Encryptie van pc en laptop

Inleiding

Laatste aanpassing: 2019-09-22

Er is op dit moment veel aandacht voor cyber crime en privacy. Daardoor willen we wel eens vergeten dat er ook nog ouderwetse inbrekers actief zijn. In dit artikel geef ik informatie over hoe je kan zorgen dat bij een fysieke inbraak je gegevens toch niet direct op straat komen te liggen.
De pc of laptop – hierna kan je voor laptop ook pc lezen – bevat steeds meer gegevens van ons. Niet alleen bankgegevens, maar ook kopieën van identiteitspapieren en privé foto's. Bij het verlies of een diefstal willen we niet dat deze gegevens in handen van anderen vallen. Hoe kunnen we ons het beste 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.

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 dat bij de optie 'snel opstarten' de inhoud van het werkgeheugen op schijf wordt opgeslagen? Het wisselbestand en het hibernate bestand 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.

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 harde schijf. Na het wissen van data bij een Solid State Drives (SSD) kan de data altijd nog staan op andere cellen. Bij SSD's komen ze zelfs in het deel van de SSD dat is gereserveerd 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.

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.

VeraCrypt

VeraCrypt is een open source programma dat is voortgekomen uit TrueCrypt. De ontwikkelaars van TrueCrypt zijn er mee gestopt. In VeraCrypt zijn een aantal problemen van TrueCrypt opgelost en zijn er 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/sticks. Voor Het versleutelen kan on-the-fly plaatsvinden, zonder dat gegevens verloren gaan.

VeraCrypt staat het toe om diverse encryptie methodes op elkaar 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. Het 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.

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.

BitLocker

Bitocker is de Microsoft oplossing 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 USB stick worden gebruikt om op te starten. Ook dit is voor de thuisgebruiker niet een interessante optie.

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.

LUKS

LUKS met dm-crypt kan schijven, partities, logical Volumes, containers , bestanden en USB schijven/Sticks versleutelen. Het is voor het Linux platform, hoewel er een niet meer onderhouden Windows versie LibreCrypt bestaat. LUKS kan ook de systeemschijf (als een Logical Volume) versleutelen. Het nadeel is dan dat de ruimte voor de kernel vast ligt. Na veel kernel updates moet de gebruiker eventueel oude kernels opruimen. Bij Ubuntu installatie is het versleutelen van de systeemschijf opgenomen in de installatie procedure: een vinkje zetten en 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 nog dan 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.

EncFS

Het open source programma EncFS is het eenvoudigste encryptie systeem op Linux. Het vereist geen root autorisatie. Het wordt door o.a. door het back-up programma ‘Back in Time’ gebruikt. Een belangrijk nadeel is dat als je een bestand twee maal versleuteld, de combinatie van beide bestanden de versleuteling is te breken. Omdat in de laatste versie een aantal problemen zijn opgelost wordt deze 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 OS-x versie beschikbaar.

VeraCrypt

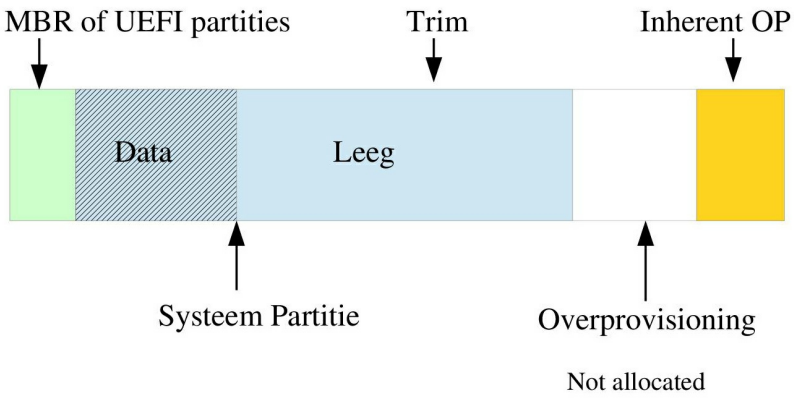
Van VeraCrypt wil ik alleen nog benadrukken dat het onder Linux geen systeem disk kan versleutelen. Voor de rest verwijs ik naar wat onder Windows is beschreven.

ZuluCrypt/Mount

ZuluCrypt/Mount is een klein wonder. Het ondersteunt versleuteling volgens zowel dm-crypt met LUKS als VeraCrypt. De mount optie 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.

