

Free Software and Privacy

(South Thyrol Free Software Conference - Bolzano, 27. November 2004)



Übersicht

- Was ist Freie Software
- Sicherheit und Freie Software
- Anwendungsgebiete
- GnuPG 1 und 2
- Smartcards

Wir sprechen über Freie Software

- "Freie Software" ist leichter verständlich
- Freie Software ist schwieriger zu missbrauchen
- Freie Software ist wohldefiniert
- Freie Software bietet zusätzliche Werte

Die 4 Freiheiten

Freie Software garantiert dauerhaft diese Freiheiten:

- Freiheit 0: Unbegrenzte Nutzung zu jedem Zweck.
- Freiheit 1: Studium und Anpassung an eigene Bedürfnisse.
- Freiheit 2: Weitergabe.
- Freiheit 3: Weitergabe von Modifikationen.

Frei für Freiheit, nicht Preis.

Definition veröffentlicht im Januar

Auguste Kerckhoffs (1835-1903)

"Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi"

(Es ist notwendig, daß das System nicht geheim gehalten wird und ohne Unannehmlichkeiten in die Hände des Feindes fallen kann)

- Im Umkehrschluss fordert man heute, daß das System öffentlich sein muß, damit Schwachstellen besser erkannt werden.
- Es genügt nicht, lediglich öffentliche Algorithmen zu verwenden.
- Nur Freie Software kann dieses Kriterium erfüllen.

Sicherung von Online Verbindungen

Secure Shell

- Remote Access Standard seit fast 10 Jahren
- OpenSSH
- GSTI

Secure Socket Layer (SSL/TLS)

- Web Standard seit 10 Jahren
- OpenSSL
- GNUTLS

IPSec

- Virtual Private Networks Standard
- OpenBSD
- FreeS/WAN
- Linux 2.6 Kernel

Sicherung von Offline Verbindungen

OpenPGP Standard

Email

- GnuPG
- Cryptix

Daten

- GnuPG
- (einfache symmetrische Verschlüsselung)

S/MIME Standard

keine verbreitete Freie Software Lösung

- OpenSSL
- Cryptlib
- GnuPG 2

Der GNU Privacy Guard

- Vollständige Implementation von OpenPGP.
- Sichert Email und gespeicherte Daten.
- Verbindet digitale Signaturen, Verschlüsselung und Schlüsselverwaltung in einer Anwendung.
- Läuft auf allen POSIX Plattformen sowie auf Windows und Mac.
- Flexibel und lange im praktischen Einsatz.
- Verfügbar unter der GNU General Public License (GPL).

Das Ägypten Projekt (GnuPG 2)

- Erweiterung von GnuPG
- Integriert OpenPGP und S/MIME
- Implementierung von Sphinx für POSIX Systeme
- Ein neues Krypto Framework für GNU/Linux.
- Einfache Integration in Mailprogramme.
 - KMail (KDE)
 - Mutt (Text basiert)
 - Sylpheed (in Arbeit)
- Unterstützt Smartcards

GnuPG Made Easy

- Library zur Benutzung von GnuPG

- OpenPGP
- S/MIME

- Verschlüsselung, Signatur, Schlüsselverwaltung

- Bindings für

- Ada
- C++
- Java

- GNU Lesser General Public License

Was sind Smartcards

□ Plastikkarten mit CPU

- 32K EEPROM
- 8/16 Bit CPU
- NPU

□ 3 Typen:

- Speicherkarten
- Symmetrische Verschlüsselung
- Public Key Verschlüsselung

□ Vorteile

- Private Key gesichert
- Ohne physikalische Zugriff nicht kompromittierbar
- Einfacher und sicherer als Password

□ Nachteile

- Kartenleser erforderlich

Smartcard Projekte

Verschlüsselung und Digitale Signaturen

- OpenSSL
- GnuPG 1.4

Login

- Poldi (PAM Modul für OpenPGP Card)
- OpenSC (PAM Modul für PKCS#15 Karten)

Secure Shell

- gpg-agent (Teil von Ägypten)

Weitere Informationen



<http://fsfeurope.org>



<http://www.gnupg.org>



<http://g10code.com>

- Vielen Dank für Ihre Aufmerksamkeit -