Christiane Rütten

Onder vuur

Veiligheid van beveiligde usb-sticks

Fabrikanten van beveiligde usb-sticks hebben behoorlijk wat trucs bedacht om het ongenode gasten moeilijk te maken je opgeslagen data te bekijken. Maar zoals zo vaak zijn het de details die het verschil maken.

Vanuit het oogpunt van de gebruiker werken usb-safes altijd volgens het volgende principe: eerst voer je een geheime toegangscode in en als die klopt geeft de geïntegreerde controller je toegang tot de data. Dat is meteen ook de enige overeenkomst. Het begint er al mee dat de toegangscode via een apart programma op de pc, via een pinpad of via een biometrische sensor op de stick wordt ingevoerd. En wat de controller precies met de toegangscode doet, kom je als gebruiker niet te weten.

Gelukkig is de procedure waarbij de authenticatie van de gebruiker volledig aan de software op de pc werd overgelaten vrijwel uitgestorven. Deze onveilige methode kwamen we begin 2008 voor het laatst tegen bij de usb-controller USBest UT176 met vingerafdruksensor. De controller wachtte daarbij alleen maar op een 'Sesam, open u'-signaal van de vingerafdruksoftware op de pc. Met het programma PLscsi kon je het identieke signaal echter ook zonder biometrische beveiligingspoespas genereren, waarna je de bestanden gewoon kon lezen.

Bij de nieuwere usb-kluizen is de deur meestal voldoende vergrendeld en krijg je zonder sleutel geen toegang. Als het slot veilig is, gaan moderne krakers echter aan de slag met freesmachines, soldeerbouten en analysesoftware. Fabrikanten van usb-safes hebben hun trukendoos dan ook moeten uitbreiden. Inmiddels maken ze gebruik van gegoten materialen, inbraakveilige behuizingen en uiteenlopende versleutelingsmethodes.

Het belangrijkste aanvalsscenario is het uitsolderen en uitlezen van de flashchips. Als de usb-kluis simpel uit elkaar gehaald kan worden, hebben handige knutselaars hiervoor alleen een speciale soldeerbout, een zelf gebouwd leesapparaat en wat vaardigheid nodig. Maar er zijn ook bedrijven die dit aanbieden als service voor het recoveren van verloren gewaande gegevens. Vaak is dit namelijk de enige manier om gegevens op een defecte usb-stick nog te kunnen benaderen. De kosten hiervoor komen meestal uit op zo'n 500 euro. Als de experts uit de door elkaar geraakte blokken flashgeheugen weer een leesbaar bestandssysteem moeten reconstrueren, wordt het ongeveer twee keer zo duur.

Vulling

Ruim vier jaar geleden bracht Corsair de Padlock op de markt, een verrassend goedkope usb-safe met een ingebouwde pinpad. Maar dit principe had een duidelijke zwakke plek. Met een simpele soldeerbrug kon je de controller ook zonder toestemming van de onafhankelijke pin-unit van stroom voorzien, waardoor je direct bij de data kon. De grootste uitdaging voor de aanvaller zat 'm erin om met een multimeter de juiste pins te vinden.

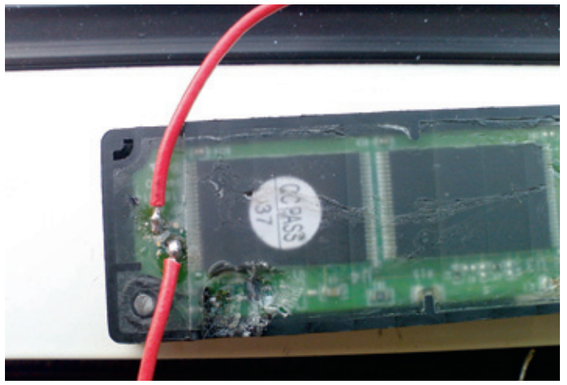
Corsair had het probleem weliswaar onderkend en de behuizingen van latere productiebatches met een gietmassa gevuld, maar het gebruikte materiaal was transparant, zacht en liet zich bovendien vervormen met behulp van warmte. Bewapend met een vijl of frees, een cutter en een soldeerbout hadden we minder dan een uur nodig om de belangrijkste soldeerpunten vrij te maken.

Sindsdien hebben de producenten bijgeleerd. De behuizing van de opvolger Corsair Padlock 2 kun je bijvoorbeeld nog steeds zonder problemen openen, maar de bovenkant van de printplaat met de interessante onderdelen is bedekt door een weerbarstige gietlaag. Als je de schakeling wilt analyseren, moet je eerst de zwarte laag over de pins verwijderen.

Dat is met fijnmechanisch gereedschap en een microscoop echter een kwestie van tijd. Sommige materialen kun je ook met vrij simpel verkrijgbare oplosmiddelen zoals aceton, nitromethaan of trichlooretheen verwijderen. Voor de printplaat en de meeste onderdelen is zo'n behandeling meestal wel funest, maar als je alleen de chips wilt hebben, is het verlies acceptabel.

Bijzonder weerbarstig zijn epoxyharsen zoals die in de Kingston Data Traveler 5000 en de Ironkey worden gebruikt. We konden geen van beide behuizingen openen zonder ze te slopen. De DT5000 bestaat uit een behuizing van hard plastic met een metalen omhulsel, de Ironkey zelfs uit een hol gefreesd aluminiumblok die we met een frees moesten bewerken.

