Uživatelsky přívětivé šifrování disku

Radek Zajíc

LinuxDays, 8. října 2017

about:me

2008 – 2012: Seznam.cz

IPv6 na webu

2012 – 2017: T-Mobile CZ

IPv6 na DSL a v mobilní síti

2017: Showmax.com

Desítky gigabitů provozu v Africe a Polsku.

Máme rádi open-source. ☺

Šifrujete?


ČT 24
A vy už jste někdy šifroval?
Ondřej Závodský náměstek pro hazard a majetek státu, MF
22:39 VEČER USTÁVÁNÍ SRÁŽEK A UBÝVÁNÍ OBLAČNOSTI.

Šifrujete na webu? A svůj disk?


```
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ...
NING: Failed to connect to lvmetad. Falling back to device scanning.
  Volume group "ubuntufde-vg" not found
  Cannot process volume group ubuntufde-vg
  WARNING: Failed to connect to lvmetad. Falling back to device scanning.
  Volume group "ubuntufde-vg" not found
  Cannot process volume group ubuntufde-vg
Please unlock disk sda5 crypt:
```

Nejlepší šifrování je takové, které uživatele moc neobtěžuje. HTTPS je příkladem toho, že i běžný uživatel šifruje, aniž o tom ví. Šifrování kořenového souborového systému na Linuxu ovšem vyžaduje zadání hesla. Alternativy jsou možné, ale obvykle vyžadují zařízení třetích stran (SmartCard, Yubikey) a nejdou použít pro bezobslužný (unattended) start. Nešlo by to udělat lépe?

Jak to dělají v sadu a u sklářů?

Systém bootuje do přihlašovací obrazovky.

Vybraní uživatelé mají práva odemčení disku
Po zadání uživatelského hesla je odemčen klíč k disku
Klíč k disku odemyká další klíč, kterým je disk šifrován

Po přihlášení uživatele je disk zpřístupněn.

Pokud uživatel zapomene heslo, lze obnovit přístup k šifrovacímu klíči skrze iCloud.

Využívá se čip TPM (Trusted Platform Module).

TPM má Storage Root Key, kterým zapečetí volume key
Pokud systém nastartuje do předem definovaného stavu, TPM rozpečetí volume key
Rozpečetěný volume key pak odemkne interní dešifrovací klíč, kterým je disk šifrován.

Po odemčení disku je tento zpřístupněn a systém bootuje.
Pokud selže rozpečetění, je uživatel požádán o recovery key.

