Počítačová bezpečnost prakticky

Ing. Štěpán Sem
<stepan.sem@gmail.com>

PragoFFest 2014

Motto

„To, že jsem paranoidní, neznamená, že po mně nejdou.“

Slidy

www.mael.cz

Hesla

- nejčastější autentizace
- slabá
  - zjevná fakta (narození, . . .)
  - fráze
    - slovníkový útok
  - „heslo někoho jiného“
    - otisk
- silná hesla
  - A-Z, a-z
  - 0-9, „interpunkce“
  - $\geqq 6\,(15)$ znaků
  - rychle se píší
  - „vzdálené“ klávesy

Tvorba silných hesel

- „báseň“

To be or not to be, that is the question
tbontbtitq
tbOntBtiTq
tb0ntBtiTq
tb0n7BtiTq
tb0^l7BtiTq
tb0^l7Bt!Tq

- ∼pseudonáhodná

Zabezpečení dat – prostředek

- typ zabezpečení
  - hardwarové
  - softwarové
- politika
  - proprietární
  - otevřené

Zabezpečení dat – cíl

- proti čemu
  - neoprávněné přečtení
  - nežádoucí obnovení
    - smazané soubory
- co zabezpečujeme
  - jednotlivé soubory
  - kompletní systém
    - konfigurace – hesla

Hardwarové zabezpečení

$$10^4 + 10^5 + \cdots + 10^{10} = 11\,111\,110\,000$$

Poznámka: ilutrační klíčenku PadLock nevlastním, po přednášce jsem se dozvěděl, že každé tlačítko jen přepíná mezi dvěma čísly, nelze tedy vytvářet úplně libovolné kombinace; počet možných kombinací je tedy ještě výrazně nižší.

- sdílený klíč
- demontáž
- Deep Crack
  - ∼90 mld klíčů/s (DES) → 9 dní

Exponenciální štít

- A-Z a-z
  - $2 \cdot 26 = 52$ znaků
  - 5: $52^5 = 380\,204\,032$
  - 6: $52^6 = 19\,770\,609\,664$
  - 7: $52^7 = 1{,}028 \cdot 10^{12}$
- ochrana před
  - eliminací kombinací
  - růstem výpočetního výkonu

Softwarové zabezpečení

- Dokumenty
  - Office $<$ 2007
    - prolomitelné
  - Office (2010)
    - *x: 128b AES
  - PDF
    - cache příklad
    - „sociální inženýrství“

PDF cracking

```
>./pdfcrack -v
pdfcrack version 0.7
>./pdfcrack
Usage: ./pdfcrack -f filename [OPTIONS]
OPTIONS:
-b, --bench              perform benchmark and exit
-c, --charset=STRING     Use the characters in STRING as charset
-w, --wordlist=FILE      Use FILE as source of passwords to try
-n, --minpw=INTEGER      Skip trying passwords shorter than this
-m, --maxpw=INTEGER      Stop when reaching this passwordlength
-l, --loadState=FILE     Continue from the state saved in FILENAME
-o, --owner              Work with the ownerpassword
-u, --user               Work with the userpassword (default)
-p, --password=STRING    Give userpassword to speed up breaking
                         ownerpassword (implies -o)
-q, --quiet              Run quietly
-s, --permutate          Try permutating the passwords (currently only
                         supports switching first character to uppercase)
-v, --version            Print version and exit
>./pdfcrack pdfs/test3.pdf -n 6 -c abcdefghijklmnopqrstuvxyz -s
PDF version 1.4
Security Handler: Standard
V: 1
R: 2
P: -64
Length: 40
FileID: f4745a09570809f9c7a20a3097d915c0
U: 8288f85c1903d007853893a5efea0c338ccf41bc249f7db635c83f18157863ba
O: 44507fd864065ac8e1d15b2c8ecbfa45187e7d099ad91368aade0d78841903de
Average Speed: 304489.7 w/s. Current Word: 'Vuvtha'
Average Speed: 335998.8 w/s. Current Word: 'kuxjqa'
found user-password: 'Avesta'
>
```

