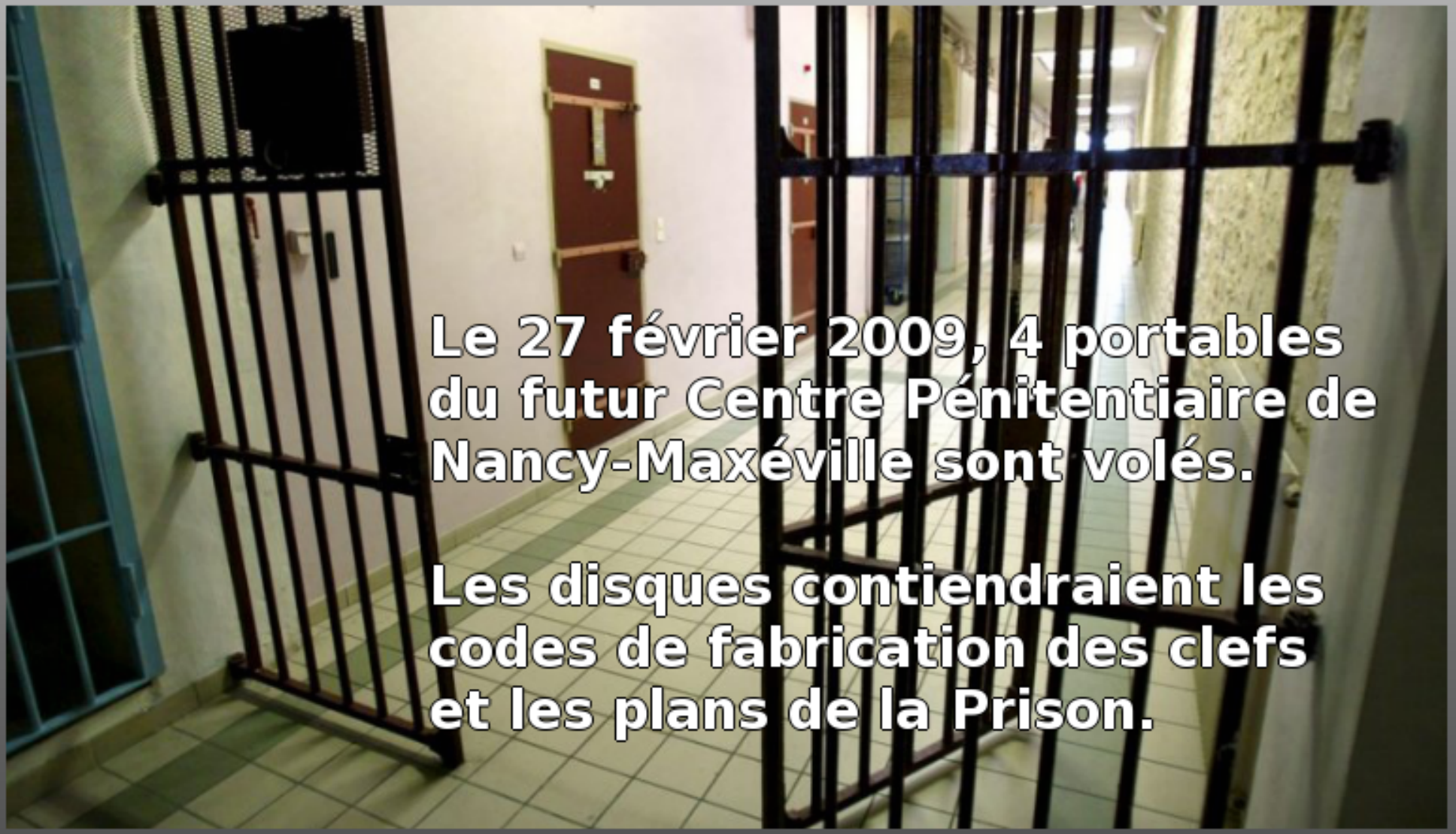
Le chiffrement de disque sous linux, vrai ou faux sentiment de sécurité?

Kevin DENIS
kevin2nis@gmail.com
http://exploitability.blogspot.com


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.

La perte
- **-par accident**
- **-le vol**
- **-le don**

L'espionnage
- **-industriel**
- **-commercial**
- **-d'état...**

Ordinateur portable
PC fixe
Serveur

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...

(..

