

11

es

Rencontres **Mondiales**
du **Logiciel Libre**
Du 6 au 11 juillet 2010



***Le chiffrement de disque sous linux,
vrai ou faux sentiment de sécurité?***

Kevin DENIS

Le 07 juillet 2010, RMLL





**Le 27 février 2009, 4 portables
du futur Centre Pénitentiaire de
Nancy-Maxéville sont volés.**

**Les disques contiendraient les
codes de fabrication des clefs
et les plans de la Prison.**





**-How Does Bruce Schneier
Protect His Laptop Data?**

-With his fists -- And PGP



Fichier

Filesystem

Device

dm-crypt

Disque

cryptsetup : outil userland
dm-crypt : module noyau





Démarrage:

- Le BIOS lance le bootloader
- Le bootloader lance le noyau et l'initramfs
- L'initramfs demande la clé LUKS
- La racine est déchiffrée et montée
- Le boot continue...





Solidité d'AES

**CPU 32 cores à 30GHz
1 cycle d'horloge par calcul
1 Milliard de machines**

**-> 11mn pour 2^{79} clés,
-> 6Mds d'années pour 2^{127}**

**Faiblesses théoriques:
insuffisantes**



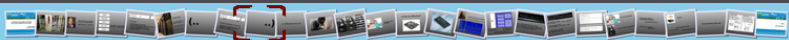




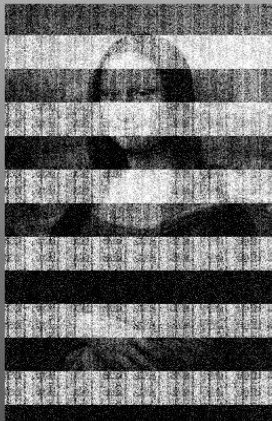
Nouveau mapping dans le container

- Utilisation de cryptsetup sans LUKS
- Attention au premier container
- Attention au filesystem



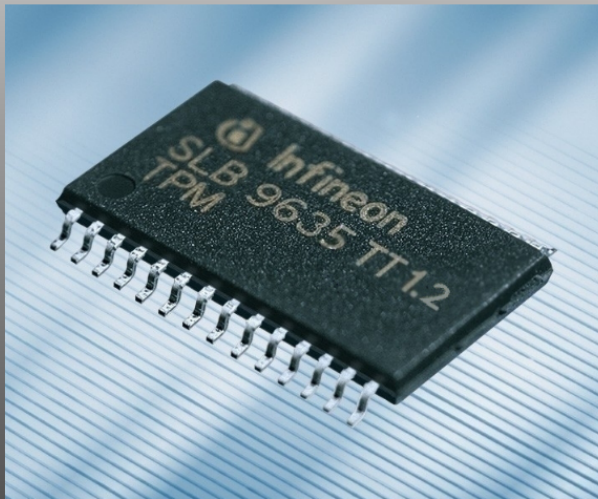






<http://citp.princeton.edu/memory/>







Can you trust your computer?

<http://www.gnu.org/philosophy/can-you-trust.html>

The screenshot shows a BIOS/UEFI setup utility with a blue background. On the left is a menu with the following items: System, System Info, Processor Info, Memory Info, Device Info, Battery Info, Battery Health, Date/Time, Boot Sequence, Onboard Devices, Video, Security, Admin Password, System Password, Internal HDD PW, Password Change, Password Bypass, Wireless Switch Change, Wi-Fi Catcher Change, CPU XD Support, TPM Security (highlighted in green), TPM Activation, Computrace(R), and Performance. The main area is titled "TPM Security" and shows two radio buttons: "Off" (selected) and "On". Below the buttons is a horizontal line, followed by the text: "This field lets you control whether the Trusted Platform Module (TPM) in the system is enabled and visible to the operating system." Below this is the explanation: "Off = The BIOS will not turn on the TPM during POST. The TPM will be non-functional and invisible to the operating system." and "On = The BIOS will turn on the TPM during POST so that it can be used by the operating system." At the bottom is a "NOTE: Setting this field to Off does not change any settings you may have made to the TPM, nor does it delete or change any information or keys you may have stored there. It simply disables the TPM so that it cannot be used. When you change this field back to Enabled, the TPM will function exactly as it did before you turned it Off."





