

eMail-Verschlüsselung




Linux Café im BIZ Nürnberg

Raum 4.18

Arno Zeitler (info@amtuxtisch.de)

4.5.2015

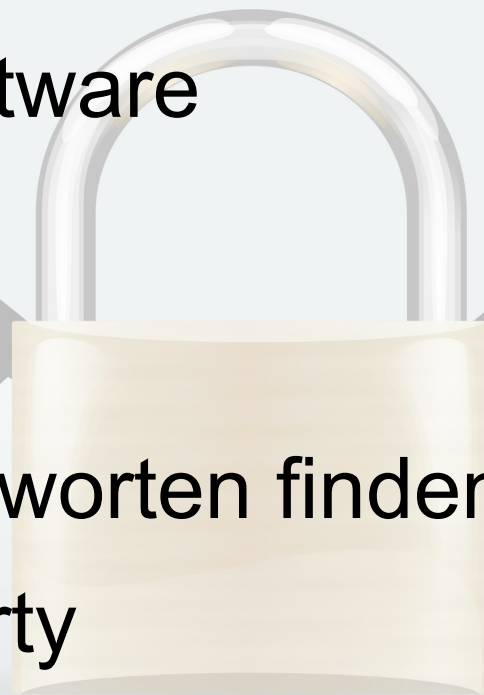
Rechtliches



Sie dürfen dieses Dokument bei Namensnennung verwenden, weitergeben und in veränderter Form unter gleichen Bedingungen nach der internationalen Creative Commons Lizenz 4.0 weitergeben – siehe <https://creativecommons.org/licenses/by-sa/4.0/deed.de>

Heute Abend

- Grundlagen
- Verwendete Software
- Funktionen
- Übungen
- Gemeinsam Antworten finden
- Key-Signing-Party



Grundlagen - Motivation

- Wahrung der Privatsphäre
- Schutz von Informationen gegen
 - Ausspähen → Verschlüsselung(Autorisierung)
 - Sabotage → Signatur(Authentizität/Integrität)
- Erschweren der Massenüberwachung
 - “So viele eMail wie möglich verschlüsseln!”
 - Achtung UNgeschützt: Wer Wann Was mit Wem!

„Privatsphäre ist ein Recht wie jedes andere. Man muss es in Anspruch nehmen, oder man riskiert es zu verlieren.“ Phil Zimmermann

Grundlagen – Techn. Ansätze

- Passwortlösung (reine, symmetrische)
- Server-basierte Verschlüsselung
 - Unternehmen (größere, de-Mail)
 - Behörden
- Public-Key-Infrastructure PKI (https)
 - TrustCenter
 - Streng hierarisch
- SmartCards (Kostenintensiv, sehr sicher)
- Client-basierte Verschlüsselung ← heute Thema
 - Lokale Schlüsselbunde
 - Web of Trust (Unterschriften öff. Schlüssel)
 - Schlüssel-Server (öff. Schlüssel, Replikate weltw.)

Verwendete Software - Übersicht

- GnuPG (Gnu Privacy Guard)
- Enigmail-Plugin für Thunderbird (Mozilla Progs)
- Auf vielen Betriebssystemen
 - unixoide (Linux, Android, xxxBSD, MacOS, Solaris ...)
 - „Exoten“ (VMS, RiscOS, OS/2, ...) und
 - Windows
 - Unterschiedliche Versionen verfügbar
 - Grundsätzl. Interoperabel (OpenPGP, RFCs)

Verwendete Software – Geschichte

- Ursprung 1991: PGP (Pretty Good Privacy)
- Hauptentwickler: Phil Zimmermann
- Open Source (Bürgerbew. <> Geheimdienste)
- Buch „PGP Source Code and Internals“ (Export)
- 1997 Kauf durch NAI (jetzt McAfee)
 - Zeit-/Teilweise Closed Source
 - Verdacht: Additional Decryption Key (ADK)!
- **VERTRAUENSVERLUST!**
- 2002 Rückkauf durch PGP Inc. (Phil Z.)

Verwendete Software – GnuPG I

- GnuPG seit 1997
- Hauptentwickler: Werner Koch
- Quelloffene Alternative kommerz. PGP
- Finanzierung
 - Firma g10Code (Art. 10 GG) „Bitrot“
 - 2012 nur wegen Snowden weiter
 - 2015 Crowdfunding sichert Fortbestand
- „Patentfreie“ Algorithmen
- OpenPGP-Standard (1995, PGP 5)
- Bisher ungebrochen!

