Šifrovaný disk v Linuxu

data v bezpečí

Petr Krčmář

ROOT.CZ_ vpsFree.cz

4. března 2018

Prezentace už teď na webu

www.petrkrcmar.cz

ROOT.CZ_ vpsFree.cz

Vtip na úvod

„Pane doktore, potřebuji pomoc, trpím paranoiou!“
„Dobře, tak my vás začneme sledovat.“

Diskové šifrování je, když...

- data jsou na disk uložena vždy v šifrované podobě
- pokud má software klíč, může číst i zapisovat
- bez znalosti klíče jen náhodný šum
- ochrana při odcizení, v servisu, i v běžném provozu
- dvě základní dělení
  - na požádání (on demand) – jednorázově zašifrovat/dešifrovat
  - za letu (on the fly) – transparentní po připojení šifrovaného svazku
- je možné šifrovat
  - celé disky (interní i externí)
  - interní oddíly
  - jednotlivé soubory
  - kontejnery uvnitř souborů

ROOT.CZ_ vpsFree.cz

Není to všelék

- šifrování neřeší všechny bezpečnostní problémy
- útok na systém s připojenými disky
- fyzický přístup umožňuje dělat další útoky (cold boot)
- v některých zemích musíte vydat heslo
- případně...

ROOT.CZ_ vpsFree.cz

Kryptoanalýza gumovou hadicí

XKCD 538, Randall Munroe, Robert Krátký, CC by-nc 2.5

ROOT.CZ vpsFree.cz

Šifrování dat nebo systému

- šifrování dat je velmi pohodlné
  - klíč při přihlašování uživatele
  - každý uživatel zvlášť šifrovaný prostor
  - systém je ale stále napadnutelný i ve vypnutém stavu
  - po disku se mohou potulovat dešifrovaná data (swap, /var, /tmp…)
- šifrování celého systému je bezpečnější
  - komplikovanější pro inicializaci a správu
  - dešifruje se už před bootem systému
  - nelze sloučit s přihlášením konkrétních uživatelů
  - zašifrována jsou opravdu všechna data
  - nelze ovlivnit vypnutý operační systém
- výhodně lze ale různě kombinovat obojí

ROOT.CZ_ vpsFree.cz

Šifrování nad soubory

- šifrují se jednotlivé soubory zvlášť
- není potřeba vytvářet kontejner/oddíl
- není nutné alokovat místo pro šifrovaná data
- adresářová struktura je zachována
- šifruje se obsah i název souboru
- pomocí pseudo-souborového systému se připojí
- jeden adresář se přes ovladač mapuje do druhého
- nešifrují se metadata (stuktura, velikosti, počty)
- adresáře, (hard|soft)linky se zachovávají
- dvě různá řešení: eCryptfs a EncFS
- modul v jádře vs. uživatelské řešení s FUSE

Demo: šifrování s EncFs

Vytvoříme šifrovaný adresář

```
$ encfs ~/.zasifrovano/ ~/odsifrovano/
```

Odpojíme šifrovaný adresář

```
$ fusermount -u ~/odsifrovano/
```

Vypíšeme informace

```
$ encfsctl ~/.zasifrovano/
```

Změníme heslo

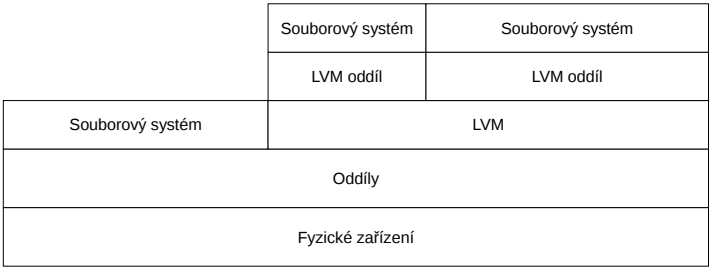
```
$ encfsctl passwd ~/.zasifrovano/
```

