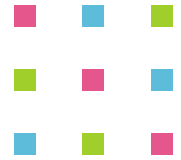
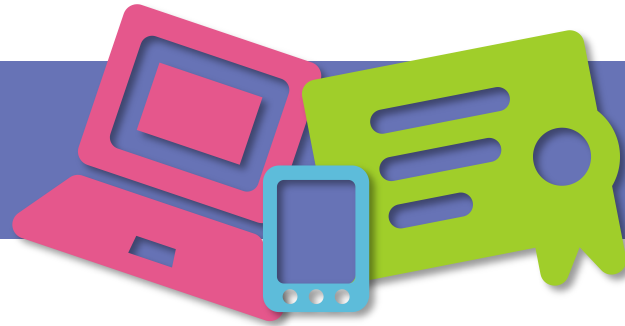


SECURITY 2014



22. ročník konference o bezpečnosti v ICT



Šifrovanie pevných diskov

Adam Brunai

AEC, spol. s r.o.



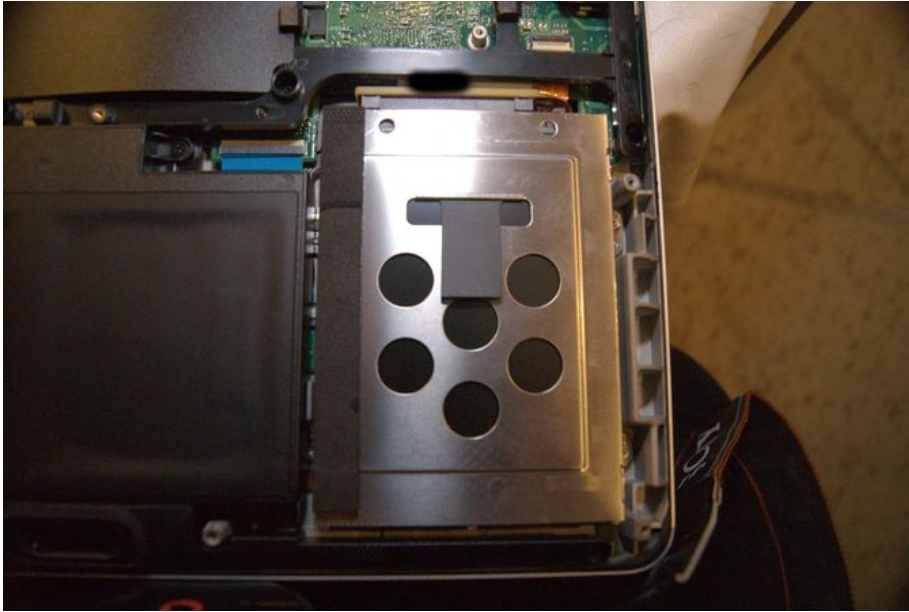
Prečo šifrovať?

- Príklad: Notebook s nešifrovaným HDD
 - Krádež
 - Strata zariadenia
 - Voľný prístup k zariadeniu (pracovisko, hotel atď.)
 - ...





Prečo šifrovať?



1.



2.



Prečo šifrovať?



```
Hiren's BootCD 13.2      GRUB4DOS0.4.5b20110327 639K/254M

^Boot From Hard Drive (Windows Vista/7 or Xp)

Dos Programs
Mini Windows Xp
Mini Linux

Windows Memory Diagnostic
MemTest86+
Offline NT/2000/XP/Vista/7 Password Changer
Kon-Boot
Seagate DiscWizard (Powered by Acronis Trueimage)
PloP Boot Manager
Smart Boot Manager 3.7.1
Fix "NTLDR is Missing"
Darik's Boot and Nuke (Hard Disk Eraser)
Custom Menu... (Use HBCDCustomizer to add your files)
More...
```