Verwendete Software – GnuPG II

- Asymmetrische Schlüsselpaare
 - Sehr große Zahlen math. verquickt
 - Privat NUR unterschreiben / entschlüsseln
 - Öff. NUR verschlüsseln / Unterschrift prüfen
 - Haupt- / Unterschlüssel (n. OpenPGP)
 - Mehrere Benutzkennungen möglich
- Hybride Verschlüsselung
 - zufälliger Sitzungsschlüssel
 - asymmetrische Schlüsselübertragung
 - symmetrische Datenübertragung
- Spez. Prog. zur Passphrase-Eingabe in GUI's

Verwendete Software – Enigmail

- Enigmail seit 2001
- Hauptentwickler: Partick Brunschwig
- Plugin für Thunderbird
- Nutzt GnuPG für Cryptofunktionen
- PGP/inline (RFC 2440, 4880)
- PGP/mime (RFC 3156)
- Bedienoberfläche für
 - Schlüsselverwaltung (generieren, Server, ...)
 - ver- und entschlüsseln
 - unterschreiben und verifizieren

Verwendete Software – Versionen

- GnuPG
 - Ubuntu 14.04.2 LTS = 1.4.16
 - Upgrade auf GnuPG2 (!) 2.0.22 erst mit nächster Enigmail Version notwendig!
 - Unterschiedliche .deb → installieren
- Thunderbird (derzeit 31.6.0)
- Enigmail-Plugin für Thunderbird
 - Ubuntu Repository veraltet / keine Updates
 - Thunderbird → Extras → Add-ons
 - Version 1.8.2

Verwendete Software – Installation

- Ubuntu Software-Center gnupg2 install. (opt)
- Thunderbird (eMail) „Konto einrichten“
- Extras → Add-ons → Suche → Enigmail
- Enigmail Einrichtungs-Assistent
 - „... ausführliche Konfiguration ...“
 - „Schlüsselpaar erzeugen“ - 8 bis 35 Minuten!
 - Import für Übung aus den *.tgz Dateien
- Tutorial:
https://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP
- Installdemo

Funktionen – Schlüssel

- Erzeugen (Schlüsselpaare, Widerrufszeit.)
- Anzeigen (private, öffentliche, „gefiltert“)
 - Schlüsseleigenschaften (Fingerabdruck, ID)
 - Unterschriften
- Importieren / Exportieren
- Schlüsselservers (suchen, hochladen, aktualis.)
- Unterschreiben (öffentlich)
- Besitzervertrauen festlegen (lokal)
- Parameter ändern (Benutzerkennungen, Ablaufdatum, Passphrase, Foto, Empfänger...)

Funktionen – eMails benutzen

- Verfassen (Bedien- / Statusleiste Enigmail)
 - Verschlüsseln
 - Unterschreiben
 - Eigenen öffentl. Schlüssel anhängen
- Empfangen (Statusleiste)
 - Automatische Unterschriftenprüfung
 - ggf. fehlende Schlüssel importieren
 - Entschlüsselung (aut. Passphraseabfr.)
- Simpleste Handhabung

Funktionen – Ablauf techn.

- Text, ggf. Anhänge komprimieren
- Zufälligen Sitzungsschlüssel erzeugen
- Komprimierte Daten damit verschlüsseln
- Ggf. mit privatem Schlüssel Unterschreiben und Signatur hinzufügen
 - Alles oder
 - Einzelne Teile
- Sitzungsschlüssel mit öffentlichem Schlüssel verschlüsseln und hinzufügen
- radix-64 kodieren (head+base64+crc24+foot)
- Senden

Funktionen – Demonstration



Übungen I

- Arbeitsplätze von 01 bis 12 für XX
- Adresse: **enigmaXX.biz@gmx.de**
- Passphrase: EnigmaXX.Geheimnis
- `'mv .thunderbird .thunderbird.orig'`
- `'mv .gnupg .gnupg.orig'`
- `'tar -xvpzf enigmaXX*.tgz'`
- **edward-de@fsf.org** (<https://emailselfdefense.fsf.org/de/> Schritt 3)
 - öffentl. Schlüssel unverschlüsselt senden
 - Edwards Antwort verschlüsselt beantworten
 - Edwards Schlüssel vom Server holen ...

Übungen II

- Öffentlichen Schlüssel auf Server
- Fingerabdruck gegenchecken
- „SitzNachbarn“ eMails schreiben
 - Verschlüsselt
 - Unterschrieben
 - An mehrere Empfänger
- Schlüssel gegenseitig signieren
- Unterschiede beobachten (unsig. / sig. / n-sig.)
- Widerrufszeugnisse erstellen (nicht hochladen)
- Eigene Ideen einbringen ...

Gemeinsam Antworten finden



„Key-Signing-Party“

- Rechner Vertrauenswürdig?! (LiveCD!)
- Echtheit der Person → Ausweisdokument!
- Öffentlichen Schlüssel identifizieren
- Eineindeutig nur via Fingerabdruck!
- Schlüssel unterschreiben
 - von Schlüsselservers laden
 - Unterschreiben
 - auf Schlüsselservers hoch laden
- Abschließende Bitte:
Übungsschlüssel widerrufen – Danke :D

Referenzen

Links:

<https://emailselfdefense.fsf.org/de/>

<https://www.gnupg.org/>

<https://www.mozilla.org/de/thunderbird/>

<https://www.enigmail.net/>

https://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP

<http://www.pgpi.org/>

http://www.selbstdatenschutz.info/e-mail_verschluesseln

<http://www.heise.de/ix/meldung/Befragung-Stand-der-E-Mail-Verschluesselung-ist-desastroses-2243124.html>

<https://de.wikipedia.org/wiki/E-Mail-Verschl%C3%BCsselung>

http://www.bfdi.bund.de/DE/Home/home_node.html