Bitlocker šifrování v Linuxovém prostředí

Diplomová práce – kontrolní den č. 2

Vojtěch Trefný

Fakulta aplikované informatiky UTB

5. 4. 2019

Osnova

Zadání

- **Vedoucí:** Ing. Michal Bližňák Ph.D.
- **Konzultant:** Ing. Milan Brož Ph.D. (Red Hat Czech/CRoCS FI MUNI)

- Seznamte se s nástrojem Windows Bitlocker pro šifrování disků.
- Popište podporované šifrovací módy a možnosti správy klíčů.
- Analyzujte použitá kryptografická primitiva a jejich atributy.
- Seznamte se s nástrojem a knihovnou libbde a možnostmi přístupu k Bitlocker obrazu disku v prostředí OS Linux.
- Navrhněte a podle možností implementujte nutná rozšíření Linuxových nástrojů pro jednoduchý přístup k obsahu Bitlocker disku.

Implementace

Získání (de)šifrovacího klíče

- Vlastní jednoduchý program, který z BitLocker hlaviček (při znalosti hesla) získá klíč pro (de)šifrování dat (FVEK).
- Klíč samotný je uložený v metadatové části zařízení zašifrovaný dalším klíčem (VMK), který je zašifrován klíčem odvozeným z hesla.

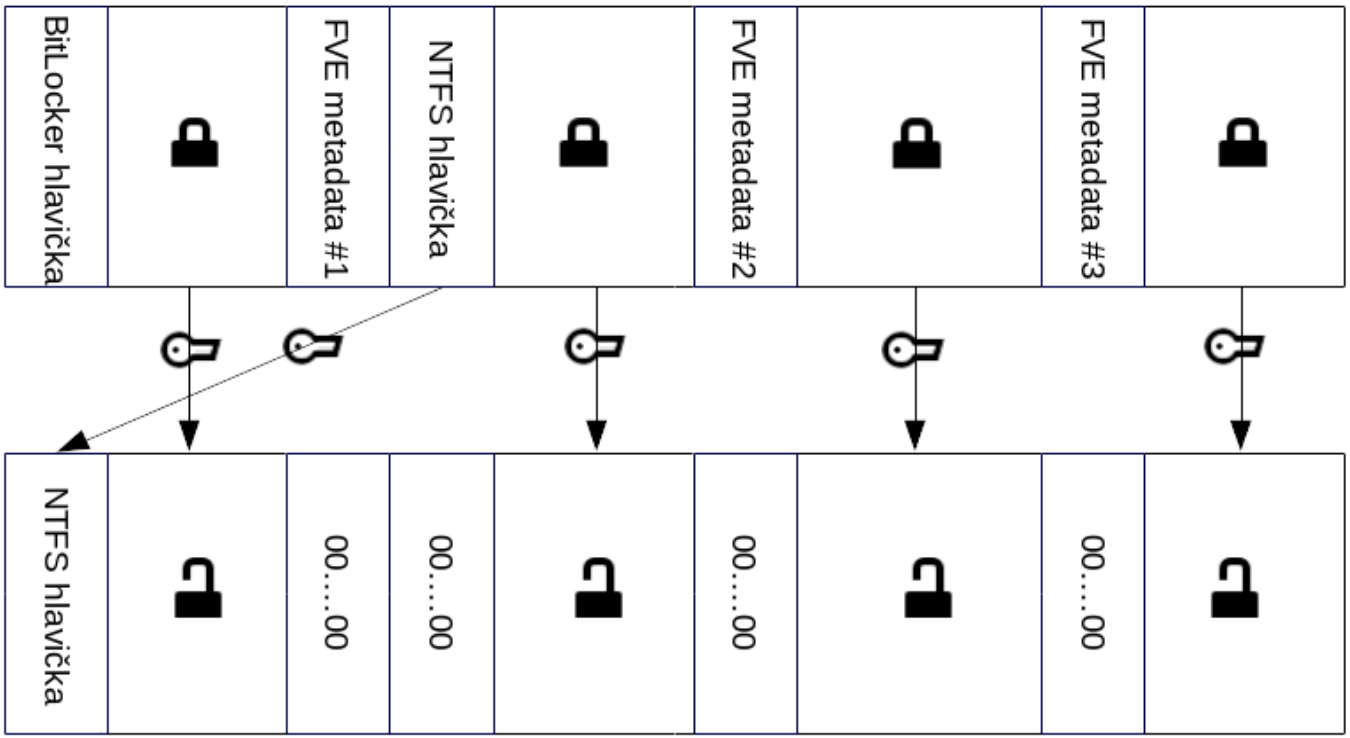
Identifikace datových oblastí

- Vlastní zašifrovaná dat jsou na disku uložena nesouvisle, prokládaná metadaty.
- Prvních 16 sektorů (NTFS hlavička) je uloženo na speciálním offsetu.

Implementace II

Device mapper

- Za znalosti (de)šifrovacího klíče a struktury dat na disku lze vytvořit device-mapper zařízení.
- Data jsou (de)šifrována dle potřeby v době čtení/zápisu daného sektoru.



```
$ sudo bitlockersetup /dev/sdc2 bitlocker
Password for '/dev/sdc2':
Created device mapper device '/dev/mapper/bitlocker'.

$ lsblk -f /dev/sdc2
NAME         FSTYPE LABEL UUID
sdc2
\_bitlocker ntfs          A4843D7D843D5352

$ sudo dmsetup table --showkeys bitlocker
0 16 crypt aes-xts-plain64 a4d0...f52 68904 8:34 68904
16 68760 crypt aes-xts-plain64 a4d0...f52 16 8:34 16
68776 128 zero
68904 16 zero
68920 21424 crypt aes-xts-plain64 a4d0...f52 68920 8:34 68920
90344 128 zero
90472 22632 crypt aes-xts-plain64 a4d0...f52 90472 8:34 90472
113104 128 zero
113232 91568 crypt aes-xts-plain64 a4d0...f52 113232 8:34 113232
```

Další kroky

- Rozsáhlejší testování – integrita dat a souborového systému po zápisu, extrémně velká zařízení, zaplnění zařízení...
- Integrace s nástroji pro správu blokových zařízení v Linuxu:
  - UDev, libblkid – detekce BitLocker signatury
  - libblockdev – API pro odemykání
  - UDisks – detekce, DBus API pro odemykání (pro GVFS)
- Doladění existující implementace – chybové stavy, záložní heslo...
- Podpora ostatních (starších a méně obvyklých) variant BitLockeru.
- Práce na textové části práce.

Procentuální splnění zadání

Rešerše

- seznámení s nástrojem BitLocker – **100 %**
- seznámení s existujícími řešeními (libbde, dislocker) – **100 %**
- popis šifrovacích módů, správy klíčů, použitých kryptografických fcí – **15 %**

Implementace

- nástroj pro práci s BitLocker v Linuxu – **90 %**
- integrace s existujícími nástroji pro práci se storage – **20 %**

Závěr

Děkuji vám za pozornost.

Prostor pro vaše dotazy.