Zaheslované archivy

- pouze pro čtení
- RAR
  - proprietární
  - původně proprietární šifrování
  - WinRAR 128b AES
    - dříve slabiny
- ZIP
  - ~~„legacy“~~ (Windows XP)
  - WinZIP / 7Zip
    - 256b AES (128 ↑ 40%)
- jména komprimovaných souborů

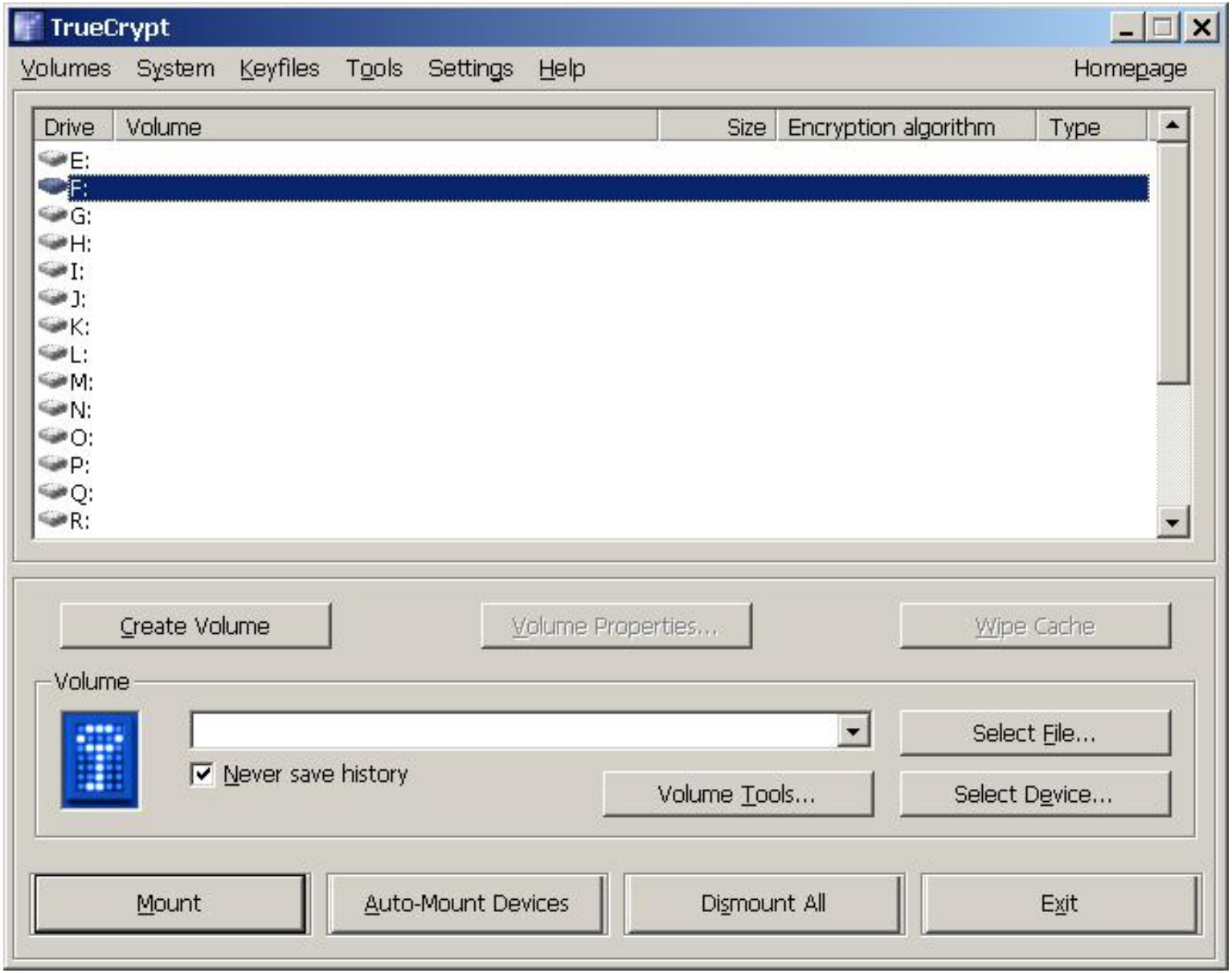
Softwarové zabezpečení – obecné

- soubory, složky
  - TrueCrypt (Windows, GNU/Linux)
    - „samonosný“
  - EFS (Windows Vista)
    - „nesamonosný“
  - (LUKS)
- disk/oddíl
  - TrueCrypt
  - BitLocker (Windows)
  - LUKS

TrueCrypt

- portable
- virtuální disk
  - (vs. šifrovaný archiv)
- oddíl vs. kontejner
- analýza zdrojových kódů
  - Klíma, Zámostný: 4.3a Win XP
    - MD5
  - potenciální výhoda *open source*

TrueCrypt


TrueCrypt
Volumes System Keyfiles Tools Settings Help Homepage
Drive Volume Size Encryption algorithm Type
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
O:
P:
Q:
R:
Create Volume
Volume Properties...
Wipe Cache
Volume
Never save history
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

TrueCrypt 7.1a (ukázka)

- rozumné výchozí nastavení
- vytvoření kontejneru
- použití
  - read-only
  - falešné heslo
- nezávislé bloky

