Open Source a šifrování dat OFTE

Pavel Machula

Zkratka OFTE

zkratka angl. On-The-Fly Encryption (šifrování za letu / v reálném čase):

- Diskové šifrování,
- Dostupnost souborů ihned po zadání klíče.
- Data jsou automaticky šifrována/dešifrována v okamžiku před načtením nebo uložením na disk bez jakéhokoliv zásahu uživatele.
- Celý šifrovaný oddíl je připojen jako by tvořil abstraktní blokové zařízení.
- Šifrované svazky OFTE tak uloženy na diskových nebo logických oddílech, celých discích, stejně i jako v podobě samostatných souborů.

Proč šifrovat?

- Ochrana (utajení) informací

- Legislativní úprava?
- Vhodné nástroje?
- Zálohování?
- Rizika?

Šifrování a legislativa ČR

Obchodní tajemství, zákon č. 513/1991 Sb., obchodní zákoník:

§ 17

Předmětem práv náležejících k podniku je i obchodní tajemství. Obchodní tajemství tvoří veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje.

§ 18

Podnikatel provozující podnik, na který se obchodní tajemství vztahuje, má výlučné právo tímto tajemstvím nakládat, zejména udělit svolení k jeho užití a stanovit podmínky takového užití.

Šifrování a legislativa ČR

zákon č. 101/2000 Sb, o ochraně osobních údajů

§ 4 Vymezení pojmů

a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu

§ 37 Oprávnění kontrolujících

b) požadovat na kontrolovaných a na jiných osobách, aby ve stanovených lhůtách předložily originální doklady a další písemnosti, záznamy dat na paměťových médiích, výpisy a zdrojové kódy programů, pokud je vlastní, výpisy a opisy dat (dále jen "doklady"), pokud to souvisí s předmětem kontroly, a provádět vlastní dokumentaci,

f) pořídit kopie obsahu paměťových médií, obsahujících osobní údaje, nacházejících se u kontrolovaného,

Šifrování a legislativa ČR

zákon č. 141/1961 Sb., trestní řád

§ 33, Práva obviněného

(1) Obviněný má právo vyjádřit se ke všem skutečnostem, které se mu kladou za vinu, a k důkazům o nich, není však povinen vypovídat.

zákon č. 2/1993 Sb., listina základních práv a svobod

Čl.37

(1) Každý má právo odepřít výpověď, jestliže by jí způsobil nebezpečí trestního stíhání sobě nebo osobě blízké.

