Bitlocker šifrování disku v Linuxovém prostředí

Bc. Vojtěch Trefný

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

*** Nascanované zadání, strana 1 ***

*** Nascanované zadání, strana 2 ***

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně .....

podpis autora

ABSTRAKT

Text abstraktu česky

Klíčová slova: Přehled klíčových slov

ABSTRACT

Text of the abstract

Keywords: Some keywords

Zde je místo pro případné poděkování, motto, úryvky knih, básní atp.

OBSAH

ÚVOD

První odstavec pod nadpisem se neodsazuje, ostatní ano (pouze první řádek, odsazení vertikální mezy odstavci je typycké pro anglickou sazbu; czech babel toto respektuje, netřeba do textu přidávat jakékoliv explicitní formátování, viz ukázka sazby tohoto textu s následujícím odstavcem).

Formátování druhého odstavce. Text text text text text text text text text text text text.

I. TEORETICKÁ ČÁST

1 BitLocker

text

1.1 Diskový formát

TODO: jak lépe říct on-disk format

1.1.1 Hlavička

Stejně jako u většiny diskových formátů, je i u BitLockeru na začátku disku takzvaná hlavička, která obsahuje základní informace o použitém formátu a jeho vlastnostech a také k jeho rychlé identifikaci. BitLocker hlavička zabírá celkem 512 bajtů a je u ní patrná inspirace u souborového systému NTFS. V tabulce 1.1 jsou zobrazeny jednotlivé (známé[1)]) položky hlavičky BitLockeru a pro srovnání také stejné položky v hlavičce souborového systému NTFS.

Struktura NTFS hlavičky je převzata z [3], struktura BitLocker hlavičky je pak částečně převzata z [2], částečně z [4] a částečně výsledkem vlastního zkoumání.

Z pohledu identifkace BitLocker zařízení je nejdůležitější částí hlavičky 8 bajtů na offsetu 3, které se u NTFS formátu nazývají *OEM název* a které slouží pro rychlou identifikace zařízení. V linuxových systémech se podobné identifikátory obvykle nazývají *signatura*. Pro BitLocker formát je (u všech verzí) signatura v ASCII podobě `-FVE-FS-`.

TODO: To by asi chtělo citaci.

Pro další práci s BitLockerem není většina položek hlavičky zajímavá. Výjimku tvoří GUID identifkátor uložený na offsetu 160 (16 bajtů dlouhý UTF-8 string) a trojice *uint32* hodnot na offsetech 176, 184 a 192, které obsahují umístění (jako relativní offset od začátku zkoumaného zařízení) tří bloků FVE metadat. Všechny tyto čtyři hodnoty jsou v BitLocker hlavičce umístěny na offsetech, které jsou v NTFS součástí *bootcode*.

Umístění všech výše zmíněných „důležitých“ částí BitLocker hlavičky je zobrazeno na obrázku 1.1.

1.1.2 FVE metadata

Samotná výše popsaná hlavička formátu BitLocker neobsahuje o samotném BitLockeru téměř žádné informace. Slouží především pro rychlou identifikaci zařízení jako zařízení šifrovaného pomocí technologie BitLocker. Všechny informace potřebné pro práci s tímto zařízením, tedy především způsob uložení dat, jejich umístění, způsob jakým jsou

[1)] Struktura formátu BitLocker není společností Microsoft nikde veřejně zcela kompletně zdokumentována, význam jednotlivých položek tedy nemusí být vždy přesně znám.

Tab. 1.1 Porování položek hlaviček BitLocker a NTFS

offset	velikost	BitLocker	NTFS
0	3	boot kód	
3	8	OEM název (signatura)	
11	2	počet bajtů na sektor	
13	1	počet sektorů na cluster	
14	2	rezervované sektory	
16	4	nepoužito	
21	1	popisek média	
22	18	nepoužito	
40	8	počet sektorů	
48	8	adresa prvního clusteru MFT	
56	8	kopie adresy prvního clusteru MFT	
64	1	velikost MFT entry	
65	3	nepoužito	
68	1	velikost indexu	
69	3	nepoužito	
72	8	NTFS serial number	
80	4	nepoužito	
84	76	boot kód	
160	16	BitLocker GUID	boot kód
176	8	offset první kopie FVE metadat	
184	8	offset druhé kopie FVE metadat	
192	8	offset třetí kopie FVE metadat	
200	310	boot kód	
510	2	signatura (`0xaa55`)	

šifrovány a hlavně klíč pro jejich (de)šifrování je uložený na třech různých místech[2)] definovaných v hlavičce. Jedná se o tři identické kopie[3)] takzvaných *FVE metadat*.