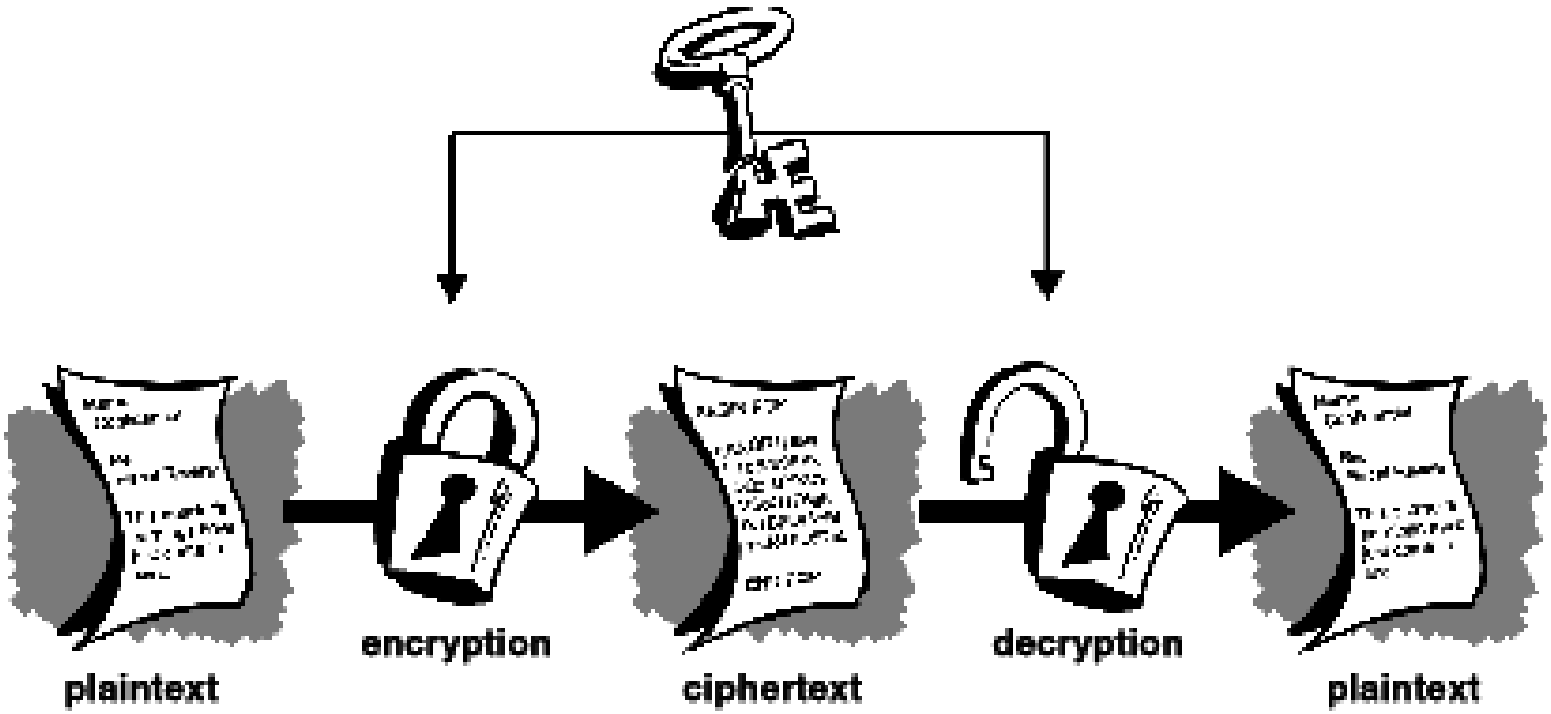
Zametení stop – bezpečné mazání

- Eraser
  - magnetická média
- `shred`
- magnetické vs. flash úložiště

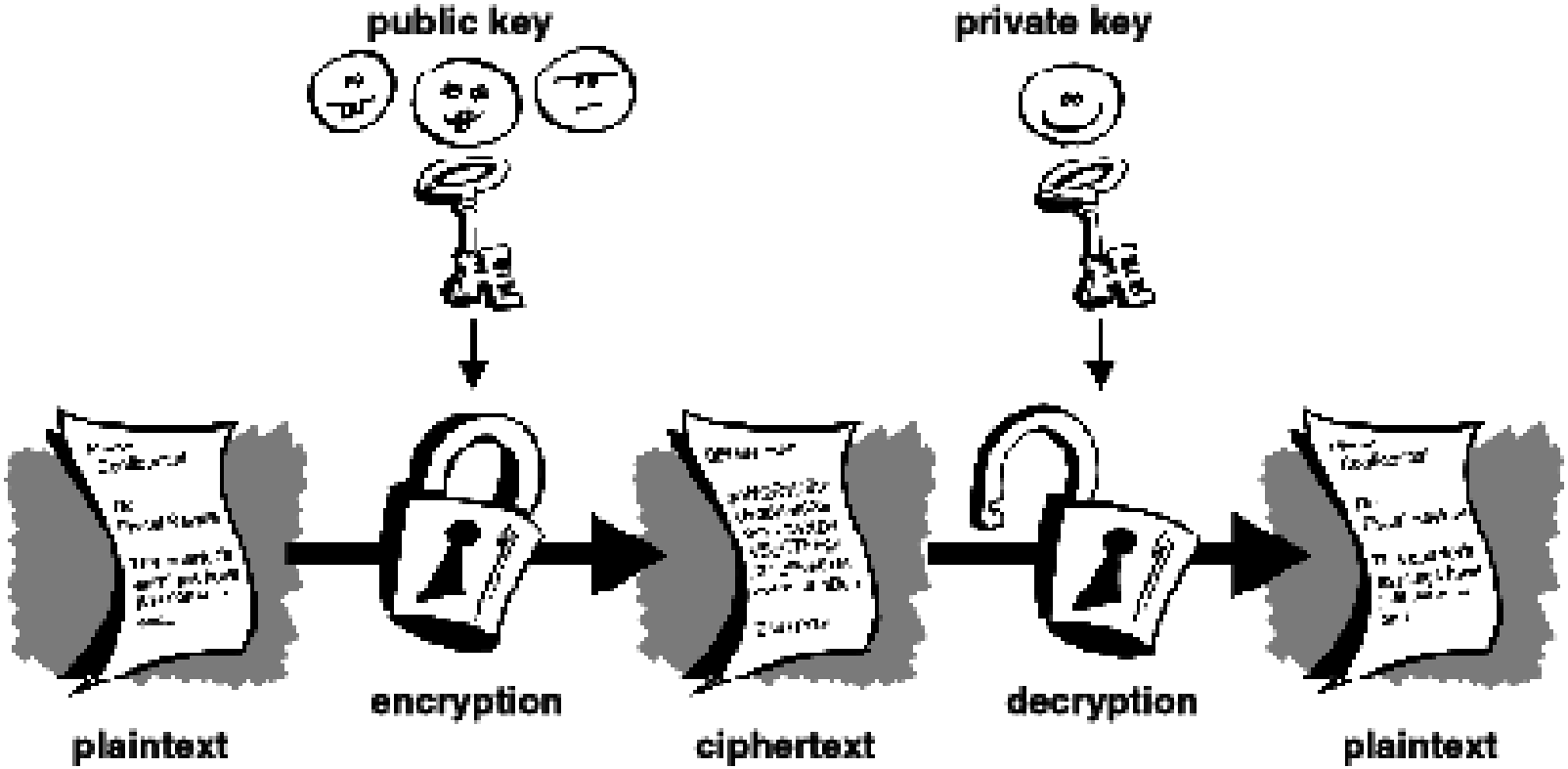
Zabezpečení systému

- heslo
  - Live médium
  - ...
- šifrovaný oddíl
  - Truecrypt
  - LUKS
- co šifrovat?
  - `/home`
  - `/swap` ?
    - hibernace (Win)

Symetrická kryptografie



Asymetrická kryptografie



Asymetrická kryptografie

- zabezpečení komunikace
  - web
  - instant messaging
  - elektronická pošta
- elektronické podepisování
- časová razítka
- ověření totožnosti

HTTPS

- SSL nad HTTP
  - koncové stroje
- certifikáty
  - „modrý“
    - ověřena doména
  - „zelený“
    - ověřenn název firmy,. . .
  - „bezpečnostní výjimka“
  - WiFi (akademická)

Instant messaging – Pidgin