Prístup k dátam

- Súborové oprávnenia sú neprenosné v rámci iného OS - **neobmedzený** prístup k dátam

```
adam@adam-NTB: /media/adam/9A38A3B638A39035
adam@adam-NTB:/media/adam/9A38A3B638A39035$ uname -mrs
Linux 3.5.0-45-generic x86 64
adam@adam-NTB:/media/adam/9A38A3B638A39035$ ls -l | grep drwx
drwx----- 1 adam adam      4096 Jan 17 21:53 Config.Msi
drwx----- 1 adam adam    40960 Jan 12 00:22 Downloads
drwx----- 1 adam adam         0 Feb 18 2013 found.000
drwx----- 1 adam adam         0 Nov 15 21:19 found.001
drwx----- 1 adam adam      8192 Jan 17 21:48 ProgramData
drwx----- 1 adam adam    12288 Jan 17 21:46 Program Files
drwx----- 1 adam adam    12288 Jan 17 22:23 Program Files (x86)
drwx----- 1 adam adam      4096 Aug  1 2012 Python27
drwx----- 1 adam adam      4096 Sep 11 2012 Python32
drwx----- 1 adam adam         0 Jun 17 2012 Recovery
drwx----- 1 adam adam         0 Jun 25 2012 $Recycle.Bin
drwx----- 1 adam adam      8192 Jan 18 10:06 System Volume Information
drwx----- 1 adam adam      4096 Oct 31 18:39 Tor Browser
drwx----- 1 adam adam      4096 Nov  7 23:32 Users
drwx----- 1 adam adam    16384 Jan 17 21:31 Windows
adam@adam-NTB:/media/adam/9A38A3B638A39035$
```



Získanie užívateľských hesiel

- C:\windows\system32\config\SAM
- Nástroje:
 - Ophcrack
 - Offline NT Password & Registry Editor
 - Kali Linux

```
==== chntpw Edit User Info & Passwords ====
```

: RID	: Username	: Admin?	: Lock?
: 01f4	: Administrator	: ADMIN	: dis/lock
: 03e8	: geek	: ADMIN	: *BLANK*
: 01f5	: Guest	:	: dis/lock

```
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)  
or simply enter the username to change: [Administrator] geek_
```



