Festplattenverschlüsselung bei Laptops

KaLUG-Treffen
29.10.2007

Sven Geggus <sven@gegg.us>

Anforderungen

- sensible Daten sollen nicht in fremde Hände gelangen (z.B. bei Diebstahl des Gerätes)
- Sicherheit gegen Manipulationsversuche (daher Verschlüsselung des Komplettsystems nicht nur der Homeverzeichnisse)
- Rechner muss von mehreren Benutzern bootbar sein
- IT-Richtlinie Fraunhofer:
  Festplatteninhalte mobiler Geräte sollen verschlüsselt werden!

Meine Lösung

- Booten von USB-Stick über syslinux, extlinux oder vom Netzwerk über PXElinux
- Festplatte enthält keine unverschlüsselten Daten
- USB-Stick enthält mehrere Kernel (einen pro Rechner), eine spezielle initrd und eine Schlüsseldatei für jede mögliche Kombination aus Benutzer und Rechner
- Die Schlüsseldateien enthalten alle den selben luks-Schlüssel, der für jeden Benutzer jeweils mit einem individuellen Passwort verschlüsselt auf dem USB-stick abgelegt ist

Vorgehensweise Verschlüsselung

- Dateisystem backup machen (z.B. xfsdump,tar)
- Nomenklatur der Schlüsseldatei:
  `key_<Rechnername>_<Benutzerkennung>.dat`
- Schlüssel erzeugen:
  `pwgen -s 256 1 | openssl enc -aes256 -out key_<Rechnername>_<Benutzerkennung>.dat`
- Device NEU anlegen:
  ```
  openssl enc -d -aes256 -in key_<Rechnername>_<Benutzerkennung>.dat |\
  cryptsetup -c aes-cbc-essiv:sha256 -s 256 luksFormat <Partition>
  ```
- Device verwenden:
  ```
  openssl enc -d -aes256 -in key_<Rechnername>_<Benutzerkennung>.dat |\
  cryptsetup -c aes -cbc-essiv:sha256 -s 256 luksOpen <Partition> croot
  ```
- croot formatieren und mounten
  ```
  mkfs.xfs /dev/mapper/croot
  mount /dev/mapper/croot /mnt/tmp
  ```
- Backup zurückspielen (z.B. xfsresore, tar)

Vor- und Nachteile

Vorteile

- Ein USB-Stick kann mehrere Geräte booten
- Mehrbenutzerfähig
- Bei Verlust eines USB-Sticks können neue Schlüssel erzeugt werden
- USB-Stick wahlweise mit vfat oder ext2
- Bootvorgang auch ohne USB-Stick per PXE möglich

Nachteile

- Der unverschlüsselte Kernel und die initrd auf dem USB-Stick sind prinzipiell manipulierbar
- Suspend to Disk ist derzeit nicht möglich
- Verschlüsselung bestehender Systeme derzeit nicht in place möglich (xfsdump/xfsrestore)

Ausblick

- Verschlüsselung der Benutzerspezifischen Schlüsseldateien mit Smartcard statt Passwort
- Integration von TPM-Hardware
- Eventuell existiert ein Bootloader der nur trusted kernel lädt?
- There is more than one way to do it :)