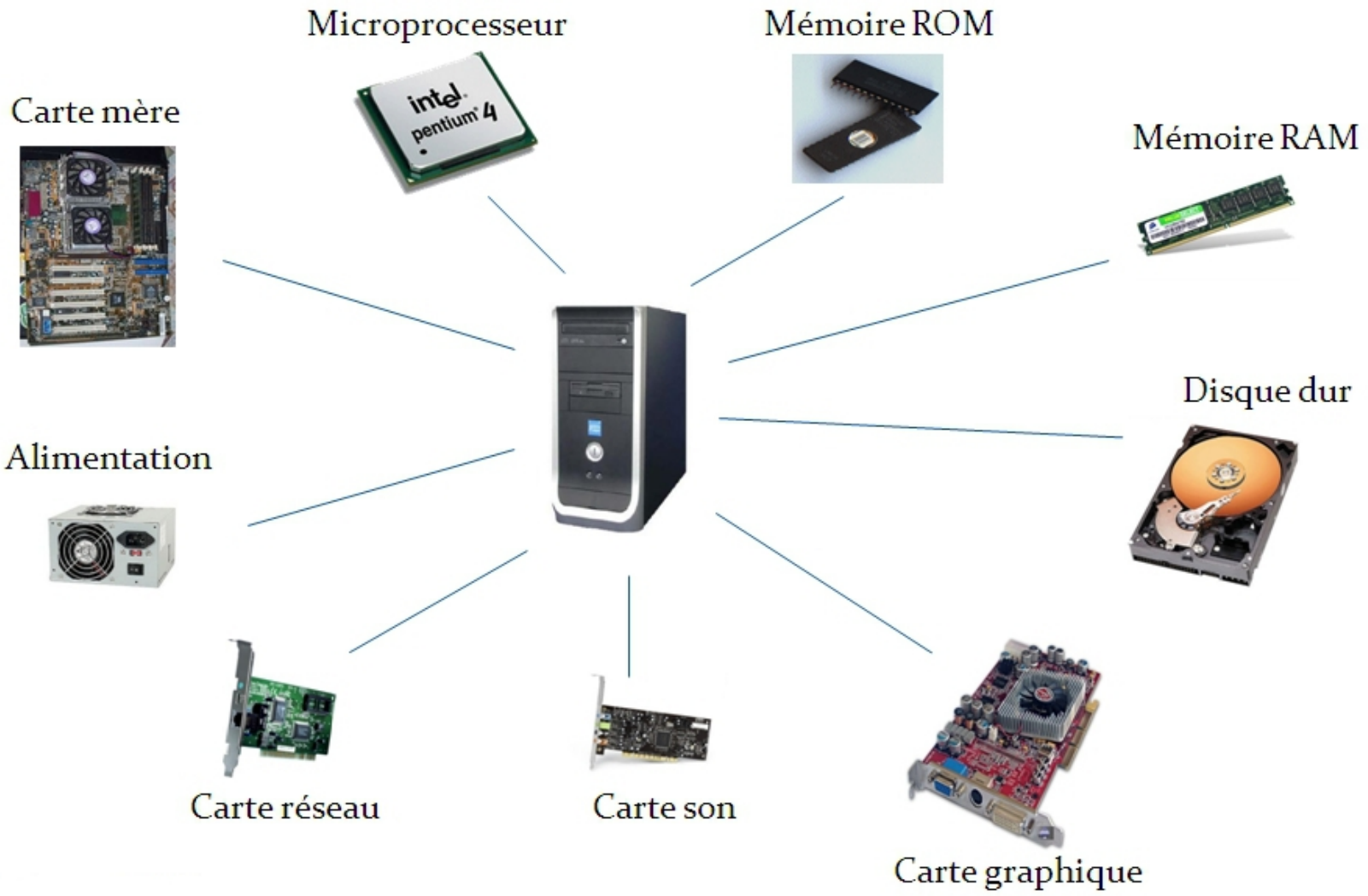
Vision SSI de l'Ordinateur

Éric BERTHOMIER
eric.berthomier@free.fr

16 mars 2022

Version 1.4 - Version Stagiaire

Composants d'un ordinateur



Carte mère

Carte mère

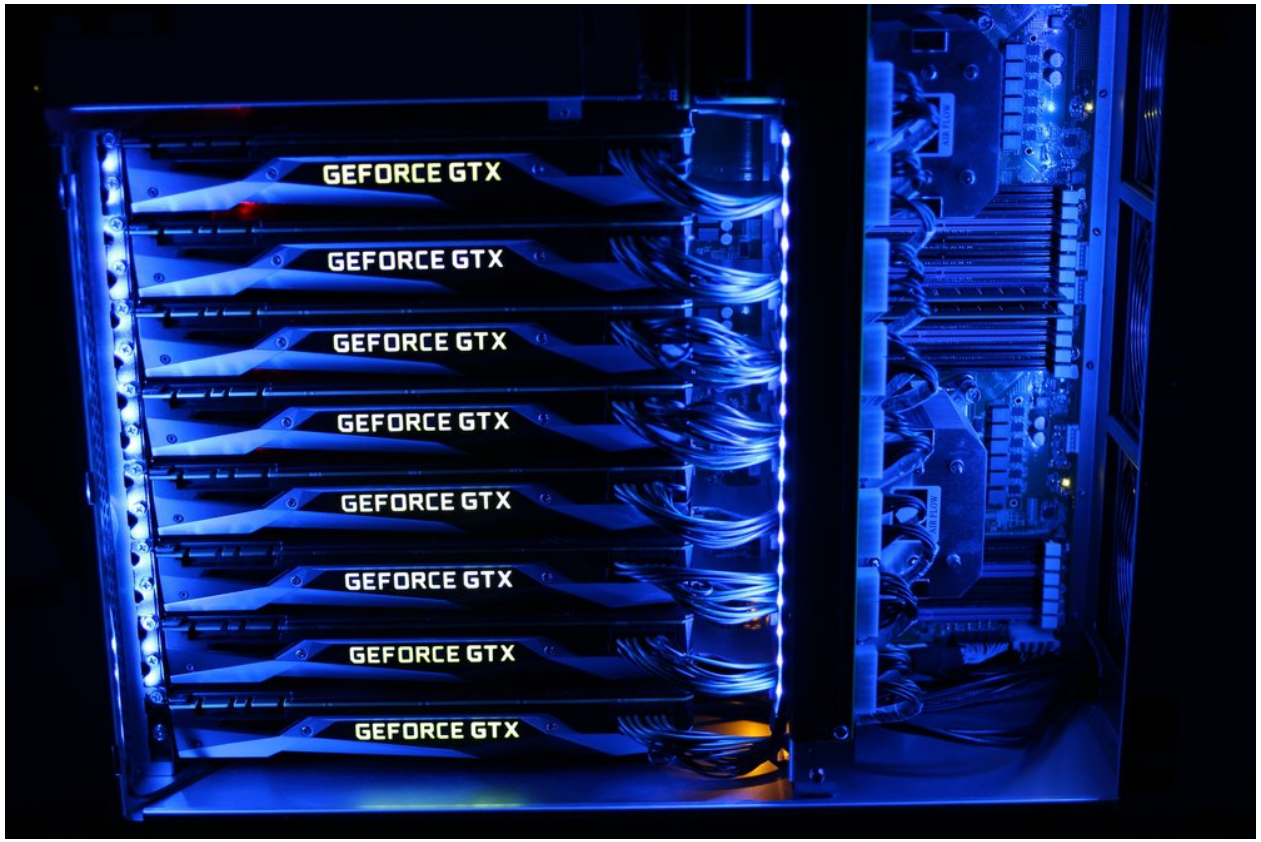
Capable de stocker de l'énergie et ainsi de créer des décharges électriques au travers d'un port de communication, USB Killer vise à détruire la carte-mère ...

