



redhat

linux



lt

Šifrování dat... a komu tím prospějete?

Milan Brož

mbroz@redhat.com

LinuxAlt 2009

Brno

kapitola I. **MOTIVACE**



From Times Online

October 10, 2008

MoD investigat

Original URL: http://www.theregister.co.uk/2008/08/26/more_details_lost/

Million bank details sold on eBay And a few more gone AWOL

By John Oate

Posted in ID, 26

A computer ha

The secondha
Bank of Scotla
numbers, mobi
enough for an

IT manager An
[Mail on Sunda](#)
35.html): "I coul
thousands and

THE AUSTRALIAN BUSINESS AUSTRALIAN IT HIGHER EDUCATION POLITICS VIDEO

IT News IT Business Reviews ExecTech Opinion Best of the Web Careers



(Richard Mills/The Times)

The identity and family details of the exposed

Richard Kerbaj and Times Online

The Ministry of Defence was today investigating its v
hard drive with details of about 100,000 servicemen a
Armed Services was found to be missing on Wednes

Sensitive details of the family members of personnel
details and passport numbers.

The portable hard drive — which is believed not to have been encrypted — was used by EDS, the MoD's main IT contractor, to test computer equipment. It could have been missing for several days.

Tax data unencrypted

Mahesh Sharma | November 04, 2008

Save Settings Font Size: Print Page:

THE Australian Tax Office will continue to use unencrypted CDs to deliver taxpayer information, and the practice could be used at other government agencies.

An unencrypted disk containing the name, address and super fund tax file numbers for 3122 trustees went missing last month when a courier failed to deliver it to the tax office.

The office could not comment on why the CD was not encrypted or whether it intended to stop the practice in favour of transferring information over secure networks.

- <http://www.timesonline.co.uk/tol/news/uk/article4918986.ece>
- http://www.theregister.co.uk/2008/08/26/more_details_lost/
- <http://www.australianit.news.com.au/story/0,,24597034-15306,00.html>

UK's families put on fraud alert

Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.

The Child Benefit data and National Insurance numbers for 10 million people.

Chancellor Alistair Darling said the data was sent to criminals - but urged vigilance to prevent "any further activity".

The Conservatives described the loss as a "major security breach".

██████ loses customers' data disc

The ██████ banking group has admitted losing a computer disc with the details of 370,000 customers.

The disc was lost four weeks ago after being sent by courier from the bank's life insurance offices in Southampton.

The customers' details included their names, dates of birth, and their levels of insurance cover.

However, there were no addresses or bank account numbers, so the potential for fraud was limited.

"We are looking into it and basically it has been a security breach," said a spokesman.

"The reinsurer we sent it to is doing a thorough search to try and find it."

"There are no financial details there in terms of anything like that," he added.

As well as name, date of birth and value of policy, the disc also held the policy number and whether or not the customer was a smoker.

Fines

Missile data found on hard drives

Sensitive information for shooting down intercontinental missiles as well as bank details and NHS records was found on old computers, researchers say.

Of 300 hard disks bought randomly at computer fairs and an online auction site, 34% still held personal data.

Researchers from BT and the University of Glamorgan bought disks from the UK, America, Germany, France and Australia.

The information was enough to expose individuals and firms to fraud and identity theft, said the researchers.

Professor Andrew Blyth said: "It's not rocket science - we used standard tools to analyse the data".

http://news.bbc.co.uk/2/hi/uk_politics/7103566.stm

<http://news.bbc.co.uk/2/hi/business/7334249.stm>

http://news.bbc.co.uk/2/hi/uk_news/wales/8036324.stm

Příklad studie...

The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market

Journal of International Commercial Law and Technology, Vol. 4, Issue 3 (2009)

- pravidelná studie od roku 2005
- náhodně nakoupené disky
- forenzní analýza obsahu

- nezbyvali se nefunkčními disky
- velká část disků obsahovala obnovitelná data
- odhaleny naivní pokusy o likvidaci dat

Doporučení

- fyzická likvidace storage
- spolehlivé smazání informací (data shredding)
- analýza rizik a stanovení procesů, školení uživatelů
- šifrování

Zneužitelná data (co se našlo)...

