Versleutelen van pc en laptop

Ton Valkenburgh

Link naar Uitgebreider verhaal over dit onderwerp

Agenda

- Waarom versleutelen?
- Welke opties heb ik?
- Software optie!
- Hardware optie!

Waarom versleutelen?

- Bescherming bij:
  - Fysieke inbraak;
  - Verlies;
  - Vakantie.

- Op je pc of laptop staan veel privé gegevens;

- Je weet niet waar het allemaal precies staat.

Opties

- Software versleuteling:
  - Schijf/partities;
  - Containers;
  - Bestanden;
  - USB sticks.

- Self Encrypted Drives:
  - Interne versleuteling van de drive;
  - Data is altijd versleuteld;
  - Locking moet worden geactiveerd.

Software versleuteling

- Flexibel:
  - Schijven, containers, bestanden en USB-sticks/disks.
- Performance impact;
  - CPU versleuteling (AES NI) reduceert impact.
- Afhankelijk van operating systeem:
  - SSD/USB-stick vereist uitgaan van een ongebruikte schone SSD/Stick.

Windows

- VeraCrypt:
  - Boot disk/partitie;
  - Data disk/partitie;
  - Containers;
  - USB sticks.
- Encrypted File System (vanaf W2k in zakelijke versies);
- BitLocker (Windows 10+ pro, enterprise of education);
  - TPM version 1.2 of extra USB-drive.

VeraCrypt

- Open source;
- Platforms:
  - Windows;
  - Linux;
  - Mac OS-X;
  - FreeBSD;
  - Raspbian (Raspberry (Pi ARM v7).
- Flexibel:
  - Hidden operating system;
  - Portable mode;
  - Kan on the fly versleutelen;
  - TrueCrypt support.

Linux

- VeraCrypt:
  - Data disk/partitie;
  - Containers;
  - USB-disks/sticks.
- Dm-crypt + LUKS (Linux Unified Key Setup):
  - Boot disk;
  - Data-disk/partitie, Logical volumes, containers, files en USB-disks/sticks.
- ZuluCrypt/ZuluMount
  - Data-disk/partitie, containers, files, USB-disks/sticks.