Nouveau mapping dans le container

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

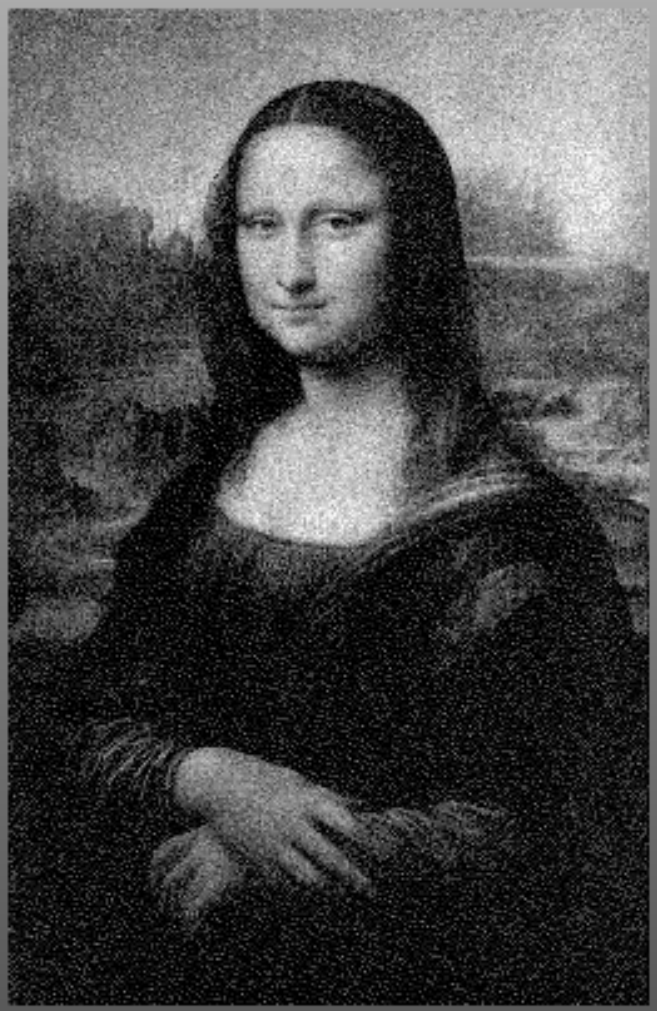
Solidité d'AES

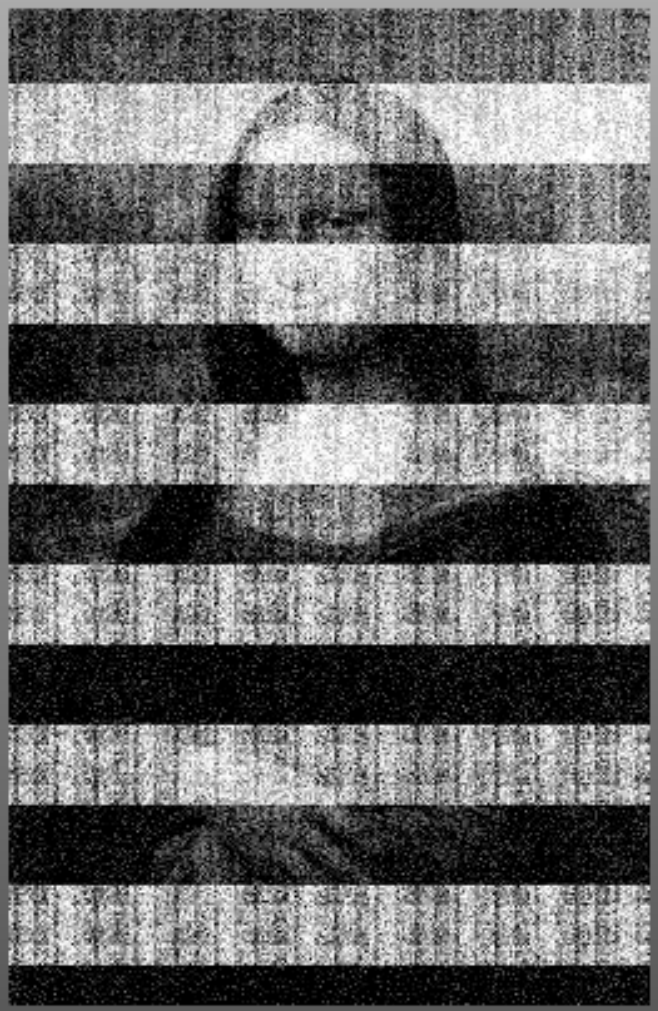
CPU 32 cores à 30GHz
1 cycle d'horloge par calcul
1 Milliard de machines

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

Faiblesses théoriques:
insuffisantes

Le chiffrement est-il sûr?



