Einführung gpg

Felix 'kro' Krohn <felix@kro.hn>

gpg: 0xC0ED0C8D4AF209DE

5. Mai 2016

about:

- Felix Krohn
- damals: Computer Networking
- jetzt: sysadmin @ OVH

shameless plug: OVH

- dedizierte server, IaaS, VPS, public cloud
- webhosting, domains
- hubic, ...

Übersicht

Auth... *WAS?*

- Authorisierung: Einräumen von Rechten
- Authentifizierung (<=> Authentisierung)
- Überprüfung der Authentizität

Auth... *WAS?*

- Authorisierung: Einräumen von Rechten
- Authentifizierung (<=> Authentisierung)
- Überprüfung der Authentizität

Asymmetrische Verschlüsselung

- private/public key
- Public key: Verschlüsseln, Signatur prüfen
- Private key: Entschlüsseln, Signieren

Asymmetrische Verschlüsselung

- private/public key
- Public key: Verschlüsseln, Signatur prüfen
- Private key: Entschlüsseln, Signieren

Asymmetrische Verschlüsselung

- private/public key
- Public key: Verschlüsseln, Signatur prüfen
- Private key: Entschlüsseln, Signieren

konkret in gpg

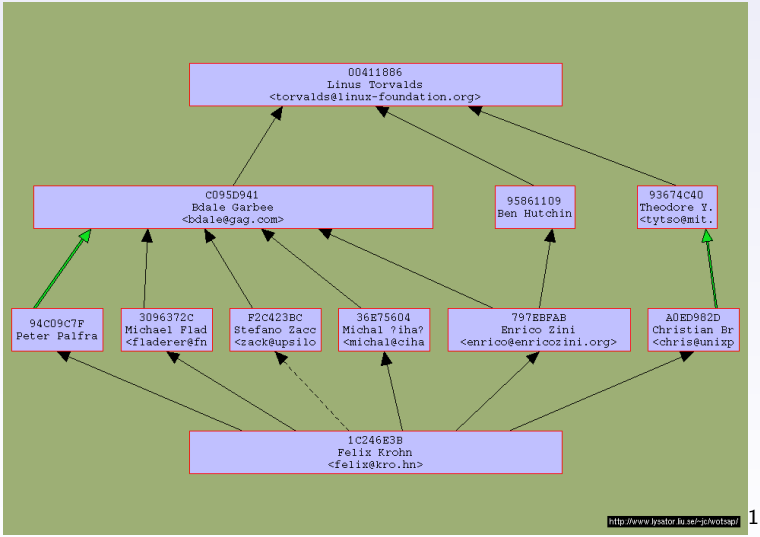
- 2 keyrings: ${HOME}/.gnupg/{sec,pub}ring.gpg
- Fingerprint: eindeutige ID des Schlüssels
- pubkeys werden idR über keyserver getauscht
- oder auch (scriptgesteuert) per mail

mailto:god@heaven.org

- Problem: ich will jemandem eine Mail schreiben, habe aber nicht mit ihm persönlich Schlüssel getauscht
- Lösung: WoT => Vertrauenspfad

mailto:god@heaven.org

- Problem: ich will jemandem eine Mail schreiben, habe aber nicht mit ihm persönlich Schlüssel getauscht
- Lösung: WoT => Vertrauenspfad


00411886
Linus Torvalds
<torvalds@linux-foundation.org>
C095D941
Bdale Garbee
<bdale@gag.com>
95861109
Ben Hutchin
93674C40
Theodore Y.
<tytso@mit.
94C09C7F
Peter Palfra
3096372C
Michael Flad
<fladerer@fn
F2C423BC
Stefano Zacc
<zack@upsilo
36E75604
Michal ?iha?
<michal@ciha
797EBFAB
Enrico Zini
<enrico@enricozini.org>
A0ED982D
Christian Br
<chris@unixp
1C246E3B
Felix Krohn
<felix@kro.hn>
http://www.lysator.liu.se/~jc/wotsap/

[1]

[1] WOTSAP

usability oder PEBKAC?

- Falscher key wegen usability?[2]
- *"click here to check if your private key is secure"*

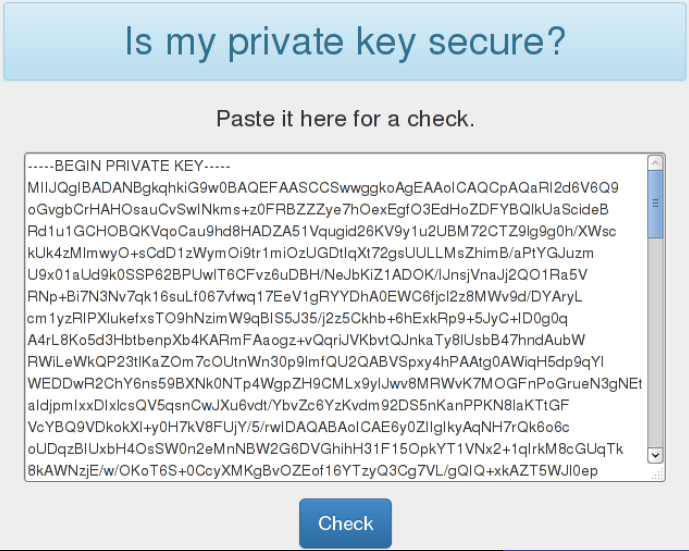
[2] http://cryptome.org/2014/04/radack-greenwald.htm

usability oder PEBKAC?

