HACK EENS... EEN USB-STICK

Wie met gegevens onderweg is, loopt het risico ze te verliezen. Dat geldt voor analoge gegevens (papier) én voor hun digitale tegenhangers (data). Een nadeel aan digitale informatie: u kunt heel veel meenemen, zeker op een relatief makkelijk te verliezen medium als een USB-stick. Gelukkig kunt u die gegevens tegenwoordig beveiligen. Maar hoe veilig zijn uw gegevens dan? Niet gegarandeerd. Kijkt u mee hoe de beveiliging te kraken is?

U kunt twee paden bewandelen om een USB-stick te beveiligen: via software informatie versleutelen of een stick kopen die middels hardware de toegangsrechten bepaalt. Voor de echt paranoïde mensen is het natuurlijk ook mogelijk om een hardwarematig versleutelde stick te voorzien van softwarematig versleutelde informatie. Wat overigens zeker geen slecht idee is.

Hack de software

Via software ingestelde encryptie is omslachtig in gebruik. Iedere keer als u de stick in een systeem duwt, moet de juiste software op het systeem staan om met uw encryptie om te gaan. De stick is daarom niet meer overal te gebruiken. We hebben daar gelijk de belangrijkste reden te pakken dat bijna niemand zijn USB-sticks versleutelt.

Een handigheidje waarmee voorkomen wordt dat gegevens onbereikbaar zijn omdat de benodigde leessoftware niet voorhanden is, is de benodigde software op een onversleuteld deel van de USB-stick meenemen of gebruikmaken van een U3-stick die de software automatisch start.

Versleutelde USB-sticks hebben twee zwakke plekken die u kunt manipuleren. De eerste is het wachtwoord dat nodig is om te ontcijferen. De tweede is het gebruikte algoritme. Dat tweede deel is het eerste punt om de aanval in te zetten. Aan de basis van alle versleuteling ligt wiskunde. De methodiek is gebaseerd op formules en in wiskundige formules kunnen fouten zitten. Die fouten zijn vervolgens uit te buiten door specialisten om alle gegevens standaard te kunnen ontcijferen. Betrouwbare encryptie maakt - verrassend genoeg - gebruik van openbaar bekende methodieken. Dat maakt het namelijk mogelijk voor wiskundig onderlegde experts om dit soort denkfouten op te sporen en recht te zetten. In beide gevallen kunnen er echter onbekende of niet-gerepareerde gaten in de beveiliging zitten. Weet u waarmee de stick is versleuteld, bijvoorbeeld omdat iemand heel handig de ontcijfersoftware op een onbeveiligd deel of U3-stick heeft gezet, dan kunt u kijken of er kant-en-klare kraaksoftware beschikbaar is.

Onkraakbare versleuteling

Heeft u geen idee waarmee de stick precies versleuteld is, dan moet u een 'brute force'-aanval doen. Geautomatiseerde tools zijn middels bovenstaande zoekterm

eenvoudig te vinden. Een brute force-aanval gokt één voor één op mogelijke wachtwoorden. Daarbij worden woordenboeken gebruikt om standaardtermen te zoeken, combinaties van woorden en letters gegokt, en bij geavanceerde software fonetisch bij elkaar aansluitende termen (wat wachtwoorden die makkelijk uit te spreken zijn, maar niet-bestaande woorden gebruiken kwetsbaar maakt). Slagen deze pogingen niet, dan gaat de software alle mogelijke cijfer/letter- en tekencombinaties af.

Hoe lang het duurt om bij de juiste combinatie te komen, is afhankelijk van de rekenkracht die u ter beschikking heeft, de complexiteit van het wachtwoord, de gebruikte encryptiemethode en de software die u gebruikt. De snelst mogelijke resultaten boekt u met commerciële forensische software, op dichte voet gevolgd door een besturingssysteem dat speciaal gemaakt is om wachtwoorden te kraken. Twee mogelijke systemen om de beveiliging van USB-sticks te breken, zijn de Linux-distributies BackTrack (www.remote-exploit.org) en S-T-D (s-t-d.org). Wilt u serieus los gaan op het ontcijferen, dan kunt u gebruikmaken van commerciële software zoals de Password Recovery ToolKit (PRTK) van AccessData (www.accessdata.com).