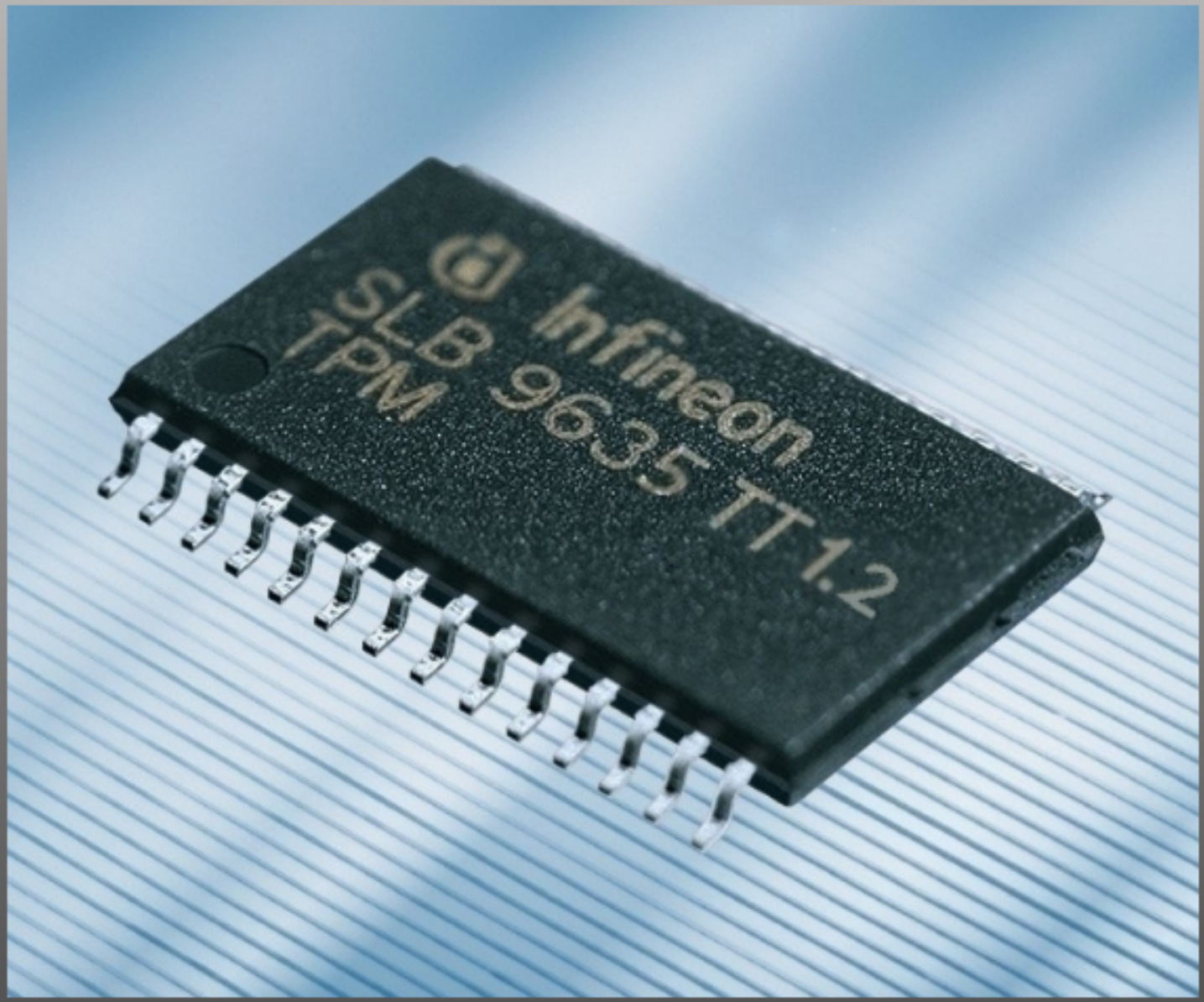


http://citp.princeton.edu/memory/

Que faire contre Evil Maid?

