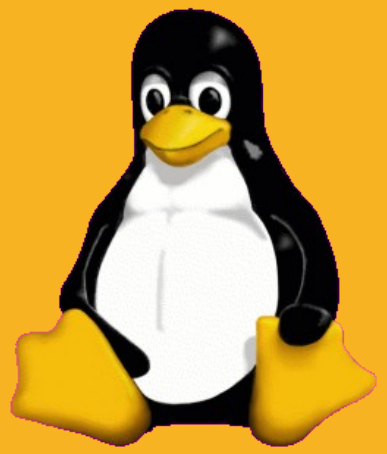
Privatnost i otvoreni kod

Tonimir Kišasondi, dipl.inf, EUCIP

DORS/CLUC 2009



$ finger tkisason

- Znanstveni novak / asistent @ Fakultet organizacije i informatike u Varaždinu

- Kontakt: tonimir.kisasondi@foi.hr
- GPG: 0x00C68442

- Ako nešto nije jasno: pitajte
- Ako treba pojašnjenje: pitajte
- Dodatne informacije, ideje: iznesite.

Kratak sadržaj

- Uvod
- Enkripcija diska, particija, containera…
- Privatna komunikacija

Baseline ☺

- Iskustvo sa kriptografskim sustavima?
- Iskustvo sa sustavima za kriptiranje diska?
- SSH tunneling, VPN i sl?

Svrha očuvanja privatnosti:

- "Selektivno otkrivanje"
- Privatnost je različita od anonimnosti!
- Zašto?
  - Krađa računala
    - Dellova studija: http://tinyurl.com/cluc-studija
    - "Total lost laptops per week: 12255, 67% never found"
  - Otuđenje backup kopija
  - Industrijska špijunaža
  - Otuđenje povjerljivih privatnih podataka (ID theft)
  - Očuvanje povjerljivosti podataka
- Alati i metode:
  - Kriptiranje diska, particija, datoteka
  - Alati privatnu komunikaciju

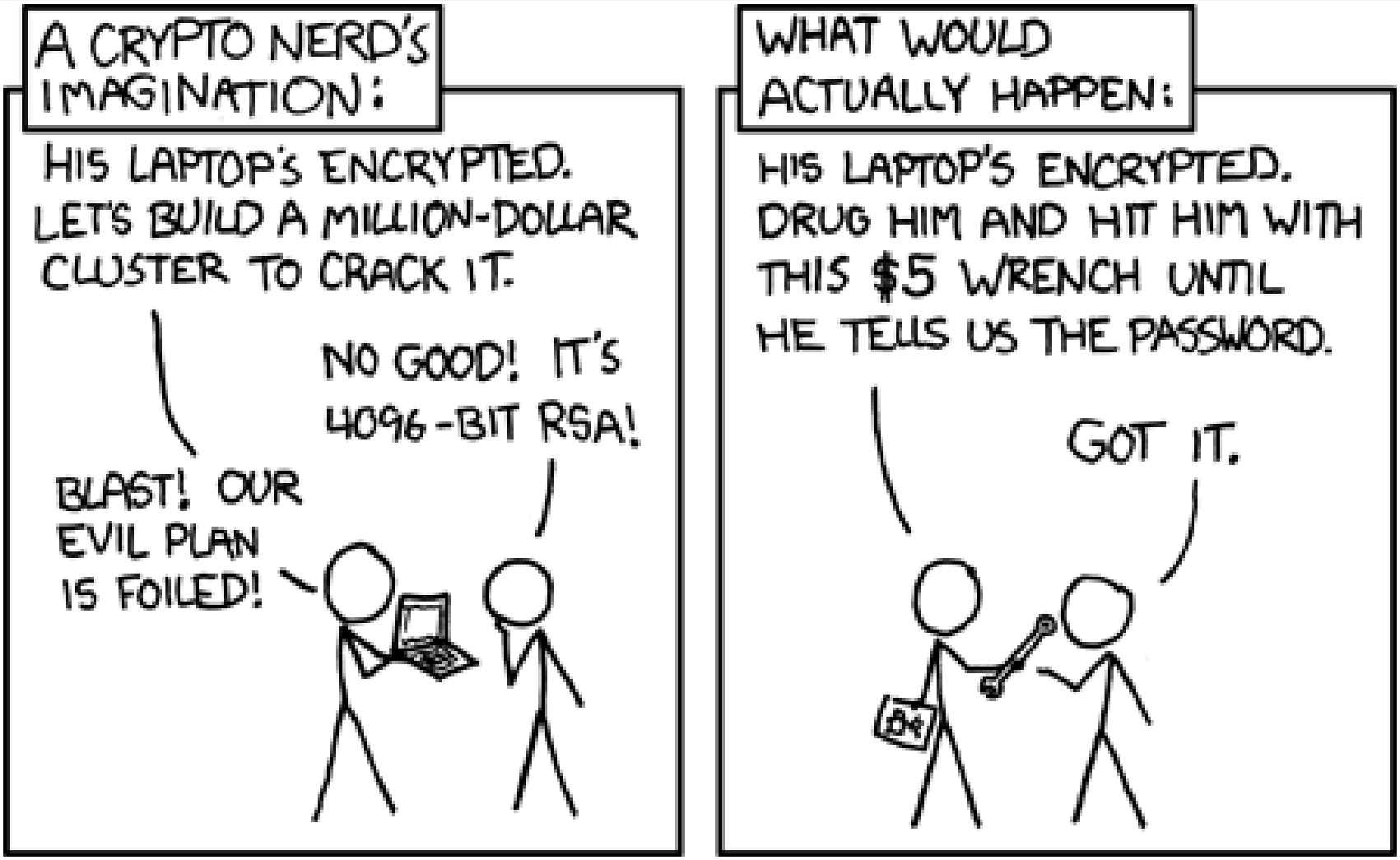
Svrha očuvanja privatnosti:

- Enkripcija diska:
  - Transparentna enkripcija
    - Transparentno prema korisniku i OS-u
    - Enkripcija particija
    - Enkripcija containera (datoteka - loopFS)
    - "On-The-Fly"
  - Nositelj/Container (npr. HDD) je kriptiran
  - Enkripcijski ključ = Spremljen u RAM-u
  - Dobra praksa = Ne vjerovati alatima koji nemaju dostupan izvorni kod
    - Backdoor
    - Nekvalitetna implementacija algoritma
    - "Beware of snake oil" – Neki komercijalni sustavi

Mitovi

- BIOS Password
  - Trivijalno zaobilaženje
  - Uklanjanje napajanja BIOSu (baterija)
- HDD Password
  - Nije kriptiranje diska, već samo blokiranje pristupa disku
  - Zamjena kontrolera na HDD-u ujedno i uklanja zaštitu
- Kriptirani disk je uvijek siguran, makar je i računalo uključeno
  - Kriptirani disk je samo spremnik, ukoliko se koristi, lozinka ili ključ za dekripciju može se saznati iz memorije.
  - Pripaziti na prava pristupa
    - Cold Boot attacks (http://citp.princeton.edu/memory/)
- Rubber hose cryptanalysis

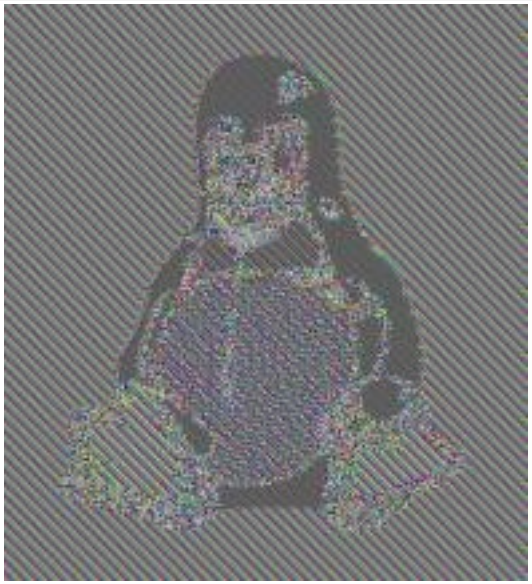
Mitovi [XKCD - Security]