Van PRTK is een indicatie van de snelheid te geven. De toepassing test eerst een lijst met 100.000 veelvoorkomende wachtwoorden en combinaties. Het kraakt daarmee ongeveer 24 procent van alle wachtwoorden in zeer korte tijd. Op moeilijke wachtwoorden wordt met meerdere machines gelijktijdig gerekend en dit verhoogt de tijd naar twee tot drie weken; als er wat meer persoonlijke informatie van de wachtwoordeigenaar bekend is, wordt dit echter teruggebracht naar een paar uur.

Korte conclusie voor softwarebeveiliging: verwacht niet dat u in tien minuten op een USB-stick komt, maar verwacht ook niet dat versleutelde informatie op een USB-stick onleesbaar is voor anderen. In de meeste gevallen zal het ontcijferen vlot gaan. De enige echt veilige manier om een USB-stick te versleutelen is namelijk met een dusdanig complex wachtwoord dat de USB-stick niet meer eenvoudig te gebruiken is.

USB-sticks zijn er in alle soorten en maten; helaas vallen ze allemaal even makkelijk uit uw broekzak, dus een beetje beveiliging kan geen kwaad.

Hardware

Het perfecte alternatief voor moeilijke wachtwoorden is een fysiek beveiligde USB-stick. Dat kan door op de stick encryptie te ondersteunen, met een pincode of - wat meer in de mode is - met biometrische beveiliging (een vingerafdrukscanner).

Op de stick encryptie ondersteunen valt een beetje uit de toon. U dient dan nog steeds wachtwoorden te onthouden, maar de encryptie en decryptie gaan vlotter dan wanneer de computer al het werk moet doen. Dat is op een modern systeem niet echt noodzakelijk, tenzij u met extreem lange sleutels wilt werken.

De pincode op een USB-stick maakt het lastiger om met brute rekenkracht in te breken. Na drie pogingen moet de USB-stick verwijderd en herplaatst worden. Dat maakt het onmogelijk om ettelijke duizenden wachtwoorden per minuut te gokken. Nadeel is dat de gebruiker nog steeds een pincode moet onthouden. Het meest gebruikte wachtwoord op de planeet is 123456; u mag zelf gokken wat de meest gebruikte pincode voor een USB-stick zal zijn.

Vingerafdrukken

Inloggen met een vingerafdruk is een stuk makkelijker. Vingerafdrukken zijn uniek en als u ze kwijt bent, heeft u grotere problemen dan een ontoegankelijke USB-stick. Helaas is het voor een beetje hacker bijna triviaal om uw vingerafdruk na te bootsen, zeker als deze nog overduidelijk op de scanner van de USB-stick staat. Daar komen we in een volgend nummer op terug.

Zowel de sticks met pincode als die met een vingerafdruklezer gaan mank onder een ander probleem. In de behuizing van de stick zitten namelijk twee printplaten: één met de vingerafdrukscanner of pincodetoetsen en een tweede met daarop het flashgeheugen met controller. Als de stick in de computer wordt ingevoerd, meldt de printplaat met beveiliging zich aan. →

Om een USB-stick met vingerafdrukscanner te kraken, hoeft u geen vingers af te hakken.

Zodra u de juiste code of vingerafdruk ingeeft, geeft deze printplaat een signaal aan de onderste printplaat en wordt het flashgeheugen aangemeld. Haalt u de stick uit elkaar en soldeert u de juiste weerstand op de samenvoegplek, dan heeft u de pincode of vingerafdruk niet meer nodig om het onderste deel zich aan te laten melden alsof de juiste code of vingerafdruk is ingegeven.

Afgevijlde serienummers

Lukt het niet om het juiste signaal na te bootsen, dan is het voor de fanatiekere hacker altijd nog een optie om een flashgeheugenleesapparaat in te zetten. U soldeert dan de geheugenchip van de open USB-stick af en plaatst deze op de lezer. Vervolgens heeft u een probleem. U moet namelijk weten welke controller de geheugenchip aanspreekt en deze nabootsen, maar de meeste fabrikanten vijlen de serienummers van deze controlechips af. Dat betekent dat u langer moet zoeken naar de juiste code. Ook is deze laatste optie niet voor iedereen weggelegd. Een geheugenlezer kost rond 4.500 euro en om de controller te achterhalen, heeft u redelijk wat ervaring met bestandssystemen nodig.