Solid State Disk

Bij de Solid State Disk is het i.v.m. software versleuteling van belang om te kijken hoe overprovisioning en garbage collection 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 er naar te schrijven. De controller schrijft dan naar een schoon blok in het overprovisioning deel. Dit wordt dus nu deel van de systeem partitie. Als er geen schone blokken meer beschikbaar zijn, moet een blok eerst worden gewist alvorens er naar 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.
Garbage collection maakt vrijgekomen blokken beschikbaar door ze te wissen en dit moet zoveel mogelijk gebeuren als er geen schrijfacties plaatsvinden.
Het operating systeem weet welke blokken op de partitie vrij zijn gekomen. Door middel van het trim commando wordt de SSD controller geïnformeerd welke blokken vrij zijn. Deze worden dus opgenomen in het garbage collection proces. Het deel van de partitie waar geen data staat, noemen we het dynamische overprovioning deel.
Je kan de benodigde statische overprovisioning verkleinen door het trim commando vaker uit te voeren en dus beter gebruik te maken van de dynamische overprovisioning.
Windows doet de trim op wekelijkse basis. Bij Linux is dit instelbaar naar bijvoorbeeld dagelijks.



Voor VeraCrypt en LUKS wordt afgeraden om het bij SSD’s te gebruiken. De achtergrond hiervoor is dat gegevens niet worden overschreven, zelfs 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.
Helaas wordt de SSD dan al snel trager. Bij het gebruik op SSD’s of USB sticks wordt aangeraden in ieder geval uit te gaan van een schoon medium. Bij de SSD moet er dan ook geen overprovisioning worden gebruikt. Het is dan wel aan te raden de TRIM op dagelijks te zetten. Voor meer informatie lees de documentatie van VeraCrypt en LUKS.
Er is echter een betere encryptie oplossing voor SSD’s: de Self Encrypted Drive.

Self Encrypted Drive (SED)

Self Encrypte Drives zijn verkrijgbaar als hard disks en Solid State Drives. Met de SSD’s is de bekendheid toegenomen, maar niet iedereen weet hoe de functie is te gebruiken. Er zijn drie uitvoeringen. Vaak allemaal beschikbaar in één SSD:

- SATA encryptie;
- 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.

SATA encryptie

SATA encryptie wordt ook wel class 0 genoemd. De vergrendeling wordt via het BIOS/UEFI hard disk wachtwoord geregeld. Niet alle BIOS/UEFI uitvoeringen ondersteunen dit. Een nadeel is dat het wachtwoord alleen uit kleine alfa-numerieke 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 herkent, omdat er karakters verloren zijn gegaan.

Opal

De trusted Computer Group heeft de Opal specificatie vastgelegd om tot een fabrikant onafhankelijke 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 source versie verkrijgbaar. Omdat de software niet standaard in de drive zit, wordt dat deze methode minder gauw gebruikt.

eDrive

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

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 Opal methode. Zij hebben een Encrypting Box Evaluation Kit uitgebracht, maar ook een open source uitvoering van de benodigde software voor de SSD.
In de evaluatie kit is een programma aanwezig, dat de software voor de Opal methode kan laden. Het programma heeft een grafische gebruikersinterface en werkt op Windows en Mac OS-X.
Bij de open source versie gaat de installatie en activatie met commando's voor Windows of Linux. Omdat het installeren van de open source versie erg illustratief is, ga ik daar dieper op in. Op de hieronder genoemde website wordt zowel de installatie vanaf de Rescue USB-stick uitgelegd. Ik bespreek de installatie zoals gedaan op mijn systeem. Ik heb op de SED Ubuntu geïnstalleerd en de SED de boot drive gemaakt.

De procedure om Opal actief te maken op een SED kan niet worden uitgevoerd vanaf een operating systeem dat op de SSD is geïnstalleerd. Het handigst is om de procedure vanaf de rescue USB-stick uit te voeren. De rescue USB-stick bevat een klein Linux systeem.
Voor MBR systemen moet je de BIOS32 image gebruiken. Voor UEFI kan je zowel de BIOS32 image als de UEFI64 image gebruiken. Het is ook mogelijk om vanaf een Windows of Linux systeem te werken. Voorwaarde is wel dat je niet vanaf een operating systeem op de SED werkt. De rescue USB-stick is het eenvoudigst en het is toch altijd goed om deze achter de hand te hebben in geval van problemen. De huidige versie 1.15.1 werkt niet vanaf Windows.

Voor een UEFI systeem is moet secure boot zijn uitgeschakeld i.v.m. de Opal implementatie.

We halen een de rescue -image vanaf de website https://github.com/Drive-Trust-Alliance/sedutil/wiki/Executable-Distributions

RESCUE32.img.gz of RESCUE64.img.gz

Pak het gz-bestand uit met 7-zip op een Windows systeem en zet het met WIN32DiskImager op een USB-stick.

