Šifrování flash a jiných datových úložišť

Michal Vahala

2. května 2011

Obsah

Úvod

- proč šifrovat datová úložiště
  - ochrana dat před: čtením, pozměněním, nalezením, ...
  - likvidace dat
- jak šifrovat
  - šifrování za běhu (bez zásahu uživatele, celý soubor není v paměti)
  - minimalizovat místo navíc pro potřeby šifrování
  - symetrická šifra
- bezpečnost
- nevýhody
  - rychlost (sekvenční čtení), problémy při mimořádné situaci, ...

Rozdělení

Úroveň šifrování

- pod úrovní OS (HW i SW)
- v rámci OS (BitLocker, Dm-crypt)
- nad OS (SW)

Dostupnost

- komerční (PGP, DriveCrypt, Steganos, ...)
- opensource (TrueCrypt, Dm-crypt, EncFS, ...)

HW šifrování

- hlavně USB flash disky – obvykle AES 256
- omezený počet špatného zadání hesla – pak se uzamkne/smaže
- zpravidla není veřejně známá přesná specifikace
- přídavná zařízení obvykle mají certifikaci
- pro HDD
  - vyšší výkon
  - často špatná dokumentace – těžké posouzení kvality
  - obtíže při výměně HW

Šifrování pomocí softwaru

- obvykle probíhá nad úrovní OS, ale existují i programy šifrující systémové disky (tj. pod OS)
- komerční
  - obvykle nejsou zdarma
  - uzavřené zdrojové kódy: mohou zvyšovat bezpečnost, ale zároveň skrýt i nedostatky, případně úmyslně vytvořené bezpečnostní díry
- opensource
  - zdarma
  - každý si může projít zdrojové kódy a přesvědčit se, že program neobsahuje chybu, backdoor, ...

Základní principy

- rychlosti a možnosti šifrování za běhu – rozdělení na sektory (obvykle 512 bytů) – šifrovány zvlášť
- sektory z důvodu bezpečnosti není vhodné zpracovávat stejně
- užívány blokové šifry – blok obvykle menší než sektor – užití módů
- různé módy – v současnosti užívaný XTS
- žádoucí vlastnosti
  - popiratelnost
  - skryté jednotky
  - neidentifikovatelnost (nerozlišitelnost od pseudonáhodných dat)
  - změna velikosti
  - záloha hlavičky

TrueCrypt

- multiplatformní (Windows, Linux, Mac) program pro šifrování datových úložišť
- pracuje na principu virtuálních disků (obdoba virtuální mechaniky), image je možno uložit v souboru nebo použít celé zařízení (pevný disk, USB flash, paměťová karta), respektive jeho partition
- umí šifrovat i systémový disk – pod úrovní OS (pouze Windows)
- podpora pokročilých technologií: paralelizace, pipelining, HW šifrování (instrukce procesoru)
- zdarma, opensource

Algoritmy a zabezpečení

- použitelné algoritmy: AES, Serpent, Twofish, kaskády (AT, ATS, SA, STA, TS)
  - všechny používají 256bitový klíč (popřípadě 2x nebo 3x 256 bitů u kaskády)
  - bloky délky 128 bitů
- hashovací funkce: RIPEMD-160, SHA-512, Whirlpool
- blokový mód XTS
- zabezpečení
  - heslo
  - heslo + keyfile (možno uložit na bezpečnostním žetonu nebo kartě)
- náhodný generátor
  - pohyb myši, stisknuté klávesy
  - vestavěný RNG (Linux, Mac); CryptoAPI, síťové statistiky, systémové proměnné (Windows)
  - plus vždy následuje zamíchání speciální funkcí (difuze)

Připojení šifrované jednotky

1. do paměti se načte částečně šifrovaná hlavička jednotky
2. z hlavičky se vezme část označovaná jako SALT a ta se spolu s heslem zadaným od uživatele použije pro vygenerování klíče pomocí hashovací funkce
3. takto získaným klíčem se dešifruje hlavička, která mimo jiné obsahuje náhodně vygenerovaný klíč, kterým je šifrována datová čast jednotky
4. nyní je již možno šifrovat a dešifrovat data na jednotce

Použitý algoritmus a hashovací funkce se programu nezadává, ale je určována metodou pokus-omyl.

Struktura jednotky

- standartní jednotka
  - hlavička + volné místo o velikosti hlavičky
  - vlastní data + volné místo
  - záložní hlavička
- skrytá jednotka
  - hlavička vnějšího svazku + hlavička skrytého svazku
  - vlastní data vnějšího svazku + volné místo
  - vlastní data skrytého svazku
  - záložní hlavičky obou svazků
- pro šifrování systémového disku obdobně dvě varianty (standartní a skrytá)
  - skrytá je řešena navíc pomocí dvou partition

Bezpečnost

Odhalení existence šifrované jednotky

navenek se jeví jako náhodná data

- jednotka v souboru – zřejmě se jedná o šifrovaný soubor
- oproti tomu: jednotka na zařízení/partition – může být například způsobeno bezpečným vymazem
- skrytá jednotka – i když je jednotka odhalena a je vynuceno zadání hesla, je zpřístupněna „falešná“ část jednotky a citlivá data zůstávají skryta
- prozrazení skryté jednotky:
  - logy, indexy, naposledy otevřené soubory
  - pozorovány změny v zašifrovaných datech, kde nemá nic být – útočník má přístup k více verzím zašifrované jednotky (reálně, defragmentace, journal FS, kopírování souborů s jednotkami, ochrana před opotřebením při častém zápisu, médium s určitelným počtem zápisů, chybné sektory disku,...)

Bezpečnost

- šifrování celého systémového disku
  - řeší závažný problém s únikem dat (dočasné soubory, swap, hibernace)
  - lze snadno poznat – pre-boot TrueCrypt zavaděč
- v případě Linuxu lze použít „live CD“
- skrytý operační systém
  - nutná opatrnost – opět možno odhalit
  - je třeba co nejvíce používat „falešný“ OS a druhý OS s citlivými daty minimálně (neaktualita „falešného“ OS, synchronizace s HW nebo v síti)
- další nebezpečí
  - nešifrovaná RAM – cold boot attack
  - keylogger, malware
  - více uživatelů a sdílení dat
  - zálohy – potřebné x nebezpečné
- není kontrola integrity a autenticity

Závěr

- vždy zvážit klady a zápory samotného šifrování
- volba HW nebo SW
- v případě SW vhodný šifrovací program
- úroveň paranoie
- způsob zálohování

Dotazy ?

Zdroje

- dokumentace TrueCrypt (http://www.truecrypt.org/docs/)
- Proč a jak na šifrování disků v Linuxu? (http://www.root.cz/clanky/proc-a-jak-na-sifrovani-disku-v-linuxu/)
- On-The-Fly Encryption: A Comparison (http://otfedb.sdean12.org/)
- Full-disk Encryption (http://www.markus-gattol.name/ws/dm-crypt_luks.html)
- http://en.wikipedia.org/