DE KRACHT VAN ENCRYPTIE EN... ZAL ER PRIVACY ZIJN IN DE CLOUD?

Dr. Pim Tuyls, CEO Intrinsic-ID

2013 zullen we ongetwijfeld blijven herinneren als het jaar van de afluisterschandalen en van schending van privacy. Wat mogen we verwachten van 2014? Zullen nieuwe security maatregelen de deur voor organisaties zoals de NSA kunnen sluiten? Volgens Pim Tuyls van Intrinsic-ID heb je nochtans niet veel nodig om digitale gegevens adequaat te beveiligen. Net zoals je eigen huis beveilig je deze best met een unieke fysieke sleutel die je in eigen handen houdt.

Uit onderzoek[1, 2] blijkt dat data-inbreuk vaker niet dan wel het gevolg is van een geplande en doelbewuste aanval op een specifiek bedrijf of een organisatie. Bijna 80% van de slachtoffers werden getroffen omdat de gelegenheid zich voordeed, en bij 96% van de gevallen was de aanval niet eens zo moeilijk. Wat de NSA betreft ligt dat enigszins anders. Voor hen werden achterpoorten mee ingebouwd in het ontwerp van de bestaande security systemen. Maar zowel de recente Adobe-hack waarbij 150 miljoen accounts[3] werden buit gemaakt als de onthulde NSA praktijken belichten de risico's die een virtuele wereld met zich meebrengt en het feit dat we ons te weinig bewust zijn van deze gevaren. De digitale wereld lijkt ons een vals gevoel van veiligheid te geven omdat we, in tegenstelling tot in onze reële wereld, de zwakke schakels en achterpoortjes niet kunnen zien.

De groei van onze virtuele wereld lijkt nochtans niet te stuiten en de anytime – anywhere cloud palmt hierbij een steeds groter aandeel in. De expansie loopt hand in hand met de Bring Your Own Device' (BYOD) trend, waarbij steeds meer gebruikers deze devices en bijhorende applicaties integreren in hun dagelijkse werkzaamheden. De security uitdagingen worden er niet eenvoudiger op en de standaard maatregelen zijn al lang niet meer up-to-date. Iedere IT manager komt al gauw tot de conclusie dat er geen eenduidige oplossing is om de toenemende risico's in te dammen en dat een gelaagde aanpak nodig is.

