

Plně šifrovaný disk na moderním systému

Ondřej Caletka



26. května 2018



Uvedené dílo podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O sdružení CESNET



	n×100 Gb/s		100 Gb/s
	n×10 Gb/s		10 Gb/s
	1-2,5 Gb/s		1-2,5 Gb/s
	uzel (PoP)		<1 Gb/s
	uživatel (user)		



MetaCentrum



UltraGrid

- fyzická bezpečnost dat **vypnutého** počítače
- nesupluje šifrování kritických uživatelských dat, např. **privátních klíčů, hesel**
- bez výrazného vlivu na výkon
- na úrovni souborů nebo blokového zařízení
- pouze cenných dat (/home) nebo celého disku

- **odcizení zařízení, servisní zásah**
 - stačí obyčejné šifrování důležitých souborů
- **cold-boot útok**
 - paměť je připájena
 - lze ji vyčíst nezabezpečeným Thunderboltem
 - lze nastartovat jednoúčelový systém po restartu
 - nelze eliminovat na straně OS
 - vyžaduje správné nastavení a důvěru ve firmware
- **evil-maid útok**
 - úprava nešifrované části systému
 - vyzradí heslo při příštím zadání



- používá UEFI
 - vyžaduje EFI System Partition
 - zbytek disku může být šifrovaný
- podporuje UEFI Secure Boot
 - spustí jen podepsané binárky
- používá pokročilý souborový systém (Btrfs/ZFS)
 - subvolumes namísto samostatných oddílů
 - podpora snapshotů
 - kontrola integrity dat

- lepší odolnost proti evil-maid
 - menší plocha viditelná útočníkovi
 - i bez MAC je problematický útok na zašifrovaná data
- vyžaduje zadání hesla při startu
 - nelze nastartovat vzdáleně a odemknout přes síť

Tradiční šifrování celého disku

- nešifrovaný oddíl /boot
- obsahuje zavaděč, jádro a initramfs
- initramfs se během startu zeptá na heslo a připojí ostatní disky
- chceme-li Secure boot, měl by zavaděč ověřovat podpisy jádra a initramfs

Nešlo by to lépe?

- zavaděč GRUB podporuje šifrované svazky
- lze tedy zašifrovat i obraz jádra a initramfs
- vlastní zavaděč musí být v nešifrované EFI System Partition
- stačí mít podepsaný zavaděč

Nešlo by to lépe?

- zavaděč GRUB podporuje šifrované svazky
- lze tedy zašifrovat i obraz jádra a initramfs
- vlastní zavaděč musí být v nešifrované EFI System Partition
- stačí mít podepsaný zavaděč

Dvojitá zadávání hesla

- zavaděčem rozšifrovaný oddíl nelze předat jádru
- klíč ale může být uložen v initramfs

Potřebuje ještě někdo LVM?

- virtualizace blokových zařízení
- možnost dělit či spojovat fyzické svazky do logických
- možnost snapshotů, thin provisioningu, zrcadlení,...
- většina funkcí implementována nativně v Btrfs

Potřebuje ještě někdo LVM?

- virtualizace blokových zařízení
- možnost dělit či spojovat fyzické svazky do logických
- možnost snapshotů, thin provisioningu, zrcadlení,...
- většina funkcí implementována nativně v Btrfs

Ideální pro swap

- nutný pro funkci hibernace
- Btrfs nepodporuje swap soubory
- stránkování do samostatného oddílu by vyžadovalo dvojité odemykání

Praktická realizace



xkcd 910 © Randall Munroe, překlad Robert Krátký, CC-BY-NC

- EFI System Partition
- LUKS kontejner
 - LVM oddíl s Btrfs
 - subvolume @gentoo
 - subvolume @fedora
 - subvolume ...
 - LVM oddíl pro swap

- automatický instalátor patrně selže
 - Fedora: oddíl /boot nesmí být typu Btrfs, nesmí být šifrovaný
- Gentoo a Arch Linux nemají instalátor, takže fungují ;)
- potřebujeme zařídit
 - aby GRUB připojil šifrovaný disk
 - aby initramfs rozšifroval disk podle klíče v něm uloženém

Jak nepřijít o výkon

cryptsetup benchmark

Testy jsou počítány jen z práce s pamětí (žádné I/O úložiště).

```
PBKDF2-sha1      1394382 iterations per second for 256-bit key
PBKDF2-sha256   1635843 iterations per second for 256-bit key
PBKDF2-sha512   1339177 iterations per second for 256-bit key
PBKDF2-ripemd160 1018034 iterations per second for 256-bit key
PBKDF2-whirlpool 777875 iterations per second for 256-bit key
```