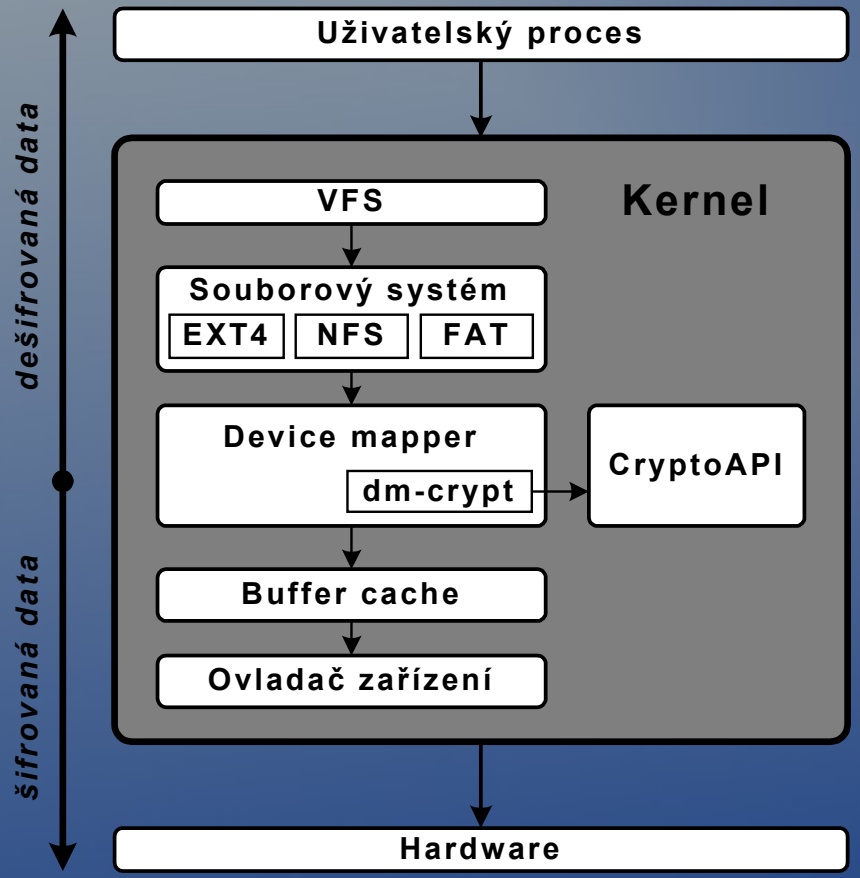
*) Nezbytným předpokladem pro naplnění zákonných znaků trestného činu maření výkonu úředního rozhodnutí je existence úředního rozhodnutí, tj. rozhodnutí soudu či jiného státního orgánu. Aby mohlo být maření úředního rozhodnutí sankcionováno podle trestního zákona je mj. nezbytné, aby toto rozhodnutí bylo vydáno soudem nebo státním orgánem v předepsaném řízení za dodržení příslušných procesních ustanovení, která postup soudu či státního orgánu před vydáním rozhodnutí upravují, aby samo rozhodnutí obsahovalo ty výroky, které zákon požaduje, a bylo vyhotoveno formou, jíž zákon předepisuje.

Legislativa a zbytek světa příklad UK

Norma: *Regulation of Invesstigatory Powers Act 2000* + dodatek s15 *Terrorism Act 2006*

- v případě odmítnutí výpovědi vztahující se k šifrované informaci ohrožující národní bezpečnost odnětí svobody na dobu 5 let
- v ostatních případech na 2 roky

dmCrypt - cryptsetup



- transparentní subsystém linuxového jádra (verze 2.6 a vyšší) pro šifrování disku
- součástí infrastruktury device-mapper

Cryptsetup

- rozhraní příkazové řádky,
- používá key management standardu LUKS (Linux Unified Key Setup)
- umožnuje užití šifrovacích módů XTS, LRW, ESSIV

- symetrické šifrování

dmCrypt - cryptsetup

Výhody:

- součást většiny současných distribucí
- key management – užití až 8-mi nezávislých klíčů
- klíč může mít podobu souboru – např na USB disku
- klíč je derivován– entropie
- šifrování swapového odílu

Nevýhody:

- hlavička obsahuje informaci o užité šifře

dmCrypt - cryptsetup

Výpis hlavičky:

- **# cryptsetup luksDump /dev/sda3**
- Version: 1
- Cipher name: aes
- Cipher mode: xts-plain
- Hash spec: sha1
- **Payload offset:** 3016
- MK bits: 256
- MK digest: 1d 6f 37 fc 3a 06 81 c6 7b 92 31 12 aa 4b d5 16 f1 7a 2b bb
- MK salt: ea 37 e0 5a 6f 49 46 5+ f7 b3 66 89 ee ad 9c 39
- 25 68 61 05 b6 c1 ad 8a 7e 42 ae 57 3d 8e bf 57
- MK iterations: 10
- UUID: d093c79f-f180-4c26-bcea-ccf4c619f3d0
- Key Slot 0: ENABLED
- Iterations: 224713
- Salt: 45 28 4d 8d 3d 14 09 ba 4e 0c 4e 4b f3 76 25 86
- 91 61 67 22 de bb 31 1c 84 83 a7 c7 99 8c 0e 8c
- Key material offset: 8
- AF stripes: 4000
- Key Slot 1: ENABLED
- Iterations: 225407
- Salt: 13 c2 ce dc 91 f7 27 02 bc d4 bc 0a 22 6c 36 30
- 93 fb 16 fb 10 8d 0f d9 51 0b 66 e9 4f 72 23 b1
- Key material offset: 384
- AF stripes: 4000
- Key Slot 2: ENABLED
- Iterations: 227679
- Salt: fb 0c a9 83 40 e8 56 70 50 b1 4b 00 0b 39 18 aa
- f1 28 c4 21 15 35 c8 21 0a cb 03 4d 45 2f 07 1a
- Key material offset: 760
- AF stripes: 4000
- Key Slot 3: DISABLED
- Key Slot 4: DISABLED
- Key Slot 5: DISABLED
- Key Slot 6: DISABLED
- Key Slot 7: DISABLED