Carte Réseau

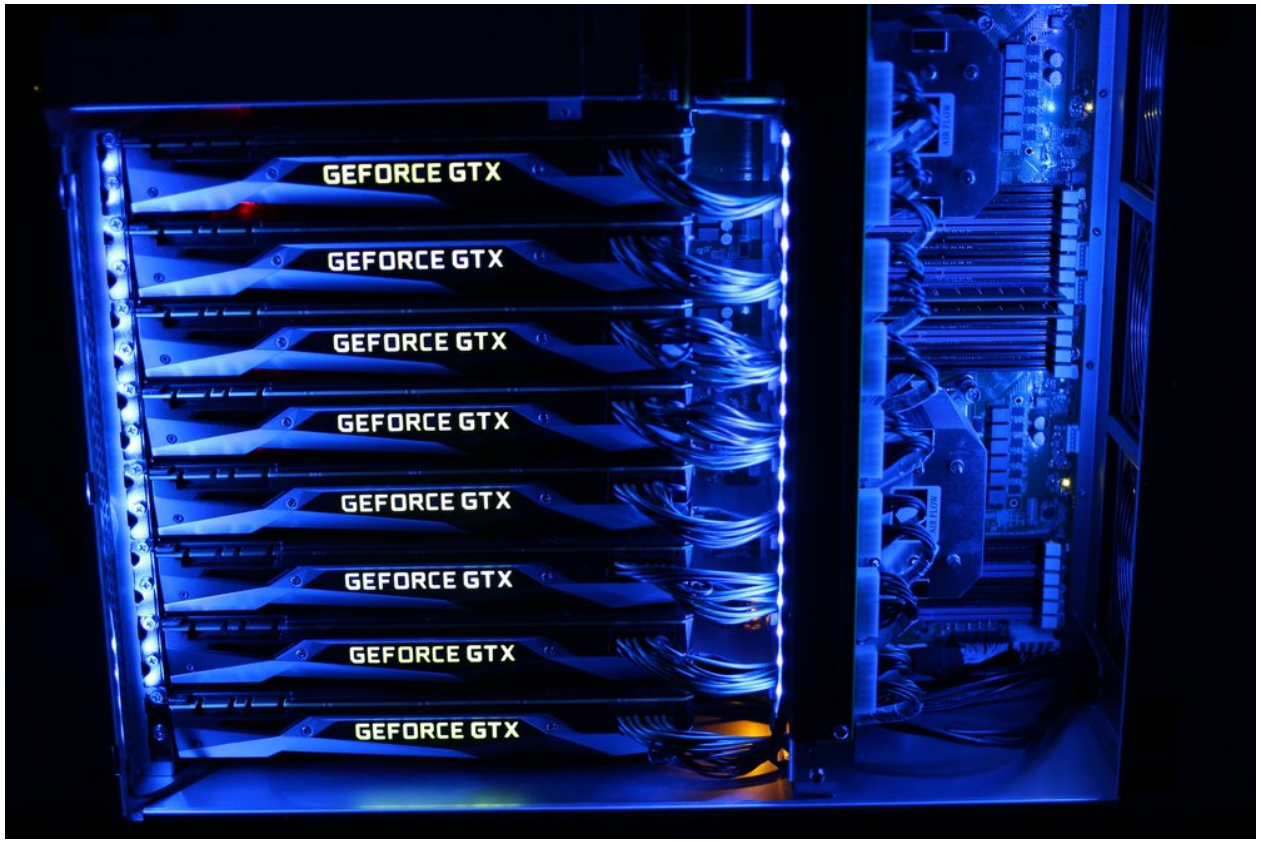
Carte Réseau

La communication réseau obéit à un protocole défini dans les normes IEEE (Institute of Electrical and Electronics Engineers). Il est donc possible de comprendre les informations qui transitent sur un câble réseau en s'interconnectant sur le câblage.

