How I Encrypted My Notebook

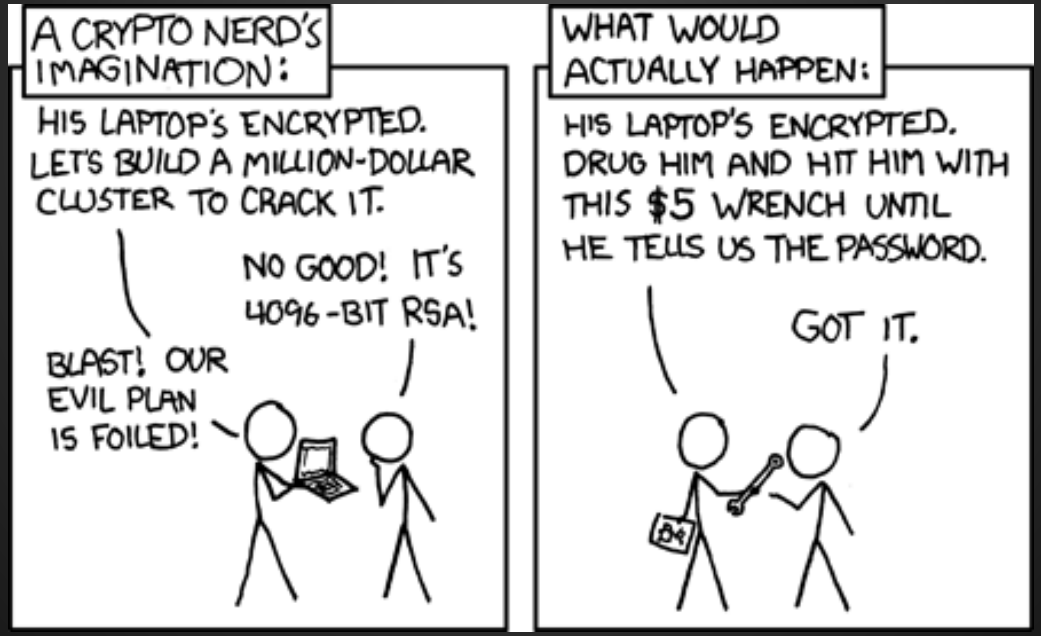
rami
<mail@raphaelmichel.de>
2014-07-02

Angreifermodell

- Laptop-Dieb
- Grenzkontrolle a.k.a. Bundestrojanerinstallparty

Nicht mein Angreifermodell

– Konkreter Angriff auf mich als Person



Bildnachweis: xkcd.com

Die Anforderungen

- Vollverschlüsselung
- Gegenüber Laien (Grenzkontrollpersonal) abstreitbar
- (Lange Passwörter merken und eintippen ist eigentlich doof, kurze Passwörter auch.)

Die Idee

- Normaler Boot startet ein Alibi-Windows
- Nur wenn ein bestimmter USB-Stick vorhanden ist, wird Linux gebootet
  - auf diesem liegt der Bootloader
  - Stick kann nach dem Booten abgezogen werden
  - Optional: Passphrase auf USB-Stick

Die Idee

- Hübscher USB-Stick für 7,48€
  - http://www.amazon.de/dp/B008QGQZAE/
  - Der Stick ist **nur hierfür und wird niemals an andere Rechner gesteckt.**

Bildnachweis: Kingston

Willkommene Nebeneffekte

– Bei vollverschlüsseltem Linux ist der Bootloader der attraktivste Angriffsvektor – den wir auf unserem USB-Stick sicher getrennt verwahren

Mein Setup

Festplatte

LUKS

LVM

/

swap

/home

Sinnvolle Reihenfolge

- Partitionieren
- Windows installieren
- LUKS/LVM aufsetzen
- Linux installieren

Meine Reihenfolge

- Partitionieren
- LUKS/LVM aufsetzen
- Linux installieren
- Linux verkleinern
- LVM verkleinern
- LUKS verkleinern
- Neu partitionieren
- Windows installieren

→ Geht, aber man sollte wissen, was man tut

Disclaimer

- Diese Anleitung ist **nicht vollständig**
- Diese Anleitung ist nicht mit anderen Distributionen als Arch Linux getestet
- Sie sollte gut übertragbar sein, aber nicht ohne nachdenken und selbst recherchieren!
- Das Arch-Wiki und Ubuntuusers sind toll.