ENCRYPTIE

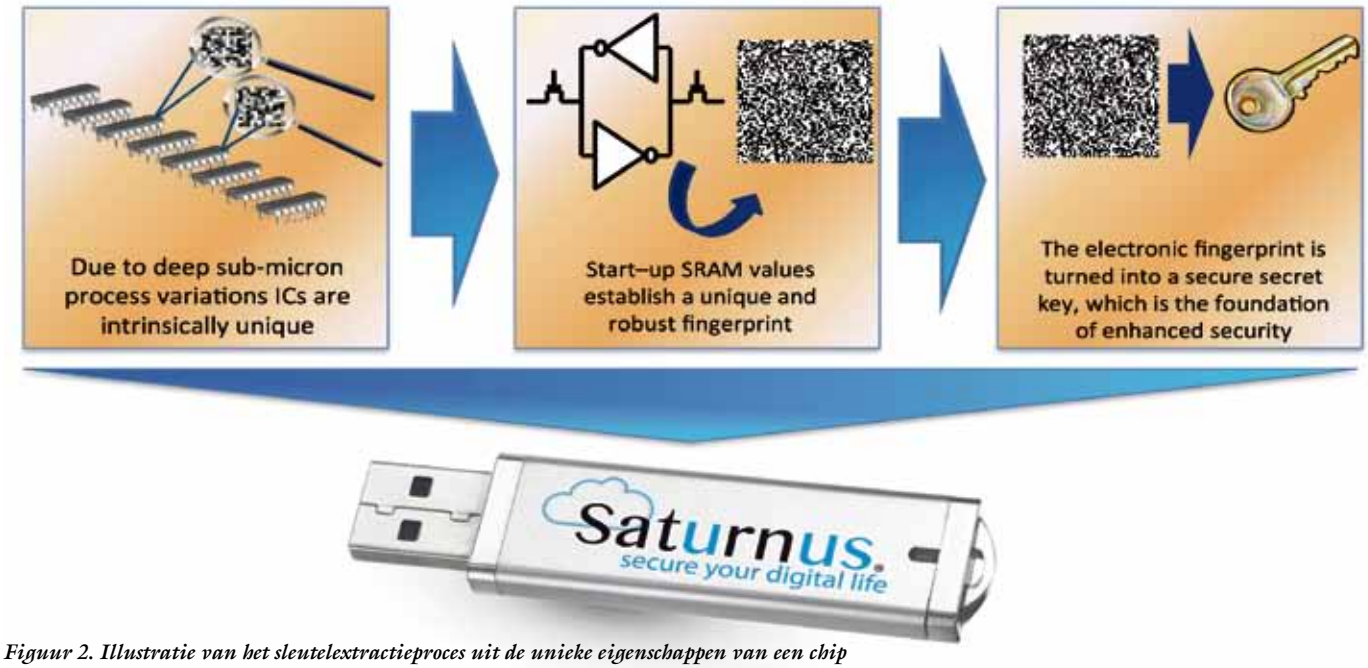
Een eeuwenoude methode om te vermijden dat gevoelige informatie in handen komt van onbevoegden is versleuteling of encryptie. Hieronder verstaan we het vercijferen van informatie met behulp van een encryptiesleutel. Ook wat de cloud betreft is bescherming door encryptie een steeds belangrijker wordende activiteit. Steeds meer Cloud providers maar ook gespecialiseerde bedrijven bieden encryptietools aan voor data in of op weg naar de Cloud. Zoals geïllustreerd in figuur 1. kan men bij de aangeboden oplossingen drie categorieën onderscheiden: server-based , gateway-based en client-based versleutelsystemen.

SERVER-BASED ENCRYPTIE

Bij server-based encry ptie is het de service aanbieder of cloud provider die voor de encryptiesleutel en het versleutel proces zorgt. Dit wil zeggen dat het ook de service aanbieder of de cloud provider is die de master encryptiesleutel bewaart. Deze me-

1. Verizon Data Breach Report 2012
2. 2013 Cost of Data Breach Study: Global Analysis (Ponemon Institute)
3. http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

Figuur 1. Encryptiesystemen voor het beveiligen van data in de cloud kunnen opgedeeld worden in drie categorieën



Figuur 2. Illustratie van het sleutelextractieproces uit de unieke eigenschappen van een chip

thode heeft twee belangrijke nadelen. Het veronderstelt een vertrouwen in de provider en wanneer diens systeem wordt gehackt, komen de gegevens van alle klanten gelijktijdig vrij. Een recent voorbeeld hiervan is de Adobe-hack waarbij meer dan 150 miljoen accounts werden ontvreemd.

GATEWAY-BASED ENCRYPTIE

Hierbij wordt er een extra "gateway" server geinstalleerd die dienst doet als digitale toegangspoort tot het bedrijfsnetwerk. Alle digitale informatie die de bedrijfsserver verlaat wordt eerst versleuteld met behulp van sleutels die door de gateway beheerd worden. Een belangrijk voordeel ten opzichte van server-based encryptie is dat het sleutelbeheer gescheiden is van de cloud opslag aanbieder. Een nadeel is het feit dat de beveiliging zich op één plek bevindt, namelijk bij de gateway. Een aanval hierop impliceert een aanval op het hele bedrijf.

CLIENT-BASED ENCRYPTIE

Bij client-based encryptie worden de gegevens versleuteld aan de kant van de gebruiker alvorens ze het device verlaten. Dit impliceert dat de sleutels aan de kant van de gebruiker worden gegenereerd en bewaard. Dit maakt een aanval op het systeem (server-based) of een bedrijf (gateway-based) onmogelijk. Elke gebruiker zal individueel aangevallen moeten worden. Bij client-based encryptie kan er verder onderscheid gemaakt worden tussen software- en hardware-matige methoden.