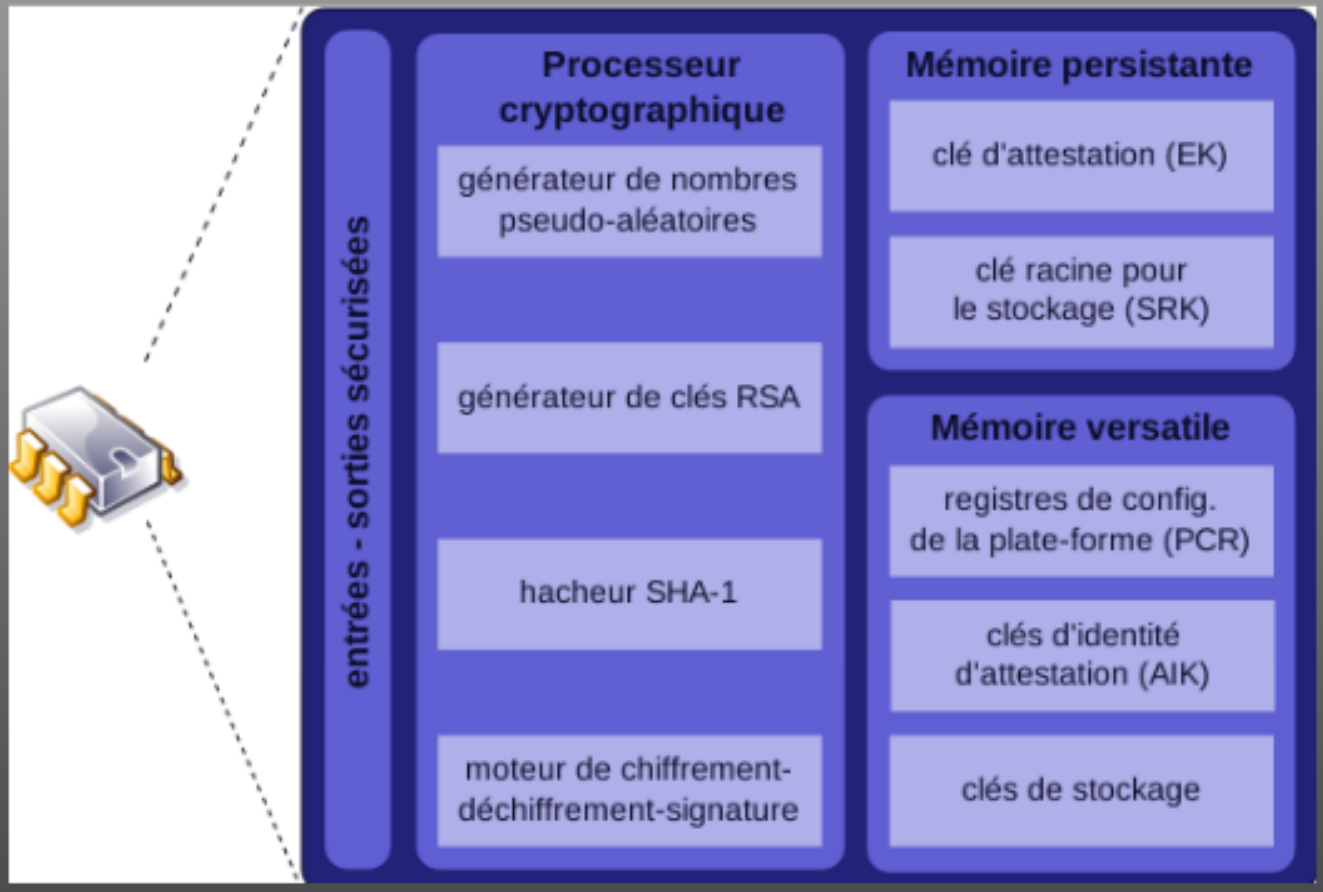
http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

L'échec du chiffrement?


Infineon
SLB 9635 TT1.2
TPM

Can you trust your computer?

