Encryptie voor pc en laptop

Ton Valkenburgh

Er is op dit moment veel aandacht voor cybercrime en privacy. Daardoor willen we wel eens vergeten dat er ook nog ouderwetse inbrekers actief zijn. In dit artikel vind je informatie over hoe je ervoor kan zorgen dat bij een fysieke inbraak je gegevens toch niet direct op straat komen te liggen.

1 Inleiding

De pc of laptop – hierna kan je voor laptop ook pc lezen – bevat steeds meer privégegevens van ons. Niet alleen bankgegevens, maar ook kopieën van identiteitspapieren en privéfoto's. Bij verlies of diefstal (bv. door inbraak) willen we niet dat deze gegevens in handen van anderen vallen. Hoe kunnen we ons het best daartegen beschermen en waarop moet je dan letten? Ik wil hier een aantal mogelijkheden uitdiepen die je kunnen helpen bij het beslissen wat voor jou de beste oplossing is.

2 Encryptie

Om te zorgen dat als de laptop in handen valt van anderen ze de gegevens niet kunnen lezen, kan je de gegevens versleutelen. Dergelijke encryptie kan op de hele schijf, maar ook op alleen de bestanden gebeuren. Is het voldoende om alleen belangrijke bestanden te versleutelen? Wie weet waar de programma's die hij gebruikt gegevens of sporen van gegevens achterlaat? Hoeveel van ons realiseren zich dat bij de optie 'snel opstarten' de inhoud van het werkgeheugen op schijf wordt opgeslagen? Het wisselbestand en het hibernatebestand wissen is vast niet voldoende.

Trouwens, wissen wil nog niet zeggen dat het echt van de schijf is verwijderd. Omdat we eigenlijk zo weinig weten van onze trouwe kameraad, is het verstandig om de hele schijf, of eigenlijk alle schijven, te versleutelen. We hebben dan de volgende opties:

- Software-encryptie;
- Self Encrypted Drive.

Programma's voor software-encryptie hebben in het algemeen veel mogelijkheden. Terwijl Self Encrypted Drives in het gebruik praktisch transparant zijn voor de gebruiker. Gezien mijn eigen ervaring concentreer ik me op de platformen Windows en Linux. Met Mac heb ik geen ervaring en ik wil zo min mogelijk uit de tweede hand vertellen.

3 Software-encryptie

Software-encryptie is flexibel en biedt de mogelijkheid om de schijf, partitie, containers of bestanden te versleutelen. Er is wel enige impact op de performance van de laptop, maar moderne systemen zijn zo krachtig dat dit wel meevalt.

Zeker als er gebruik wordt gemaakt van de CPU-eigenschap AES NI. Een nadeel is dat ze vaak afhankelijk zijn van het platform waarop het systeem draait. Dat kan vervelend zijn als je meer dan één platform gebruikt. Ook moet er rekening worden gehouden met de technologie van de schijf. SSD's en hybride schijven en USB-sticks werken anders dan een 'gewone' harde schijf. Na het wissen van data bij een Solid State Drive (SSD) kan de data altijd nog staan in andere cellen. Bij SSD's komen ze zelfs in het deel van de SSD dat gereserveerd is voor overprovisioning. Het is daarom verstandig bij het gebruik van software-encryptie op dergelijke media (flash drives) uit te gaan van ongebruikt of schoon (veilig gewist) materiaal.

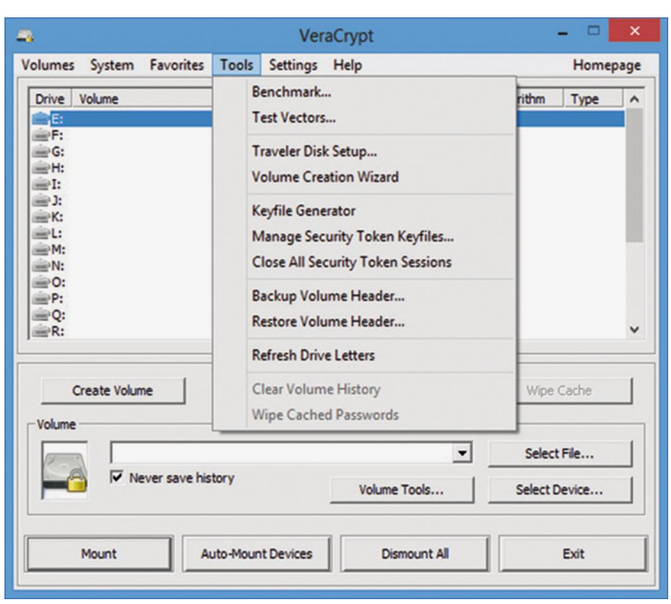
3.1 Windows

Ik wil hier niet alle programma's voor Windows behandelen, dat zou het artikel veel te lang maken. Ik beperk me dus tot de bekendste, respectievelijk interessantste:

- Veracrypt;
- Encrypted File System (EFS);
- BitLocker.