Odemčení rootfs na Linuxu

BIOS/UEFI

↓

(SHIM+)?GRUB

↓

kernel

↓

initramdisk

↓

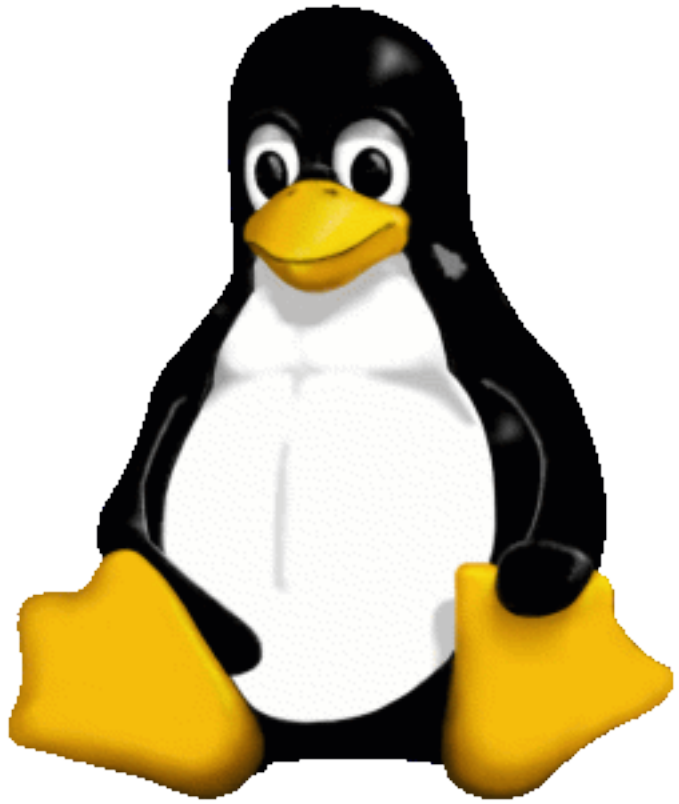
heslo pro odemčení rootfs

↓

odemčení šifrovaného oddílu

↓

Spuštění `/sbin/init` z rootfs



Odemčení rootfs na Linuxu

BIOS/UEFI

(SHIM+)?GRUB

kernel

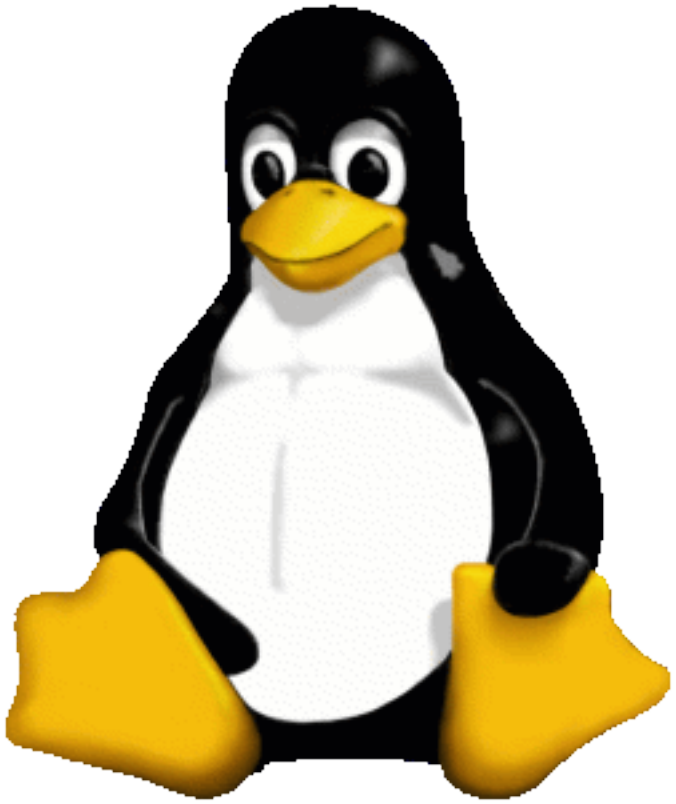
initramdisk

heslo pro odemčení rootfs

odemčení šifrovaného oddílu

Spuštění `/sbin/init` z rootfs

Co kdybychom fázi ručního hesla pro odemčení rootfs nahradili něčím jiným?



Automatické odemčení rootfs

Přidání `keyscript=...` do `/etc/crypttab`

Odemčení přes síť (SSH): Google `remote unlock of LUKS volume`

Obfuskovaný dešifrovací klíč např. na USB sticku

Keyscript spustí skript, jehož výstupem bude heslo, které pak použije pro odemčení disku. Kde ho ale skript vezme? A bude to bezpečné?
Odemčení přes síť funguje, ale jelikož si initramdisk může kdokoli rozbalit a spustit vlastního SSH démona se stejným privátním klíčem, nikdy nevíte, ke komu se vzdáleně připojujete.
Skripty pro načtení klíče z USB sticku musí být součástí initramdisku, tedy si je útočník může v případě sbalení hardwaru přečíst a spustit.

Automatické odemčení rootfs

Přidání `keyscript=...` do `/etc/crypttab`

Odemčení přes síť (SSH): Google `remote unlock of LUKS volume`

Obfuskovaný dešifrovací klíč např. na USB sticku

LUKS + TPM?

Co takhle použít k uložení klíče TPM? Co by to znamenalo? Jak TPM vlastně funguje, je pro něj podpora v kernelu a existuje funkční kód pro odemykání LUKSových oddílů?

