privacy Guard

- GNU Project, 1999
- Lizenz: GNU GPLv3 (FOSS!)
- Kompatibel mit OpenPGP
- Nutzt Hybrid aus Asymmetrischer und Symmetrischer Verschlüsselung
- Ermöglicht Signierung und/oder Verschlüsselung von Daten



Web-Of-Trust

- Begriffsdeutung



- Differenz zu PKI

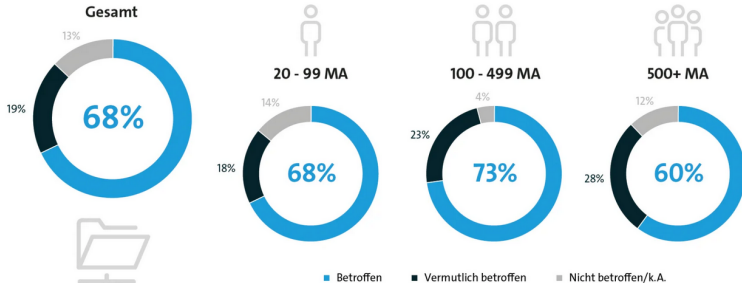
Risiken und Schäden

- WISKOS-Studie 2018: 100 Mrd Schaden
- “Unternehmen sollten E-Mail-Kommunikation auslagern“
- bitkom: mehr 53% der Unternehmen betroffen
- 41% der Informationen über E-Mail erlangt

Betroffene Unternehmen

Mittelständler werden am häufigsten angegriffen

War Ihr Industrieunternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen?



Basis: Alle befragten Unternehmen (n=503)
Quelle: Bitkom Research

bitkom

HTWK

Betroffene Daten

- Allgemeine E-Mails
- Finanzdaten (36%)
- Kundendaten (17%)
- Patente/Forschung (11%)
- Mitarbeiterdaten (10%)

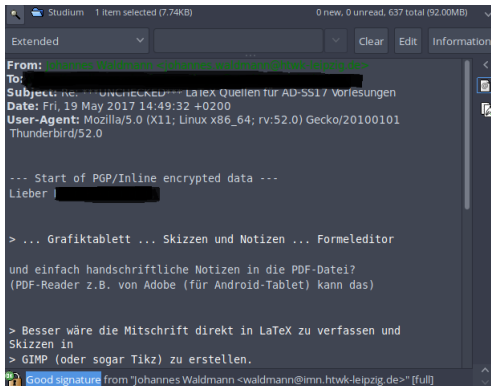
Täter

- ehemalige Mitarbeiter (62%)
- Kunden / Mitbewerber (41%)
- Hobbyhacker (21%)
- organisierte Kriminalität (7%)
- nur 1/3 der Angriffe aus Deutschland

Beispielhafte Verwendung

```
$ gpg --gen-key
```

Nutzung in Mail-Clients



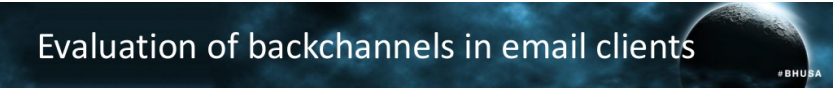
(a) Ansicht im Mail-Client

The screenshot shows the raw source code of the email. It includes the same header as in (a), followed by 'References: <78d1c5a9-ae26-0b44-9c4...>', 'From: Johannes Waldmann <johannes.waldmann@imn.htwk-leipzig.de>', 'Message-ID: <72abcfe2-49a2-026f-81e...>', 'Date: Fri, 19 May 2017 14:49:32 +0200', 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Thunderbird/52.0', 'MIME-Version: 1.0', 'In-Reply-To: <78d1c5a9-ae26-0b44-9c4...>', 'Content-Type: text/plain; charset=utf-8', 'Content-Language: en-MW', 'Content-Transfer-Encoding: 8bit', and 'X-Loop: Forward von [redacted]'. The body text is shown as a single line: '-----BEGIN PGP MESSAGE-----\nCharset: utf-8\nVersion: GnuPG v2\n\nhQIMA6iiEKPCeIxQAQ/+KrCTMEPvzdeYFF8;\nslCscyW6xwolh9fK2DYHgr0cIm/2I9xe7xr\n-----END PGP MESSAGE-----'.

(b) Quellcode

Sicherheitsrisiken

- Nutzer
 - Fehlerhafte Benutzung / Einrichtung
 - Nutzung inkonsequenter E-Mail-Programme



Windows	Outlook IBM Notes	Postbox Foxmail	Live Mail Pegasus	The Bat! Mulberry	eM Client WLMail	W8Mail W10Mail
Linux	Thunderbird Evolution	KMail Trojita	Claws Mutt			
macOS	Apple Mail	Airmail	MailMate			
iOS	Mail App	CanaryMail	Outlook			
Android	K-9 Mail R2Mail	MailDroid Nine				
Webmail	GMail Outlook.com	Yahoo! iCloud	GMX HushMail	Mail.ru FastMail	ProtonMail Mailfence	Mailbox ZoHo Mail
Webapp	Roundcube RainLoop	Horde IMP AfterLogic	Exchange Mailpile	GroupWise		

