Bitlocker šifrování v Linuxovém prostředí

Diplomová práce – kontrolní den č. 1

Vojtěch Trefný

Fakulta aplikované informatiky UTB

1. 3. 2019

Osnova

Zadání

- **Vedoucí:** Ing. Michal Bližňák Ph.D.
- **Konzultant:** Ing. Milan Brož (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.

Dostupné zdroje informací

- Původní implementace pro Windows Vista je popsána Nielsem Fergusonem v článku *AES-CBC + Elephant diffuser A Disk Encryption Algorithm for Windows*
- Novější varianty částečně popisuje Dan Rosendorf v článku *Bitlocker: A little about the internals and what changed in Windows 8*.
- Velmi dobrou specifikaci formátu BitLocker obsahuje také dokumentace ke knihovně `libbde` od Joachima Metze.
- Existují i další zdroje, které se většinou věnují prvním verzím BitLockeru v době jeho vzniku v roce 2006.

Podpora použitých kryptografických funkcí

Userspace

- Používané kryptografické algoritmy:
  - AES-CCM
  - SHA256
- Plně podporované ve standardních kryptografických knihovnách (`libopenssl`, `libgcrypt`).

Kernel

- Používané kryptografické algoritmy:
  - AES-CBC 128/256bit (Windows Vista)
  - AES-CBC 128/256bit + Elephant Diffuser (Windows Vista)
  - AES-XTS 128/256bit (Windows 7+)
- V kernel crypto API podporavané kromě Elephant.

Prototyp pro práci s BitLockerem v Linuxu

- Jednoduchý „proof-of-concept“ napsaný v Pythonu s použitím knihovny `pycryptoraphy`.
- Pouze základní podpora pro data šifrovaná pomocí AES-XTS (BitLocker varianta ve Windows 7+).

- V současné době zvládá:
  - Odvodit dešifrovací klíč z hesla nebo záložního (recovery) hesla.
  - Dešifrovat klíče uložené v BitLocker hlavičce (`VMK` a `FVEK`).
  - Dešifrovat první sektor disku (NTFS hlavička) pomocí `FVEK`.

Ukázka – BitLocker hlavička

```
Encryption:         AES-XTS 128-bit encryption
Identifier:         1f8bf933-8323-4c97-8a89-a67625ac8f40
Creation time:      2019-02-03 09:10:22.265406
Description:        DESKTOP-NPM7RCA G: 2/3/2019

VMK
        Identifier:         f0f61678-fb6f-4ab1-934a-...
        Type:               VMK protected with password
        Salt:               03 d1 b4 23 6b f4 5b df ...
        AES-CCM encrypted key
                Nonce:      2019-02-03 09:10:36.052000
                Count:      3
                Key:        0d a8 61 01 ...
```

Ukázka – BitLocker první sektor

```
00000000: eb 52 90 ... 08 00 00 |.R.NTFS     .....|
00000010: 00 00 00 ... 28 03 00 |........  ?....(..|
00000020: 00 00 00 ... 00 00 00 |........  ........|
00000030: 55 21 00 ... 00 00 00 |U!......  ........|
00000040: f6 00 00 ... 3d 84 a4 |........  RS=.}=..|
...
00000180: b4 0e bb ... 20 64 69 |........  ....A di|
00000190: 73 6b 20 ... 20 6f 63 |sk read   error oc|
000001a0: 63 75 72 ... 4d 47 52 |curred..  .BOOTMGR|
000001b0: 20 69 73 ... 64 00 00 | is comp  ressed..|
000001c0: 0a 50 72 ... 6c 74 2b |.Press C  trl+Alt+|
000001d0: 44 65 6c ... 74 0d 0a |Del to r  estart..|
000001e0: 00 00 00 ... 00 00 00 |........  ........|
```

Další kroky

- Rozšíření současného prototypu o podporu pro čtení celého šifrovaného disku.
- Testování s použitím standardních nástrojů pro tvorbu blokových zařízení v Linuxu (`device-mapper`/`dmsetup`).
- Případné rozšíření `dm-crypt` modulu o chybějící funkcionalitu (pravděpodobně podpora odvození IV).
- Implementace prototypu jako knihovny v jazyce C tak, aby jej šlo použít v existujících nástrojích/knihovnách jako `cryptsetup` a/nebo `UDisks`.
- Podpora ostatních (starších a méně obvyklých) variant BitLockeru.

Závěr

Děkuji vám za pozornost.

Prostor pro vaše dotazy.