TPM

Trusted* Platform Module

Trusted Platform Module. Pasivní kryptočip, původně zavrhovaný GNU komunitou. Relativně bezpečný, diskrétní: připojený přes LPC sběrnici, integrovaný v chipsetu, nebo tzv. firmware TPM = součást procesoru (běží ve vyhrazeném trusted execution environment). 2010: CIA prý dokázala vyčíst data uložená v NVRAM.

Odpor GNU k TPM padl až v roce 2015
(https://www.gnu.org/philosophy/can-you-trust.html.en)

TPM 1.2 (2006+)

vs.

TPM 2.0 (2016+)

TPM 2.0: Počítače s certifikací Windows 10 od 28 července 2016

TPM1.2: jednoduchá hierarchie vnitřního úložiště, jednoduché datové typy, omezené množství podporovaných hashovacích funkcí, relativně dobrá podpora v Linuxu (kernel i nástroje). TPM2.0: Nová verze specifikace, masivní změna přístupu, víceúrovňová hierarchie úložiště, komplexní datové typy, více hashovacích funkcí, špatná podpora v Linuxu (kernel i nástroje). Zpětně nekompatibilní. TPM1.2: Enterprise Windows-certified PCs

Inicializace TPM 1.2

CLEAR

TAKE OWNERSHIP

READ/WRITE DATA

EXTEND PCR

TPM čip je třeba povolit a smazat (CLEAR v BIOSu/UEFI, následně je potřeba tzv. převzít vlastnictví (nastavit Owner heslo). Pak je možné využívat funkce TPM, např. čtení/zápis do NVRAM. BIOS a OS provádí tzv. Extend PCR operaci a to i tehdy, když TPM není clear/owned.

TPM 1.2 device v Linuxu

```
# modprobe tpm_tis
# find /sys -name tpm0
/sys/kernel/security/tpm0
/sys/devices/pnp0/00:09/tpm/tpm0
/sys/class/tpm/tpm0

# cat /sys/class/tpm/tpm0/enabled
1

# cat /sys/class/tpm/tpm0/owned
1
```

TPM 1.2 nástroje v Linuxu (trousers, tpm-tools)

tpm_changeownerauth
tpm_clear
tpm_createek
tpm_getpubek
tpm_nvdefine
tpm_nvinfo
tpm_nvread
tpm_nvrelease
tpm_nvwrite
tpm_resetdalock
tpm_restrictpubek
tpm_restrictsrk
tpm_revokeek
tpm_sealdata
tpm_unsealdata
tpm_selftest
tpm_setactive
tpm_setclearable
tpm_setenable
tpm_setoperatorauth
tpm_setownable
tpm_setpresence
tpm_takeownership
tpm_version

Registry TPM 1.2

TPM čip obsahuje tzv. Platform Control Registry. Tyto jsou při startu počítače inicializované na nulu a postupně plněné pomocí tzv. Extend operace (vizte dále).

#	BIOS/UEFI registry
PCR#0	Hash BIOSu/UEFI
PCR#1	Hash datových struktur BIOSu/UEFI
PCR#2	Hash rozšiřujících karet
PCR#3	Hash datových struktur rozšiř. karet
PCR#4	Hash MBR kódu/UEFI aplikace
PCR#5	Hash MBR/GPT partition tabulky
PCR#6	State transition/wake events
PCR#7	Obvykle jen SecureBoot data
PCR#8 – PCR#15	**K použití operačním systémem**
PCR#16 – PCR#24	Vyhrazené (debug, DRTM)

PCR#10 – využívá Linux IMA (nepoužívejte)