Bloková zařízení v Linuxu

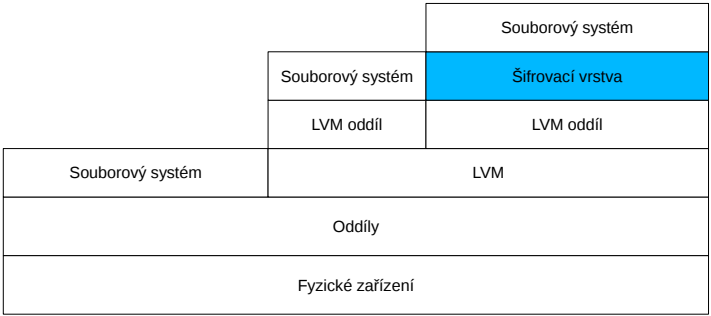
- Linux přistupuje k úložištím jako k blokovým zařízením
- vše je interpretováno jako soubor
- na nejnižší úrovni `/dev/sda` jako celý disk
- ovladače vytvářejí další virtuální pohledy (`/dev/sda1`)
- takto možno přidávat další vrstvy (téměř) bez omezení
- vrstvy se stohují (stacking) nad sebou
- podle potřeby různé pořadí vrstev
- pole (RAID), LVM, šifrovací vrstva, souborový systém
- uživatel pak přistupuje k nejvyšší vrstvě
- vše se transparentně propisuje nahoru i dolů

ROOT.CZ vpsFree.cz

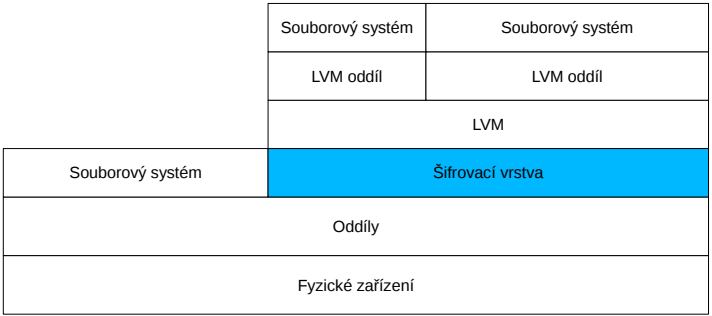
Schématický pohled na bloky



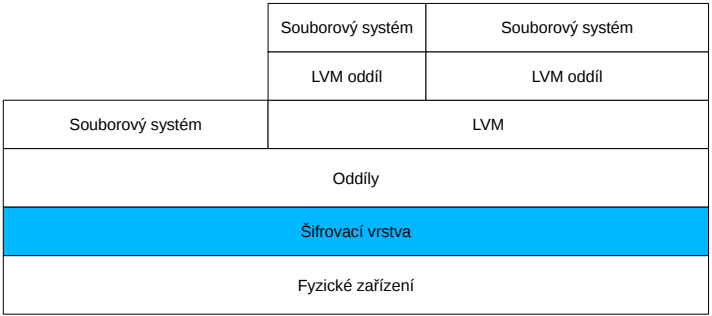
Schématický pohled na bloky



Schématický pohled na bloky



Schématický pohled na bloky



Šifrování blokových zařízení

- funguje **pod** souborovým systémem
- přidává další mezivrstvu mezi dělení disků a souborový systém
- cokoliv je zapsáno do blokového zařízení, je šifrováno
- včetně všech metadat (počty, velikosti, práva…)
- pokud je zařízení odpojeno, jeví se jako náhodná data
- po připojení máme k dispozici dešifovaný disk
- na něm obvykle souborový systém (nebo LVM) pro připojení

ROOT.CZ_ vpsFree.cz

Různá řešení

Loop-AES
: nejstarší řešení, v jádře, pro starší systémy

dm-crypt + LUKS
: současné řešení, v jádře, doporučováno

VeraCrypt
: používá FUSE, hodně rozšířené mimo Linux (TrueCrypt)