3.1.1 VeraCrypt

VeraCrypt is een open source-programma dat is voortgekomen uit TrueCrypt. De ontwikkelaars van TrueCrypt zijn ermee gestopt. In VeraCrypt zijn een aantal problemen van TrueCrypt opgelost en er zijn nieuwe mogelijkheden bij gekomen. VeraCrypt werkt op de platformen Windows, Linux, Mac OS-X en Raspbian.
Het ondersteunt het versleutelen van schijven, partities, containers en USB-schijven en -sticks. Het versleutelen kan on-the-fly plaatsvinden zonder dat gegevens verloren gaan. VeraCrypt staat toe om diverse encryptiemethodes te stapelen. Dat maakt het (voorlopig) National Security Agency-bestendig.



Voor Windows is het ook mogelijk de systeemschijf te versleutelen. Voor de andere platformen geldt dit niet. Het kent een zogenaamde verborgen partitie. Er is dan niet zichtbaar dat er een versleuteld systeem is. Van USB-schijven en -sticks kan je een traveler-versie maken.
Verder kan je de oude TrueCrypt-versleuteling gebruiken of zonder verlies van gegevens omzetten naar VeraCrypt-versleuteling.

3.1.2 EFS
EFS is aanwezig in de zakelijke versies van Windows. Het kan schijven, partities en bestanden versleutelen. Vanaf Windows 2000 zijn de functies stap voor stap uitgebreid. Omdat dit voor de zakelijke markt is, ga ik er niet verder op in.

3.1.3 BitLocker
Bitlocker is de Microsoftoplossing voor encryptie. Het is aanwezig in de zakelijke versies van Windows. Om het te kunnen gebruiken moet aan de volgende voorwaarden worden voldaan: de laptop moet een Trusted Platform Module versie 1.2 hebben of er moet een USBstick worden gebruikt om op te starten. Ook dit is voor de thuisgebruiker geen interessante optie.

3.2 Linux
Voor Linux zijn de volgende programma's interessant:
- DM-Crypt met Linux Unified Key Setup (LUKS);
- Encrypted File System (EncFS);
- VeraCrypt;
- ZuluCrypt/Mount.

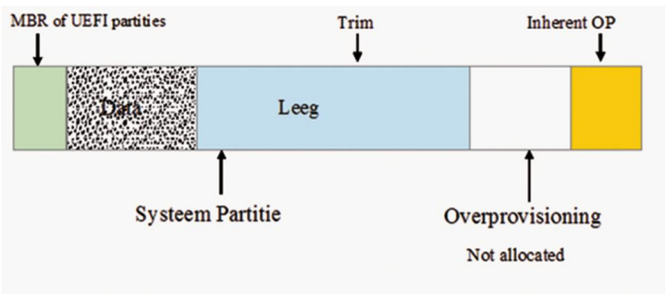
Ik zal ze niet allemaal even uitgebreid behandelen.
3.2.1 LUKS
LUKS met DM-Crypt kan schijven, partities, logical volumes, containers, bestanden en USB-schijven/sticks versleutelen. Het is voor het Linuxplatform, hoewel er een niet meer onderhouden Windowsversie LibreCrypt bestaat. LUKS kan ook de systeemschijf (als een logical volume) versleutelen. Het nadeel is dan dat de ruimte voor de kernel vastligt. Na veel kernelupdates moet de gebruiker eventueel oude kernels opruimen. Bij Ubuntu-installatie is het versleutelen van de systeemschijf opgenomen in de installatieprocedure: een vinkje zetten en het wachtwoord invoeren. Dit kan dus ook een niet-ervaren gebruiker uitvoeren.
Op dit moment is het mogelijk de autorisatie te passeren. Je komt dan op een beperkte shell. Er is dan nog geen toegang mogelijk tot de versleutelde gegevens. Het komt qua veiligheid overeen met de situatie dat de schijf uit de laptop is gehaald.
Zie Interessante links (link 9).

3.2.2 EncFS
Het eenvoudigste encryptiesysteem op Linux is het open sourceprogramma EncFS, dat geen rootautorisatie vereist. Het wordt gebruikt door o.a. het backupprogramma 'Back in Time'. Een belangrijk nadeel is, dat als je een bestand tweemaal versleutelt, de versleuteling van de combinatie van beide bestanden is te breken. Omdat in de laatste versie een aantal problemen zijn opgelost, wordt deze versie aanbevolen. Bij het installeren van EncFS onder Linux wordt er een waarschuwing gegeven betreffende de huidige zwakheid van EncFS.
Van EncFS is zowel een Windows als een Mac OSX versie beschikbaar.

