PIRATEN
OBERBAYERN

Passwörter und Schlüssel
sichern

PIRATEN
WÄHLEN

WORUM GEHT'S?

* S/MIME
* Gute Passwörter.
* Mehr Sicherheit?

S/MIME VERWENDEN!

- Industriestandard und auf fast jedem Computer bereits ohne
- Zusatzsoftware unterstützt
- basiert auf sog. X.509 Zertifikaten
- X.509 wird auch für SSL (sichere Webverbindungen) und
- Software-Zertifikate genutzt
- Ist inkompatibel mit PGP
- Hauptunterschied: Austausch und Beglaubigung von public keys

PIRATEN WÄHLEN

S/MINE

BEGLAUBIGUNG

- für PGP und S/MIME ist der direkte persönlicher Austausch der public keys am vertrauenswürdigsten
- für indirekte Beglaubigung über Dritte:
- bei PGP: Beglaubigung über mehrere Unterschriften des public keys (web of trust)
- bei S/MIME: Beglaubigung durch eine Unterschrift einer Certificate Authority (CA)
- die Unterschrift der CA kann wiederum von einer Root-CA unterschrieben sein
- alle geprüften (sehr aufwendig und teuer) Root-CA sind den meisten Betriebssystemen bereits bekannt
- daher kann jedes ausgestellte X.509 Zertifikate einer solchen Root-CA sofort überprüft werden

PIRATEN WÄHLEN

X.509 ZERTIFIKATE

- CAs können auch ein eigenes web of trust implementieren (startSSL, CAcert)
- der public key ist im X.509 Zertifikat enthalten und wird idR per Anhang mit versandt
- der Austausch per key server ist unüblich
- besserer Datenschutz, da nur eine CA das Zertifikat beglaubigt und daher kein soziales Netzwerk rekonstruiert werden
- allerdings der Gefahr von Kompromittierung der CA
- übliche Gültigkeitsdauer des Zertifikats daher ca. 1-2 Jahre
- freie einfache X.509 Zertifikate für S/MIME erhältlich über Comodo, startSSL, CAcert (Root CA must installiert werden)

DATEN SICHERN

Es trachten nicht nur Geheimdienste nach deinen Daten.

Pack die wichtigen Sachen in einen Tresor.

PIRATEN WÄHLEN

PASSWÖRTER
ABER SICHER!

Nicht für alles dasselbe Passwort verwenden.
Passwörter nicht teilen.
Gute Passwörter wählen.
Passwörter öfter wechseln.
Passwörter wie PINs behandeln.

Wie soll ich mir das alles bloss merken???

PIRATEN WÄHLEN

GUTE PASSWÖRTER?

Buchstaben, Groß- und Kleinschreibung, Ziffern und Sonderzeichen.

Ganz schlecht: Susanne
Kaum besser: Susanne34, Susanne1979
Besser: Suu_S4ne!
Noch besser: S%v4g!_Gja
Oder sinnlose Wortketten: Bunt gebacken Quartal Spiegel Trambahn

Mein Pferd mag mich, aber dich nicht! Und Hugo?
= MPmm,3dn!UH?

Eselsbrücken?
NYcab%YeLL_0w?
Wieviel Prozent der New Yorker Taxis (Cab) sind gelb?

PIRATEN WÄHLEN

WIE

DENN?

Wo lagert man Passwörter?

Auf kleinen gelben Klebezetteln?
Auf Karteikarten?
In einem Passwortsafe?
Welche Produkte gibt es?

PIRATEN WÄHLEN

PASSWÖRTER AUFBEWAHREN

Für jedes Betriebssystem - auch für Smartphones - gibt es Passwortsafes.

PIRATEN WÄHLEN

PASSWORT TRESORE

Auswahl:

KeePass (Win, Mac, Linux, iOS, Android usw.)
VIM und GnuPG (Linux/Unix)
Password Safe (Windows)

Mitnahme auf USB-Stick o.ä. Sinnvoll.

PIRATEN WÄHLEN

SELBER MACHEN?

Mit GnuPG und VIM:

Gleiches Tool zur Verschlüsselung von Dateien, Mails und Passwörtern.