Carte Graphique - GPU



Carte Graphique - GPU



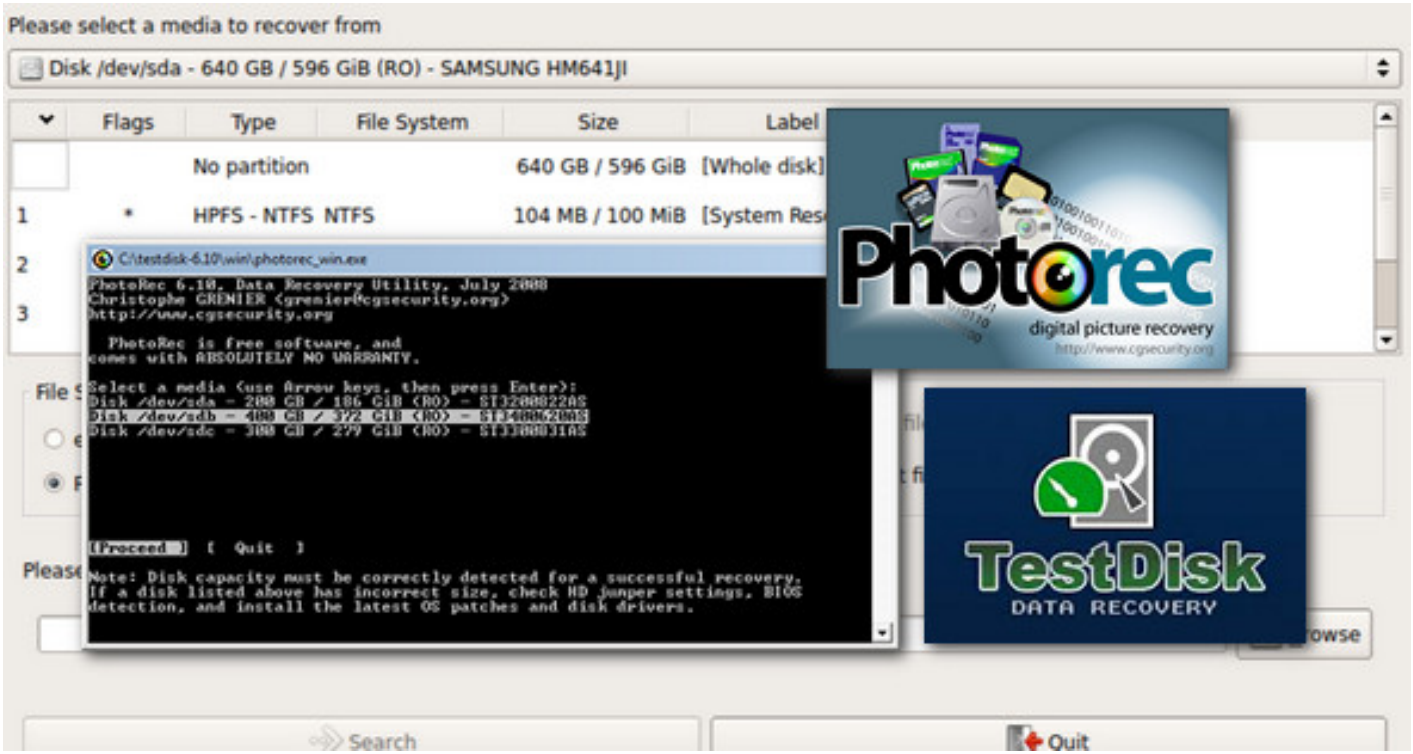
Utilisation de la GPU pour cracker des mots de passe

Exemple. . .

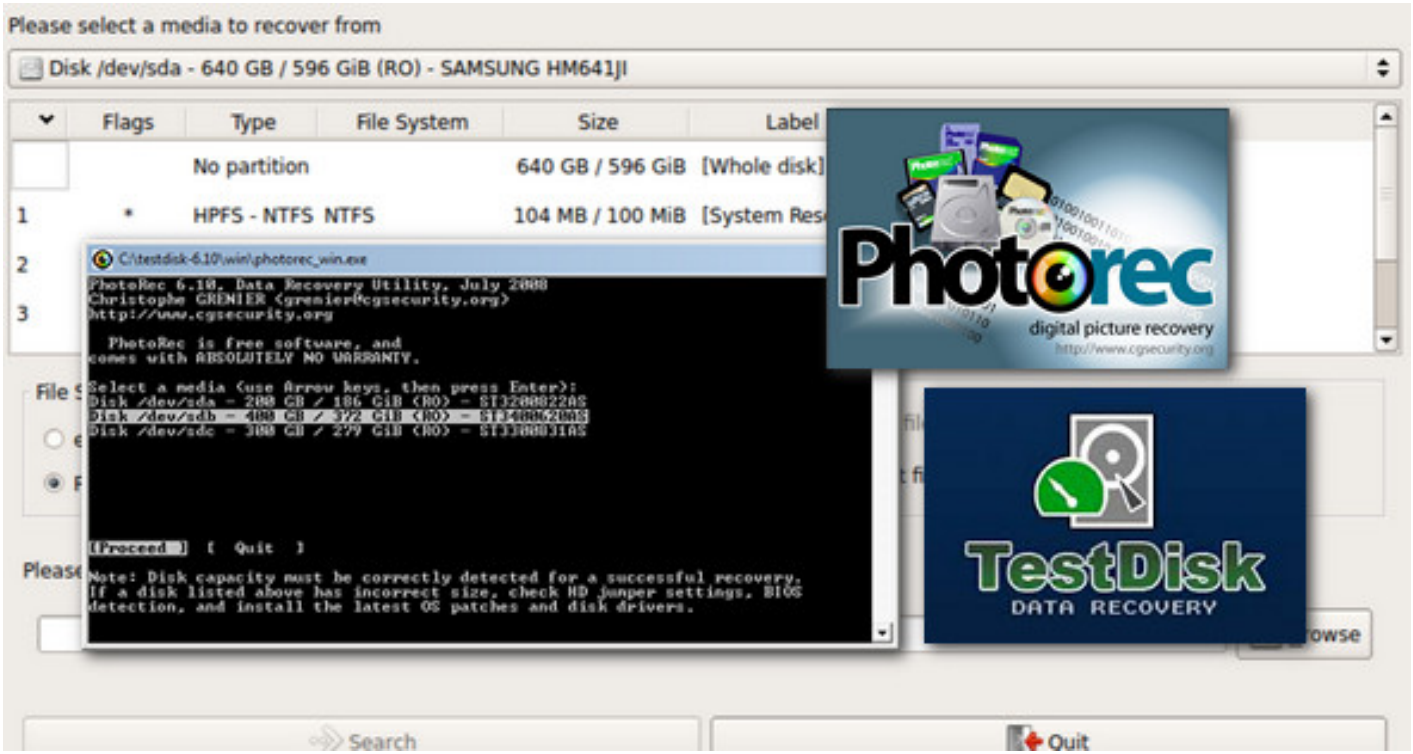
Prix en Octobre 2020 : environ 2.000 €

PhonAndroid - La GeForce RTX 3090 cracke les mots de passe à la vitesse de léclair