Standardní linuxové řešení

- device mapper – rozhraní pro stohování blokových zařízení
- standardní způsob: blok ↔ DM ↔ modifikace ↔ blok
- uživatelský prostor využívá `libdevmapper.so`
- ze shellových skriptů možno použít `dmsetup`
- virtuální zařízení pak v `/dev/mapper/`
- používá ho LVM, RAID, dm-crypt, TrueCrypt a další

dm-crypt

- dm-crypt – šifrovací subsystém od jádra 2.6 (2003)
- technicky je to jeden z „cílů“ pro device mapper
- používá standardní jaderné Crypto API pro šifrování bloků
- nízkoúrovňový nástroj, sám nespravuje klíče
- při připojování vždy nastavíte, co se má čím šifrovat
- neumí některé kryptografické funkce (třeba sůl)
- utility `cryptsetup` a `cryptmount`
- lze použít na disk, oddíl, LVM, RAID, soubor...

LUKS

- LUKS – Linux Unified Key Setup
- rozšíření dm-crypt – std. a dokumentovaná správa klíčů
- existuje od roku 2004 – žádná „hurá novinka“
- spojení dm-crypt/LUKS je standardním linuxovým řešením
- přístup pomocí hesla nebo souboru s klíčem
- klíč může být v hlavičce vícekrát, šifrován různými hesly
- více uživatelů s různými hesly, možnost hesla měnit
- používá se utilita `cryptsetup`
- původně jen pro dm-crypt, později rozšířen o LUKS a další:
  - LUKS
  - plain (čistý dm-crypt)
  - loop-AES
  - TrueCrypt (včetně rozšíření z VeraCrypt)

ROOT.CZ vpsFree.cz

Demo: šifrování s LUKS

Vytvoříme šifrovaný svazek

```
# cryptsetup -y -v luksFormat /dev/sdb
```

Připojíme šifrovaný svazek

```
# cryptsetup luksOpen /dev/sdb bezpecny
# ls -l /dev/mapper/bezpecny
```

Vypíšeme informace

```
# cryptsetup -v status bezpecny
```

Vytvoříme souborový systém

```
# mkfs.ext4 /dev/mapper/bezpecny
# mount /dev/mapper/bezpecny /mnt/data/
```

Odpojíme, zavřeme

```
# umount /mnt/data/
# cryptsetup luksClose bezpecny
```

Boot ze šifrovaného disku

- lze zašifrovat i systémový oddíl `/`
- oddíl s obsahem `/boot` ale musí být nešifrovaný
- Grub odtud natáhne jádro a init ramdisk
- v ramdisku potřebné skripty, moduly a utility
- zeptá se na heslo, připojí root a spustí init
- stále možnost kompromitace nešifrované části (evil maid)
- `/boot` je možné mít i jinde – třeba na flash disku
- distribuce na to bývají připravené (skripty pro `mkinitramfs`)
- podporu šifrovaného systémového disku obvykle stačí zapnout
- Alpine Linux na to má podrobný návod

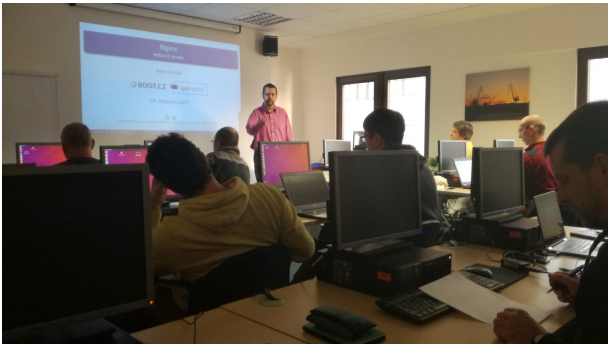
ROOT.CZ_ vpsFree.cz

Co se taky dá dělat

- firemní počítač s Windows → NTFS
- bootovací flash disk s jádrem a initramfs
- na NFTS velký soubor šifrovaný LUKS
- v něm LVM se všemi oddíly – systém i data
- bezpečný dualboot v „nepřátelském prostředí“

ROOT.CZ_ vpsFree.cz

Otázky?



Petr Krčmář (petr.krcmar@iinfo.cz)

ROOT.CZ vpsFree.cz