BitLocker šifrování v Linuxovém prostředí

Diplomová práce

Vojtěch Trefný

Fakulta aplikované informatiky UTB

4. června 2019

Vedoucí: Ing. Michal Bližňák, Ph.D.
Konzultant: Ing. Milan Brož, Ph.D.
Oponent: Mgr. Martin Kolman

Motivace

Šifrování disku

- Jediná spolehlivá metoda ochrany dat v případě ztráty nebo krádeže přenosného zařízení.
- Především pro ochranu notebooků a přenosných disků.

Heterogenní prostředí

- Neexistuje jednoduchý způsob řešení šifrování v prostředí MS Windows i GNU/Linux.
- Bez nástrojů třetích stran nefungují nativní řešení jednoho prostředí v druhém.
- Multiplatformní řešení vyžadují ruční instalaci a nejsou integrována do systému.

Cíl práce

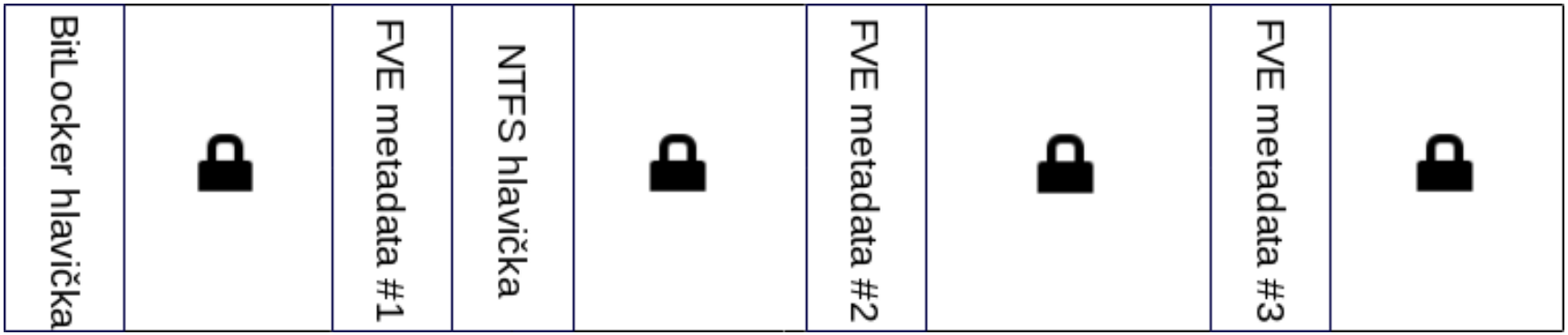
- Prozkoumat technologii BitLocker a možnosti její podpory v linuxovém prostředí.
- Vytvořit nové nebo upravit stávající nástroje pro práci s BitLocker v prostředí GNU/Linux.
- Integrovat řešení do stávajících nástrojů tak, aby nebyla vyžadována interakce ze strany uživatele.
- Ideálně by uživatel neměl poznat, že nepracuje s nativním šifrováním.

BitLocker

- Nativní šifrování disku v prostředí Microsoft Windows.
- Poprvé představen ve Windows Vista.
- Není oficiálně standardizován, ale používá standardizované kryptografické funkce:
  - AES-CCM pro šifrování klíčů,
  - AES-XTS (AES-CBC) pro šifrování dat a
  - SHA256 pro odvození klíče.

Struktura BitLocker zařízení

- Hlavička – identifikace zařízení
- FVE metadata – klíče
- NTFS hlavička – šifrovaná hlavička pro otevřené zařízení
- Šifrovaná data



LUKS/dm-crypt

Device mapper

- Kernelový ovladač sloužící pro tvorbu „mapovaných“ blokových zařízení.
- Primárně slouží pro vytvoření menších blokových zařízení nad jedním diskem nebo naopak spojení více disků do jednoho zařízení.