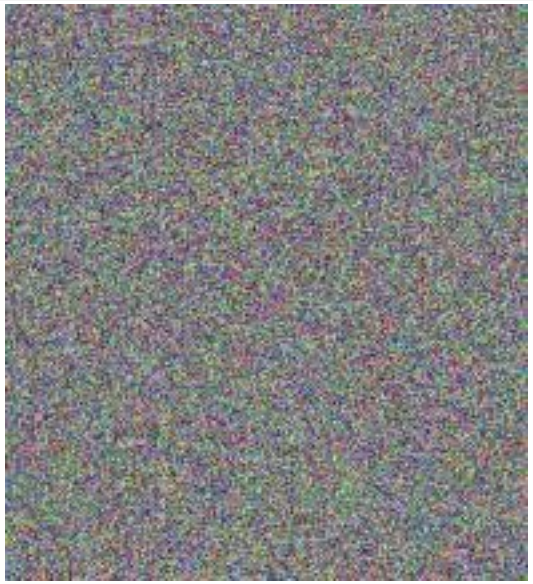


Enkripcija diska, particije, FS-a, containera

- Postoji velika količina FLOSS DE alata.
- Problem sa održavanjem i kvalitetom rješenja
- Kvalitetni:
  - **dm-crypt / LUKS** (Cross Platform)
  - **EncFS (FS) + (cryptkeeper!)**
  - LoopAES / aespipe
  - TrueCrypt
  - CryptoFS
- FreeOTFE (Win Korisnici)
- Ne preporuča se koristiti:
  - Cryptoloop (deprecated, watermark attack)
  - Bitlocker, Filevault (Closed Source – nemogućnost verifikacije sigurnosti)

Metode rada šifri: ECB, CBC, et.al.





- ECB Plain CBC
- Više načina rada blok šifri
- NE koristiti ECB (electronic codebook način)
- Preporuča se koristiti XEX-TCB-CTS (IEEE P1619)
  - Sigurno do 1TB po ključu

dm-crypt/LUKS

- Najpotpunije rješenje (particija, swap, container, cryptoraid, removable storage…)
- Mogućnost enkripcije cijelog diska
- Linux kernel standard
- KM implementacija kriptografskog algoritma (Brzina)
- Dodatna prednost: brzina asm optimiranih modula
  - aes_generic.ko vs aes_i586.ko (17,32Mb/s vs 23,59 Mb/s)
  - twofish.ko vs. twofish_i586.ko
- Keying: Passphrase, File…
- Korištenje više passphrasea (npr, recovery passphrase)

dm-crypt/LUKS - particija

foi

```
modprobe dm_crypt aes_i586 sha_256
dd if=/dev/urandom of=/dev/sdb1
cryptsetup luksFormat /dev/sdb1
cryptsetup luksOpen /dev/sdb1 cryptostick
mkfs.vfat /dev/mapper/cryptostick
cryptsetup luksClose /dev/mapper/cryptostick
```

Open:

```
cryptsetup luksOpen /dev/sdb1 cryptostick
mount /dev/mapper/cryptostick /mnt/crypto
```

Close:

```
umount /mnt/crypto
cryptsetup luksClose /dev/mapper/cryptostick
```

dm-crypt/LUKS – loopback file

foi

```
modprobe dm_crypt loop aes_i586 sha_256
dd if=/dev/urandom of=file bs=1M count=1024
losetup /dev/loop0 file
cryptsetup luksFormat /dev/loop0
cryptsetup luksOpen /dev/loop0 cryptofile
mkfs.vfat /dev/mapper/cryptofile
cryptsetup luksClose /dev/mapper/cryptofile
```

Open:

```
losetup /dev/loop0 file
cryptsetup luksOpen /dev/loop0 cryptofile
mount /dev/mapper/cryptofile /mnt/crypto
```

Close:

```
umount /mnt/crypto
cryptsetup luksClose /dev/mapper/cryptofile
losetup -d /dev/loop0
```