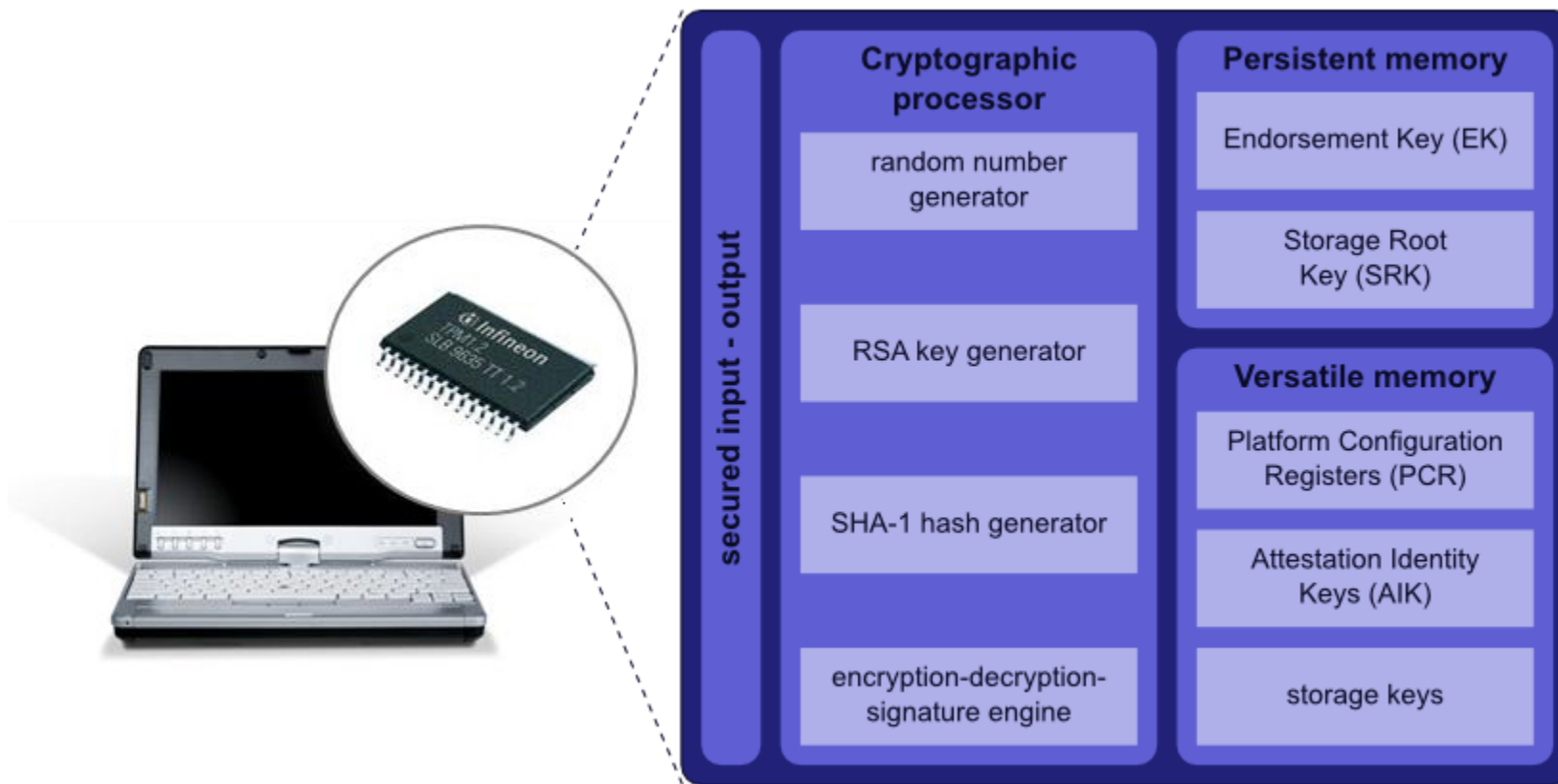
OK, chceme disk šifrovať

- Ako na to?
- **BitLocker**
 - Proprietárny software zahrnutý vo vyšších edíciách Windows
 - *Používa* TPM chip
 - AES-CBC
- **TrueCrypt**
 - Dostupný zdrojový kód
 - *Nepoužíva* TPM chip
 - AES-XTS, Serpent, Twofish a ich kombinácie



Trusted Platform Module (TPM)

- Štandardizovaný kryptoprocessor (ISO/IEC 11889)