- Falscher key wegen usability?[2]
- *"click here to check if your private key is secure"*

[2] http://cryptome.org/2014/04/radack-greenwald.htm

http://privatekeycheck.com/



technische Infrastruktur

- keyserver Infrastruktur
- keine Hierarchie
- Vorteil/Nachteil?

Keysigning Party - Vorbereitung

- schlüssel erzeugen: *gpg –gen-key*
- schlüssel hochladen: *gpg –keyserver pgp.uni-mainz.de –send-key 0xdeadbeefb01dface*
- schlüssel exportieren: *gpg –export –armor 0xdeadbeefb01dface*
- (key-ID sind die letzten 4 Tupel des fingerprints

Keysigning Party

- pubkey (oder key-ID) senden an keysigning@unfuck.eu
- DEADLINE: morgen (Freitag) 10 Uhr CEST
- (alternativ: genügend fingerprints ausdrucken und mitbringen)
- mitbringen: ein (besser: zwei) Ausweisdokumente (Perso, Reisepass, Führerschein)

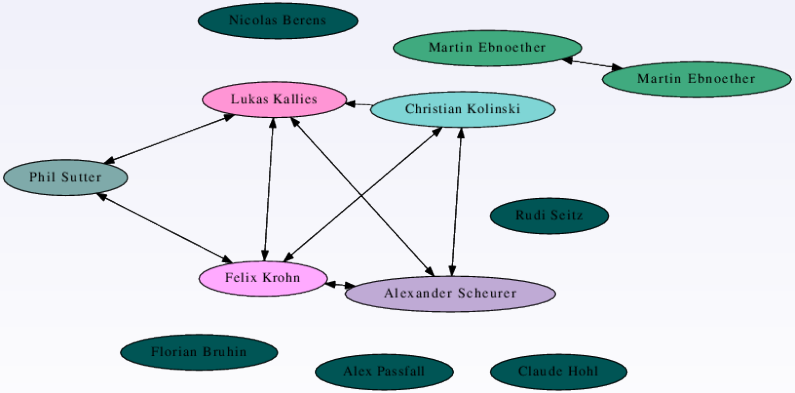
Ablauf Keysigning Party

- verschiedene Algorithmen, je nach Anzahl Teilnehmer und Vorlauffrist
- Hier: einfache (leicht chaotische) Variante
- Liste der Teilnehmer & deren fingerprints wird ausgeteilt
- Zuerst überprüft jede/r seinen fingerprint auf der Liste
- Aufteilen in 2 Reihen
- Jede/r prüft Jede/n anhand von Ausweisdokument