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

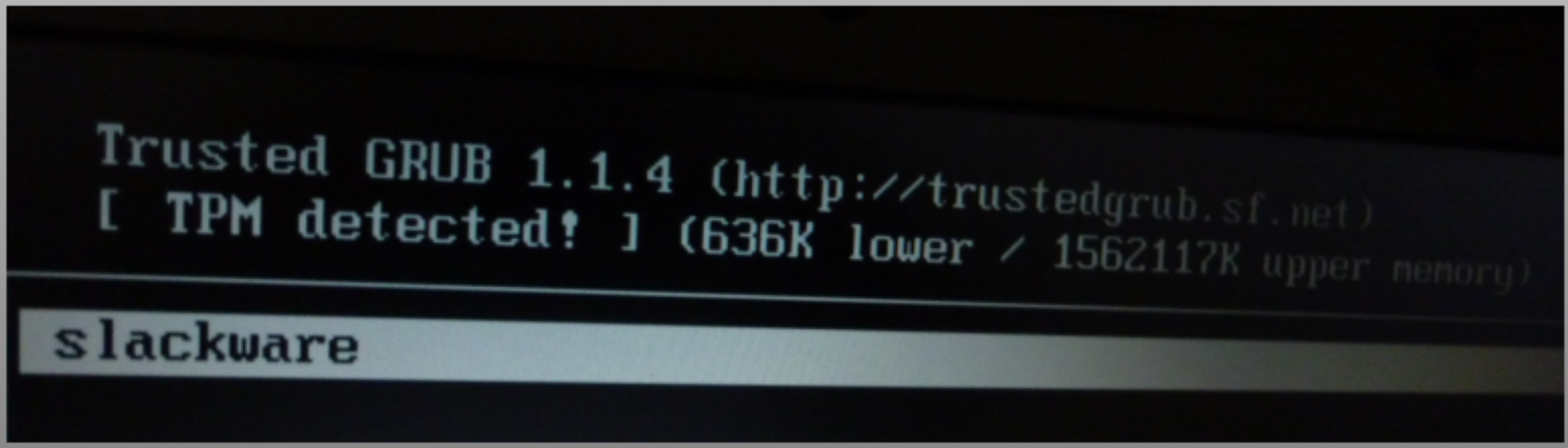


TrouSerS tools

http://trousers.sourceforge.net/

Un démon tcsd
des outils tpm_*

tpm_takeownership -z -y



PCR 4: MBR information and stage1
PCR 8: bootloader information stage2 part1
PCR 9: bootloader information stage2 part2
PCR 12: commandline arguments
PCR 14: all files loaded (Linux kernel, initrd...)

```
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 (engine 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
    tcsd
    tpm_unsealdata -z -i /key/seal.key | cryptsetup luksOpen $ROOTPART $ROOT
    killall tcsd
  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:~# tcsd
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
```

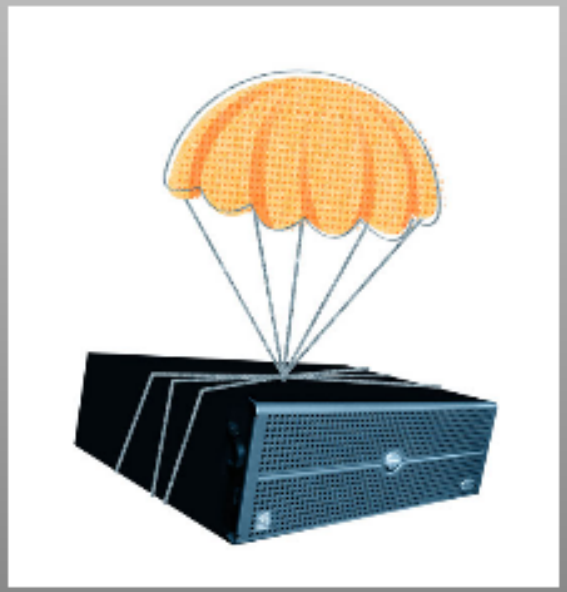
Evil Maid neutralisée

Cold Boot attack dangereuse!