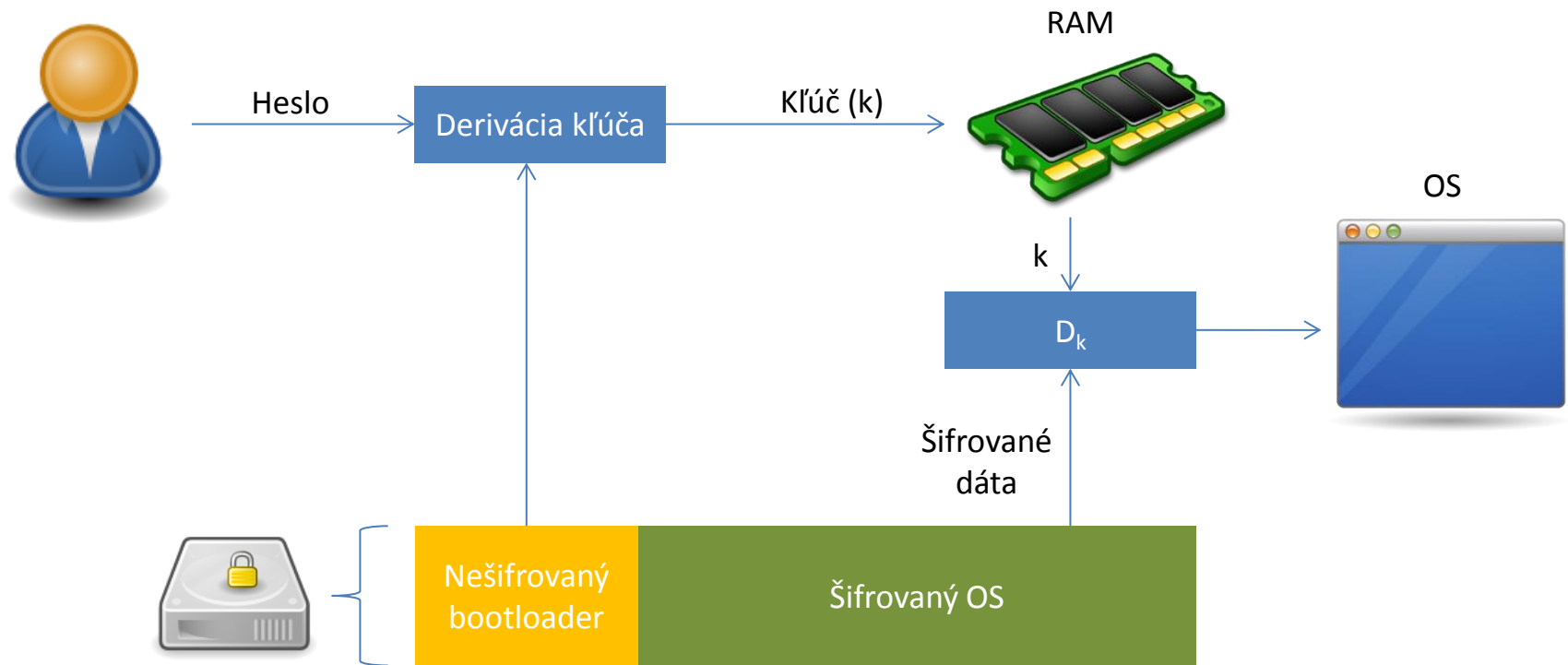




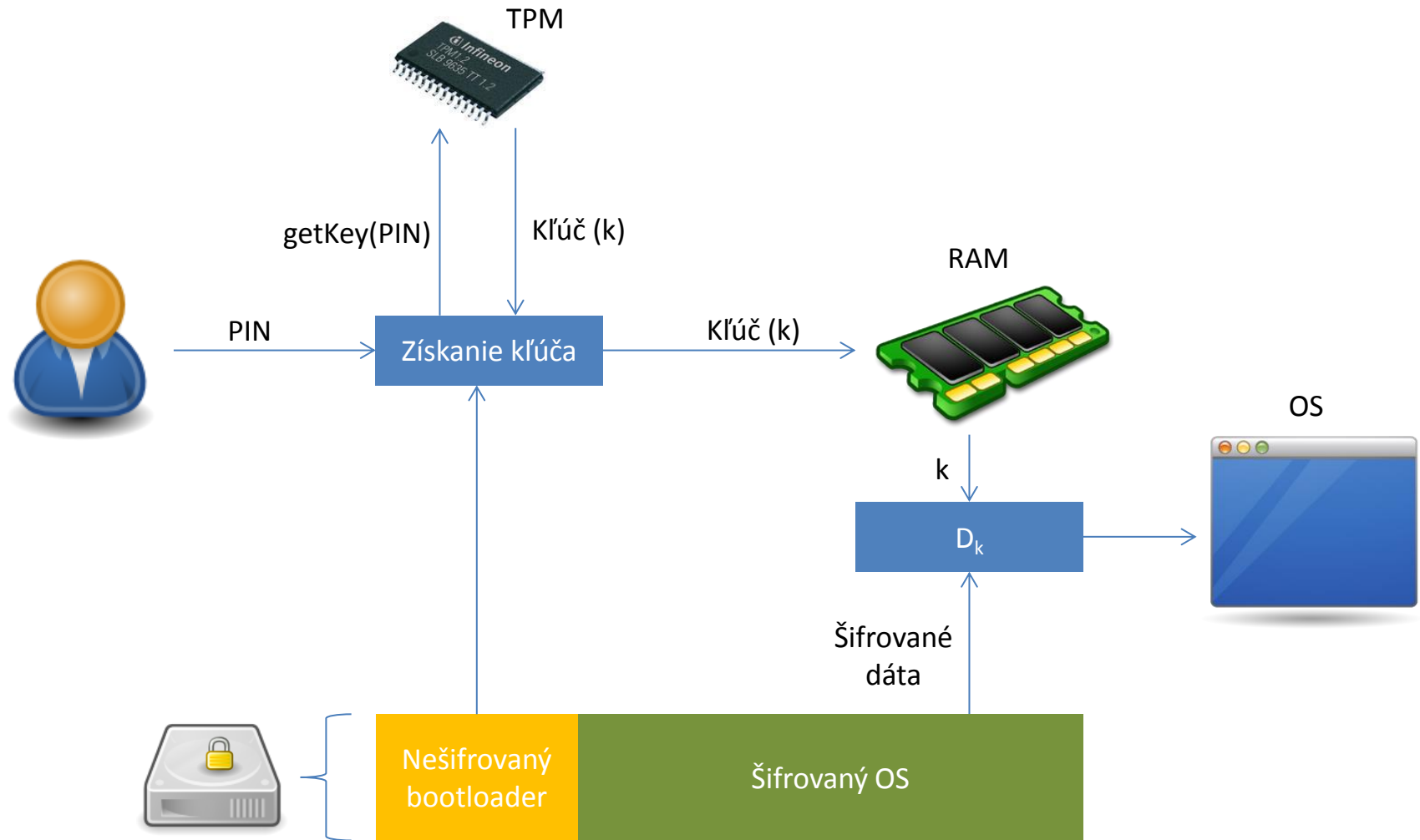
Trusted Platform Module (TPM)