#	Algorithm	Key	Encryption	Decryption
	aes-cbc	128b	1112,2 MiB/s	3501,2 MiB/s
	serpent-cbc	128b	93,5 MiB/s	713,3 MiB/s
	twofish-cbc	128b	212,7 MiB/s	385,7 MiB/s
	aes-cbc	256b	840,4 MiB/s	2788,0 MiB/s
	aes-xts	256b	2558,9 MiB/s	2560,5 MiB/s
	aes-xts	512b	2207,0 MiB/s	2223,6 MiB/s

Je potřeba mít zavedený modul `aesni_intel`

cryptsetup benchmark bez podpory AES-NI

#	Algorithm	Key	Encryption	Decryption
	aes-cbc	128b	277,9 MiB/s	321,9 MiB/s
	aes-cbc	256b	215,8 MiB/s	241,1 MiB/s
	aes-xts	256b	327,4 MiB/s	325,0 MiB/s
	aes-xts	512b	245,2 MiB/s	243,0 MiB/s

Rychlost NVMe SSD

```
# hdparm -Tt --direct /dev/nvme0n1
```

```
/dev/nvme0n1:
```

```
Timing 0_DIRECT cached reads: 2758 MB in 2.00 seconds = 1381.80 MB/sec
```

```
Timing 0_DIRECT disk reads: 4460 MB in 3.00 seconds = 1486.59 MB/sec
```


Vytváříme strukturu zařízení

LUKS kontejner

```
cryptsetup luksFormat /dev/nvme0n1p2  
cryptsetup luksOpen /dev/nvme0n1p2 container
```

LVM mezivrstva

```
pvccreate /dev/mapper/container  
vgcreate VG /dev/mapper/container  
lvcreate -n btrfs -L 200G VG  
lvcreate -n swap -L 16G VG
```

System souborů

```
mkfs.btrfs /dev/mapper/btrfs  
mkswap /dev/mapper/swap
```

- nezávislé části Btrfs filesystemu
- samostatně se snapshotují
- dobrá praxe je mít kořenový systém souborů v subvolume
- plochý nebo zanořený model
 - plochý** všechny subvolumes jsou v kořeni, následně jsou připojeny pomocí vícenásobného záznamu ve `fstab`
 - zanořený** subvolumes jsou umístěny přímo na svém místě, jsou připojeny automaticky s připojením rodiče
- vhodné pro logické oddělení uživatelských, systémových a dočasných dat

- nástroj na pravidelné snapshotování z dílny openSUSE
- předloha pro nástroj schnapps z TurrisOS
- automaticky vyrábí a maže snapshoty
- jsou vytvářeny v `.snapshots`
- je nutno nakonfigurovat pro každý subvolume zvlášť
- pro rollback je dobré mít logy na samostatném subvolume

- generátor initramfs obrazů
- vyvinut v RedHat, adoptován kernel.org
- portován na Debian, Gentoo, openSUSE,...
- dokáže **odemknout LUKS svazek klíčem v souboru**

Uložení souboru s klíčem do initramfs

```
# dd if=/dev/random of=/boot/lukskey bs=1 count=4096
# chmod 400 /boot/lukskey
# cryptsetup luksAddKey /dev/nvme0n1p2 /boot/lukskey
# dracut -I /boot/lukskey
```

- podporuje Btrfs, LVM i LUKS
- vlastní konfiguraci čte už ze šifrovaného disku
 - vlastní fonty, barvy, pozadí se objeví až po zadání hesla

Konfigurační parametry v `/etc/default/grub`

```
GRUB_ENABLE_CRYPTODISK=y  
GRUB_CMDLINE_LINUX="rd.luks=1 rd.luks.key=/boot/lukskey:/  
rd.luks.uuid=luks-... rd.luks.allow-discards"
```

Lepší dialog zadání hesla

- sestavíme vlastní obraz GRUBu
- fonty a obrázky zabalíme do tar archivu memdisk.tar

early-grub.cfg

```
loadfont (memdisk)/ter-x28b.pf2
set gfxmode=auto
terminal_output gfxterm
background_image -m stretch (memdisk)/background.png
cryptomount (hd0,gpt2)
set prefix=(lvm...)/root/boot/grub
configfile grub.cfg
```

Sestavení vlastního obrazu

```
grub-mkimage -c early-grub.cfg -o grubx64.efi -O x86_64-efi -m memdisk.tar all_video
gfxterm gettext png part_gpt cryptodisk luks gcry_rijndael gcry_sha256 lvm btrfs memdisk
tar configfile gfxterm_background echo
```

- ochrana proti externí změně dat na disku
- čtyři databáze klíčů

Platform Key slouží výrobci k aktualizaci ostatních klíčů

Key Exchange Key klíče dodavatelů software, podepsané PK

db databáze klíčů/otisků povoleného softwaru

dbx databáze revokovaného softwaru

- je třeba kompletně vymazat a nahradit vlastní sadou klíčů
- dual-boot spolu s Windows je možný
- nástroje i postupy jsou k dispozici

BRACE YOURSELVES



LIVE DEMO IS COMING

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
[https://Ondřej.Caletka.cz](https://Ondrej.Caletka.cz)

