

Bitlocker šifrování disku v Linuxovém prostředí

Bc. Vojtěch Trefný



*** 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	8
I TEORETICKÁ ČÁST	8
1 BITLOCKER	10
1.1 DISKOVÝ FORMÁT.....	10
1.1.1 Hlavička	10
1.1.2 FVE metadata	12
1.2 KLÍČE.....	12
1.2.1 Volume Master Key	12
1.2.2 Full Volume Encryption Key	12
1.3 ŠIFROVANÁ DATA	12
1.3.1 Použité šifrovací algoritmy	12
1.3.2 Způsob uložení data.....	12
1.3.3 Postup při dešifrování	12
2 EXISTUJÍCÍ ŘEŠENÍ PRO PRÁCI S BITLOCKEREM V LINUXU ...	13
2.1 LIBBDE	13
2.2 DISLOCKER	13
3 DALŠÍ NADPIS	14
3.1 PODNADPIS	14
3.1.1 Podpodnadpis	14
3.1.2 Podpodnadpis	14
II PROJEKTOVÁ ČÁST	14
4 NADPIS	16
4.1 PODNADPIS.....	16
ZÁVĚR	17
SEZNAM POUŽITÉ LITERATURY	18
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	19
SEZNAM OBRÁZKŮ	20
SEZNAM TABULEK	21
SEZNAM PŘÍLOH	22

ÚVOD

První odstavec pod nadpisem se neodsazuje, ostatní ano (pouze první řádek, odsazení vertikální mezy odstavci je typické 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.

I. TEORETICKÁ ČÁST

1 BitLocker

text

1.1 Diskový formát

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 (známé¹⁾) položky hlavičky BitLockeru a pro srovnání také stejné položky v hlavičce souborového systému NTFS.

Struktura NTFS hlavičky je převzata z [2], struktura BitLocker hlavičky je pak částečně převzata z [1], částečně z [3] a částečně výsledkem vlastního zkoumání.

Listing 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	78xxxxxxx
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	xxxxxxxxx.....
000001f0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	00	1f	2c	55	aa,U..
00000200																	

Z pohledu identifikace BitLocker zařízení je nejdůležitější částí hlavičky 8 bajtů na offsetu 3, které se u NTFS formátu nazývají *OEM název* a které slouží pro rychlou

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

TODO:
jak
lépe
říct
oh-
disk
for-
mat

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)	

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 identifikátor uložený na offsetu 160 (16 bajtů dlouhý UTF-8 string) a trojice *uint32* hodnot na offsech 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 offsech, které jsou v NTFS součástí *bootcode*.

Umístění všech výše zmíněných „důležitých“ částí BitLocker hlavičky je zobrazeno na výpisu 1.

TODO:
Jak tomu sakra říkat

1.1.2 FVE metadata

1.2 Klíče

1.2.1 Volume Master Key

1.2.2 Full Volume Encryption Key

1.3 Šifrovaná data

1.3.1 Použité šifrovací algoritmy

1.3.2 Způsob uložení data

1.3.3 Postup při dešifrování

2 Existující řešení pro práci s BitLockerem v Linuxu

2.1 libbde

2.2 Dislocker

3 Další nadpis

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



Obr. 3.1 Popisek obrázku

3.1 Podnadpis

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

Tab. 3.1 Popisek tabulky

	1	2	3	4	5	Cena [Kč]
<i>F</i>	(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] Library and tools to access the BitLocker Drive Encryption (BDE) encrypted volumes. 2018. Dostupné z: <https://github.com/libyal/libbde>
- [2] Carrier, B.: *File system forensic analysis*. London: Addison-Wesley, první vydání, 2005, ISBN 978-0321268174.
- [3] 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
GUID	Globally Unique Identifier
MFT	Master File Table
NTFS	New Technology File System
OEM	Original Equipment Manufacturer

SEZNAM OBRÁZKŮ

Obr. 3.1	Popisek obrázku	14
----------	---------------------------	----

SEZNAM TABULEK

Tab. 1.1	Porování položek hlaviček BitLocker a NTFS	11
Tab. 3.1	Popisek tabulky	14

SEZNAM PŘÍLOH

P I.	Název přílohy
------	---------------

PŘÍLOHA P I. NÁZEV PŘÍLOHY

Obsah přílohy