Verschlüsselung von Daten

Bernd Müller für die LIT2010 in Augsburg

Warum Verschlüsselung?

Privatsphäre

Duden: *ganz persönlicher Bereich [1]*

Wikipedia: *Die Privatsphäre einer Person bezeichnet den Bereich, der nicht öffentlich ist, in dem nicht im Auftrag eines Unternehmens, Behörde oder ähnliches gehandelt wird, sondern der nur die eigene Person angeht. [2]*

Privatsphäre

Ich habe nichts zu verbergen!

Wer interessiert sich für mich!

Diese Sätze sind keine Ausrede für mangelnden Umgang mit der eigenen Privatsphäre, den ich muss nicht jedem zeigen, dass ich nichts zu verbergen habe!

Grundrecht

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. 27.02.2008

[3]

Kann mit richterlichem Beschluss und ausreichenden Gründen nicht mehr gewährleistet werden.

Bezug auf:

Art. 1 Abs. 1 GG

Art. 2 Abs. 2 GG

Art. 10 Abs. 1 GG

[4]

Datenverlust

- Sicherheitslücken

  Würmer, Trojaner, Viren, Exploits, Adware, Spyware, ...
- Verlust/Diebstahl [5]

  Diebstahl 1H09 75 von 250 Vorfälle (30%)

Welche Möglichkeiten gibt es?

Es gibt zwei Möglichkeiten die Daten auf einem Speichermedium zu verschlüsseln:

Hard- und Softwareverschlüsselung

Was erwarte ich von einer Verschlüsselung?

- Performant
- Ausreichende Sicherheit
- Wenig Aufwand bei Zugriff mit Live-CD
- Kostenlos
- Unterstützung
- Komplette Partitionen/HDD

Hardwareverschlüsselung

FDE (Full Disk Encryption) [6]

- entlastet den Prozessor
- komplette HDD ist verschlüsselt
- Controller Unterstützung
- HDD Unterstützung

Erfüllt Hardwareverschlüsselung die Erwartungen?

- Performant
- Ausreichende Sicherheit
- Wenig Aufwand bei Zugriff mit Live-CD
- Kostenlos
- ~~Unterstützung~~
- Komplette Partitionen/HDD

Softwareverschlüsselung

- TrueCrypt [7]
- OpenPGP/GPG Schlüssel [8]
- dm-crypt/LUKS/cryptsetup [9] [10] [11]

…

- Crypto-FS [12]
- Enc-FS [13]

TrueCrypt

- Linux/GNU, Windows und Mac OS X
- Pakete für OpenSUSE und Ubuntu
- OpenSUSE Repository über Build Service
- Containererstellung
- Passphrase und/oder Keyfile
- Zugriff mit Live-CD setzt Internetverbindung zur Installation voraus
- GUI und CLI

Erfüllt TrueCrypt die Erwartungen?

- Performant
- Ausreichende Sicherheit
- ~~Wenig Aufwand bei Zugriff mit Live-CD~~
- Kostenlos
- Unterstützung
- ~~Komplette Partitionen/HDD~~

OpenPGP/GPG Schlüssel

- einzelne Dateien ver-/entschlüsseln

 # gpg -se -r <User> <File>

 # gpg -d <File>

- Für E-Mail ver-/entschlüsseln

Thunderbird/Enigmail/GnuPG

Erfüllt OpenPGP/GPG die Erwartungen?

- ~~Performant~~
- Ausreichende Sicherheit
- ~~Wenig Aufwand bei Zugriff mit Live-CD~~
- Kostenlos
- Unterstützung
- ~~Komplette Partitionen/HDD~~

dm-crypt/LUKS/cryptsetup

- Linux/GNU und Windows (FreeOTFE [14])
- Auf Live-CD enthalten, Ausnahme Ubuntu Desktop Version
- Passphrase (8 Slots) und/oder Keyfile
- Containererstellung über Loopdevice
- Bis auf /boot kann alles verschlüsselt werden

Erfüllt dm-crypt/LUKS/cryptsetup die Erwartungen?

- ~~Performant~~
- Ausreichende Sicherheit
- Wenig Aufwand bei Zugriff mit Live-CD
- Kostenlos
- Unterstützung
- ~~Komplette Partitionen/HDD~~

Verschlüsselte Daten

Wie richte ich mit Hilfe von dm-crypt/LUKS/cryptsetup eine Verschlüsselung ein?

Bernd Müller für die LIT2010 in Augsburg

Vorbereitung

Cryptsetup installieren

 # aptitude/yum/zypper install cryptsetup

Kernelmodul dm-crypt laden

 # update-rc.d dm-crypt defaults

 # insserv dm-crypt

 # chkconfig dm-crypt

Welche Verschlüsselungen sind geladen?

Geladene Kernelmodule einsehen

 # cat /proc/crypto

…

name : aes

driver : aes-asm

module : aes_x86_64

priority : 200

refcnt : 5

selftest : passed

type : cipher

blocksize : 16

min keysize : 16

max keysize : 32

...

Welche Verschlüsselung kann geladen werden?

 # ls -A /lib/modules/<kernel>/kernel/crypto

aes-generic.ko … blowfish.ko … des-generic.ko … sha256_generic.ko sha512_generic.ko ...

Datenträger/Partition verschlüsseln

Verschlüsseln mit AES und 256bit

 # cryptsetup -c aes -s 256 -y luksFormat /dev/sdXX

WARNING!

=========

This will overwrite data on /dev/sdXX irrevocably.

Are you sure? (Type uppercase yes): YES

Enter LUKS passphrase:

Verify passphrase:

Command succesful.

Verschlüsseltes mappen

 # cryptsetup luksOpen /dev/sdXX crypt

Enter LUKS passphrase:

key slot unlocked.

Command succesful.

 # ls /dev/mapper/

… crypt ...

Formatieren

Den verschlüsselten Datenträger/Partition formatieren:

- LVM2 (pvcreate, vgcreate, lvcreate)
- Ext2/3 (mkfs.ext2/3)
- ReiserFS (mkfs.reiserfs)
- ...

Mounten und in das System einbinden

 # mount -t <FS> /dev/mapper/crypt /mnt/crypt

 # echo “/dev/mapper/crypt /mnt/crypt <FS> defaults 0 1” >> /etc/fstab

Zugriff via Live-System

 # aptitude/yum/zypper install cryptsetup

 # cryptsetup luksOpen /dev/sdXX crypt

 # mount -t <FS> /dev/mapper/crypt /mnt/crypt

Troubleshooting

Ist es ein LUKS?

 # cryptsetup isLuks /dev/sdXX

Welcher Schlüssel und Slot?

 # cryptsetup luksDump /dev/sdXX

Linksammlung

- [1] http://www.duden-suche.de/suche/trefferliste.php?suchbegriff%5BAND%5D=priv
- [2] http://de.wikipedia.org/wiki/Privatsph%C3%A4re
- [3] http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
- [4] http://www.artikel5.de/gesetze/gg.html
- [5] http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=03
- [6] http://de.wikipedia.org/wiki/Full_Disk_Encryption
- [7] http://www.truecrypt.org/
- [8] http://www.gnupg.org/
- [9] http://www.saout.de/misc/dm-crypt/
- [10] http://code.google.com/p/cryptsetup/

Linksammlung II

- [11] http://code.google.com/p/cryptsetup/wiki/Cryptsetup110
- [12] http://freshmeat.net/projects/cryptofs/
- [13] http://www.arg0.net/encfs
- [14] http://www.freeotfe.org/