- Kontrola integrity HW a SW
- Heslo vs. PIN
- Vývoj:
 - AMD
 - Microsoft
 - Intel
 - ...
 - NSA?

Pre-boot autentizácia (SW)



Pre-boot autentizácia (TPM)





Metódy autentizácie

Metóda	Úroveň ochrany
TPM	★
TPM + PIN	★ ★
Heslo (bez TPM)	★ ★
TPM + USB flash disk	★ ★
TPM + USB flash disk + PIN	★ ★ ★

Bezpečnosť šifrovania HDD

Super, ale je to bezpečné?





DMA attack

- Zneužitie rozhrania IEEE 1394 SBP-2 k získaniu **prístupu do pamäte RAM**
- Požiadavky (počítač obete):
 - FireWire, Thunderbolt, ExpressCard port
 - 4 alebo menej GiB pamäte
 - Režim spánku, alebo TPM bez autentizácie
- Požiadavky (počítač útočníka):
 - Linux s nainštalovanou utilitou `inception`
- **Authentication bypass**



DMA attack

Video ukážka



DMA attack

- Čo sa skrýva pod kapotou?

msv1_0.dll - signatúra

```
754EE920 . FF15 88114E75 CALL DWORD PTR DS:[<&ntdll.RtlCompareMemory>] ntdll.RtlCompa
754EE926 . 83F8 10      CMP EAX,10
754EE929 . 75 13      JNZ SHORT msv1_0.754EE93E <-- fix this!
754EE92B > B0 01      MOV AL,1
754EE92D > 8B4D FC      MOV ECX,DWORD PTR SS:[EBP-4]
754EE930 . 5F      POP EDI
754EE931 . 5E      POP ESI
```