Bij **software-matige methoden** worden de encryptiesleutels afgeleid van wachtwoorden die door de gebruiker zelf worden aangemaakt en bewaard. Juist vanwege deze `menselijke' component, zijn deze sleutels meestal niet erg random en onvoorspelbaar gekozen waardoor ze makkelijk te kraken zijn door middel van vrij eenvoudige aanvallen zoals `brute force' en `guessing'.

Bij **hardware-matige methoden** worden de sleutels gegenereerd door een hardware component; een security chip in de vorm van een smartcard, USB stick of microSD kaart die in het bezit is van de gebruiker. Hierbij kunnen lange sleutels met de hoogste entropie (randomness) worden gegenereerd waardoor deze niet te raden of te kraken zijn met huidig beschikbare middelen. Tevens biedt een hardware security chip een zeer veilige manier van sleutel opslag. Client-based encryptie met behulp van een hardware of fysieke sleutel biedt daarmee de beste bescherming en bovendien is het niet nodig om een andere persoon of organisatie in vertrouwen te nemen. Deze oplossing geeft de controle terug aan de gebruiker en heeft een duidelijke parallel met het beveiligen van onze fysieke wereld. Wanneer we ons huis of onze auto verlaten, grendelen we deze ook af met een unieke fysieke sleutel. Bij de grote Cloud mastodonten zoals Google en Facebook wordt al volop met dit soort hardware sleutels geëxperimenteerd in eerste instantie door eigen werknemers voor het beveiligen van interne bedrijfsgegevens.

De security oplossingen voor onze virtuele wereld moeten niet alleen sterke sleutels bevatten, ze moeten ook goedkoop zijn en eenvoudig toe te passen, zonder ons normale werkgedrag (surfen, bewaren of opslaan, synchroniseren en informatie delen) te storen. Onder de naam Saturnus brengt Intrinsic -ID een eerste Cloud beveiligingsapplicatie op de markt die aan al deze voorwaarden voldoet. Bovendien werkt Saturnus volgens het "zero knowledge" principe: de sleutels worden per gebruiker door de hardware aangemaakt en zijn daardoor bij niemand bekend. Ook niet bij Intrinsic-ID of bij de cloud storage provider.
Deze hardware gebaseerde sleutels zijn niet na te maken en worden beschermd door de gepatenteerde Hardware Intrinsic Security (HIS*) technologie. Deze technologie biedt de beste bescherming voor het genereren en bewaren van hardware gebaseerde sleutels.

HIS* TECHNOLOGIE

Traditioneel, zonder gebruik te maken van de HIS technologie, worden de sleutels opgeslagen in het niet-vluchtige geheugen van de chip (EEPROM, E-fuses). Maar voor een expert die de chip in handen krijgt zijn er effectief bewezen aanvallen om hieruit de encryptiesleutel te ontfutselen. Chips worden opengemaakt en het geheugen wordt op invasieve wijze uitgelezen. Bij HIS is de sleutel niet permanent aanwezig op de chip en zelfs nooit aanwezig wanneer de chip uit staat, maar wordt deze gegenereerd uit de unieke hardware-eigenschappen (of vingerafdruk) van de chip (zie figuur 3.). Tijdens de fabricage van een chip maken kleine verchillen in het zogenaamde doperingsproces elk stukje halfgeleider-materiaal en dus ook elke chip uniek. Hierdoor zijn de opstartwaarden van de SRAM (Static Random Access Memory, of statisch geheugen) voor elke chip verschillend. Deze waarden kunnen worden gezien als een `elektronische vingerafdruk' waaruit HIS de meest veilige geheime encryptiesleutels genereert.

BEVEILIGEN VAN DATA IN DE CLOUD

Met de Saturnus applicatie van Intrinsic-ID is het mogelijk om bestanden veilig op te slaan in Dropbox en om bestanden veilig te delen met andere Saturnus gebruikers. De software werkt op Windows en Android

systemen. De encryptiesleutel wordt gegenereerd uit de chip van een USB stick maar in principe zijn diverse vormen van hardware mogelijk. Gegevens kunnen enkel versleuteld of ontcijferd worden wanneer deze stick is aangesloten op de PC of het mobiele device. Op het moment dat de stick uit het device wordt gehaald, zijn de versleutelde data in de cloud niet langer toegankelijk en kunnen ook geen bestanden meer beveiligd worden voor opslag in de cloud.