firemní data

- „company confidential“ - účetnictví, smlouvy, plány, know-how
- adresáře, přístupové kódy
- zdravotnická dokumentace, personalistika
- právníké dokumenty
- konfigurace interní sítě, firewallu

soukromá data

- fotografie, videa
 - hesla, přístupové kódy, privátní klíče
(bankovní služby, obchody, sociální sítě...)
 - elektronická pošta
-
- zálohy dat
 - nelegální SW, pornografie, audio/video (p2p sítě)
 - některá data lze využít i k vydírání
 - informace využitelné konkurencí, při soudních sporech

kapitola II.
TECHNOLOGIE

Šifrování disků – kde pomůže HW?

speciální HW (disk) s podporou šifrování

- vendor lock-in, firmware není opensource
- **HW based full disk encryption (FDE)**
 - HDD FDE (disk obsahuje data + key management)
 - Chipset FDE (disk + chipset + TPM)

HW akcelerace

- **VIA Padlock, Geode** (~koprocessor)
- **AES-NI** (optimalizované instrukce CPU pro AES, Intel Westmere)
- plně podporováno v Linux kernelu (původně zejména pro IPsec)

Šifrování souborového systému

Souborový systém: (EncFS, eCryptfs, ...)

- šifrování na úrovni filesystemu
- metadata algoritmu v souboru nebo adresáři, kopírují se s daty
- některá metadata filesystemu nejsou šifrovaná
- selektivní výběr, co se šifruje (které soubory nebo adresáře)

...

Dále se budeme věnovat pouze šifrování na úrovni blokového zařízení.

Šifrování disků – v Linuxu

Virtuální blokové zařízení

- šifrování na úrovni sektorů
- transparentní pod souborovým systémem
- v kombinaci s volume managementem (LVM)
- swap partition

dm-crypt / LUKS (preferované řešení:-)

- stejně jako LVM řešení postavené na device-mapperu
- cryptsetup/LUKS jednoduchá správa hesel – až 8 hesel k disku
 - metadata přímo na disku, speciální návrh

truecrypt

- multiplatformní řešení, na Linuxu využívá dm-crypt jako backend

loop-aes

- separátní projekt mimo hlavní strom, nad loop ovladačem, multikey

cryptsetup / dm-crypt – co je nového

Většina distribucí již v základní instalaci

- v budoucnu integrace s LVM
- dříve či později návrh LUKS2

cryptsetup (verze 1.1)

- nové API pro libcryptsetup
- volitelný hash algoritmus pro LUKS (dříve jen SHA1)
- záloha LUKS hlavičky (luksHeaderBackup/Restore)
- podpora pro „suspend“ s vymazáním klíče z paměti
luksSuspend, luksResume
- možnost použití předgenerovaného klíče
- (admin recovery, využívá se pro Key Escrow)

dm-crypt

- společně s celým device-mapperem nyní podporuje bariéry (důležité pro ext4, xfs a podobné souborové systémy)

kapitola III.

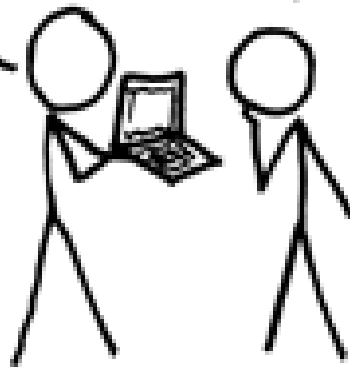
ÚTOK

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

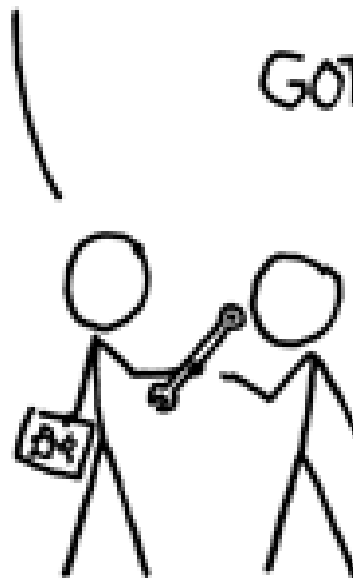
NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



kapitola IV.

ÚTOK II.

Attacks always get better, they never get worse.

Útoky se vždy jen vylepšují, nikdy se už nezhorší.