KEIN BACKUP

KEIN MITLEID

Die Details: Partitionieren

- Man nehme das Live-Linux seiner Wahl
- Kommandozeile → `fdisk`
- Grafisch → `GParted`

Die Details: LUKS

```
# cryptsetup luksFormat /dev/sda1

# cryptsetup open /dev/sda1 lvm
```

Die Details: Die Backup-Passphrase

```
# pwgen -sy 20 1
}3['BEmDO`FzyFJ0r2@|

# pwgen -nB 30 1
aed3esheech9Keiv4NequeeJie9Ooh
```

Die Details: LVM

```
# pvcreate /dev/mapper/lvm
# vgcreate hostname /dev/mapper/lvm

# lvcreate -L 100G hostname -n rootvol
# lvcreate -L 8G hostname -n swapvol
# lvcreate -L 300G hostname -n homevol
```

Die Details: LVM

```
# mkfs.ext4 /dev/mapper/hostname-rootvol
# mkfs.ext4 /dev/mapper/hostname-homevol
```

Swap: see https://wiki.archlinux.org/index.php/Dm-crypt/Swap_encryption

Die Details: Der USB-Stick

```
# mkfs.ext2 /dev/sdb1
```

Mount as /mnt/boot during install (and all updates!). System already installed?

```
# cp -Rid /boot/* /media/sdb1/
# vim /etc/fstab
# grub-install /dev/sdb1
```

Die Details: Die Grub-Config

```
# cat /etc/default/grub
GRUB_CMDLINE_LINUX_DEFAULT="quiet
cryptdevice=/dev/sda2:arlen
cryptkey=/dev/keystick:8192:2048
resume=/dev/mapper/arlen-swapvol"
...
```

Die Details: Die Kernel-Config

```
# cat /etc/mkinitcpio.conf
FILES="/etc/udev/rules.d/50-myusb.rules
/etc/modprobe.d/modprobe.conf"
HOOKS="base udev autodetect modconf
block encrypt lvm2 resume filesystems
keyboard fsck"
```

Die Details: *Die udev-Regel*

```
# cat /etc/udev/rules.d/50-myusb.rules
SUBSYSTEMS=="usb", ATTRS{serial}=="
C860123BDBACCEDA08FA340C8", KERNEL=="
sd*", SYMLINK+="keystick%n"
```

Die Details: Der Bootloader

```
# mkinitcpio -p linux
# grub-mkconfig -o /boot/grub/grub.cfg
```

Die Details: *Das Keyfile*

```
# dd if=/dev/urandom of=keyfile bs=512
count=4
# cryptsetup luksAddKey /dev/sda1
keyfile
# dd if=keyfile of=/dev/sdb bs=512
seek=16
# shred --remove --zero keyfile
```

Bessere Tutorials

- https://wiki.archlinux.org/index.php/Dm-crypt
- https://wiki.archlinux.org/index.php/Dm-crypt/Encrypting_an_entire_system#LVM_on_LUKS
- https://wiki.archlinux.org/index.php/Dm-crypt/Swap_encryption#LVM_on_LUKS
- https://wiki.archlinux.de/title/Festplatte_verschl%C3%BCsseln#System_per_USB-Stick_entschl.C3.BCsseln
- https://wiki.archlinux.org/index.php/Dm-crypt/Specialties#Securing_the_unencrypted_boot_partition
- http://wiki.ubuntuusers.de/System_verschl%C3%BCsseln
- http://wiki.ubuntuusers.de/System_verschl%C3%BCsseln/Entschl%C3%BCsseln_mit_einem_USB-Schl%C3%BCssel

Offene Probleme

– Jemandem versiertes fällt schnell auf, dass das Windows nur einen kleinen Teil der HDD benutzt, jemand noch versierteres findet unsere LUKS-Header

→ Dies schützt euch nicht vor Geheim-diensten, aber hilft beim nicht auffallen

Offene Probleme

- Wer das Video zu diesem Talk sieht, weiß, wozu der USB-Stick an meinem Schlüsselbund gut ist
  - Spricht deutlich gegen das Keyfile ;)

Weiter

- Die Linux-Partitionen im Windows etwas besser verstecken

Weiter

- Keyfile mit weiterer Passphrase schützen
  - „2-factor-Auth“
  - Weiterer LUKS-Container auf dem USB-Stick

Weiter

- Plausible deniability
  - Kann LUKS nicht.
  - Funktioniert in der Praxis auch nicht einmal halb so gut, wie es klingt.

Weiter

- LUKS-Header auf USB-Stick auslagern
  - Kein Fallback mehr!

KEIN BACKUP

KEIN MITLEID

DANKE.

FRAGEN?