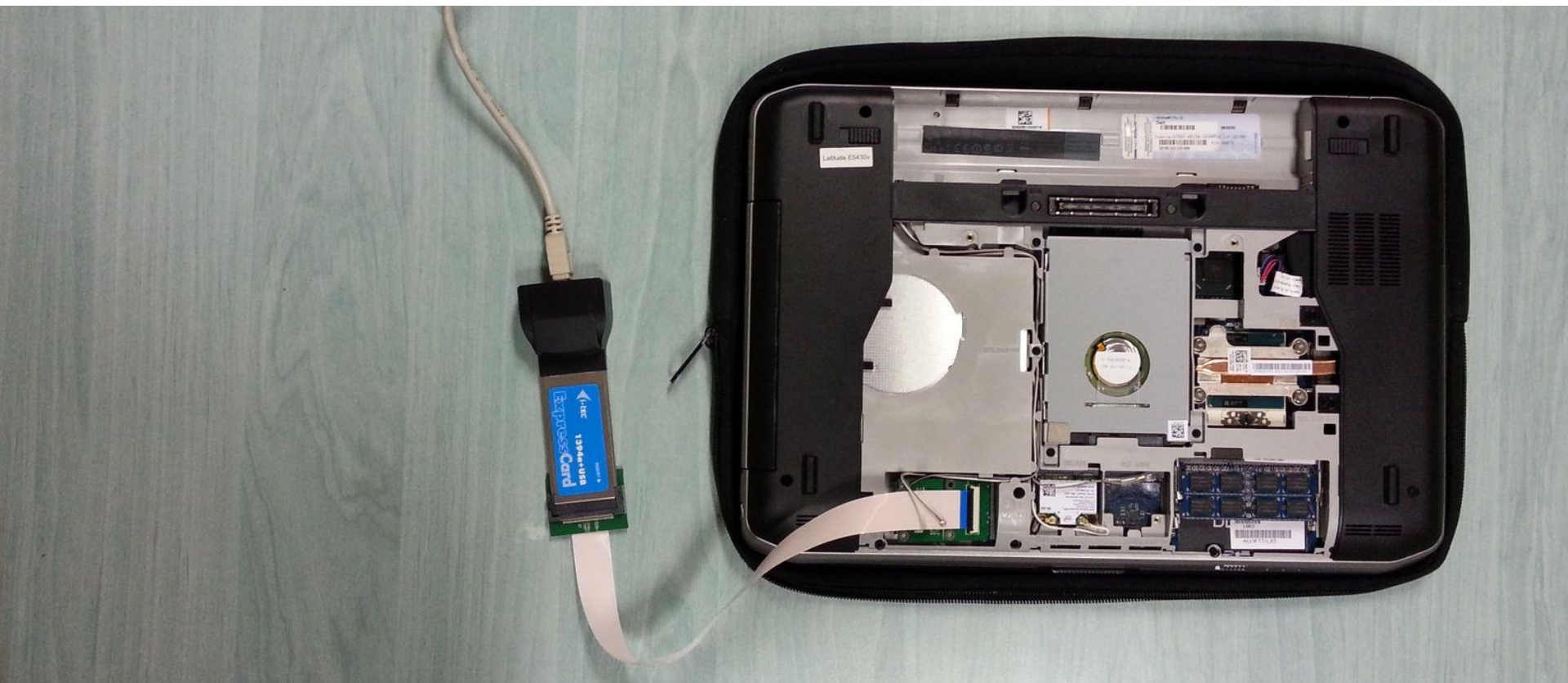
msv1_0.dll – záplata (patch)

```
754EE920 . FF15 88114E75 CALL DWORD PTR DS:[<&ntdll.RtlCompareMemory>] ntdll.RtlCompa
754EE926 . 83F8 10      CMP EAX,10
754EE929 . 90      NOP <-- done
754EE92A . 90      NOP
754EE92B > B0 01      MOV AL,1
754EE92D > 8B4D FC      MOV ECX,DWORD PTR SS:[EBP-4]
754EE930 . 5F      POP EDI
754EE931 . 5E      POP ESI
```



DMA attack

- Použiteľné taktiež na každom zariadení s PCIe mini slotom





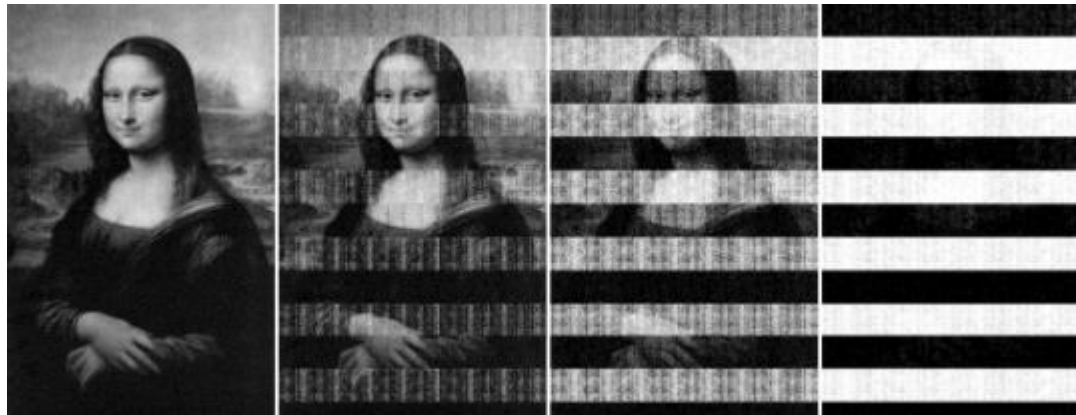
Cold boot attack





Cold boot attack

- DRAM uchováva dáta pri veľmi nízkych teplotách i niekoľko minút po odpojení napájania
- Pamäť **obsahuje šifrovacie kľúče** k disku



Analýza dát na zbernici





DRAM

Operačná pamäť je slabý článok bezpečnosti
šifrovania pevného disku.

Vieme s tým niečo spraviť?



Evil maid attack



19. února 2014

SECURITY 2014



Evil maid attack

1.