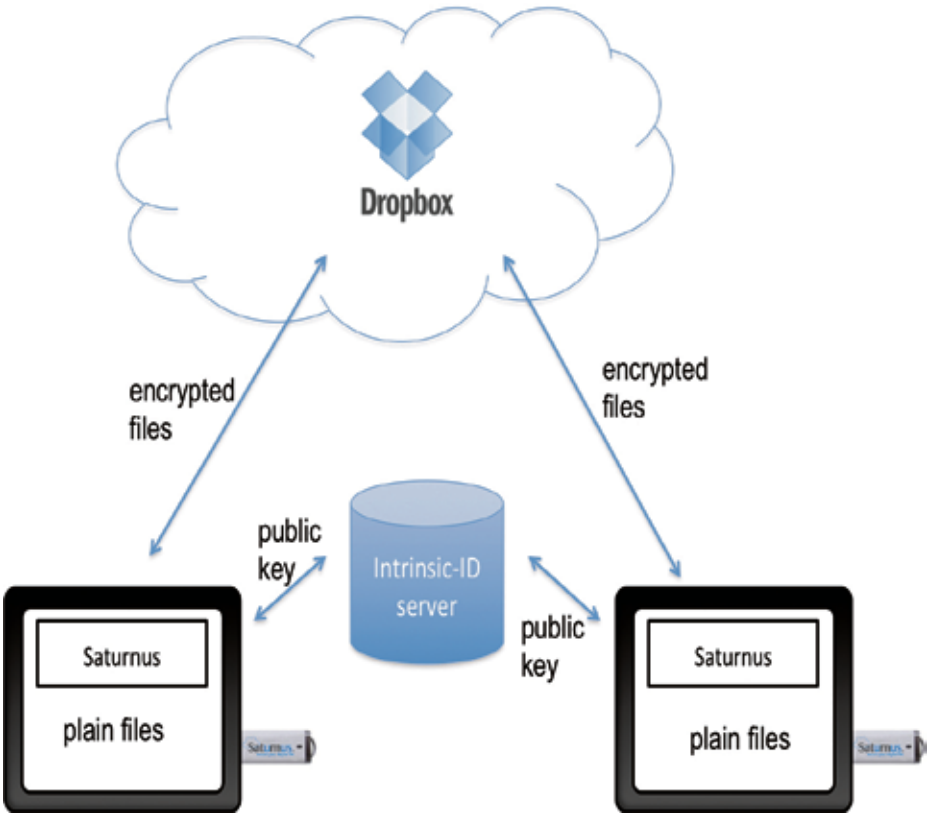
Wanneer de stick in op het device wordt aangesloten, moeten Saturnus gebruikers zich eerst aanmelden. Dit doen ze met behulp van een gebruikersnaam en wachtwoord. Deze authenticatiemethode die twee onafhankelijke factoren combineert; een token die men heeft en een paswoord dat men weet, noemt men twee-factor-authenticatie. Dit maakt het voor mogelijke aanvallers onmogelijk om toegang tot de versleutelde data in de cloud te verkrijgen. Men moet èn over de USB token beschikken èn over de gebruikersnaam met wachtwoord.

VEILIG OPSLAAN VAN BESTANDEN

Wanneer een file in Dropbox wordt opgeslagen via Saturnus, zal deze automatisch en ongemerkt snel eerst versleuteld worden waarna de file naar de Cloud wordt gestuurd. Hierbij gebruikt Saturnus symmetrische cryptografie die gebaseerd is op de AES standaard. (Advanced Encryption Standard). Bij symmetrische sleutel cryptografie worden de bestanden versleuteld en ontcijferd met dezelfde sleutel. Zoals eerder beschreven werd deze sleutel gegenereerd en beveiligd via de Saturnus USB token door middel van HIS technologie. Omdat het versleutelen aan de kant van de gebruiker plaatsvindt, is de informatie in de bestanden volledig beschermd, ook al mocht een bestand onderschept worden op weg naar of in de Cloud. Wanneer de legitieme gebruiker één of meerdere bestanden in de Cloud wil openen, worden ze zeer snel en haast ongemerkt eerst op de PC of het mobiele device gedownload en ontcijferd waarna ze klaar zijn voor gebruik.