EncFS – oldschool ☺

mkdir /home/tkisason/.stuff
mkdir /media/crypto

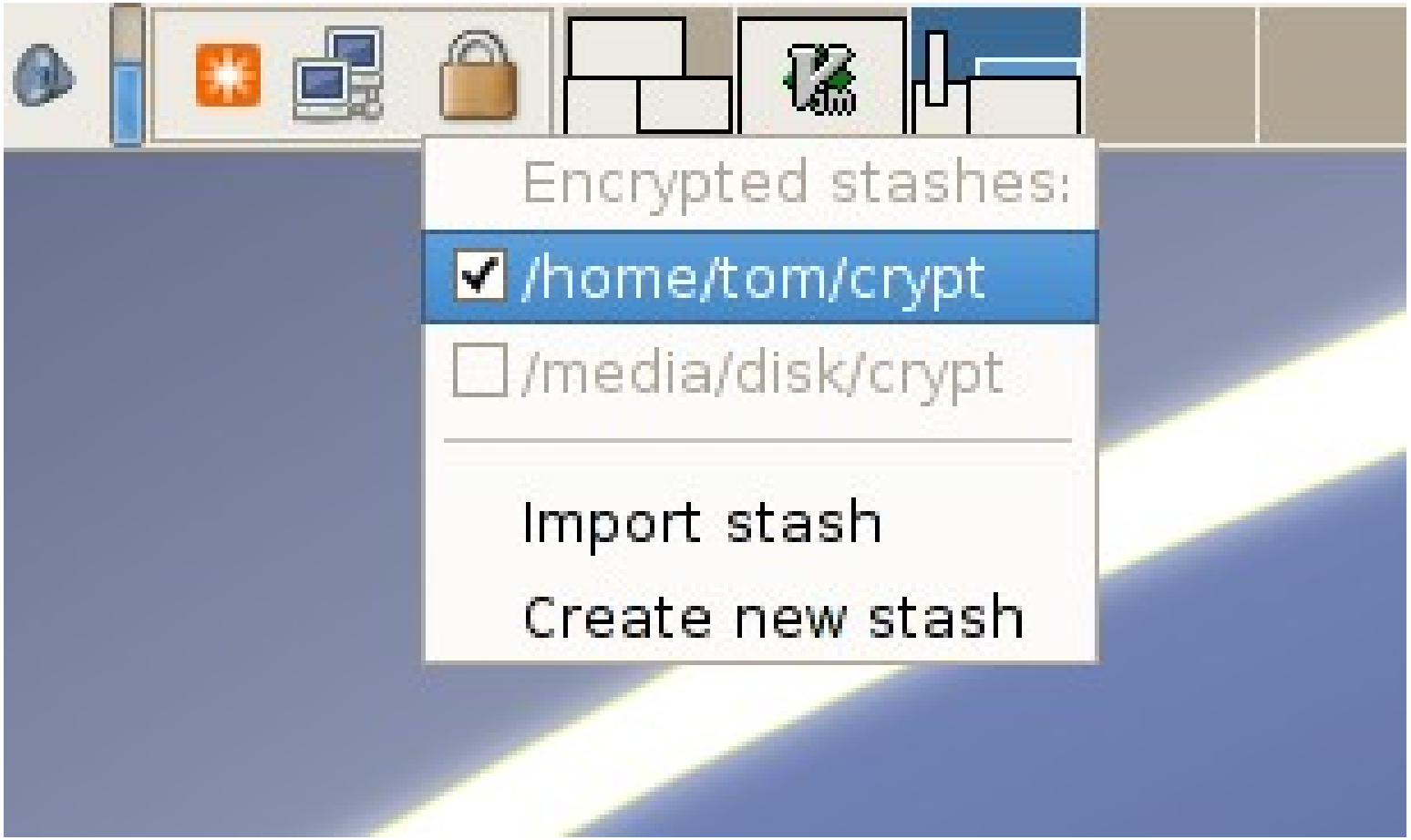
Open:

encfs /home/tkisason/.stuff /media/crypto

Close:

sync && fusermount -u /media/crypto

EncFS – GUI – CryptKeeper, KEncFS (http://tom.noflag.org.uk/cryptkeeper.html)



EncFS vs Dm-Crypt

foi

- Ukoliko korisnik ima prava za FUSE grupu, može koristiti EncFS bez superuser prava.
- Transparentan backup
- Sporije od dm-crypta
- Sporna podrška pod ostalim platformama

- Dm-Crypt & FreeOTFE win support
- Brže nego EncFS
- Mountanje prilikom boota pomoću /etc/crypttab

Strategije

- Strategija razina sigurnosti:
- Operacijski sustav, aplikacije, neosjetljive datoteke
  - Nekriptirano
- Osjetljive datoteke
  - Kriptirane unutar spremnika (datoteke) ili posebne particije
- Preporuka – Spremnik (container):
  - Mogućnost uklanjanja od sustava (Npr, USB stick)
  - Mogućnost selidbe spremnika (Npr, FlatFile container)
  - Udaljeni pristup (NFS, SSH…)
- Cryptostick
- Kriptoparticija "otključana" USB stickom

Zašto ne X?