Een andere, veelvoorkomende beveiliging is een lijm waarin de geheugenchip wordt gegoten. Wie probeert de chip los te krijgen met een soldeerbout breekt de chip en de data is weg. Vooralsnog blijken de lijmen gevoelig voor het juiste oplosmiddel en zijn ook deze chips los te krijgen, waarna u ze op de chiplezer kunt leggen. Dit is natuurlijk geen klus voor iemand zonder enig gevoel voor chemie.

Doe het zelf

Eenvoudige brute force-aanvallen op de software kunt u uitvoeren zonder budget mits u al in het bezit bent van een redelijk courante computer, veel geduld en wat basiskennis van Linux. Aanvallen op de hardware vereisen basiskennis van elektronica, een soldeerset en een collectie reserveonderdelen, inclusief dunne soldeerdraad. Wederom kan geduld geen kwaad. Dit zal op de meeste normale USB-sticks afdoende zijn om bij de gegevens te komen.

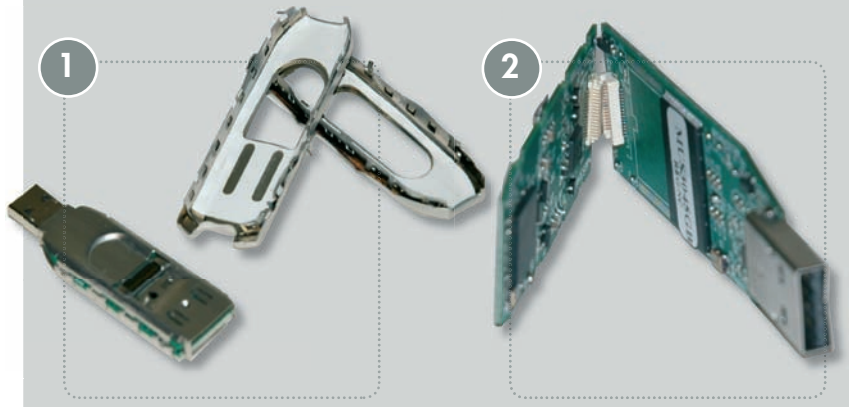
Het spreekt voor zich dat het chemisch smelten van speciale lijmen, de aanschaf van chiplezers die meer kosten dan een zeer deftig computersysteem of forensische software met gelijksoortige prijskaartjes niet voor hobbyisten weggelegd zijn. Aan de andere kant zijn deze investeringen triviaal als de waarde op de USB-stick groter is.

Goede beveiliging

Om uw gegevens te beschermen tegen een gemiddelde gelukkige vinder volstaan vingerafdruklezers, pincodes en wachtwoorden als u het makkelijk wilt houden. Wilt u dat uw gegevens beschermd blijven tegen de fanatiekere hobbyist die uw stick vindt? Dan is het verstandig om softwarematige encryptie te combineren met hardwarebescherming. Geld uitgeven aan software is voor thuisgebruik overbodig. De gratis toepassing TrueCrypt (www.truecrypt.org) kan gegevens dusdanig versleutelen dat zelfs een heel fanatieke hobbyist een heel goede reden nodig heeft om door de beveiliging te breken.

Heeft u zeer gevoelige informatie (bijvoorbeeld patiëntgegevens of militaire plannen) of gegevens die geld waard zijn (een databank met kredietkaartgegevens), dan is er maar één manier om te zorgen dat een potentiële dief niet bij die gegevens komt: ze niet op een USB-stick zetten. Voor een relatief laag budget is het mogelijk om praktisch iedere USB-stick te kraken. Als die informatie al overal toegankelijk moet zijn, dan hoort ze op professioneel beveiligde servers te staan. [M.G.]

Een beveiligde USB-stick kraken



Als u de behuizing van een beveiligde USB-stick openmaakt, vindt u twee op elkaar geplakte printplaatjes (afb. 1). De twee plaatjes worden verbonden met een contactpunt (afb. 2). Als via dit punt de printplaat met beveiliging (afb.3 links) aangeeft dat de juiste code of vingerafdruk is ingevoerd, dan zal de printplaat met de controller en het geheugen (afb.4 rechts) zich zoals iedere normale USB-stick aanmelden bij het systeem.