Šifrování flash a jiných datových úložišť

Petr Bohuslav

24. dubna 2014

Obsah přednášky

Pár slov úvodem

Proč šifrovat?

- ochrana citlivých dat nebo záloh
- sdílení dat jen s vybranými osobami

Pár slov úvodem

Proč šifrovat?

- ochrana citlivých dat nebo záloh
- sdílení dat jen s vybranými osobami

Pár slov úvodem

Proč šifrovat?

- ochrana citlivých dat nebo záloh
- sdílení dat jen s vybranými osobami

Úrovně zabezpečení

Hardwarové šifrování

- hlavně u USB flashdisků a externích HDD
- obvykle AES 128/256 bit
- Po opakovaném zadání špatného hesla se HDD zamkne/smaže.

\+ nezávislé na OS

\+ Je-li integrované, nesnižuje výkonnost.

– často špatná dokumentace $\Rightarrow$ možnost zadních vrátek

Úrovně zabezpečení

Softwarové šifrování

- komerční
  - uzavřený zdrojový kód
  - DriveCrypt, FileVault
- open source
  - zdarma
  - otevřený zdrojový kód (kontrola)
  - TrueCrypt, FreeOTFE, dm-crypt,$\cdots$

Úrovně zabezpečení

Softwarové šifrování

- komerční
  - uzavřený zdrojový kód
  - DriveCrypt, FileVault
- open source
  - zdarma
  - otevřený zdrojový kód (kontrola)
  - TrueCrypt, FreeOTFE, dm-crypt,$\cdots$

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - zřetězovací módy (např. XTS)

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - zřetězovací módy (např. XTS)

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - zřetězovací módy (např. XTS)

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - řetězovací módy (např. XTS)

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - zřetězovací módy (např. XTS)

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - zřetězovací módy (např. XTS)

Základní požadavky na metody šifrování

1. bezpečnost
2. šifrování i dešifrování v reálném čase (on-the-fly encryption)
   - rozdělení disku na sektory (obvykle 512 bytů)
   - každý sektor šifrujeme zvlášť a jiným způsobem(!)
3. malé nároky na místo na disku
   - použití blokových šifer
   - zřetězovací módy (např. XTS)

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- open source nástroj pro šifrování dat na disku
- pro Windows, Linux a MacOS X
- možnosti ukládání dat:
  1. virtuální disk
  2. šifrovaný diskový oddíl
  3. šifrovaný systémový oddíl
  4. traveller mode
  5. skrytý oddíl

TrueCrypt

- šifrovací algoritmy
  1. AES
  2. Twofish
  3. Serpent
  4. jejich zřetězení (v módu XTS)
- hashovací algoritmy
  a) RIPEMD-160
  b) SHA-512
  c) Whirlpool

TrueCrypt

- šifrovací algoritmy
  1. AES
  2. Twofish
  3. Serpent
  4. jejich zřetězení (v módu XTS)
- hashovací algoritmy
  a) RIPEMD-160
  b) SHA-512
  c) Whirlpool

TrueCrypt

Heslo

- posloupnost znaků
- posloupnost znaků + keyfile

Doporučení:

- délka hesla aspoň 20 znaků (max. 64)
- nepoužívat slova nalezitelná ve slovníku, ani jejich kombinace
- žádná jména ani data narození
- používat kombinace malých a velkých písmen, číslic a speciálních znaků

Děkuji za pozornost.

Zdroje

V. Klíma, T. Rosa: Kryptologie pro praxi - vydání 7,8/2007
http://en.wikipedia.org/wiki/Disk_encryption_hardware
http://en.wikipedia.org/wiki/Disk_encryption_theory
http://en.wikipedia.org/wiki/Disk_encryption_software
http://www.truecrypt.org/
http://www.root.cz/clanky/truecrypt-profesionalni-ochrana-dat-zdarma/