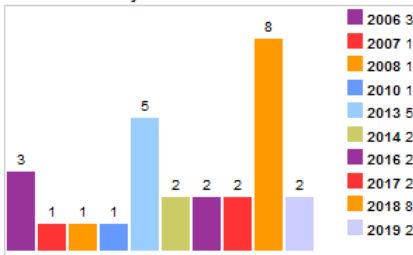
Backchannels found

■ ask user
 ■ leak by default
 ■ leak via bypass
 ■ script execution

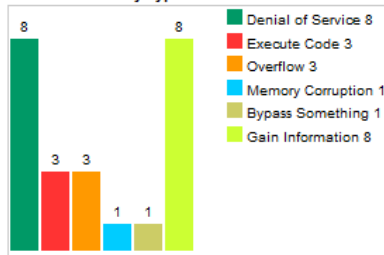
Sicherheitsrisiken

- GnuPG
 - unbekannte Lücken
 - CVE-2016-6313
 - CVE-2017-7526
 - SigSpoof

Vulnerabilities By Year



Vulnerabilities By Type



Sicherheitsrisiken

- Regierungen
 - <https://fm4.orf.at/stories/3008930/>
 - Generalschlüssel für E2E-verschlüsselten Chats

Fazit

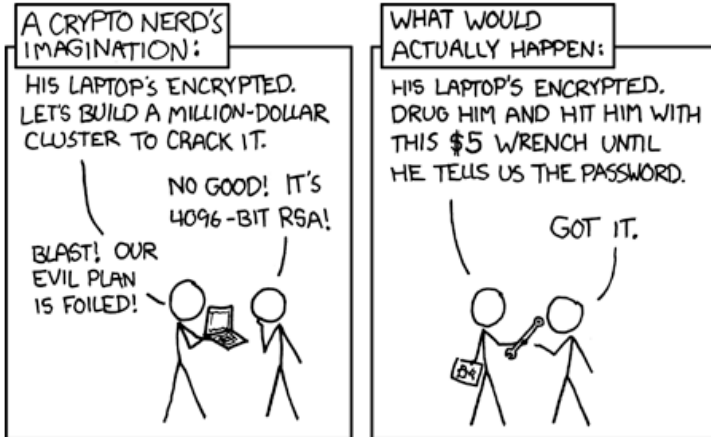
- Betrieblicher Mehrwert:
 - Bei korrekter Anwendung spart man Geld
 - technische Bildung
- Allgemeiner Mehrwert:
 - Privatsphäre
 - Umstieg auf sichere Systeme
 - Schutz vor Überwachungskapitalismus →
<https://www.imn.htwk-leipzig.de/waldmann/talk/19/ubkap/>

Zitat von der Bitkom-Studie

»Gut geschulte Mitarbeiter sind der effektivste Schutz. So lassen sich unbeabsichtigte Schäden vorbeugen, Angriffe von außen werden besser abgewehrt und sind sie doch erfolgreich, lässt sich schnell gegensteuern.«

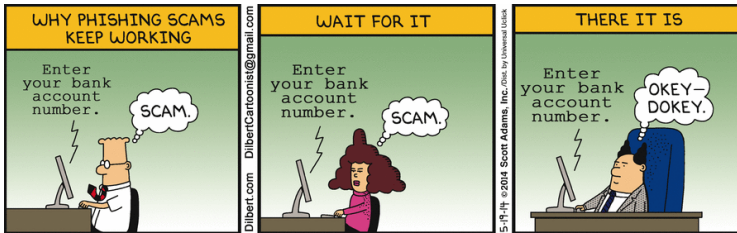
Achim Berg, Bitkom-Präsident, Berlin 2020

Memes



<https://xkcd.com/538/>

Memes



<https://i.pinimg.com/originals/f6/78/7d/f6787d977847056dd8701707d5ba5c5b.gif>

Literaturnachweis I



https://en.wikipedia.org/wiki/Pretty_Good_Privacy



<https://en.wikipedia.org/wiki/S/MIME>



<https://medium.com/@cipherpunk/efail-a-postmortem-4bef2cea4c08>



https://en.wikipedia.org/wiki/GNU_Privacy_Guard



<https://www.slideshare.net/cisoplatfrom7/efail-breaking-smime-and-openpgp-email-encryption-using-exfiltration-channels>



https://media.ccc.de/v/35c3-9463-attacking_end-to-end_email_encryption#t=295



https://de.wikipedia.org/wiki/Datei:Web_of_Trust_2.svg



<https://www.cvedetails.com/vendor/4711/Gnupg.html>

Literaturnachweis II



https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf



<https://www.infopoint-security.de/wirtschaftsspionage-wiskos-studie-beziffert-schaden-bei-kmus-auf-100-mrd/a18166>



<https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/presse/p/20170721-bfv-bitkom-vorstellung-studie-wirtschaftsspionage-sabotage-datendiebstahl>



<https://www.heise.de/news/Terrorbekaempfung-und-Verschluesselung-EU-Rat-forciert-umstrittene-Crypto-Linie-4960069.html>



<https://efail.de/>



<https://wiki.archlinux.org/index.php/GnuPG>