HET VEILIG DELEN VAN BESTANDEN

Voor het veilig delen van bestanden maakt Saturnus gebruik van asymmetrisch of publieke sleutel cryptografie. Voor elke Saturnus gebruiker wordt een publiek/privaat sleutelpaar gegenereerd bij aanmaak van het account. Hoewel deze sleutels verschillend zijn, is er een mathematische link tussen de twee. De publieke sleutel wordt gebruikt om bestanden te versleutelen, terwijl de private sleutel dient om beveiligde bestanden terug te ontcijferen. De private sleutel blijft altijd veilig opgeborgen in de hardware van de gebruiker terwijl de publieke sleutel wordt



Figuur 3. Informatieoverdracht door Saturnus voor het veilig delen van bestanden in de cloud

opgeslagen in de databank van Saturnus. De opslag van de publieke sleutels in een database is perfect veilig omdat hiermee namelijk geen data kunnen worden ontcijferd. Het eventueel onderscheppen van deze sleutel levert dus geen gevaar voor de veiligheid van de informatie.

Om een bestand te delen met een andere Saturnus gebruiker, wordt door de applicatie eerst de publieke sleutel van deze gebruiker uit de Saturnus databank gehaald. Met behulp van deze publieke sleutel wordt het bestand versleuteld bij de verzender alvorens het naar de Cloud wordt verstuurd om daar opgeslagen te worden op een plaats die toegankelijk is voor de ontvanger. De ontvanger zal in de Saturnus applicatie de melding krijgen dat er een bestand wordt gedeeld. Alvorens het bestand kan worden geopend, zal het in de achtergrond van de applicatie ongemerkt snel gedownload en ontcijferd worden met de private sleutel van de ontvanger. De ontvanger is de enige persoon die de private sleutel bezit en dus ook de enige persoon die het bestand kan ontcijferen. Een aanvaller die het bestand zou onderscheppen kan het niet openen en de informatie niet lezen omdat deze niet beschikt over de juiste private sleutel.

Wie zijn huissleutel verliest kan het huis niet meer binnen en moet een nieuw slot installeren. Met Saturnus is dit niet anders. De gebruiker zal een nieuwe token moeten aanschaffen en de Saturnus applicatie (het slot) opnieuw moeten installeren. Alleen de legitieme eigenaar van de data in de cloud kan dit doen en opnieuw toegang krijgen tot zijn of haar beveiligde data in de cloud.

CONCLUSIE EN TOEKOMST

Een systeem zoals Saturnus dat twee-factor authenticatie combineert met het hardwarematig verankeren van de encryptiesleutel m.b.v. HIS technologie is dus extreem veilig om gegevens op te slaan en te delen in de cloud. Het laat toe om medewerkers van de juiste informatie te voorzien overal en op elk moment via om het even welk device (BYOD) zonder het risico te lopen dat niet-geautoriseerde personen de informatie kunnen onderscheppen of wijzigen. Het werken met een token maakt het voor werkgevers makkelijk om toegang tot informatie te verlenen of terug te ontnemen.

Gegeven de toenemende bewustwording van de risico's die de digitalisering met zich meebrengt, is Intrinsic-ID ervan overtuigd dat het soort fysieke sleutels dat gebaseerd is op een `elektronische vingerafdruk' een scala aan toepassingen zal vinden. Niet enkel voor data encryptie, authenticatie en beveiligd betalingsverkeer, maar ook voor internet-gebaseerde communicatie tussen machines (het zogenaamde 'machine-to-machine' of M2M gebeuren), de verbindingen tussen slimme energiemeters en netwerk beheerders, object tracering, en vele andere toepassingen die spoedig hun ingang zullen vinden dankzij het allom tegenwoordige internet.