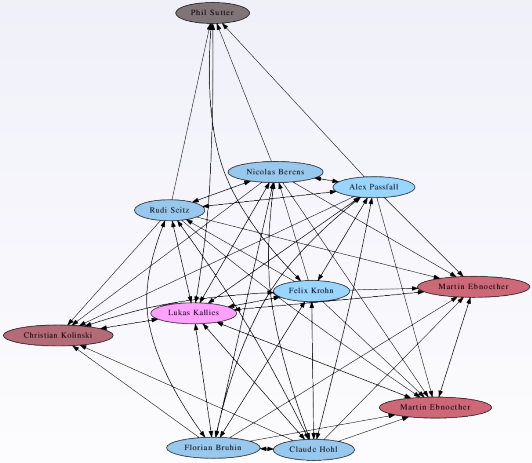
Pixelschubsen

- *gpg –list-sigs 0xdeadbeef | sig2dot | neato -Tps | convert – ${FILE}.png*

Vor der Party

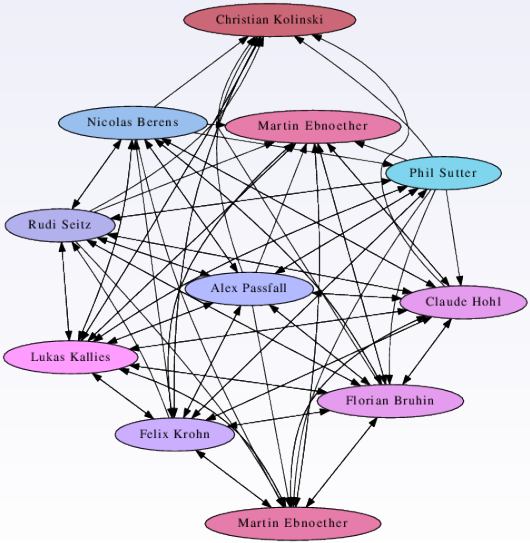


Der Tag danach



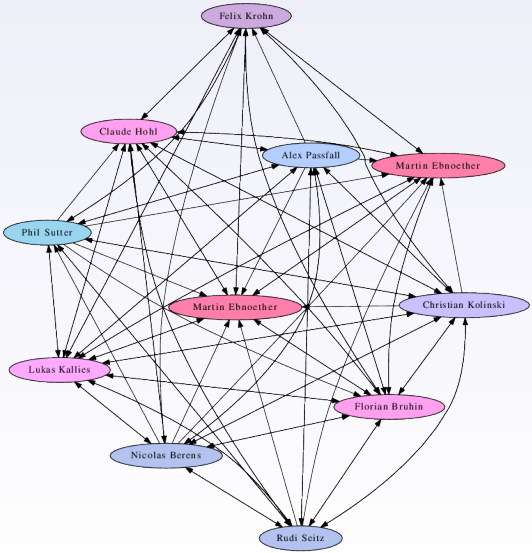
UnFUCK 2016
UNix Friends and User group
Campus Kamp

3 Tage später



UnFUCK 2016
UNix Friends and User group Campus Kamp

1.5 Jahre später



UnFUCK 2016
UNix Friends and User group Campus Kamp

Die Moral der Geschichte...

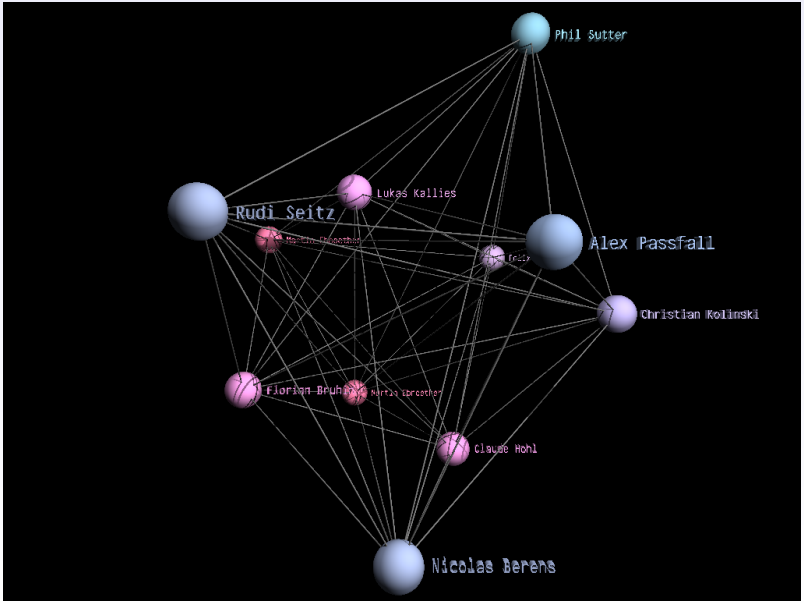
- Möglichst in den 3 Tagen nach der Party signieren, sonst wird's vergessen
- etwas Hilfe: aptitude install signing-party
- caff - CA Fire and Forget

Pixelschubsen[3]

- *gpg –list-sigs 0xdeadbeef | sig2dot | springgraph.pl -s2.5 -p > ${FILE}.pov*
- *povray +I${FILE}.pov +O${FILE}.tga +W1024 +H768*
- Brille aufsetzen...

Pixelschubsen[3]

- *gpg –list-sigs 0xdeadbeef | sig2dot | springgraph.pl -s2.5 -p > ${FILE}.pov*
- *povray +I${FILE}.pov +O${FILE}.tga +W1024 +H768*
- Brille aufsetzen...


Phil Sutter
Lukas Kallies
Rudi Seitz
Alex Passfall
Christian Kolinski
Florian Bruhin
Claude Hohl
Nicolas Berens

Checkliste

- Wann: Morgen (Freitag) 11:00 Uhr (CEST!)
- Wo: $HIER
- Mitbringen:
  - Fingerprint (*gpg –fingerprint 0xdeadbeef*)
  - Amtliches Ausweisdokument mit Bild (Perso, NPA, Pass)
  - Zettel/Stift (oder hier als Werbematerial abgreifen)
  - offline-party: kein Elektronikspielzeug nötig/erwünscht

Fragen?

UnFUCK 2016
UNix Friends and User group Campus Kamp