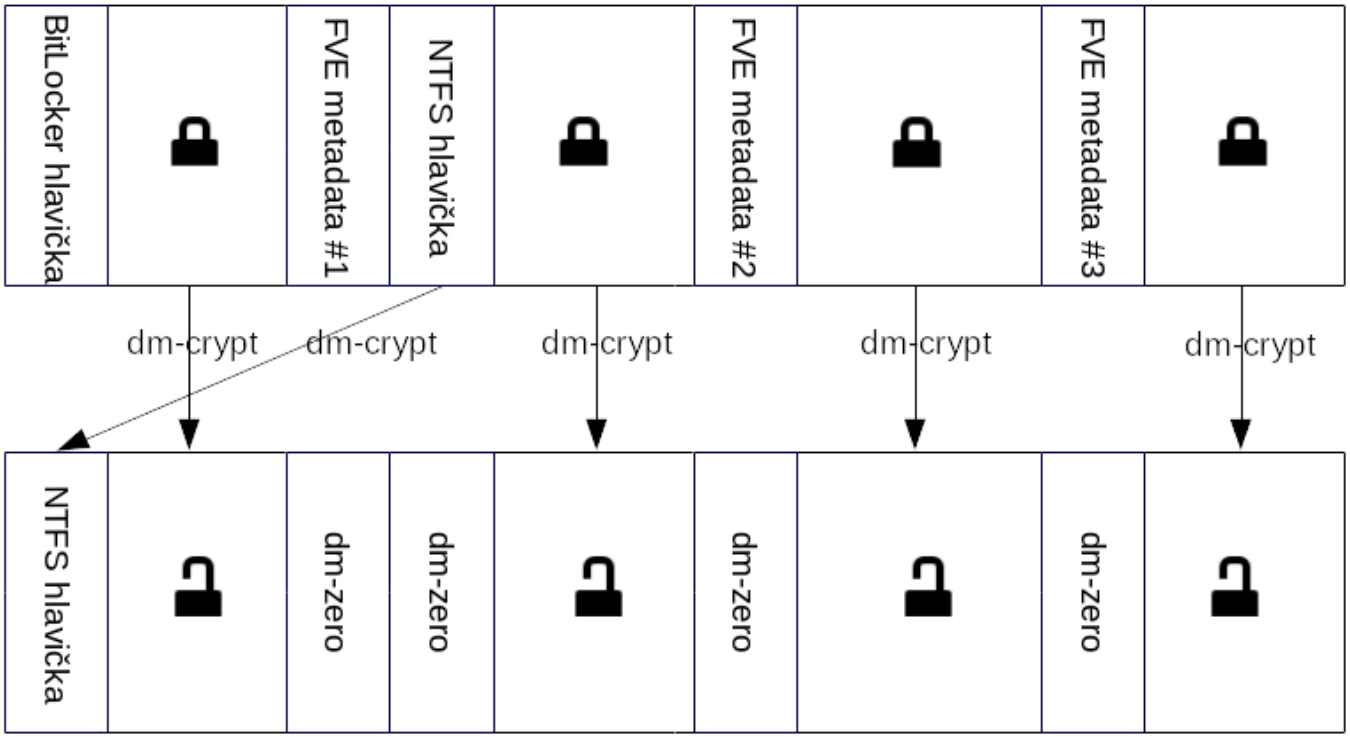
LUKS/dm-crypt

- Nativní technologie pro šifrování disků v linuxových systémech.
- Crypto target slouží pro vytvoření zařízení, které při čtení/zápisu data transparentně (de)šifruje.
- Ve výchozím nastavení používá pro šifrování dat AES-XTS.

BitLocker v Linuxu

Device mapper

- Device mapper potřebuje znát:
  - použitou šifru (AES-XTS),
  - inicializační vektor (číslo sektoru),
  - klíč a
  - umístění dat na zařízení.



Nástroj bitlockersetup

- Nově vytvořený nástroj pro práci s BitLocker zařízeními.
- Umožňuje odemknout a uzamknout dané zařízení.
- Při odemykání:
  - Z BitLocker metadat získá klíč (dešifruje jej pomocí uživatelem zadaného hesla) a strukturu zařízení (umístění jednotlivých datových oblastí) a
  - pomocí nástroje `dmsetup` vytvoří otevřené zařízení.

```
$ sudo bitlockersetup open /dev/sdb1
Password for '/dev/sdb1':
Created device mapper device '/dev/mapper/bitlocker-1f8bf...8f40'.
```

Integrace do existujících nástrojů

UDisks

- UDisks je systémový démon, který poskytuje API pro práci s blokovými zařízeními.
- Poskytuje také funkcionalitu pro odemykání šifrovaných zařízení.
- V rámci práce byla to UDisks přidána podpora pro práci s BitLocker zařízeními pomocí nástroje bitlockersetup.
- UDisks díky tomu označí BitLocker zařízení jako šifrovaná a poskytne funkce pro jeho odemčení a uzamčení.
- Z pohledu uživatelů UDisks API není rozdíl mezi zařízením šifrovaným pomocí BitLocker a LUKS/dm-crypt.