We zijn nu klaar om het echte werk te beginnen. Start je pc of laptop op vanaf de USB-stick. Je krijgt een login pompt: enter "root". Er is geen wachtwoord nodig.

Geef het volgende commando: sedutil-cli - -scan (**N.B.** tussen de twee koppeltekens moet geen spatie staan, zo ook hieronder)

Dit geeft bijvoorbeeld het onderstaande resultaat:

Scanning for Opal compliant disks
/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

Een 2 in de tweede kolomn geeft aan dat het een Opal SSD is. We weten nu het drivenummer van de Opal drive, bijvoorbeeld: Samsung SSD 960 EVO.
Eventueel kan je meer informatie van een specifieke schijf opvragen met bijvoorbeeld het volgende commando:

sedutil-cli – -query /dev/nvme0 (maar dit is niet echt noodzakelijk)

We gaan nu de drive klaarmaken met een aantal commando's (Voorlopig gebruiken we als wachtwoord debug):

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

Om van de SED een boot drive te maken moeten we het PBA image laden. Dat kan vrij lang duren, wordt dus niet ongeduldig. Daarbij bebruiken we het gewenste wachtwoord. Voor een UEFI systeem:

gunzip /usr/sedutil/UEFI64-n.nn.n.img.gz (n.nn.n is het release nummer)
sedutil-cli - -loadpbaimage debug /usr/sedutil/UEFI64-n.nn.n.img /dev/nvme0 (n.nn.n is het release nummer)

Nu gaan we de SED vergrendelen met het volgende commando's: (<password> is het wachtwoord wat je wilt gaan gebruiken)

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

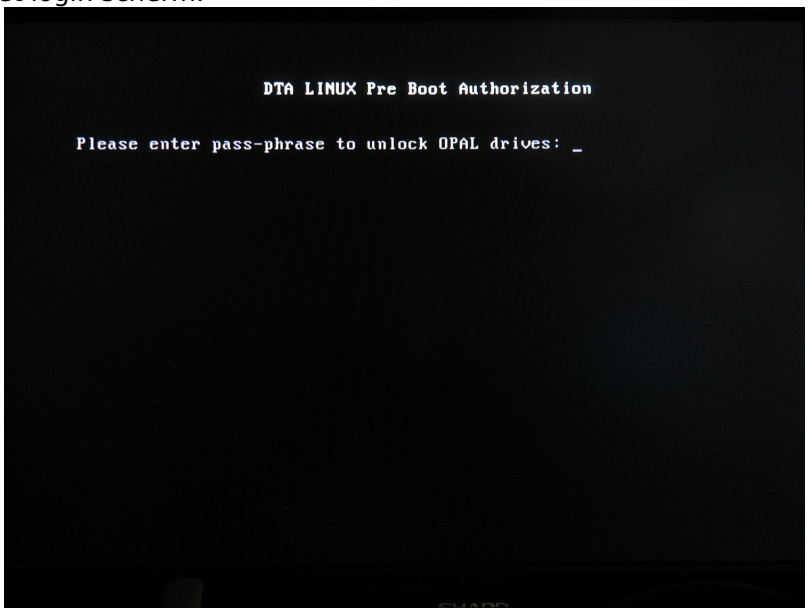
Om nu de vergrendeling te effectueren schakelen we laptop uit. Daarna starten we de laptop weer op. De SED vraagt dan om het door ons geïnstalleerde wachtwoord. Na invoer van dit wachtwoord wordt de SED ontgrendeld. Dan herstart het systeem en start in mijn geval Ubuntu op vanaf de SED. De SED zal weer worden vergrendeld zodra de spanning van de SED af is geweest.
De vergrendeling kan worden gedeactiveerd met de volgende commando’s:

sedutil-cli - –disablelockingrange 0 <password> /dev/nvme0
sedutil-cli – -setMBREnable off <password> /dev/nvme0

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

sedutil-cli - –enableLockingRange 0 <password> /dev/nvme0
sedutil-cli – -setMBREnable on <password> /dev/nvme0

Als je de pc of laptop nu opstart, krijg je het login scherm.



Na het invoeren van het wachtwoord herstart de pc of laptop en kom bij het besturingssyteem.

Conclusie

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

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.

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 bieden. De andere opties komen met een firmware update die lang op zich kan laten wachten. Voorbeeld is de 950 pro. De 960 evo en pro ondersteunen Class 0 (SATA) en Opal 2.0.
De SED is geschikt voor ieder operating systeem.
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.

USB sticks

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

Exposures

Ook SED's kunnen uiteraard beveiligingslekken hebben. De link wijst naar een melding van problemen die zijn ontdekt door de Radboud Universiteit Nijmegen.

Interessante links

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