3.2.3 VeraCrypt
Van VeraCrypt wil ik alleen nog benadrukken dat het onder Linux geen systeemdisk kan versleutelen. Voor de rest verwijs ik naar wat onder Windows is beschreven.

3.3.4 ZuluCrypt/Mount
ZuluCrypt/Mount is een klein wonder. Het ondersteunt versleuteling volgens zowel Dm-Crypt met LUKS als VeraCrypt. De mountoptie maakt het eenvoudig om met één klik versleutelde schijven, partities of containers te openen. Het programma is nog vrij nieuw en er zijn nog wel wat verbeteringen nodig, maar het is veelbelovend.

3.4 Solid State Disk (SSD)
Bij de Solid State Disk is het in verband met softwareversleuteling van belang om te kijken hoe overprovisioning en garbagecollection werken.
Het schrijven op een SSD kan alleen naar een blok dat nullen bevat. De controller van de SSD ziet echter pas welke blokken vrij zijn gekomen als er een poging wordt gedaan om ernaar te schrijven. De controller schrijft dan naar een schoon blok in het overprovisioning deel. Dit wordt dus nu deel van de systeempartitie. Als er geen schone blokken meer beschikbaar zijn, moet een blok eerst worden gewist alvorens ernaar geschreven kan worden. Dit vertraagt de schrijfactie. De fabrikant heeft daarom een deel met lege blokken voor overprovisioning gereserveerd. De gebruiker kan hier niet bij. Deze inherent overprovisioning kan voldoende zijn bij weinig schrijfacties op de SSD. De gebruiker kan de overprovisioning ruimte groter maken door een deel van de schijf niet te alloceren voor een partitie.
Garbagecollection maakt vrijgekomen blokken beschikbaar door ze te wissen en dit moet zoveel mogelijk gebeuren als er geen schrijfacties plaatsvinden.
Het operatingsysteem weet echter welke blokken op de partitie vrij zijn gekomen. Door middel van het trimcommando wordt de SSDcontroller geïnformeerd welke blokken vrij zijn. Deze worden dus opgenomen in het garbagecollection-proces. Het deel van de partitie waar geen data staat, noemen we het dynamische overprovisioning-deel.
Je kan de benodigde statische overprovisioning verkleinen door het trimcommando vaker uit te voeren en dus beter gebruik te maken van de dynamische overprovisioning.
Windows doet de trim standaard op wekelijkse basis. Bij Windows 10 en Linux is dit instelbaar naar bijvoorbeeld dagelijks.



VeraCrypt wordt afgeraden voor gebruik op SSD's. De achtergrond hiervoor is dat gegevens niet worden overschreven, zelfs niet als de opdracht is om de oude gegevens te overschrijven. Ook wordt afgeraden om trim te gebruiken, omdat dan meer van de structuur van de data zichtbaar wordt voor het kraken van de encryptie. Bij het gebruik op SSD's of USBsticks wordt aangeraden in ieder geval uit te gaan van een schoon medium.
Voor meer informatie: Lees de documentatie van VeraCrypt.
Er is echter een betere encryptieoplossing voor SSD's: de Self Encrypted Drive (SED).

4 Self Encrypted Drive (SED)

Self Encrypted Drives zijn verkrijgbaar als harddisks en als Solid State Drives. De bekendheid met de SSD's is toegenomen, maar niet iedereen weet hoe de functie te gebruiken is. Er zijn drie uitvoeringen, vaak allemaal beschikbaar in één SSD:
- SATAencryptie;
- Opal Security Subsystem Class;
- Encrypted Drive (eDrive).

De gegevens op een Self Encrypted Drive zijn altijd versleuteld. De controller regelt dit. De bovengenoemde opties zijn de methodes om de toegang tot de versleutelde gegevens te vergrendelen en te ontgrendelen. Standaard is de toegang open en merkt de gebruiker niet dat zijn gegevens zijn versleuteld. Een secure erase verandert de versleuteling. De SSD is dan ook weer ontgrendeld.
De vergrendeling kan ongedaan worden gemaakt zonder dat de gegevens op de SSD verloren gaan. Dat maakt het ook relatief eenvoudig om van vergrendelingsmethode te wisselen.