Disque Dur


Please select a media to recover from
Disk /dev/sda - 640 GB / 596 GiB (RO) - SAMSUNG HM641JI
Flags
Type
File System
Size
Label
No partition
640 GB / 596 GiB
[Whole disk]
1
*
HPFS - NTFS NTFS
104 MB / 100 MiB
2
3
C:\testdisk-6.10\win\photorec_win.exe
PhotoRec 6.10, Data Recovery Utility, July 2008
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.
Select a media (use Arrow keys, then press Enter):
Disk /dev/sda - 200 GB / 186 GiB (RO) - ST3200822AS
Disk /dev/sdb - 400 GB / 372 GiB (RO) - ST3400620NS
Disk /dev/sdc - 300 GB / 279 GiB (RO) - ST3300831AS
[Proceed] [Quit]
Note: Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has incorrect size, check HD jumper settings, BIOS
detection, and install the latest OS patches and disk drivers.
Photorec
digital picture recovery
TestDisk
DATA RECOVERY
Search
Quit

Disque Dur



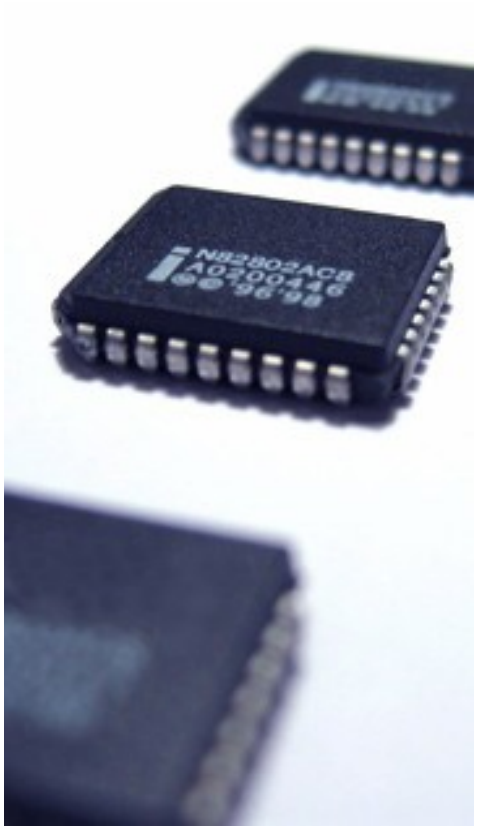
Un fichier supprimé ne l'est jamais vraiment . . .

Mémoire RAM

https://hackernewsdog.com/best-memory-dump-tools-for-forensics/

Mémoire ROM - EPROM

Le projet OpenBios avait pour but de rendre l'ordinateur totalement "Libre"



https://www.openbios.org

BIOS / UEFI

BIOS Basic Input Output System

BIOS / UEFI

BIOS Basic Input Output System

UEFI Extensible Firmware Interface, signifiant en français :
« Interface micrologicielle extensible unifiée »

BIOS / UEFI

BIOS Basic Input Output System

UEFI Extensible Firmware Interface, signifiant en français :
« Interface micrologicielle extensible unifiée »

Rakshasa Un malware qui remplace le Bios

BIOS / UEFI

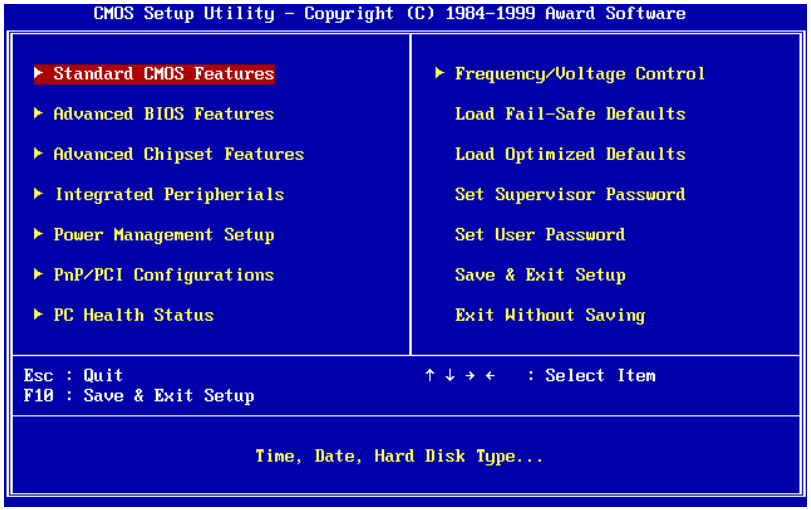
BIOS Basic Input Output System

UEFI Extensible Firmware Interface, signifiant en français : *« Interface micrologicielle extensible unifiée »*

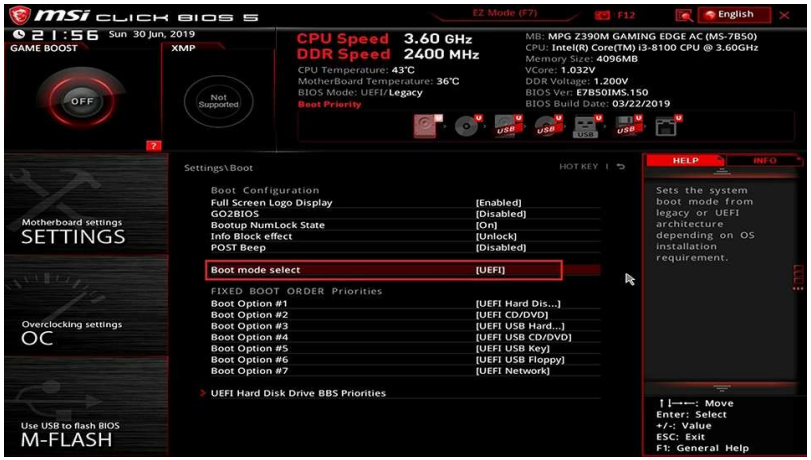
Rakshasa Un malware qui remplace le Bios

LoJax Un premier malware se logeant dans l'UEFI découvert (2018)...

BIOS / UEFI



BIOS



UEFI

Lojax : le premier rootkit UEFI

Autour de Septembre 2018, ESET met à jour un rootkit UEFI.

Lojax : le premier rootkit UEFI

Autour de Septembre 2018, ESET met à jour un rootkit UEFI.