Útočník nahradí bootloader modifikovanou verziou



2.



Autentizácia legitímneho
užívateľa



Heslo je uložené na
nešifrovanú časť HDD



3.



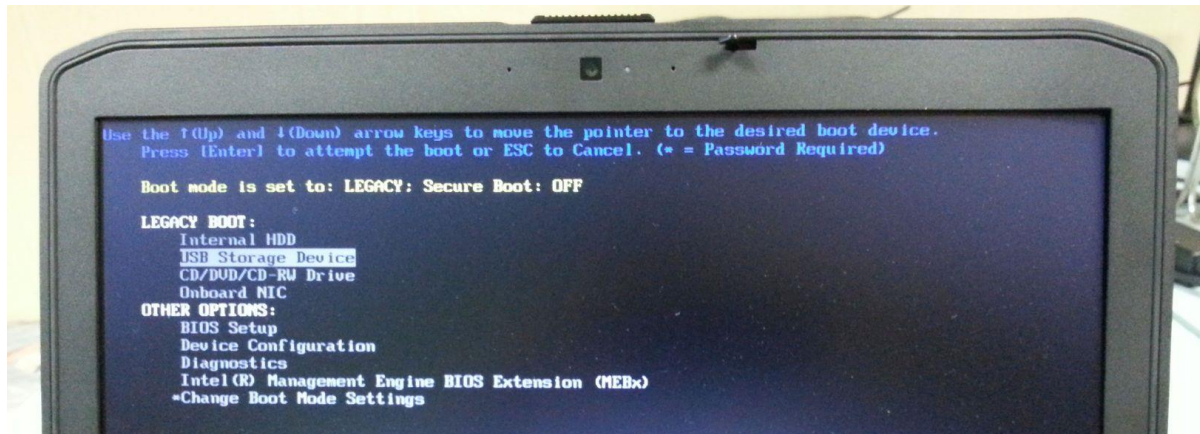
Útočník získa heslo uložené na HDD





Evil maid attack

- Kompromitácia systému vyžaduje aspoň jednu z nasledujúcich podmienok:
 - a) Možnosti naboťovať OS z externého média
 - b) Umiestniť do zariadenia HW keylogger
- Je útok možný aj pri použití TPM?





Útok hrubou silou na Truecrypt

Predpokladajme heslo s dĺžkou **8** znakov, zložené s **malých a veľkých písmen, číslic a špeciálnych znakov**. Ďalej predpokladajme, že útočník použije k útoku **paralelné výpočty** prostredníctvom grafickej karty (technológia CUDA).

Rýchlosť takéhoto útoku na bežnom PC je približne $r = 300$ *hesiel za sekundu*. Pre počet všetkých možných hesiel C platí:

$$C = S^l [\text{hesiel}]$$

Kde S je počet všetkých povolených znakov v hesle a l je dĺžka hesla. V našom prípade $S = 26 + 26 + 10 + 32 = 94$ a $l = 8$. Teoretický čas t potrebný k útoku (polovica maximálneho času) vypočítame ako:

$$t = \frac{C}{2r} [s]$$

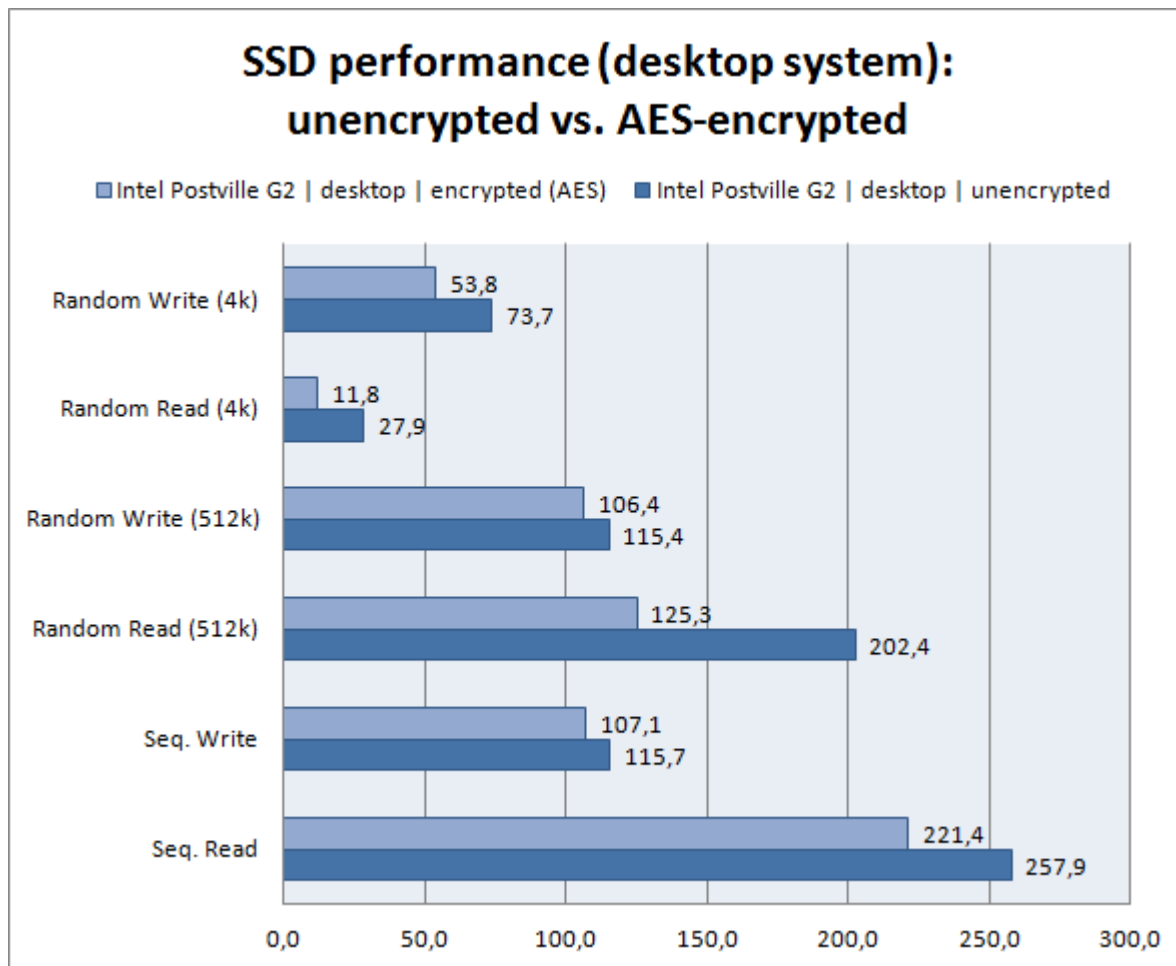
$$\text{Čiže } t = \frac{S^l}{2r} = \frac{94^8}{2 \cdot 300} = 10\,159\,482\,309\,018\,s = \underline{\underline{322\,155\,rokov}}$$



Ako sa brániť?

- V prípade použitia hesla voliť silné heslá
- Používať viac faktorovú autentizáciu
- Zakázať DMA pre externé zariadenia
- Zakázať quick boot a nastaviť heslo na BIOS
- Používať Secure Boot ak je to možné
- Používať hibernáciu namiesto režimu spánku

Pokles výkonu (5-20%)



Self-encrypting drives (SED)

- Zanedbateľná strata výkonu
- Podporuje dual boot, nezávislosť na OS, atď.
- Pre-boot autentizáciu zabezpečuje read-only software uložený na pevnom disku
- Približne 2x tak drahé ako klasický HDD





Ďalšie informácie

Lámanie/reset hesla k Windows (nešifrovaný HDD)

- <http://epyxforensics.com/node/34>
- <http://www.techrepublic.com/blog/windows-and-office/reset-lost-windows-passwords-with-offline-registry-editor/639/>

DMA attack (nástroj Inception)

- <http://www.breaknenter.org/projects/inception/>

Zablokovanie Firewire rozhrania

- <http://support.microsoft.com/kb/2516445>

Cold boot attack

- <https://citp.princeton.edu/research/memory/>

Evil maid attack (s TPM)

- http://testlab.sit.fraunhofer.de/bitlocker_skimming/

Výkon

- <http://www.7tutorials.com/what-performance-impact-system-encryption-truecrypt>



Ďakujem za pozornosť.

Adam Brunai

AEC, spol. s r.o.

adam.brunai@aec.cz