4.1 SATAencryptie
SATAencryptie wordt ook wel Class 0 genoemd. De vergrendeling wordt via het BIOS/UEFI harddiskwachtwoord geregeld. Niet alle BIOS/UEFI-uitvoeringen ondersteunen dit. Een nadeel is dat het wachtwoord alleen uit kleine alfanumerieke tekens mag bestaan. Dit geeft dus een beperkte tekenset. Mijn ervaring met mijn ASUS laptop is, dat je de wachtwoorden niet te snel moet intikken. Het wachtwoord wordt dan soms niet herkend doordat er karakters verloren zijn gegaan.

4.2.Opal
De Trusted Computer Group heeft de Opalspecificatie vastgelegd om tot een fabrikantonafhankelijke uitvoering te komen. Er is extra software nodig om de autorisatie uit te voeren.
Deze software wordt in de SSD opgeslagen, maar is niet standaard aanwezig. De software kan bij commerciële bedrijven worden gekocht, maar er is ook een open sourceversie verkrijgbaar. Omdat de software niet standaard in de drive zit, wordt deze methode minder gauw gebruikt.

4.3 eDrive
De eDrive is een door Microsoft uitgebreide Opalimplementatie volgens IEEE 1667. Het vereist UEFI 2.3.1, BitLocker en TPM 1.2 of een USB-stick.

4.4 Drive Trust Alliance
De Drive Trust Alliance heeft als doel voor bekendheid en implementaties van de Self Encrypted Drive te zorgen. Hun focus ligt op de Opalmethode. Zij hebben een Encrypting Box Evaluation Kit uitgebracht, en ook een open source-uitvoering van de benodigde software voor de SSD.
In de evaluatiekit is een programma aanwezig dat de software voor de Opalmethode kan laden. Het programma heeft een grafische gebruikersinterface en werkt op Windows en Mac OS X.

Bij de open sourceversie bestaat de installatie en activatiesoftware uit commando's voor Windows of Linux.
Omdat het installeren van de open sourceversie erg illustratief is, ga ik daar dieper op in. Ik zal dit doen aan de hand van de Windowsversie. Voor Linux gaat het in principe hetzelfde, maar zijn de parameters voor commando's iets anders. Op de hieronder genoemde website wordt de installatie op zowel Windows als Linux uitgelegd. Ik bespreek de installatie zoals gedaan op mijn Windowssysteem. Ik heb Ubuntu geïnstalleerd op de SED en deze de bootdrive gemaakt.

We halen een aantal bestanden op van de website https://github.com/DriveTrustAlliance/sedutil/wiki:
- sedutil_WIN.zip (een Windowstooltje);
- PBA: LINUXPBARelease.img.gz of UEFI64Release.img.gz (De eerste voor een MBRschijf, de tweede voor een UEFIschijf);
- Rescue.img.gz (een programma om in geval van problemen te herstellen).

Pak sedutil_WIN.zip uit met 7zip. Dat geeft: sedutilcli.exe.
Daarna pakken we het PBAimage uit met 7zip voor de SED.
We kiezen voor de MBRversie LINUXPBARelease.img.gz.
Dat geeft: LINUXPBARelease1.12.img.
We zijn nu klaar om het echte werk te beginnen. Geef in de Windows-opdrachtprompt het volgende commando:

```
sedutilcli --scan
```

Dit geeft bijvoorbeeld het onderstaande resultaat:

```
\.\PhysicalDrive0 2 Crucial_CT120M500SSD3 MU05
\.\PhysicalDrive1 2 ST500LT0251DH142 0001SDM7
\.\PhysicalDrive2 No Hitachi HDT725040VLA360
   V5COA7BA
\.\PhysicalDrive3 12 Samsung SSD 850 EVO 500GB
   EMT01B6Q
```

We weten nu het nummer van de Opaldrive Samsung SSD 850 EVO.
Eventueel kan je meer informatie opvragen met het volgende commando:

```
sedutilcli query \.\PhysicalDrive3
```

maar dit is niet echt noodzakelijk.

We gaan nu de drive klaarmaken met een aantal commando's in de Windowsopdrachtprompt:

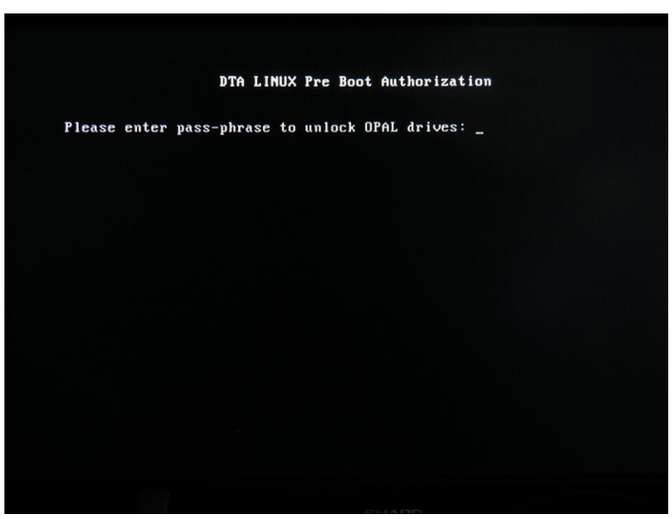
```
sedutilcli  initialsetup <password>
\.\PhysicalDrive3
```