Ce dernier se base sur le logiciel Computrace Lojak qui permet de retrouver son PC volé. Il est préinstallé dans le micrologiciel d'un grand nombre d'ordinateurs portables fabriqués par différents OEMs (Original Equipment Manufacturer).

Lojax : le premier rootkit UEFI

Autour de Septembre 2018, ESET met à jour un rootkit UEFI.

Ce dernier se base sur le logiciel Computrace Lojak qui permet de retrouver son PC volé. Il est préinstallé dans le micrologiciel d'un grand nombre d'ordinateurs portables fabriqués par différents OEMs (Original Equipment Manufacturer).

Les cybercriminels ont détournés ce logiciel pour le faire communiquer avec des serveurs de contrôle (C&C : Command and Control) et en faire un Trojan (Cheval de Troie).

Lojax : le premier rootkit UEFI

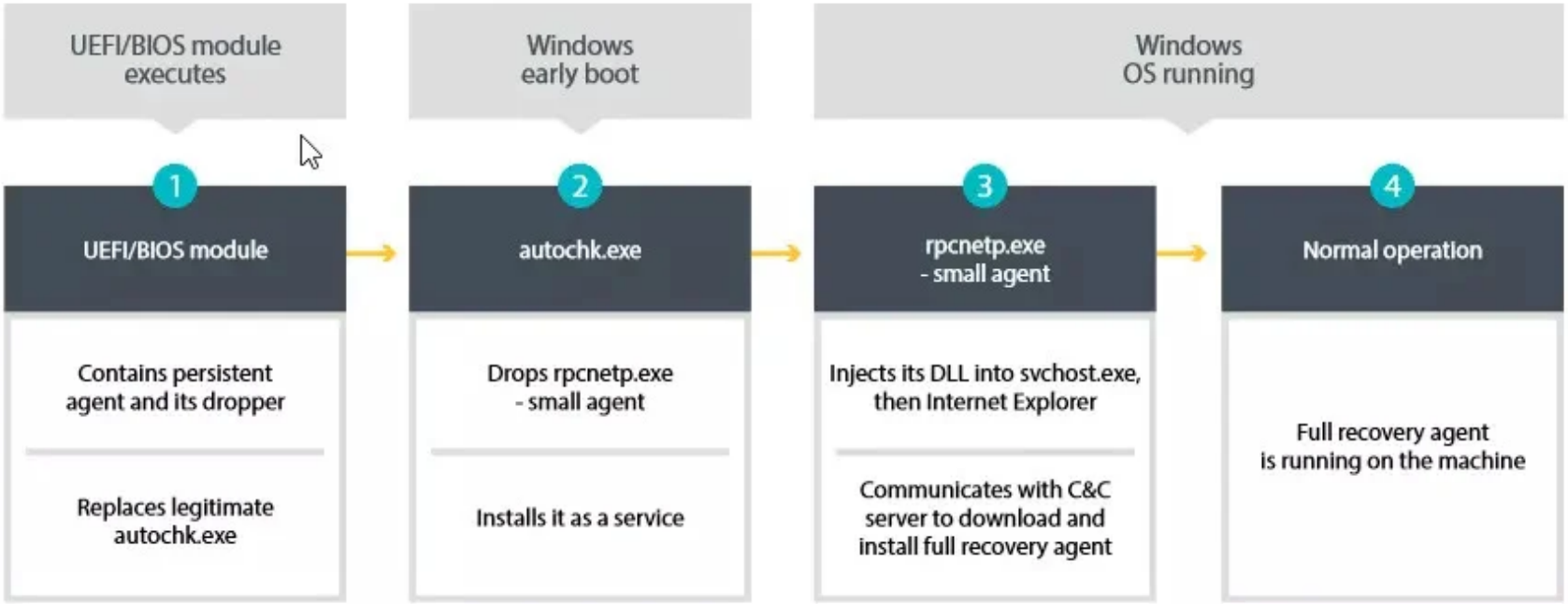
Autour de Septembre 2018, ESET met à jour un rootkit UEFI.

Ce dernier se base sur le logiciel Computrace Lojak qui permet de retrouver son PC volé. Il est préinstallé dans le micrologiciel d'un grand nombre d'ordinateurs portables fabriqués par différents OEMs (Original Equipment Manufacturer).

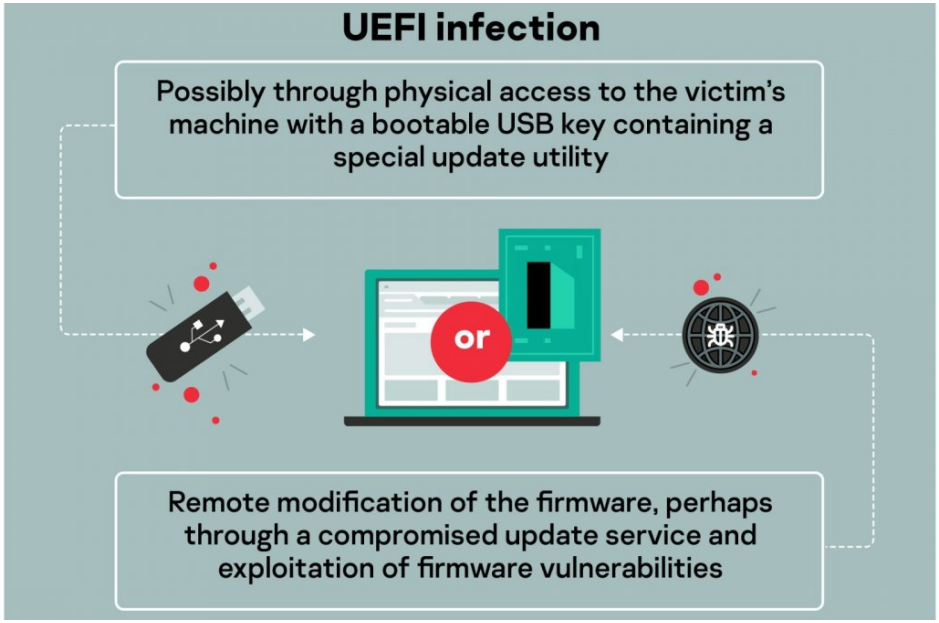
Les cybercriminels ont détournés ce logiciel pour le faire communiquer avec des serveurs de contrôle (C&C : Command and Control) et en faire un Trojan (Cheval de Troie).