- ICQ, Jabber,...
- pidgin:e $\leftrightarrow$ pidgin:e
- OTR
- Pidgin-Encryption
- Gaim-E

Pidgin (ukázka)

Poznámka: kvůli technickým problémům během přednášky na ukázky v Pidginu nedošlo. Můžete se ale podívat na krátké video ilustrující hlavní principy, které připravil Ondřej Profant.

OTR

- Off the Record

- šifrování
- autentizace
- odvolatelnost
- „robustnost“

PGP (GPG)

- GPG

- *Cory Doctorow: Malý bratr*
- sítě důvěry
  - keyserver (věrohodný)

Instant messaging – Jabber

- SSL ($\rightarrow$„HTTPS“)
  - koncoví uživatelé?
- PGP
  - součást protokolu (XMPP)
  - klientX $\leftrightarrow$ klientY
- Xabber
  - Android, OTR
- Gajim
  - PGP
- Bombus
  - J2ME

Elektronická pošta

- OTR?
- odesílatel neprůkazný
- „křížová validace“
  - oceňování
- PGP
  - Thunderbird: EnigMail

(Linuxové) experimenty

- flashdisk
- live CD/DVD
- virtualizace

Děkuji za pozornost

http://www.pictureshut.com/funny-photos/wifi-available/

Zdroje

- Principy digitální komunikace (Jiroušek a kol., LEDA 2006)
- Strong Passwords (Official Ubuntu Documentation)
- Corsair Padlock
- www.truecrypt.org
- Root.cz: TrueCrypt: profesionální ochrana dat zdarma (Klíma, Zámostný; TC 4.3a)
- Šifrovaný popis (geo)cache
- PDFCrack
- Wikipedia: RAR
- Wikipedia: Zip (file format)
- 7-zip
- Off-the-Record messaging
- How PGP works

Doplňující informace

- Ochrana přenášených dat
- „Šifrované“ klíčenky Kingston, Sandisk, Verbatim nešifrují!
- Principy digitální komunikace
  - utajení sdělení v GIF obrázku, . . .
  - podrobnější popis šifrovacích, kompresních algoritmů