Záloha hlavičky:

- # dd if=/dev/hda3 of=/root/header.hda3 count=3016
- 3016+0 records in
- 3016+0 records out
- 1544192 bytes (1.5 MB) copied, 0.0492465 s, 31.4 MB/s

Hlavička:

- LUKSşž@Aaes@@@@@@@@@@@@@@@@@@@@@@@@@lrw-benbi@@@@@@@@@@@@@@@@@@@@@@@sha1@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
- d093c79f-f176-3a26-bcea-ccf4c609f3d0@@@@@Źqó@Cl9E(MM=T şNLNKóv %FQag"Țť1\DC§ÇYLNL@@@H@@O @Źqó@CplSÂÎÜB÷'Bź
- ËC\E/FZ@@Bř@@O @@Ț-@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@Dp@@O @@Ț-@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@E
- P@@O @@
- F@@KF@@LF@@MF@@NF@@OF@@PF@@QF@@RF@@SF@@TF@@UF@@V
- @@@@@@@@@@@@@H@@@@@@@@@@@@@@@@A@@@
- NFG/…

TrueCrypt

- OpenSource aplikace, ver. 6.3, 21/10/2009, http://www.truecrypt.org/
- Operační systémy Linux, Mac OS X, Microsoft Windows
- Symetrické šifrování dat
- Autentikace heslem, klíčem (souborem), od ver. 6 PKCS11
- Instalace v podobě balíčku nebo kompilací zdrojového kódu
- GUI, příkazová řádka

TrueCrypt - módy ukládání dat

- Virtuální disková jednotka
- Šifrovaný diskový oddíl
- Šifrovaný systémový oddíl

Další možnosti ukládání:

- Traveler Mode - při připojení přenosného zařízení byla zobrazena žádost o zadání hesla.
- Hidden volume (skrytý oddíl) - skrytý oddíl je uložen uvnitř běžného oddílu a má své vlastní heslo. Není možné zjistit, že se v daném oddílu skrytá část nachází

TrueCrypt -šifrovací algoritmy

Sifrovací algoritmy	velikost klíče [bit]	velikost bloku [bit]
AES	256	128
Serpent	256	128
Twofish	256	128
AES-Twofish	256,256	128
AES-Twofish-Serpent	256,256,256	128
Serpent-AES	256,256	128
Serpent-Twofish-AES	256,256,256	128
Twofish-Serpent	256,256	128

Hašhovací funkce:

- RIPEMD-160
- SHA-512
- Whirlpool

TrueCrypt

Výhody:

- hlavička nenese informaci o užité šifře
- silné šifrování: kombinace hesla a klíče
- klíč může mít podobu souboru/ů – např na USB disku

Ostatní SW

- FreeOFTE
- PGP Desktop Security

Hrozby

Integrita a dostupnost:

- nefunkční zálohování

Utajení:

- fyzický přístup k hw
- key loggery
- datový balast

Falešný pocit bezpečí...

Závěr

☺ kdo je připraven, není překvapen... ☺