Le rootkit utilise une version non signée de l'UEFI. Si le Secure Boot est activé, le rootkit UEFI ne pourra se charger. C'est pour cela qu'il n'est pas recommandé de désactiver le Secure Boot.

Lojax

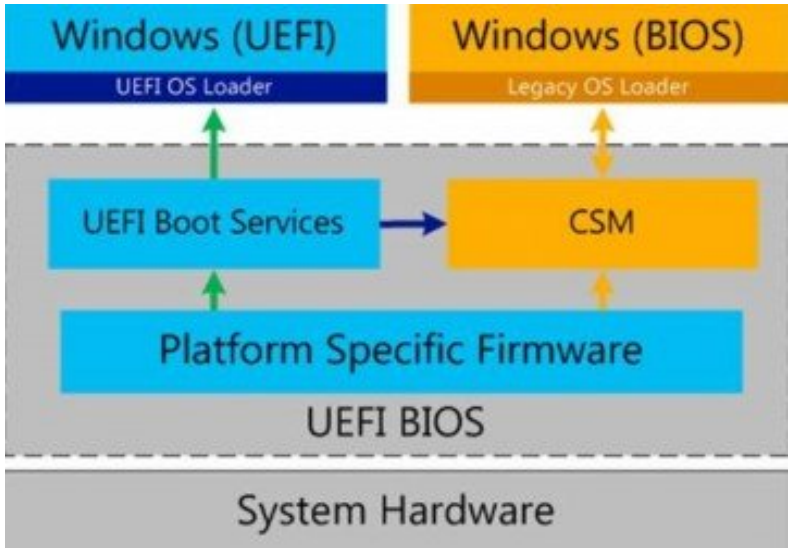

UEFI/BIOS module executes
Windows early boot
Windows OS running
1
UEFI/BIOS module
Contains persistent agent and its dropper
Replaces legitimate autochk.exe
2
autochk.exe
Drops rpcnetp.exe - small agent
Installs it as a service
3
rpcnetp.exe - small agent
Injects its DLL into svchost.exe, then Internet Explorer
Communicates with C&C server to download and install full recovery agent
4
Normal operation
Full recovery agent is running on the machine

MosaicRegressor



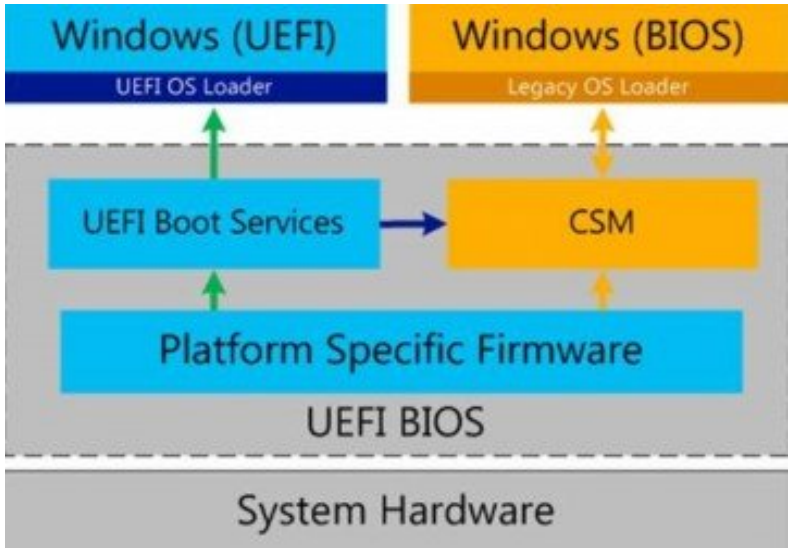
06/10/2020 - Deux ans après la découverte par Eset d'un rootkit affectant la technologie de démarrage sécurisé d'ordinateurs Unified Extensible Firmware Interface, un deuxième baptisé MosaicRegressor a été découvert par Kaspersky.

BIOS / UEFI - MBR - GPT



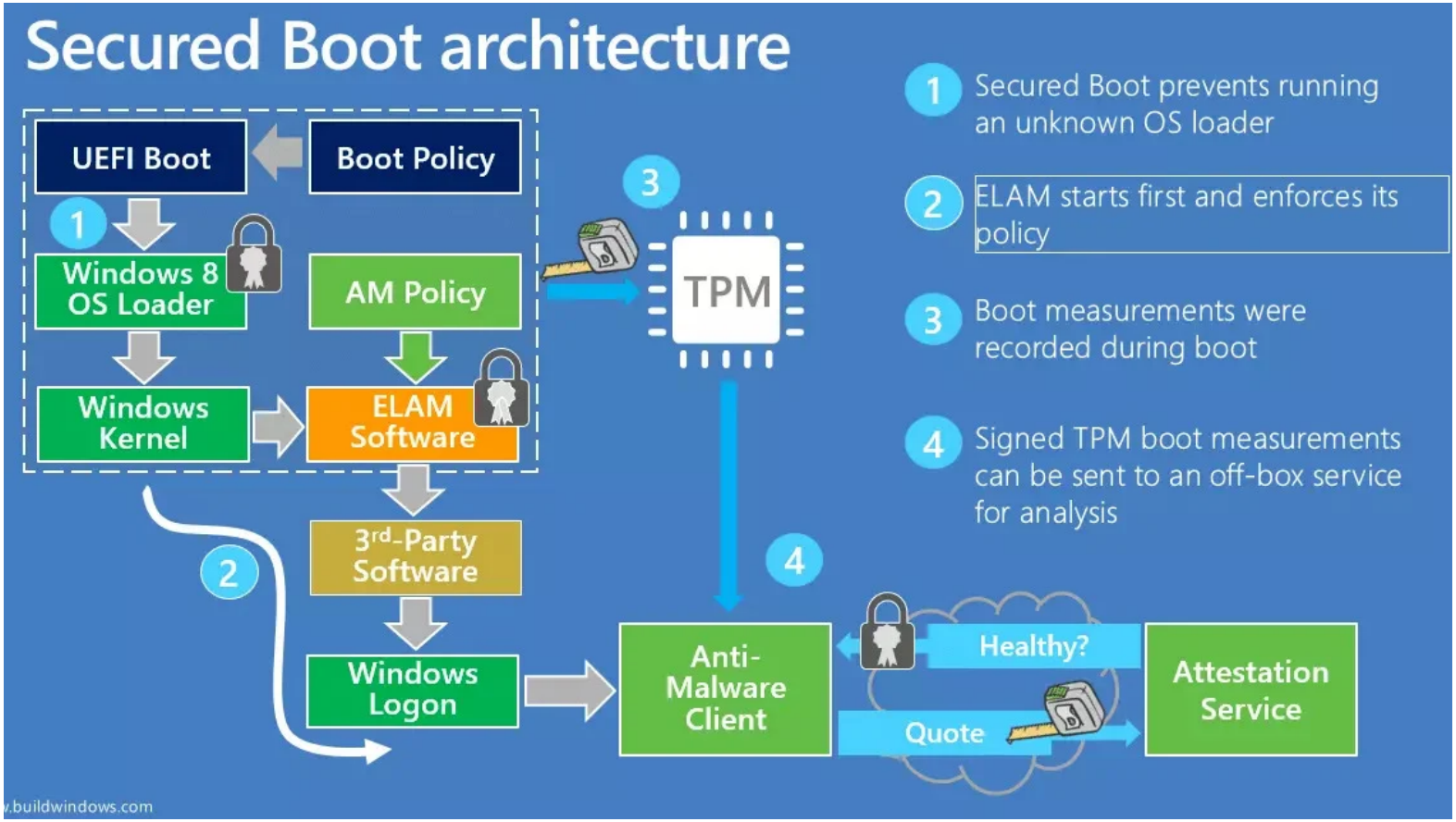
La mise à jour du BIOS vers l'UEFI a permis de prendre en compte les disques de grande taille.