Om van de SED een bootdrive te maken moeten we het PBAimage laden. Dat kan vrij lang duren, dus word niet ongeduldig.

```
sedutilcli loadPBAimage <password> LINUXPBA-
Release1.12.img  \.\PhysicalDrive3
sedutilcli setMBREnable on <password>
\.\PhysicalDrive3
```

Nu gaan we de SED vergrendelen met het volgende commando:

```
sedutilcli enableLockingRange 0 <password>
\.\PhysicalDrive3
```



Om nu de vergrendeling te effectueren sluiten we Windows netjes af tot en met powerdown. Daarna starten we de laptop weer op. De SED vraagt dan om het door ons geïnstalleerde wachtwoord. Na invoer van dit wachtwoord wordt de SED ontgrendeld. Dan herstart het systeem en start in mijn geval Ubuntu op vanaf de SED. De SED zal weer worden vergrendeld zodra de spanning van de SED af is geweest.

De vergrendeling kan worden gedeactiveerd met de volgende commando's:

```
sedutilcli -disableLockingRange 0 <password>
\.\PhysicalDrive3
sedutilcli -setMBREnable off <password>
\.\PhysicalDrive3
```

Wil je de vergrendeling van de SED weer activeren, geef dan de volgende commando's:

```
sedutilcli –enableLockingRange 0 <password>
\.\PhysicalDrive3
sedutilcli –setMBRDone on <password>
\.\PhysicalDrive3
sedutilcli –setMBREnable on <password>
\.\PhysicalDrive3
```

Nu moeten we de rescueUSB-stick nog klaarmaken. Zet met Win32DiskImager van Sourceforge het image op de USB stick. Je hebt dan een opstartUSB verkregen met een klein Linux-systeem dat dezelfde mogelijkheden biedt als sedulcli.

5 Conclusie

Welke encryptiemethode je het beste kan kiezen is afhankelijk van HET type schijf en het gebruikte platform. Laten we uitgaan van de schijf.

5.1 Hard Disk Drive
De goedkoopste optie is om hier software-encryptie te gebruiken. Dat is voor Windows lager dan 10: VeraCrypt en voor Linux LUKS.

5.2 SSD
Bij een SSD moet je eigenlijk kiezen voor een Self Encrypted Drive. Let er wel op of Opal wordt ondersteund. Samsung heeft de gewoonte SED met encryptie uit te brengen die alleen Class 0 encryptie biedt. De andere opties komen met een firmwareupdate die lang op zich kan laten wachten. Voorbeeld is de 950 Pro, waarvoor zelfs de update voor Opalsupport is uitgesteld wegens onvoldoende beschikbaarheid van commerciële software. De 960 Pro en Evo ondersteunen Class 0 (SATA) en Opal wel.

De SED is geschikt voor ieder operatingsysteem.

Windows 10-gebruikers die hun schijf willen versleutelen raad ik aan een Self Encrypted Drive te gebruiken. Upgrades van Windows 10 vereisen dan niet het ontsleutelen van de schijf alvorens de upgrade te kunnen uitvoeren.

5.3 USB-sticks
De USB-sticks worden geleverd met zowel hardware-encryptie als software-encryptie. Bij software-encryptie kan je beter zelf de encryptie regelen met bijvoorbeeld VeraCrypt. Eventueel uitgevoerd als een travelerdisk. Besef wel dat er hardwareversleutelingen zijn die heel makkelijk zijn te omzeilen.
Check dus op internet of het een betrouwbare stick is.

6 Interessante links

https://veracrypt.codeplex.com/
https://mhogomchungu.github.io/zuluCrypt/
http://www.7zip.org/
https://www.drivetrust.com/
https://github.com/DriveTrustAlliance/sedutil/wiki
https://sourceforge.net/projects/win32diskimager/
https://mhogomchungu.github.io/zulucrypt/
https://github.com/DriveTrustAlliance/sedutil/wiki
http://hmarco.org/bugs/CVE20164484/CVE20164484_cryptsetup_initrd_shell.html#fix