Ilustrační příklady – AES

Útok na vlastní algoritmus

- donedávna neexistoval útok na plnou implementaci AES-256.
- dnes je již publikován (plně prakticky neproveditelný)
„Related-key attack on the full AES-256“

Útok na implementaci

- využití postranních kanálů
- často zmiňovaný **„AES Cache-collision Attack“**
(některé operace trvají déle, nejsou-li data v cache procesoru)

Ale více obvyklé jsou spíše snahy získat klíč přímo...

- napadení hw (keylogger, Cold Boot)
- malware – modifikace boot, OS, hypervisoru
- social engineering :-)

No security product on the market today can protect you if the underlying computer has been compromised by malware with root level administrative privileges.

That said, there exists well-understood common sense defenses against “Cold Boot,” “Stoned Boot,” “Evil Maid,” and many other attacks yet to be named and publicized.

Marc Briceno, PGP Corporation

<http://blog.pgp.com/index.php/2009/10/evil-maid-attack/>

V současnosti neexistuje žádné bezpečnostní řešení, které vás ochrání, když v počítači je instalován zákeřný software běžící s právy administrátora systému.

Přesto existují dobře známé, rozumné a snadno pochopitelné postupy, jak se bránit proti „Cold Boot“, „Stoned Boot“, „Evil Maid“ a mnoha dalším útokům, které na své pojmenování a zveřejnění teprve čekají.

**If you let your machine out of your sight,
it's no longer your machine.**

Počítač ponechaný chvíli bez dohledu už nemusí patřit jen vám.

Myšlenka „útoků“ není nová, ale často je vedlejším efektem zviditelnění...

Cold Boot využívá vlastnosti pamětí DRAM udržet informaci po nějakou dobu po výpadku napájení.

Stoned boot varianta root/boot kitu (modifikace zavaděče)

Evil Maid „šílená pokojská“ zaútočí na šifrovaný notebooku (ponechaném na hotelovém pokoji) tak, že nabojuje z jiného média (USB) a modifikuje zavaděč systému. (Po odchyčení hesla/klíče odstraní malware.)

- Většina těchto útoků je v principu aplikovatelná na libovolné systémy, Linux nevyjímaje.
- Dokonce jsou na Linuxu možnosti mnohem větší, neboť je dostupný zdrojový kód – lze tedy jednoduše modifikovat přímo kernel či ovladače.

Praktický příklad

útok Cold Boot na dm-crypt (LUKS)

Útok vychází ze studie (a zdrojových kódů)

Lest We Remeber: Cold Boot Attacks on Encryption Keys

Princeton University, <http://citp.princeton.edu/memory/>

- **Paměť DRAM** udrží data ještě nějakou dobu po výpadku napájení.
- Pro šifrování, které provádí hlavní procesor, **musí být v paměti RAM přítomen klíč.**
- Pokud získáme klíč k blokové šifře, **již není třeba žádná hesla.**
- Odchytíme tedy klíč z paměti po násilném resetu systému nebo uspání.

Pomocné programy na zálohu a sken paměti

- optimalizace AES umožňuje efektivní vyhledávání klíče
- ale i opravu, pokud dojde ke ztrátě několika bitů!

Příklad: útok Cold Boot na dm-crypt (LUKS)

Konfigurace počítače, na který se útočí

```
[root@192.168.2.4]# cryptsetup luksDump /dev/sda2
LUKS header information for /dev/sda2
Cipher name:      aes
Cipher mode:      xts-plain
MK bits:          512
...
```

```
[root@192.168.2.4]# dmsetup table --showkeys
luks-...: 0 155882682 crypt aes-xts-plain \
ffe8b78d9f652e5eddc822885d3c2b47b3... \
75f5d220a30dbd40a506a6fdc9ad571e7b... 0 8:2 4040
vg-lv_swap: 0 2818048 linear 253:0 153051520
vg-lv_root: 0 153051136 linear 253:0 384
```

- násilný reset (bez napájení cca 1 sekundu)
- nabootování PXE zavaděče
- přenesení RAM image přes síť
- sken na přítomné klíče

```
$ ./pxed 192.168.2.4 >img
request segment0 [base: 0x0 size: 579584]
request segment1 [base: 0x100000 size: 736034816]
request segment2 [base: 0x2bf00000 size: 1048576]
```

```
$ ./aeskey -t 50 img
ffe8b78d9f652e5eddc822885d3c2b47b3...
75f5d220a30dbd40a506a6fdc9ad571e7b...
Keyfind progress: 100%
```

záporný
jedinec!