Dm-crypt/Linux Unified Key Setup

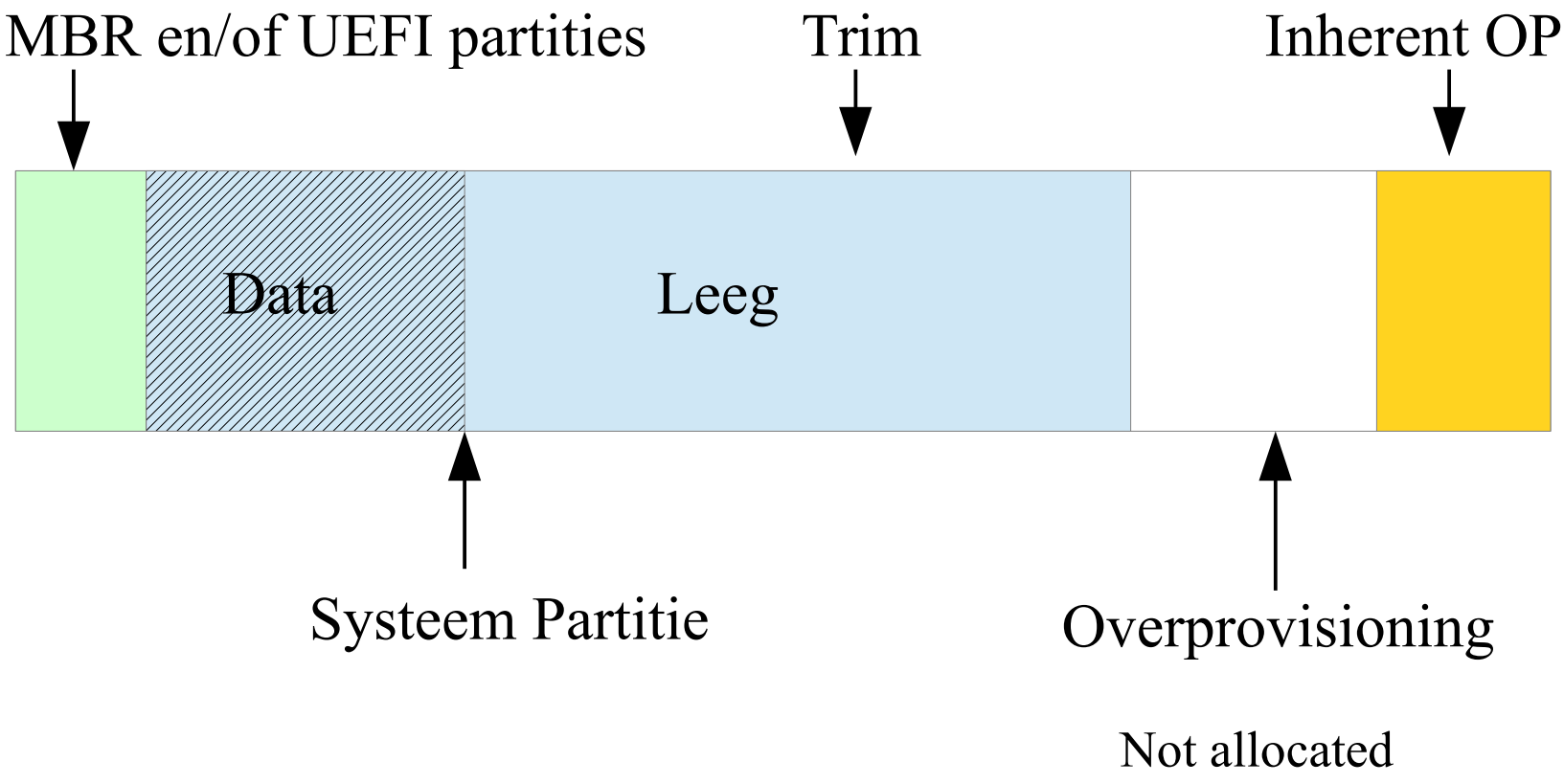
- Open source;
- Linux;
  - Containers;
  - USB-disks/sticks;
  - Files.

- Boot disk in Logical Volume
  - Kernel disk-ruimte is fixed;
  - Autorisatie kan worden gepasseerd (bug);
    - Zie laatste link op link pagina.

ZuluCrypt/Mount

- Open source;
- Linux;
- Flexibel, ondersteunt:
  - Dm-crypt/LUKS;
  - VeraCrypt;
  - TrueCrypt.

Solid State Disk



Self Encrypted Drive

- Geen performance impact:
  - Drive is altijd versleuteld (controller functie);
  - Versleuteling kan worden gewijzigd;
  - Locking moet worden geactiveerd.

- Drie soorten:
  - SATA encryptie – BIOS/UEFI HDD wachtwoord;
  - Trusted Computer Group Opal – extra software in drive van derden;
  - eDrive, Opal + IEEE 1667 + UEFI 2.3.1 + Microsoft BitLocker.

SATA encryptie

- HDD wachtwoord, BIOS/UEFI
  - Wachtwoord: lower case alfa en numeriek;
  - Snel intikken wachtwoord problematisch;
  - Niet alle system boards ondersteunen dit;
  - Kan worden geactiveerd en gedeactiveerd zonder dat data verloren gaat:
  - Geen extra software nodig.

Trusted Computer Group Opal

- Extra software in Drive van derden;
  - Commercieel verkrijgbaar;
  - Open Source;
  - Moet voldoen aan TCG Opal specificatie.
- System board onafhankelijk;
- Kan worden geactiveerd en gedeactiveerd zonder dat data verloren gaat.

eDrive

- Opal + IEEE 1667 + UEFI 2.3.1;
- Software: Microsoft BitLocker:
  - Windows 10 pro, enterprise en education.
  - Moet voldoen aan TCG Opal specificatie.
- System board:
  - TPM version 1.2 of extra USB-drive;
  - TCG-compliant BIOS/UEFI.
- Kan worden geactiveerd en gedeactiveerd zonder dat data verloren gaat.