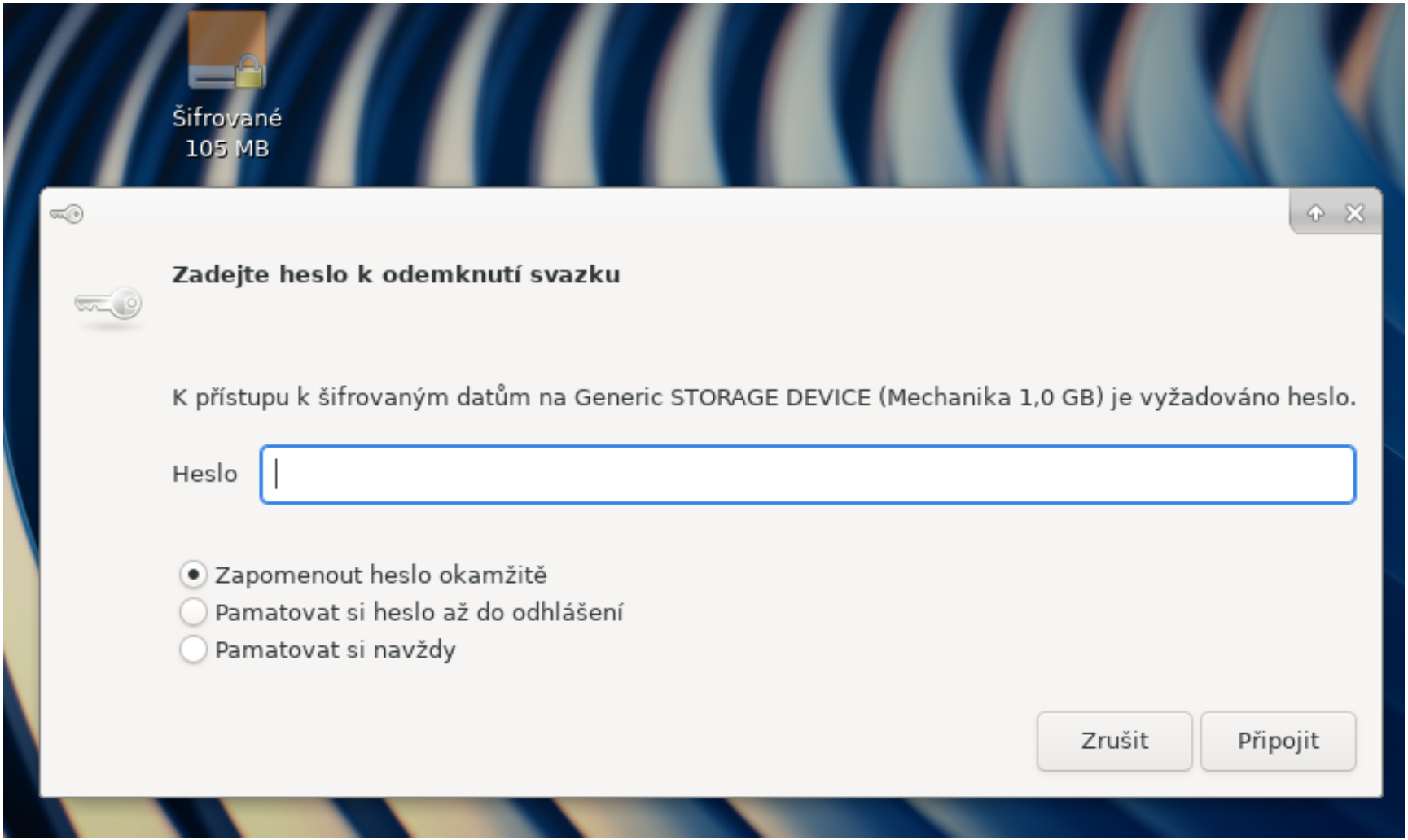
Integrace do existujících nástrojů

```
/org/freedesktop/UDisks2/block_devices/sda2:
  org.freedesktop.UDisks2.Block:
...
    Id:
    IdLabel:
    IdType:                    BitLocker
    IdUUID:                    1f8bf933-8323-4c97-...
    IdUsage:                   crypto
  org.freedesktop.UDisks2.Encrypted:
    ChildConfiguration:        []
    CleartextDevice:           '/'
    HintEncryptionType:         BitLocker
```

UDisks

- Používá bitlockersetup pro identifkace BitLocker zařízení a zjištění dodatečných informací.
- Nabízí funkce `Unlock` a `Lock` pro odemčení a uzamření zařízení.

Grafické rozhraní



Možná rozšíření do budoucna

- Podpora ostatních (starších a méně obvyklých) variant BitLockeru. (Bude vyžadovat změny v kernelu.)
- Přidání vytvořeného nástroje do oficiálních repozitářů vybraných linuxových distribucí.
- Začlenění do projektu cryptsetup, který poskytuje knihovnu a nástroj pro práci s šifrovanými zařízeními v Linuxu (LUKS, VeraCrypt, Loop-AES).

Dotazy k obhajobě

Otázka

Myslím si, že po začlenění podpory pro Bitlocker do linuxových distribucí by tato technologie mohla sloužit jako dobrý nástroj pro přenos šifrovaných dat mezi Windows a Linuxem bez nutnosti doinstalování softwaru třetích stran. Pro plné využití tohoto potenciálu by se však hodila možnost vytvářet nová Bitlocker zařízení nejen na Windows, ale i na Linuxu. Je tvorba nových Bitlocker zařízení na Linuxu v budoucnu proveditelná?

Odpověď

Teoreticky to možné je. Bohužel v BitLocker metadatech je stále mnoho neznámých položek, takže by mohlo být složité vytvořit zařízení, které bude v MS Windows skutečně stoprocentně funkční. Nabízí se také otázka, jak by se k takové implementaci postavila společnost Microsoft.

Závěr

Děkuji vám za pozornost.

Prostor pro vaše dotazy.