Praktický příklad ...

Vše co je ukázáno na příkladu dm-cryptu v Linuxu, lze ale v principu aplikovat ostatní systémy (Cold Boot je útok na HW) a to ve všech operačních systémech, což bylo opakovaně provedeno.

Snahou vývojářů je poskytnout maximální možnou obranu (je-li to možné).

Ale nikoliv implementovat řešení, která jsou nekompletní a neřeší podstatu problému.

Pro dm-crypt/LUKS:

- luksSuspend/luksResume – vymazání klíče z paměti
- přímá podpora TPM bude, ale až jako část komplexního řešení
- wrappery pro TPM existují, ale nijak nezvýší bezpečnost

Pokud někdo tvrdí, že má neprolomitelné řešení, vzpomeňte si na scénu s nerozbitnou skleničkou :-)

k

t

 V.
Abort, Retry, Ignore?

Před čím šifrování disku chrání?

- při ztrátě notebooku nedojde k úniku dat
- při ztrátě či poruše disku (a „oživení“) nehrozí únik dat

Toto platí ale jen, když ...

- **šifrování je nakonfigurováno správně**
 - obvykle se preferuje šifrovat celý disk
 - swap musí být šifrovaný také
 - není použit parametr degradující celé řešení (slabé heslo)
- **notebook není ve sleep režimu**
 - RAM nesmí obsahovat aktivní data resp. klíč
 - hibernace při šifrovaném swapu obvykle není problém
- **„nálezce“ nemá k dispozici klíč v jiné formě**
 - bývalý uživatel má zálohu hlavičky se starým heslem (LUKS, Truecrypt)
- **uživatel již nikdy do navráceného systému nezadáva autentizační údaje (bez auditu vylučující napadení)**

Většina systémů při vypnutí a hibernaci maže šifrovací klíč z paměti, ale není to pravidlem, proto je dobré systém hlídat i jistou dobu po vypnutí (minuty).

Před čím šifrování disku plně NEchrání?

- **Před cíleným útokem, kdy útočník má (opakovaně) k dispozici**

- **Fyzický přístup k HW**

- může tedy instalovat malware – upravit BIOS, fw disku, boot loader, initramdisk, moduly kernelu, ...
- instalovat hw keylogery, kamery snímající klávesnici apod.
- provádět na zařízení různá měření (odběr proudu, vyzařování, ...)

- **Administrátorská oprávnění v systému**

- nejde jen o vlastní OS, ale například i hypervisor nad ním
- lze tedy odchytil systémová volání, čtení z disku apod.

- **Řešením je „trusted computing“
ale pouze jako komplexní řešení (a to nikdo zatím nemá!)**

Některé systémy sice využívají TPM (Trusted Platform Module) pro ukládání hesla, ale pokud šifrování provádí hlavní CPU, stejně se klíč musí dříve či později objevit v RAM.

Na použití TPM jsou rozporuplné názory, budoucnost ukáže.

A navíc, pouze velmi nové systémy disponují potřebným HW (nebo ještě ani nejsou na trhu).

- **Tyto útoky tedy nelze se současným hw/sw vyloučit,
ale lze je velmi zkomplikovat (nebo alespoň detekovat)**

Před čím šifrování disku plně NEchrání?

- **nechrání před únikem dat mezi oprávněnými uživateli**

- transparentní šifrování na úrovni disku je skryté před FS (pracuje na úrovni sektorů, nemá ponětí, které jsou alokované)
- pokud aplikace nepřepíše data, sektor stále existuje se starým obsahem
- forenzní nástroje a recovery aplikace fungují beze změny (např. schopnost obnovit smazané soubory)

Pokud má k odemčenému disku přístup i jiný uživatel, bezpečné mazání starých souborů je tedy stále nutné.

- **nechrání před nezodpovědným uživatelem**

- „klíč je pod rohožkou“

- **je vhodné kombinovat více způsobů autentizace**

- two-factor authentication (heslo + token)
- před mapováním šifrovaného disku

- **Ani bezpečný HW není zárukou absolutní bezpečnosti.**

- **použití šifrování ve virtuálních strojích a „cloudech“**

- nešifrovaná pozastavená VM obsahuje volně přístupný klíč v suspended RAM image
- hypervisor musí být důvěryhodný
- sdílení výpočetního výkonu otevírá nové možnosti útoku

děkuji za pozornost