FVE metadata se skládají z celkem tří částí – hlavičky FVE bloku (*FVE metadata block header*), samotné FVE hlavičky (*FVE metadata header*) a různého množství FVE záznamů (*FVE metadata entry*, které obsahují samotné klíče a další důležité informace[2][4)].

Důležité položky v obou hlavičkách, jejich velikosti a offsety (vztažené vůči začátku dané hlavičky) jsou uvedeny v tabulce 1.2. Kompletní struktura obou hlaviček

[2)] Na offsetech přibližně ve 33 %, 44 % a 55 % u testovaných BitLocker zařízeních.

[3)] Tři kopie jsou zvoleny pravděpodobně jako záloha pro případ náhodného poškození metadat. Vzhledem k tomu, že bez kompletní nepoškozené kopie těchto metadat není možné data na zařízení dešifrovat, je vícenásobná záloha na místě.

[4)] Toto dělení zavádí Joachim Metz v [2]. Teoreticky by se daly dvě první části metadat spojit, protože na disku se nachází vždy hned za sebou, ale rozdělení dává smysl, protože první část se týká popisu samotných metadat (signatura, verze, umístění všech tří bloků), zatímco druhá část už obsahuje samotná metadata (GUID, čas vytvoření, použitý šifrovací algoritmus).

Obr. 1.1 BitLocker hlavička se zvýrazněnou signaturou, GUID a trojicí offsetů FVE metadat

```
00000000  eb 58 90 2d 46 56 45 2d  46 53 2d 00 02 08 00 00 |.X.-FVE-FS-.....|
00000010  00 00 00 00 00 f8 00 00  3f 00 ff 00 00 28 03 00 |........?....(..|
00000020  00 00 00 00 e0 1f 00 00  00 00 00 00 00 00 00 00 |................|
00000030  01 00 06 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
00000040  80 00 29 00 00 00 00 4e  4f 20 4e 41 4d 45 20 20 |..)....NO NAME  |
00000050  20 20 46 41 54 33 32 20  20 20 33 c9 8e d1 bc f4 |  FAT32   3.....|
00000060  7b 8e c1 8e d9 bd 00 7c  a0 fb 7d b4 7d 8b f0 ac |{......|..}.}...|
00000070  98 40 74 0c 48 74 0e b4  0e bb 07 00 cd 10 eb ef |.@t.Ht..........|
00000080  a0 fd 7d eb e6 cd 16 cd  19 00 00 00 00 00 00 00 |..}.............|
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
000000a0  3b d6 67 49 29 2e d8 4a  83 99 f6 a3 39 e3 d0 01 |;.gI)..J....9...|
000000b0  00 50 19 02 00 00 00 00  00 d0 c1 02 00 00 00 00 |.P..............|
000000c0  00 a0 73 03 00 00 00 00  00 00 00 00 00 00 00 00 |..s.............|
000000d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
*
00000100  0d 0a 52 65 6d 6f 76 65  20 64 69 73 6b 73 20 6f |..Remove disks o|
00000110  72 20 6f 74 68 65 72 20  6d 65 64 69 61 2e ff 0d |r other media...|
00000120  0a 44 69 73 6b 20 65 72  72 6f 72 ff 0d 0a 50 72 |.Disk error...Pr|
00000130  65 73 73 20 61 6e 79 20  6b 65 79 20 74 6f 20 72 |ess any key to r|
00000140  65 73 74 61 72 74 0d 0a  00 00 00 00 00 00 00 00 |estart..........|
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 |................|
*
00000190  00 00 00 00 00 00 00 00  78 78 78 78 78 78 78 78 |........xxxxxxxx|
000001a0  78 78 78 78 78 78 78 78  78 78 78 78 78 78 78 78 |xxxxxxxxxxxxxxxx|
*
000001e0  78 78 78 78 78 78 78 78  ff ff ff ff ff ff ff ff |xxxxxxxx........|
000001f0  ff ff ff ff ff ff ff ff  ff ff ff 00 1f 2c 55 aa |.............,U.|
00000200
```

je součástí přílohy .