Drive Trust Alliance

- Self – Encrypting Box Evaluation Kit;
  - Windows, Mac;
  - Opal;
  - MBR- en UEFI-ondersteuning;.
- Sedutil;
  - Windows, Linux;
  - Open source;
  - Opal;
  - MBR en 64-bit UEFI-ondersteuning;
  - Secure boot uitschakelen.

Sedutil (voorbereiding voor rescue-stick)

- Download: RESCUE32.img.gz of RESCUE64.img.gz;
- RESCUE32 is voor een MBR-systeem;
- RESCUE64 is voor een 64-bits UEFI-systeem;
- Pak het uit met 7-Zip;
- Zet het met WIN32DiskImager op een USB-stick.

Rescue-stick.

- Start pc vanaf de gemaakt USB-stick;
- Pak sedutil.zip uit met gunzip;
- Je krijgt een login pompt: enter „root”;

  Er is geen wachtwoord nodig!
- Geef het volgende commando:

  sedutil-cli - -scan

Rescue-stick..

- Resultaat (bijvoorbeeld):

/dev/nvme0 2 Samsung SSD 960 EVO 250GB 2B7QCXE7
/dev/sda 2 Crucial_CT250MX200SSD1 MU04
/dev/sdb 12 Samsung SSD 850 EVO 500GB EMT01B6Q
/dev/sdc 2 ST500LT025-1DH142 0001SDM7
/dev/sdd 12 Samsung SSD 850 EVO 250GB EMT01B6Q
No more disks present ending scan

Rescue-stick...

- Geef de volgende commando's:

sedutil-cli – –initialsetup debug /dev/nvme0

sedutil-cli – –enablelockingrage 0 debug /dev/nvme0

sedutil-cli – –setlockingrage 0 lk debug /dev/nvme0

sedutil-cli – –setmbrdone off debug /dev/nvme0

Rescue-stick….

- We gaan een boot-drive van de SED maken;
- We geven nu de commando's:

```
gunzip /usr/sedutil/UEFI64-n.nn.n.img.gz

sedutil-cli  --loadpbaimage debug /usr/sedutil/UEFI64-n.nn.n.img
    /dev/nvme0
```

N.B. n.nn.n is het release nummer

Rescue-stick…..

We gaan nu de SED vergrendelen met de commando's:

sedutil-cli – –setsidpassword debug <password> /dev/nvme0

sedutil-cli – –setadmin1pwd debug <password> /dev/nvme0

sedutil-cli – –setmbrdone on <password> /dev/nvme0

Gebruik

- Verwijder de rescue-stick;
- Zet de pc uit;
- Zet de pc aan;
- Je krijgt nu het inlog scherm:

Opal Inlog scherm

Ontgrendeling

- Geef het wachtwoord;
- De pc herstart en komt in het operating systeem;
- Uitzetten van de pc vergrendelt de SED.

Conclusies

- HDD:
  - Windows:
    - VeraCrypt voor Systeem Disk/Partitie, data disk/partitie, containers en USB disks. Windows 10 upgrade issue.
  - Linux:
    - LUSK voor Boot disk;
    - VeraCrypt of ZuluCrypt voor data disk/partitie, containers, en USB disks.
- SSD:
  - Self Encrypted Drives: SATA of Opal, Windows 10
- USB Sticks:
  - VeraCrypt of ZuluCrypt (zie de VeraCrypt documentatie);
  - Hardware encryptie.

Interessante sites

- https://veracrypt.codeplex.com/
- https://mhogomchungu.github.io/zuluCrypt/
- http://www.7-zip.org/
- https://www.drivetrust.com/
- https://github.com/Drive-Trust-Alliance/sedutil/wiki
- https://sourceforge.net/projects/win32diskimager/
- https://mhogomchungu.github.io/zulucrypt/
- https://github.com/Drive-Trust-Alliance/sedutil/wiki
- http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html#fix