PIRATEN WÄHLEN

KEY ERSTELLEN

Bitte vorher durch einen Blick ins Verzeichnis ~/.gnupg werfen, ob da schon etwas liegt. Dann kann man sich die nachfolgende Prozedur eventuell sparen.

Erstelle ein GnuPG-Schlüsselpaar MIT PASSPHRASE:

```
Bash $ gpg --gen-key
Type: DSA and Elgamal
Keysize: 2048 bits
Validity: unlimited (key does not expire)
Real Name: Donna Knispel
Email: Donna.Knispel@maildingsbums.de
Comment:
```

KEY-ID FINDEN?

Die eigene Key-ID herausfinden

```
bash$ gpg --list-key
/home/dknispel/.gnupg/pubring.gpg
------------------------------------
pub   1024D/BX7AAVQB 2007-11-07
uid   Donna Knispel <donna.knispel@maildingsbums.de>
sub   2048g/E924D8CB 2007-11-07
```

DATEIEN SICHERN

Datei anlegen und erstmal nur irgendeinen Schlonz reinschreiben

```
bash$ vi geheim
```

Datei verschlüsseln

```
bash$ gpg -e geheim
Geben Sie die User-ID ein.
```

Beenden mit einer leeren Zeile: DEINEKEYID <enter>
(Es wird danach nochmal gefragt, bitte nur ENTER drücken)
Ansehen

```
bash$ ls geheim*
geheim
geheim.gpg
```

VIM NUTZEN

Vi IMproved - enhanced vi editor

Vim-addon-manager

Konfig: .vimrc

```
let g:GPGPreferArmor=1
let g:GPGDefaultRecipients=["nicole.britz@piratenpartei-bayern.de"]
```

Plugin:

```
dyfa@luxor:~/.vim/plugin$ ll
total 8
drwxrwxr-x 2 dyfa dyfa 4096 May 10  2012 ./
drwxrwxr-x 3 dyfa dyfa 4096 Jun 13 21:01 ../
lrwxrwxrwx 1 dyfa dyfa   39 May 10  2012 gnupg.vim ->
   /usr/share/vim-scripts/plugin/gnupg.vim
```

Aufruf: vim geheim.gpg

KEY SIGNING

Warum?

Öffentlichen Schlüssel signieren.
Netzwerk des Vertrauens aufbauen.
“Vertrauenswert” eines Schlüssels verbessern.

Wie?

http://rhonda.deb.at/projects/gpg-party/gpg-party.de.html

Eine Kurzfassung des “Wie” kommt jetzt.

FINGERPRINT ERZEUGEN

Der GPG Fingerprint ist quasi die “Visitenkarte” deines Schlüssels.

```
gpg --fingerprint
/home/dyfa/.gnupg/pubring.gpg
------------------------------
pub   4096R/0BDBA187 2009-09-06
Key fingerprint
= 63F9 F16F D2EE 2948 7757  012C 7773 9BA1 0BDB A187
uid                  Nicole Britz <dyfa@guug.de>
uid                  Nicole Britz <dyfa@addict.de>
uid                  Nicole Britz <nicole@britz.org>
uid                  Nicole Britz <dyfa-pirat@addict.de>
sub   4096R/0FF4F0C0 2009-09-06
```

PIRATEN WÄHLEN

SCHRIFT

ÜBERSCHRIFT

Ausdrucken, damit Leute ihn mitnehmen können:
Auf Zettel, auf Visitenkarten E-Mailadresse dazuschreiben.

PIRATEN WÄHLEN

MEHR?

ÜBERSCHRIFT

Fingerprint vorlesen lassen, mit vorliegendem Ausdruck vergleichen,
Personalausweis zeigen lassen.

Stimmt alles überein?
Dann kannst du den fremden Key signieren.

Demnächst: Key Signing Party

Ankündigung auf http://www.piratenpartei-bayern.de/cryptoparty

PIRATEN WÄHLEN

PRÄSENTIERT

VON

Nicole Britz
@dyfustic
<nicole.britz@piratenpartei-bayern.de>

http://britz.org/

Downloads zum Event:
http://www.piratenpartei-bayern.de/cryptoparty