TODO: odkaz na přílohu

Mezi pro nás zajímavé položky v hlavičce patří její celková velikost (včetně velikosti samotné hlavičky a velikosti za ní následujících záznamů), šifrovací algoritmus použitý pro zašifrování dat uložených na disku (možné algoritmy jsou popsány v části 1.3.1) a v některých případech může být užitečný i čas vytvoření, který je uložen ve formátu `FILETIME`[5)].

1.1.3 FVE záznamy

Za výše uvedenou hlavičkou se nechází blíže nespecifikované množství FVE záznamů. Ty slouží v podstatě jako key-value úložiště pro jakékoli další „informace“, které jsou pro práci s BitLockerem potřebné. Tím, že není třeba předem určeno, kolik takových

[5)] FILETIME je ve skutečnosti struktura sestávající ze dvou 32bit integer hodnot, které dohromady udávají počet 100 nanosekundových intervalů, které k danému datu uplynuly od 1. ledna 1601.[1]

Tab. 1.2 Zjednodušená struktura FVE metadat

Hlavička FVE bloku		
offset	velikost	popis
0	8	signatura (`-FVE-FS-`)
10	2	verze (1 nebo 2)
32	8	offset první kopie FVE metadat
40	8	offset druhé kopie FVE metadat
48	8	offset třetí kopie FVE metadat

FVE hlavička		
0	4	velikost metadat (včetně záznamů)
16	16	GUID
36	4	šifrovací algoritmus
40	8	datum a čas vytvoření

záznamů bude za hlavičkou uloženo, je možné přidávat nové položky při zachování zpětné kompatibility[6)].

Jelikož známe celkovou velikost FVE metadat (je uvedena v hlavičce, viz tabulka 1.2) a celková velikosti hlaviček FVE metadat je pevná (64 a 48 bajtů), pro přečtení všech záznamů stačí číst data ve smyččce, dokud nedojdeme na konec metadat, nebo dokud následující záznam nemá nulovou velikost.

Struktutra FVE je relativně jednoduchá a je popsaná v tabulce 1.3. Důležitou součástí je velikost záznamu, protože podle svého typu může mít různou délku.

Tab. 1.3 Struktura FVE záznamu

offset	velikost	popis
0	2	velikost záznamu
2	2	typ záznamu
4	2	typ hodnoty záznamu
6	2	verze (1)
8		data

Typ a hodnota označují, co je v daném záznamu uloženo. Známé typy a hodnoty jsou popsány v tabulce 1.4. U typů se typicky jedná buď o klíč (FVEK, VMK) nebo obecnou property, hodnota pak dále specifikuje, jak je daný typ uložen (zašifrovaný klíč, unicode string).

Způsob uložení dat záleží na tom, jaká konkrétní data jsou v záznamu uložena. U

[6)] Celková největší možná velikost FVE metadat je 64 KiB (alespoň tedy tolik je pro FVEm metadata vyhrazeno na vytvořených BitLocker zařízeních), teoreticky je tedy možné mít až 64 KiB - 112 B metadat.

„jednoduchých“ záznamů, jako je například popisek je v datech uložen textový řetězec uložený v kódování UTF-16, u „složitějších“ záznamů, jako jsou například klíče, mají data vlastní strukturu včetně dalších záznamů.