TPM 1.2 device v Linuxu – PCR data

Ukázka hodnot PCR (v podobě hexadecimálního dumpu) z běžíciho systému s tpm-luks.

```
# cat /sys/class/tpm/tpm0/pcrs

PCR-00: 84 BE A5 4B 82 66 19 BA B8 76 42 E4 A4 38 E1 BD 17 43 14 ED
PCR-01: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR-02: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR-03: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR-04: 54 32 DA FC 2A CF CB EC D5 86 E8 34 D1 43 19 CD C5 B3 E5 14
PCR-05: 71 3A 7F F3 CC 94 E9 55 9F F7 E3 C1 7D A1 03 F2 9E 30 D8 06
PCR-06: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR-07: 5B 93 BB A0 A6 64 A7 10 52 59 4A 70 95 B2 07 75 77 03 45 0B
PCR-08: 38 B1 56 2E A4 CE 6E 0F F7 6A 5D 6D EF 37 59 A9 28 38 43 98
PCR-09: 1E 38 C3 7C 91 D0 32 F4 36 18 1E 72 40 54 31 FE FB F0 25 B4
PCR-10: E4 02 55 67 4E AB 1E 8D 94 67 30 E5 D6 DB A7 0F A3 F3 C2 76
PCR-11: 0A 12 D7 0A 69 04 C6 A8 E7 76 DB C5 AC 5C C5 5C 17 69 3C 3F
```

Measured boot

Každá událost (načtení kódu nebo dat) při bootu je zahashována

Události z bootu/OS se hashují jen tehdy, pokud bootloader/OS podporují operaci PCR Extend.

Hashe jsou použity pro tzv. extenzi PCR

PCR[x] = SHA-1(PCR[x_old] || SHA-1(ExtendData))

Po každé PCR extenzi je TPM v unikátním stavu

Measured BIOS boot

Využití PCR v tpm-luks při legacy (BIOS) bootu.

#	Obsah
PCR#0	BIOS code
PCR#1	BIOS data
PCR#4	MBR code (GRUB stage1)
PCR#5	MBR data (part table)
PCR#9	GRUB stage1.5
PCR#9	GRUB stage2
PCR#8	GRUB moduly
PCR#11	GRUB příkazy
PCR#9	kernel
PCR#9	kernel command line
PCR#9	initramdisk

Measured UEFI boot

Využití PCR v tpm-luks při UEFI bootu.

#	Obsah
PCR#0	UEFI code
PCR#1	UEFI data (některé proměnné)
PCR#4	EFI aplikace (SHIM nebo GRUB), GRUB aplikace (pokud se používá nový SHIM)
PCR#5	GPT data
PCR#7	Konfigurace SecureBoot
PCR#9	GRUB aplikace (pokud se používá starý SHIM)
PCR#8	GRUB moduly
PCR#11	GRUB příkazy
PCR#9	kernel
PCR#9	kernel command line
PCR#9	initramdisk

TPM device v Linuxu – proběhlá měření

```
# cat /sys/kernel/security/tpm0/ascii_bios_measurements

0 dfcfef6bb33aebaa4f36d477311ae24d04a17a64 07 [S-CRTM Contents]
0 7a32c13c59aaf9a3ac1ef943c289184eb4ca9bfd 07 [S-CRTM Contents]
0 c072a07a291e53fe2ed2bfe4ee55ac83c934d547 07 [S-CRTM Contents]
0 a2e99f88eb32f4bc207611f7b84cdc9bf1ed7374 07 [S-CRTM Contents]
4 6d93b649037a9047c423e3fda6983e8ee8c4062d 0c [Compact Hash]
5 521e66aef74ca8a2afe6dac7807940f03e9aabae 0c [Compact Hash]
9 69f376657011624e616b1ff51b8a7eef930332e8 0c [Compact Hash]
9 b9b516017bc0a784e376112554bc0caa2b644497 0c [Compact Hash]
9 91b28eb21499728b972337be15431d2b4be9351d 0d [IPL]
9 91c7919039204bc5dc7f1e184561ece79d6edefa 0d [IPL]
9 5b249d0edb711dc18d889c97040d51340d4d4c39 0d [IPL]
# hexdump -C /sys/kernel/security/tpm0/binary_bios_measurements
```

Proběhlá měření se zaznamenávají. To má výhodu, že dokážete zrekonstruovat hash v PCR registru na základě hashů jednotlivých měření. Zároveň víte, která měření jsou „vaše“ a která BIOSu.