- Izuzev dm-crypt, EncFS i LoopAES / aespipe jako malo rješenja je "kvalitetno"
- Analiza od provjerene treće strane
- Ranjivosti (npr, cryptoloop)
- Nepostojanje XTS / CBC modova.
- Support i razvoj

Performanse

foi

- Enkripcija na razini datotečnog sustava (FUSE ili aplikativno rješenje npr EncFS) sporija je nego ona koja radi sa jezgrinom implementacijom (dm-crypt)
- U pravilu – 5% do 10% sporije (Bez enkripcije / dm-crypt) – Ovisi o HW-u
- Dodatna prednost optimizacije ili posebni HW moduli (npr. VIA padlock)
  - padlock-sha.ko, padlock-aes.ko
- Neki HDD imaju ugrađenu enkripciju cijelog diska
  - Neki imaju XOR sa statičnim ključem (snake-oil)
  - Većina nema kvalitetnu implementaciju (ECB)
- Noviji mobilni procesori imaju zavidne kriptografske performanse (npr. VIA Nano)

Zakon

- Voditelj zbirke osobnih podataka i korisnik dužni su poduzeti tehničke, kadrovske i organizacijske mjere zaštite osobnih podataka…
- Potrebno je prikladno štititi osjetljive podatke
- U slučaju neotkrivanja ključeva pod sumnjom kaznenog djela – ometanje istrage i "priznavanje krivnje"

Sigurnost

- Pravila ponašanja sa passphraseom ili ključem vrijede i u ovom slučaju
- Cold Boot Attacks
- HW implementacije – pripazite na algoritam enkripcije i način rada algoritma
- Enkripcija diska ne štiti vas ukoliko napadač može pristupiti dekriptiranom spremniku
  - Trojan, Rootkit, Backdoor, Fizički pristup
- Separacija datoteka po važnosti
- Ako ne koristite spremnik ili particiju, zatvorite ju!

Forenzička analiza

- MouseJiggler + HotPlug
- USB HID device = Umjetno micanje miša
- Spajanje računala na UPS + uklanjanje sa električne mreže
- Omogućuje micanje servera, radne stanice i sl.

- Provjera kvalitete DE rješenja
- Jednostavnije:
  - hexdump analiza
  - Analiza entropije (pripaziti na plaintext!!!)
- Kompleksnije:
  - Kriptoanaliza

Kriptirane komunikacije

- Pristup povjerljivim podacima putem sigurne veze
- Alati poput cain, dsniff, sslstrip, ettercap…
- Nažalost, prejednostavni za korištenje i predobro dokumentirani
  - Script Kiddies, Rogue AP, Honeypots.
- Iznimna jednostavnost prikupljanja lozinki i svog prometa
- Rješenje: SSH tuneliranje
  - Sva komunikacija prolazi kroz SSH tunel prema "sigurnom" serveru

SSH filesystem

- sshfs: ssh filesystem (FUSE)
  - sshfs tkisason@serv:/home/tkisason remote_home
- Nautilus + GVFS + FUSE

- Kratki test:
- NAS (ARM CPU)
  - SSHFS (25Mb file) = 51.1s
  - SMB (25Mb file) = 40.2s
  - ~20% overhead zbog enkripcije
- Ovisno o brzini računala

SSH tunneling

- Dynamic forwarding
- Na server.foi.hr u conf. /etc/ssh/sshd_config
  - AllowTcpForwarding yes
- ssh –D 5555 tkisason@server.foi.hr
- U browseru postaviti SOCKS proxy na localhost:5555

- Plain : 3.97 / 0.27
- SSH tunneled: 3.97 / 0.26
- Ping 25% do 50% veći

SSH

- Dozvoliti samo SSHv2
- "Nestandardni" SSH port
- Zabraniti login kao root
- PublicKey autentikacija
- AllowUsers
- Fail2Ban
- TCPWrappers
- CrackLib

Umjesto zaključka

- Instalacija i korištenje DE softwarea je dovoljno jednostavno
- Pripazite na loše ili krive implementacije
- Osigurajte povjerljive podatke, uz današnji razvoj alata, ne postoji izlika za ne korištenje SW-a za privatnost

End rant…

- Pitanja, komentari, ideje, primjedbe?
- tonimir.kisasondi@foi.hr

End rant…

- HVALA!