Mot de passe SRK (-z)
00000000000000000000

tpm_takeownership -y

Mot de passe clé RSA:
indisponible



Backup

apt-get upgrade kernel

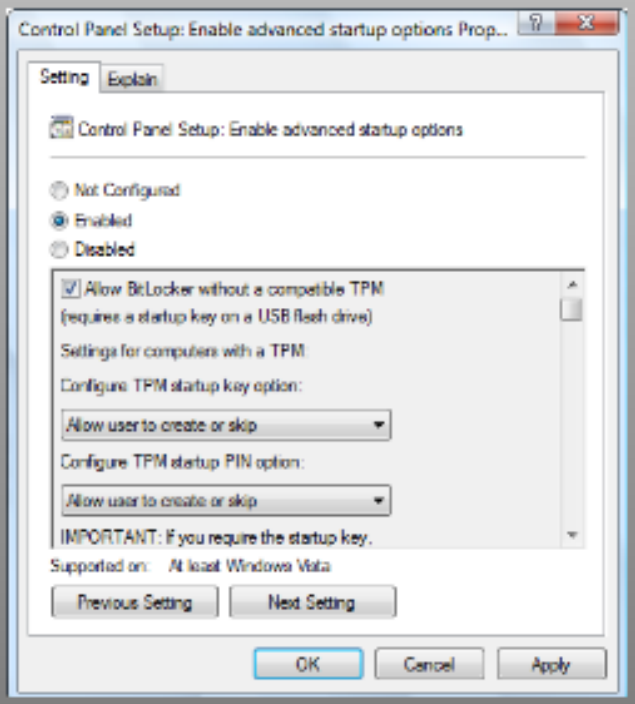
rpm -Uvh kernel

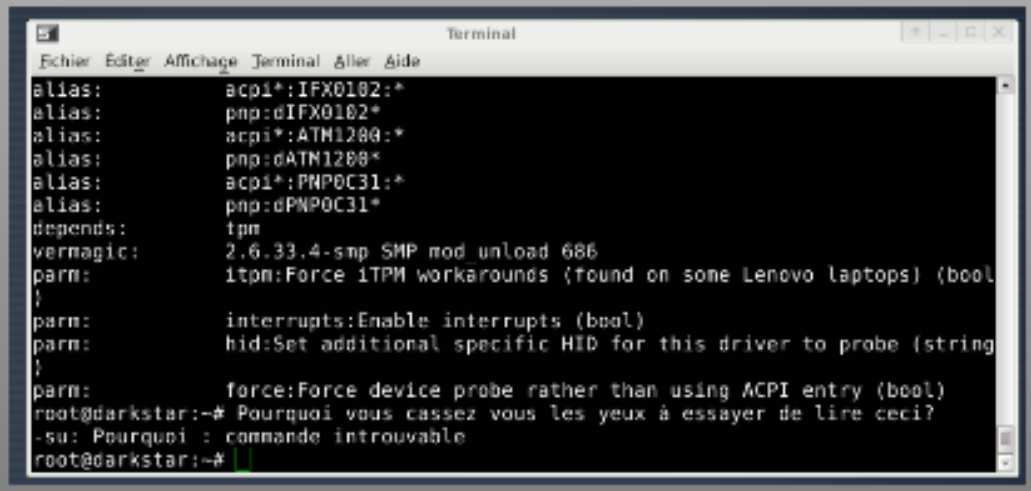
slackpkg upgrade kernel

TSS pas encore mature
Fonctionne... mais incomplet
V 0.3.4: Coredump lors du tpm_sealdata