Vnitřní paměť TPM (NVRAM)

Jednotky kilobyte

Paměť adresovaná pomocí číselných indexů

Každý index paměti může mít různá oprávnění:
- lze číst/zapisovat kýmkoli
- lze číst/zapisovat na základě znalosti owner/NVRAM hesla
- lze číst/zapisovat na základě konkrétního stavu PCR registrů

Inicializace TPM a práce s NVRAM

```
tpm_takeownership

tpm_nvinfo

tpm_nvdefine

tpm_nvwrite

tpm_nvread
```

```
# tpm_nvinfo
NVRAM index    : 0x00000002 (2)
PCR read selection:
 PCRs          : 0, 2, 4, 5, 6, 9
 Localities    : ALL
 Hash          : f49edf4f5e9b837b72ddd6bc584cf6ed6a1acba3
PCR write selection:
 Localities    : ALL
Permissions    : 0x00040004 (AUTHREAD|AUTHWRITE)
bReadSTClear   : FALSE
bWriteSTClear  : FALSE
bWriteDefine   : FALSE
Size           : 32 (0x20)
```

```
# tpm_nvread -i 2 --password=xxx
spi_NV_ReadValue failed: 0x00000018 - layer=tpm,
code=0018 (24), Wrong PCR value

# tpm_nvinfo
NVRAM index    : 0x00000011 (17)
PCR read  selection:
PCRs      : 0, 2, 4, 5, 6, 9
Localities    : ALL
Hash      : f95e729fba2a11129e288e1c66ba8eced66b1619
PCR write selection:
Localities    : ALL
Permissions    : 0x00040004 (AUTHREAD|AUTHWRITE)
bReadSTClear  : FALSE
bWriteSTClear : FALSE
bWriteDefine  : FALSE
Size          : 32 (0x20)

# tpm_nvread -i 17 --password=xxx
00000000  78 37 42 ee f2 2a 8a 29 4d c5 f8 7a a6 5a 18 75
00000010  b7 3f f9 de 64 78 10 09 19 bc 52 eb 28 98 4f d2
```

Vnitřní paměť TPM (NVRAM)

Mem Index#	Stav PCR registrů	Oprávnění
2	PCR[0]=356a192b7913b04c54574d18c28d46e6395428ab PCR[2]=da4b9237bacccdf19c0760cab7aec4a8359010b0 PCR[4]=77de68daecd823babbb58edb1c8e14d7106e83bb PCR[9]=1b6453892473a467d07372d45eb05abc2031647a composite_hash=7110eda4d09e062aa5e4a390b0a572ac0d2c0220	AUTHREAD|AUTHWRITE
3	PCR[0]=356a192b7913b04c54574d18c28d46e6395428ab PCR[2]=da4b9237bacccdf19c0760cab7aec4a8359010b0 PCR[4]=0d1609486182776c987aa00d32d5156845bf9edb PCR[9]=825256d5a3b28f88e18d2fc2f6c93d07ecd4fdd5 composite_hash=9dd01068d41ff370f712b6f1c2f0e873e6ed4e27	AUTHREAD|AUTHWRITE

Ukázka dvou NVRAM indexů a podmínek, za kterých dojde k vydání dat z NVRAM (má-li uživatel oprávnění – NVRAM password – a jsou-li PCR ve správném stavu).

Jak používat LUKS spolu s TPM?

Nástroje podporující TPM

trousers, TPM-enabled Grub, skripty

Vygenerování initramfs + úprava konfigurace GRUBu

```
+panic=60 -splash
GRUB_DEFAULT=saved
GRUB_SAVEDEFAULT=true
update-grub && grub-install /dev/sdX
update-initramfs -k all -u
reboot
```

Inicializace TPM

```
TPM clear (BIOS) + tpm_takeownership
```

Jak používat LUKS spolu s TPM?