BIOS / UEFI - MBR - GPT

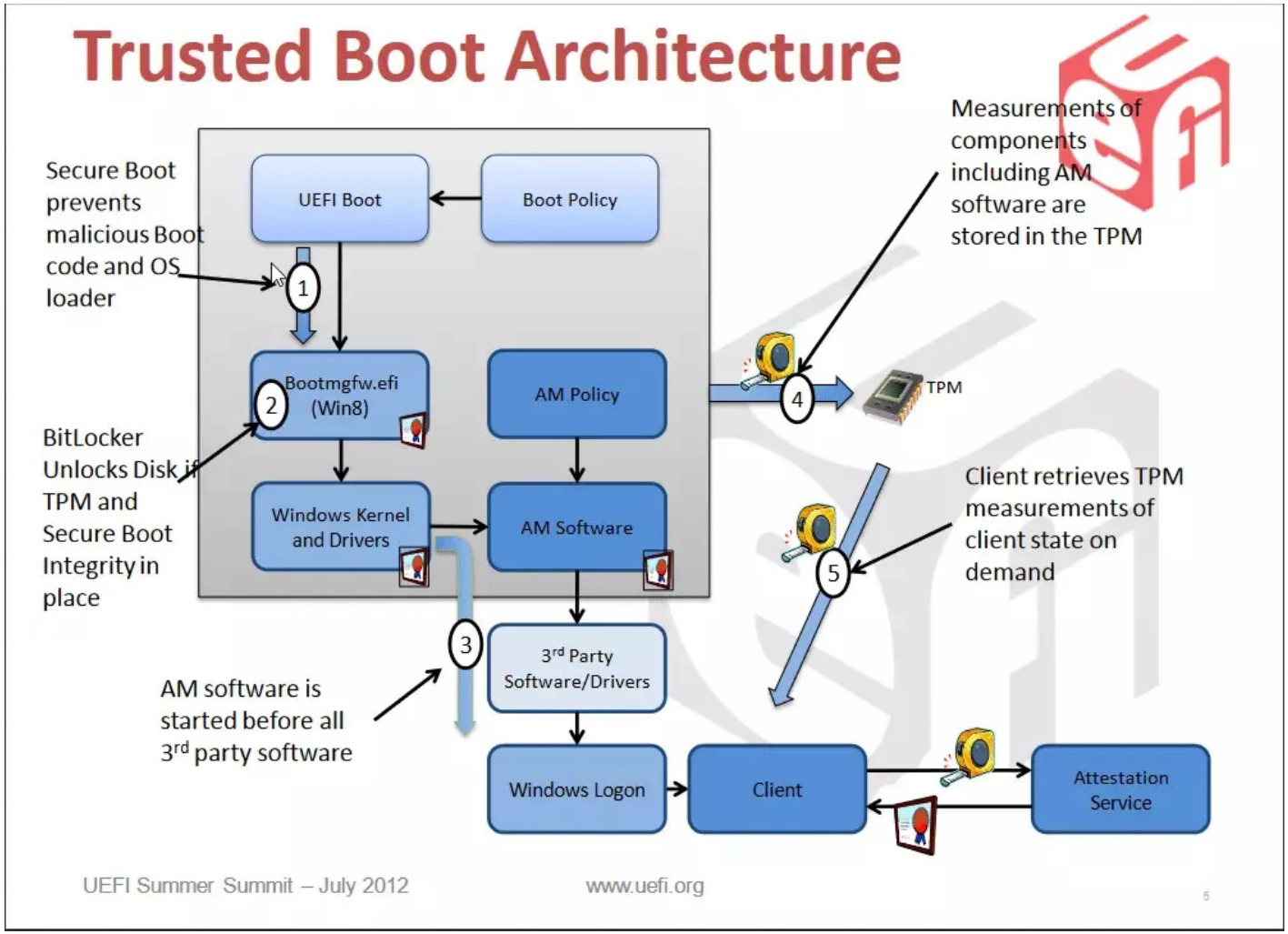


La mise à jour du BIOS vers l'UEFI a permis de prendre en compte les disques de grande taille.
Cependant ceci s'est accompagné d'un changement de l'architecture du disque, passant ainsi du MBR (Master Boot Record) au GPT (GUID Partition Table).