entrées - sorties sécurisées

Processeur cryptographique

générateur de nombres
pseudo-aléatoires

générateur de clés RSA

hacheur SHA-1

moteur de chiffrement-
déchiffrement-signature

Mémoire persistante

clé d'attestation (EK)

clé racine pour
le stockage (SRK)

Mémoire versatile

registres de config.
de la plate-forme (PCR)

clés d'identité
d'attestation (AIK)

clés de stockage

TrouSerS tools

<http://trousers.sourceforge.net/>

Un démon tcstd des outils tpm_*

tpm_takeownership -z -y




```
kevin@darkstar:~$ cat /sys/class/misc/tpm0/device/pcrs \
> | grep -E '(-04|-08|-09|-12|-14)'
PCR-04: 8B CF 76 06 39 53 75 90 1D A1 C9 2B F1 C1 88 30 EE DE 0C 44
PCR-08: 94 E8 E7 9F 9C 0F F0 5A ED F8 BE 54 4F 32 2A C4 E9 10 85 4A
PCR-09: 00 16 0C C8 9C 5A DA 17 5D E9 89 40 A1 BC 26 EA 56 F6 B9 A5
PCR-12: 8B 48 54 31 87 2C 17 6F 15 C6 1A EC DC 2F B5 87 34 F9 3E 9A
PCR-14: 02 97 8D FC 02 2F 5C D8 EA 09 98 8E DF 77 12 54 35 5D DA B1
kevin@darkstar:~$
```

Scellement d'un blob

tpm_sealdata -z -p(...) -i file -o seal.file

Déscellement du blob:

tpm_unsealdata -z -i seal.file -o clear

Utilisation des clés RSA

non disponible (openssl?)



```
if [ -x /sbin/cryptsetup ]; then
  echo "We are in the cryptsetup magic part "
  mount $BOOTPART /key
  if [ -f /key/seal.key ]; then
    echo "TPM boot mode activated .."
    ifconfig lo 127.0.0.1
    tcspd
    tpm_unsealdata -z -i /key/seal.key | cryptsetup luksOpen $ROOTPART $ROOT
    killall tcspd
  else
    # asking user to unlock
    cryptsetup luksOpen $ROOTPART $ROOT
  fi
  umount /key
  echo " Finishing cryptsetup .."
fi
```

```
root@slack:~# reboot
```

```
root@slack:~# modprobe tpm_tis
root@slack:~# tcspd
root@slack:~# cryptsetup luksAddKey /dev/sda1 random_key
root@slack:~# tpm_sealdata -z -p4 -p8 -p9 -p12 -i random_key -o seal.key
root@slack:~# cp seal.key /boot
root@slack:~# shred random_key
root@slack:~# cryptsetup luksDelKey /dev/sda1 0
root@slack:~# reboot
```

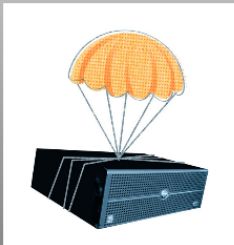


Mot de passe SRK (-z)
000000000000000000000000

tpm_takeownership -y

Mot de passe clé RSA:
indisponible





Backup

apt-get upgrade kernel

rpm -Uvh kernel

slackpkg upgrade kernel



Un mécanisme enfin sûr?



A CRYPTO NERD'S
IMAGINATION:

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

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



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.



11

es

Rencontres **Mondiales**
du **Logiciel Libre**
Du **6 au 11** juillet 2010



Merci

<http://exploitability.blogspot.com>