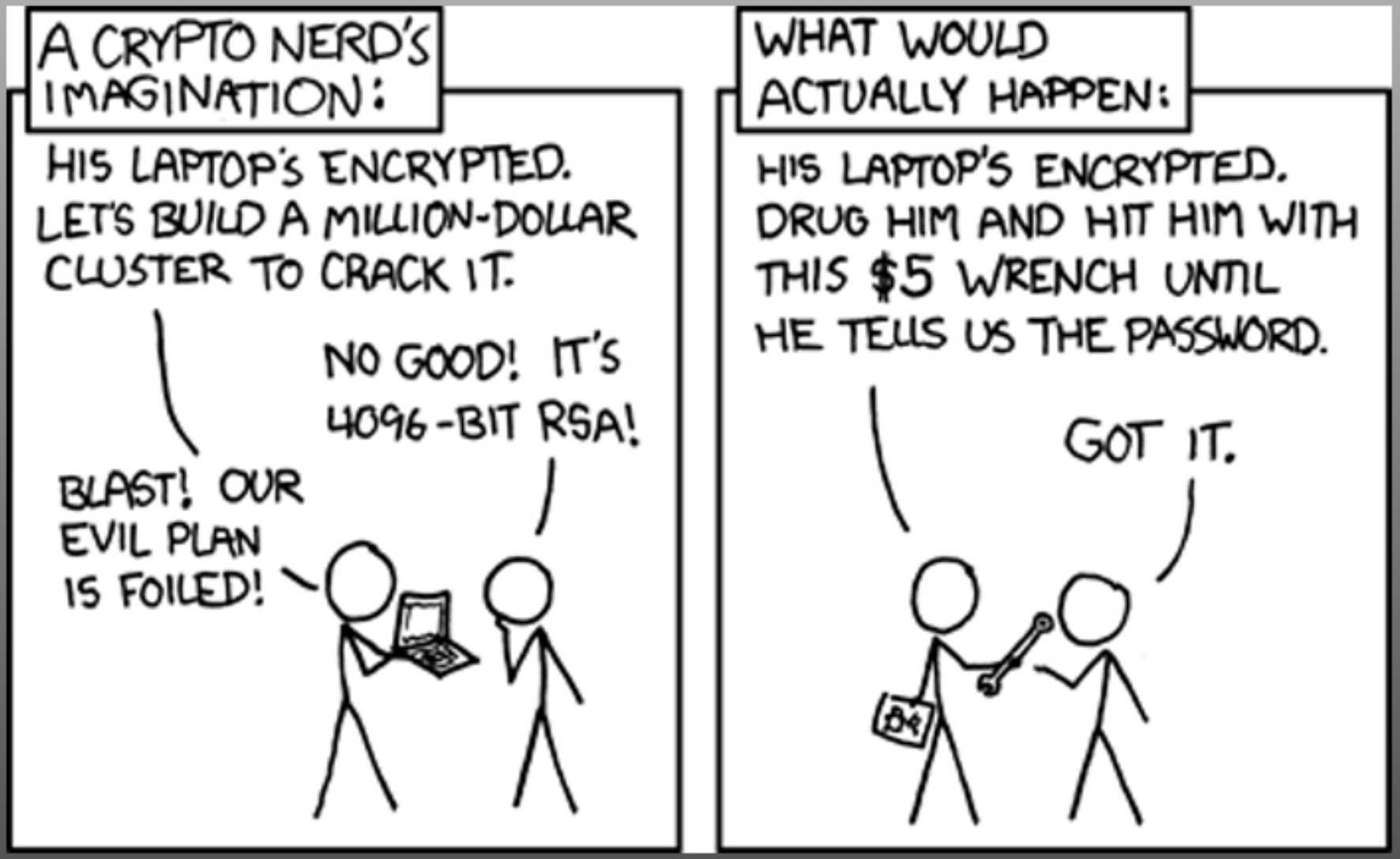
```
root@darkstar:~# slackpkg search trustedgrub
Looking for trustedgrub in package list. Please wait... DONE
No package name matches the pattern.
root@darkstar:~#
```

Refus de l'équipe de GRUB
d'incorporer les patchs TPM


Control Panel Setup: Enable advanced startup options Prop...
Setting
Explain
Control Panel Setup: Enable advanced startup options
Not Configured
Enabled
Disabled
Allow BitLocker without a compatible TPM
(requires a startup key on a USB flash drive)
Settings for computers with a TPM
Configure TPM startup key option:
Allow user to create or skip
Configure TPM startup PIN option:
Allow user to create or skip
IMPORTANT: If you require the startup key.
Supported on: At least Windows Vista
Previous Setting
Next Setting
OK
Cancel
Apply


Terminal
Fichier Éditer Affichage Terminal Aller Aide
alias: acpi*:IFX0102:*
alias: pnp:dIFX0102*
alias: acpi*:ATM1200:*
alias: pnp:dATM1200*
alias: acpi*:PNP0C31:*
alias: pnp:dPNP0C31*
depends: tpm
vermagic: 2.6.33.4-smp SMP mod_unload 686
parm: itpm:Force iTPM workarounds (found on some Lenovo laptops) (bool
)
parm: interrupts:Enable interrupts (bool)
parm: hid:Set additional specific HID for this driver to probe (string
)
parm: force:Force device probe rather than using ACPI entry (bool)
root@darkstar:~# Pourquoi vous cassez vous les yeux à essayer de lire ceci?
-su: Pourquoi : commande introuvable
root@darkstar:~#

Un mécanisme enfin sûr?



http://xkcd.com/538/

Merci

Des questions?

Kevin DENIS
kevin2nis@gmail.com
http://exploitability.blogspot.com