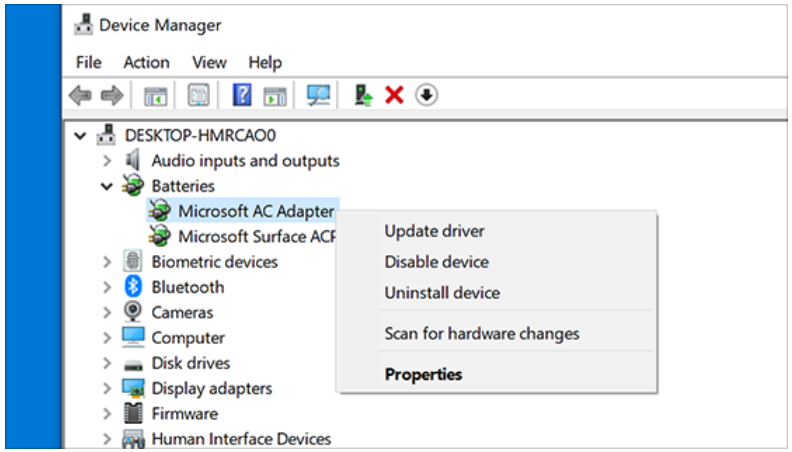
Windows Secure Boot



Windows Boot UEFI Protection contre les malwares

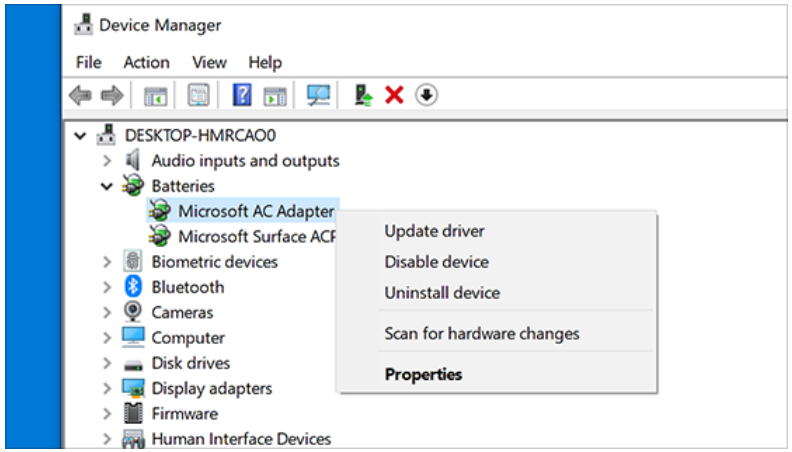


Drivers



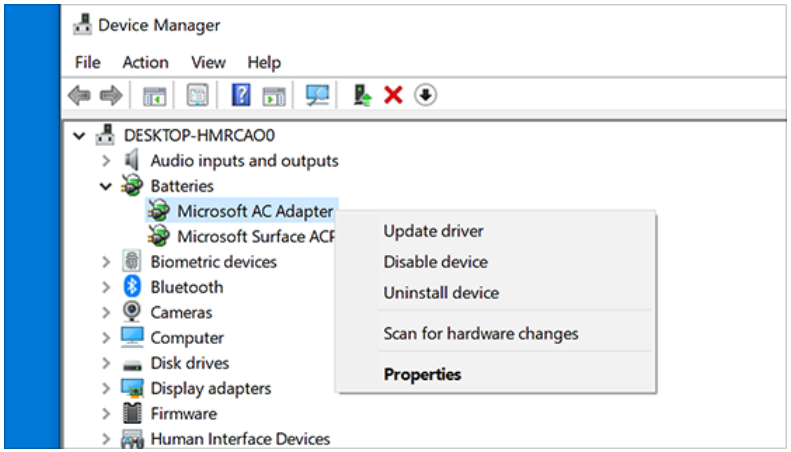
Drivers : `c:\windows\system32\drivers`

Drivers



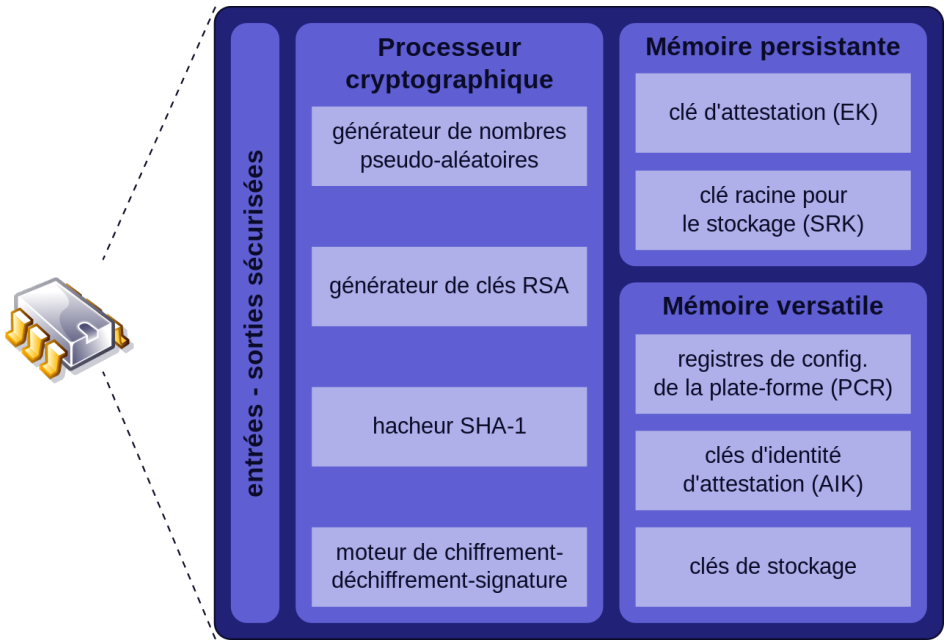
Drivers : `c:\windows\system32\drivers`
Les versions 64 bits de Windows 8 et 10 intègrent une fonctionnalité "contrôle obligatoire des signatures de pilotes" qui permet de ne charger que les pilotes qui ont été signés par Microsoft.

Drivers



Drivers : `c:\windows\system32\drivers`
Les versions 64 bits de Windows 8 et 10 intègrent une fonctionnalité "contrôle obligatoire des signatures de pilotes" qui permet de ne charger que les pilotes qui ont été signés par Microsoft.
Mais désactivable : `bcdedit /set testsigning off`

TPM



Trusted Platform Module

Équipement passif, il ne peut pas donner d'ordre à l'ordinateur tel que bloquer le système, ou surveiller l'exécution d'une application. Toutefois, il permet de facilement stocker des secrets (tels que des clés de chiffrement), de manière sécurisée.

Un PC sécurisé . . .