Tab. 1.4 Známé typy FVE záznamů

Typy	
typ	popis
0	property
1	VMK
2	FVEK
7	popisek
15	hlavička disku[7)]

Hodnoty	
typ	popis
0	smazáno
1	klíč
2	string
5	AES-CCM šifrovaný klíč
6	TPM klíč
8	VMK
15	offset a velikost

Příklad „jednoduchého“ záznamu je uveden na obrázku 1.2, kde vidíme záznam typu *description*. Ten v podstatě obsahuje jméno počítače, na kterém bylo dané BitLocker zařízení vytvořeno a také datum vytvoření. Můžeme tedy vidět, že toto konkrétní BitLocker zařízení bylo vytvořeno na počítači `DESKTOP-NPM7RCA` a to 3. února 2019. Tato informace je uloženo jako standardní string v kódování UTF-16. Kromě tohoto stringu jsou pak na obrázku zvýrazněny i další údaje: velikost celého záznamu (64 bajtů), jeho typ (7 – popisek) a hodnota (2 – string) a verze (1).

Obr. 1.2 Příklad FVE záznamu typu „description“ (popisek)

```
02195070  40 00 07 00 02 00 01 00  44 00 45 00 53 00 4b 00 |@.......D.E.S.K.|
02195080  54 00 4f 00 50 00 2d 00  4e 00 50 00 4d 00 37 00 |T.O.P.-.N.P.M.7.|
02195090  52 00 43 00 41 00 20 00  47 00 3a 00 20 00 32 00 |R.C.A. .G.:. .2.|
021950a0  2f 00 33 00 2f 00 32 00  30 00 31 00 39 00 00 00 |/.3./.2.0.1.9...|
```

U jednoduchého zařízení — v našem případě USB flash disku — se bude obvykle vyskytovat pouze pět záznamů a to již výše zmíněný popisek, dvojice záznamů typu VMK, jeden záznam typu FVEK (o obou více v části 1.2 a jeden záznam obsahující informace o umístění hlavičky disku (o tomto záznamu více v části 1.3.2).

[7)] Umístění a velikost NTFS hlavičky otevřeného zařízení. Odpovídá hodnotě 15. Podrobnější informace o umístění NTFS hlavičky na šifrovaném zařízení jsou v části 1.3.2.

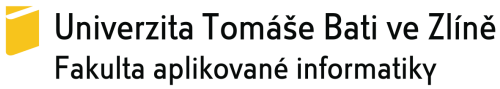
2 Existující řešení pro práci s BitLockerem v Linuxu

2.1 libbde

2.2 Dislocker

3 Další nadpis

Tato sekce obsahuje ukázku vložení obrázku (Obr. 3.1).



Obr. 3.1 Popisek obrázku

3.1 Podnadpis

Tato sekce obsahuje ukázku vložení tabulky (Tab. 3.1).

Tab. 3.1 Popisek tabulky

	1	2	3	4	5	Cena [Kč]
F	(jedna)	(dva)	(tři)	(čtyři)	(pět)	300

3.1.1 Podpodnadpis

3.1.2 Podpodnadpis

Citace knihy.

II. PROJEKTOVÁ ČÁST

4 Nadpis

4.1 Podnadpis

ZÁVĚR

Text závěru

SEZNAM POUŽITÉ LITERATURY

[1] Programming reference for Windows API. Dostupné z: `https://docs.microsoft.com/en-us/windows/desktop/api/minwinbase/ns-minwinbase-filetime`

[2] Library and tools to access the BitLocker Drive Encryption (BDE) encrypted volumes. 2018. Dostupné z: `https://github.com/libyal/libbde`

[3] Carrier, B.: *File system forensic analysis*. London: Addison-Wesley, první vydání, 2005, ISBN 978-0321268174.

[4] Ferguson, N.: AES-CBC + Elephant diffuser. 2006.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ASCII	American Standard Code for Information Interchange
FS	File System
FVE	Full Volume Encryption
FVEK	Full Volume Encryption Key
GUID	Globally Unique Identifier
MFT	Master File Table
NTFS	New Technology File System
OEM	Original Equipment Manufacturer
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VMK	Volume Master Key

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I. NÁZEV PŘÍLOHY

Obsah přílohy