Nové heslo pro LUKS

`luksAddKey`

Spočítání stavu systému po rebootu

`Replay BIOS událostí,`
`hashe grubu/kernelu/cmdline/initramfs`

Uložení hesla pro LUKS do TPM NVRAM s využitím spočítaného stavu

`tpm_nvdefine + tpm_nvwrite`

Odemčení disku při bootu pomocí skriptů v initramfs

`Vyčtení NVRAM a použití dat pro luksOpen`

Nástroje pro uložení LUKS hesla v TPM

Nástroje pro uložení LUKS hesla v TPM

NEJSOU

Nástroje pro uložení LUKS hesla v TPM

NEBO...?

https://github.com/shpedoikal/tpm-luks
https://github.com/fox-it/linux-luks-tpm-boot
https://security.stackexchange.com/questions/124338/right-way-to-use-the-tpm-for-full-disk-encryption

Existuje neudržovaná verze tpm-luks od GITHUB uživatele shpedoikal pro Fedoru 16. Existuje manuální postup od Github uživatele fox-it. Žádná z nich nepodporuje předpočítávání stavu při update initramdisku, kernelu, boot loaderu.

Nástroje pro uložení LUKS hesla v TPM

github.com/zajdee/tpm-luks

(vyžaduje ~~*Neumím nainstalovat Debian*~~ Ubuntu 16.10/17.04)

BIOS boot s MBR
vs.
BIOS boot s GPT
vs.
UEFI boot s GPT

Všechny výše uvedené kombinace bootu jsou tpm-luksem podporovány.

Measured boot
vs.
Secure boot

Se secure bootem tpm-luks nefunguje – hlavně proto, že se používá vlastní (nepodepsaný) Grub. Pokud si dokážete podepsat Grub, fungovalo by to taky.

Změny v systému, reinstalace

Aktualizace initrd

Upgrade grubu nebo update konfigurace

Reinicializace tpm-luks

Upgrade systému

Pokud aktualizujete initrd, stav systému (po rebootu) se dopočítá a uloží se nový index do NVRAM. Pokud updatujete grub nebo jeho konfiguraci, musíte nechat stav systému přepočítat ručně – doporučuji spustit update-initramfs -k all -u. Pokud ztratíte přístup k datům v TPM NVRAM, stačí reinicializovat tpm-luks pomocí tpm-luks-init (nezapomeňte pomocí luksKillSlot smazat starý tpm-luks index v LUKS konfiguraci). Upgradujete-li systém, Ubuntu vám odebere PPA repozitáře – před rebootem systému je tedy znovu přidejte, proveďte upgrade a reinstalaci grubu a tpm-luks, přegenerování initramfs a rebootujte. Pro případ nouze mějte vždy jiný způsob, jak zadat heslo po rebootu!

DEMO

2010: Po šesti měsících a mnoha zničených TPM modulech se podařilo jeden konkrétní model TPM čipu chirurgicky rozkuchat a data vyčíst. Útok typu Cold-boot zmrazí paměť a vyčítá ji po rebootu a snaží se najít LUKS master key, DMA vyčítá paměť za běhu PC (např. pomocí FireWire/Thunderbolt nebo PCI-E karty), Evil-maid attack infikuje počítač např. úpravou initramfs, který zaloguje uživatelem zadané heslo/pošle je po síti (projeví se výzvou LUKSu – zadej heslo).

Bezpečnost

Zranitelnost v TPM je hrozivá* (2010)

http://computerworld.cz/securityworld/zranitelnost-v-tpm-je-hroziva-47442

TPM reset attack (~2005) (LPC attack)

http://trousers-users.narkive.com/TVSfSEu8/tpm-reset-attack-on-lpc-bus

tpm-luks

kernel cmdline: **`panic=60`**

účet **Guesta**

`tpm_nvread` z **běžícího systému**

použití kernel keyringu pro uložení LUKS hesla

Cold-boot, DMA, Evil-maid attack

Názory? Dotazy?

Děkuji za pozornost

@zajDee