Keysigning Party

Netzsicherheit Vorlesung

Keysigning: The Party

Was ist eine *Keysigning-Party*?

- Zugrundeliegendes PKI-Modell → Anarchie
  - jeder User ist eine CA
  - Annahme transitiven Vertrauens → Web-of-Trust
- Ziel einer Keysigning-Party
  - viele Benutzer zertifizieren sich gegenseitig

  → Web-of-Trust wird enger geknüpft
    - Wahrscheinlichkeit für Pfadfindung im Web-of-Trust erhöht

Keysigning-Party: Nächste Woche nach der Vorlesung!

Zertifizierung PGP-Keys

Vorbereitung

1. Schlüssel erzeugen

- PGP/GnuPG installieren, Schlüsselpaare erzeugen
  - Liste von verfügbarer Software: http://www.pgpi.org/download/
  - Binaries von GnuPG: http://www.gnupg.org/download
  - Anleitung für GnuPG: http://hp.kairaven.de/pgp/gpg/index.html
  - `> gpg --gen-key`
  - `> gpg --list-keys`

2. Öffentlichen Schlüssel auf Keyserver hochladen

- Verbreitung (kann nicht rückgängig gemacht werden!=
- `> gpg --keyserver ldap://keyserver.pgp.com --send-keys [key_id]`

3. Fingerprint ausdrucken

- Schlüssel wird durch einen Hash-Wert identifiziert
  - `gpg --fingerprint KeyID`
- Fingerprint auf kleinen Zetteln mehrfach drucken und mitnehmen
  - jeder Teilnehmer kriegt Fingerprint jedes anderen Teilnehmers

4. Ausweis mitbringen

Beispiel des auszudruckenden Zettels

Key auf Keyserver hochladen und z.B. hier ausgeben lassen:

http://www.rubin.ch/pgp/searchkey.html
http://wwwkeys.de.pgp.net/

Achtung, „Show the fingerprints“ auswählen

Search results for 'schoeller marcus'

```
Type bits/keyID     cr. time   exp time   key expir
------------------------------------------------------------------------------
pub  1024D/912E88B8 2003-10-22
         Hash=11DC1973923438F7701B05DFDC1CEF59
         Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid Marcus Schöller <marcus.schoeller@tm.uka.de>
sig  sig3  912E88B8 2003-10-22 __________ __________ [selfsig]
sig  sig3  57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig  sig   2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub  1024g/2B728CDD 2003-10-22
sig sbind  912E88B8 2003-10-22 __________ __________ []
```

Beispiel des auszudruckenden Zettels

```
pub   1024D/912E88B8 2003-10-22
           Hash=11DC1973923438F7701B05DFDC1CEF59
           Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig   sig3   912E88B8 2003-10-22 __________ __________ [selfsig]
sig   sig3   57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig   sig    2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub   1024g/2B728CDD 2003-10-22
sig sbind   912E88B8 2003-10-22 __________ __________ []
-----------------------------------------------------------------------------------------------------
pub   1024D/912E88B8 2003-10-22
           Hash=11DC1973923438F7701B05DFDC1CEF59
           Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig   sig3   912E88B8 2003-10-22 __________ __________ [selfsig]
sig   sig3   57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig   sig    2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub   1024g/2B728CDD 2003-10-22
sig sbind   912E88B8 2003-10-22 __________ __________ []
-----------------------------------------------------------------------------------------------------
pub   1024D/912E88B8 2003-10-22
           Hash=11DC1973923438F7701B05DFDC1CEF59
           Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig   sig3   912E88B8 2003-10-22 __________ __________ [selfsig]
sig   sig3   57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig   sig    2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub   1024g/2B728CDD 2003-10-22
sig sbind   912E88B8 2003-10-22 __________ __________ []
-----------------------------------------------------------------------------------------------------
pub   1024D/912E88B8 2003-10-22
           Hash=11DC1973923438F7701B05DFDC1CEF59
           Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig   sig3   912E88B8 2003-10-22 __________ __________ [selfsig]
sig   sig3   57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig   sig    2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub   1024g/2B728CDD 2003-10-22
sig sbind   912E88B8 2003-10-22 __________ __________ []
-----------------------------------------------------------------------------------------------------
pub   1024D/912E88B8 2003-10-22
           Hash=11DC1973923438F7701B05DFDC1CEF59
           Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig   sig3   912E88B8 2003-10-22 __________ __________ [selfsig]
sig   sig3   57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig   sig    2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub   1024g/2B728CDD 2003-10-22
sig sbind   912E88B8 2003-10-22 __________ __________ []
-----------------------------------------------------------------------------------------------------
pub   1024D/912E88B8 2003-10-22
           Hash=11DC1973923438F7701B05DFDC1CEF59
           Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig   sig3   912E88B8 2003-10-22 __________ __________ [selfsig]
sig   sig3   57B4026D 2005-05-14 __________ __________ Achim Hof <hof@tm.uka.de>
sig   sig    2710DA48 2005-08-10 __________ __________ Lars Voelker (University) <lars@tm.uka.de>

sub   1024g/2B728CDD 2003-10-22
sig sbind   912E88B8 2003-10-22 __________ __________ []
```

Ablauf

- Hier, nach der Vorlesung
  1. alle Teilnehmer stellen sich in eine Reihe
  2. jeweils Erste läuft an dieser Reihe vorbei
  3. jeder in der Reihe prüft dessen Ausweis und notiert auf Fingerprint-Zettel, dass Zuordnung geprüft wurde

Person =? Bild

Name =? uid

```
pub  1024D/912E88B8 2003-10-22
     Hash=11DC1973923438F77C1B05DFDC1CEF59
     Fingerprint=7A42 B433 C81B 25E6 17B5  85E2 0393 36C5 912E 88B8

uid  Marcus Schöller <marcus.schoeller@tm.uka.de>
sig  sig3  912E88B8 2003-10-22 _____ _____ [selfsig]
sig  sig3  57B4026D 2005-05-14 _____ _____ Achim Hof <hof@tm.uka.de>
sig  sig   2710DA48 2005-08-10 _____ _____ Lars Voelker (University) <lars@tm.uka.de>

sub  1024g/2B728CDD 2003-10-22
sig sbind  912E88B8 2003-10-22 _____ _____ []
```

Nachbereitung

Später, zu Hause

- Für jeden Zettel welcher validiert wurde
  - Schlüssel herunterladen
    - `> gpg --keyserver ldap://keyserver.pgp.com --recv-keys [key_id]`
  - Fingerprint ausgeben lassen, uid und Fingerprint prüfen
    - `> gpg --fingerprint [key_id]`
  - Signieren des PGP-Schlüssels

    `> gpg --sign-key [key_id]`
  - Signierten Schlüssel an Besitzer schicken (besser als direkt auf Keyserver hochladen)
    - `> gpg --export -a KeyID | mail -s "Your signed key" user@example.com'`

Informationen

Viele Informationen im Web

- Komprimiert
  - http://keysigning.org/methods/adhoc
  - http://commandline.org.uk/command-line/ten-steps-for-attending-a-keysigning-party/
- Ausführliche mit viel Hintergrundinformation
  - http://cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html

Fragen zum Keysigning?