Als je de behuizing van een stick volspuit met vulmateriaal, belemmert dit echter onvermijdelijk het warmtetransport. En als er bij het ontwerpen van de schakeling geen rekening wordt gehouden met de thermische bijzonderheden – bijvoorbeeld door stroombesparende of hittebestendige onderdelen – legt de ingegoten elektronica al snel het loodje.

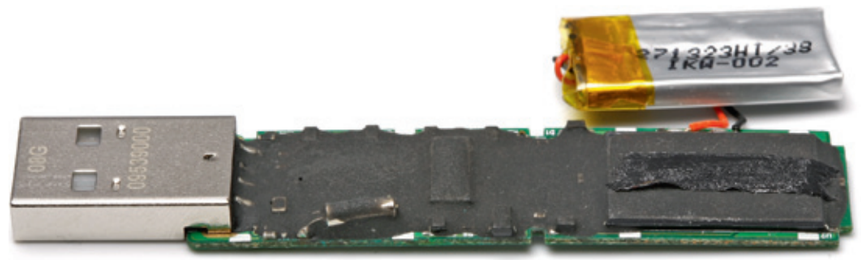


Zo moet het niet! Een transparante en vervormbare gietmassa zoals in de Padlock van Corsair maakt hardwareaanvallen onnodig makkelijk.

Zo kozen de ontwikkelaars van de volgens FIPS 140-2 gecertificeerde Corporate Secure USB Drive van Verbatim en die van de 2009-versie van de SafeStick Business van Blockmaster voor een ook nog eens goedkoper compromis. Ze goten alleen ondoorzichtige hars over de beveiligingskritieke onderdelen. In de Corporate Secure waren dat de controller, die de gegevens met AES-versleuteling in het flashgeheugen opslaat, en de spanningsstabilisator.

De laatste is bedoeld om zogenaamde side-channel attacks moeilijker te maken. Via een techniek die Differential Power Analysis genoemd wordt, kun je onder bepaalde omstandigheden de op een processor draaiende berekeningen achterhalen. Afhankelijk van het ontwerp van de ic's en de manier van programmeren kun je de programmavoortgang zelfs doelgericht beïnvloeden door de spanningstoevoer voor korte tijd te verminderen (Fault Injection). Een paar jaar geleden stapelden de berichten zich op over ongeautoriseerde transacties met verloren pinpassen, waarvan de eigenaren bij hoog en bij laag bezworen dat ze hun pincode aan niemand hadden verraden. Beveiligingsexperts constateerden toentertijd dat de pin-invoer door de toenmalige generatie van bankpaschips, waarbij de programmeurs geen tegenmaatregelen hadden genomen, met Fault Injection omzeild kon worden. Voor zulke geavanceerde aanvallen is echter de directe toegang tot de pins voor de spanningstoevoer van de ic's nodig. Momenteel richt veel beveiligingsonderzoek zich dan ook op dit soort technieken.

De SafeStick-designers goten de gietmassa daarentegen evenmin over de hele printplaat, maar alleen over de pins van de op de printplaat bevestigde flashchips. Dat maakt het weliswaar moeilijker om ze los te solderen, maar kan ook tot problemen leiden. Op de stick met 512 MB wordt namelijk maar een flash-chip gesoldeerd, terwijl



Vaak vind je een harde beschermende laag op de kant van de printplaat met de interessante onderdelen, hier in de verbeterde Padlock 2 van Corsair. Dit maakt het moeilijk om de hardware los te solderen. Maar soms zitten er ook interessante printbanen of eilandjes op de achterkant, waar je ze met draadjes kunt aftappen.

Volgegoten metalen behuizingen uit één stuk, zoals die van de Ironkey, moet je met zwaar gereedschap te lijf gaan.

Ook nadat de zware behuizingen met geweld zijn geopend, zitten de printplaten van de DT5000 van Kingston en van de Ironkey nog in een dik pantser van een ontzettend sterke epoxyhars. Dat maakt een hardwareaanval niet onmogelijk, maar wel heel moeilijk en duur.

er ruimte is voor twee. De SMD-eilandjes (pads) voor de tweede chip op de achterkant blijven in deze versie vrij toegankelijk. In zo'n configuratie zijn de pins van de flashchips echter parallel geschakeld om op datalijnen te besparen. De enige uitzondering is de chip select-pin, waarmee de controller de chip selecteert die aangesproken moet worden, zodat één set datapins voldoende is. Daardoor hoef je alleen de gietmassa van de chip-select-pin te verwijderen. De overige contacten van de flashchip bereik je door dunne elektriciteitsdraadjes op de pads van de vrij toegankelijke onderkant te solderen.

Versleuteling

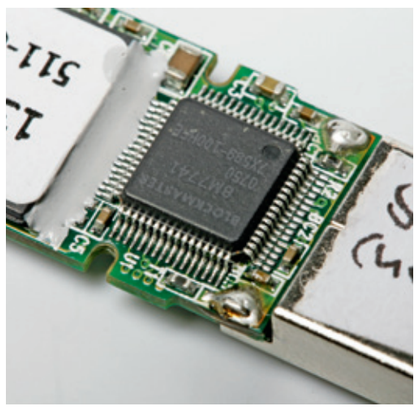
Of er nou wel of geen gietmassa is gebruikt: fysieke beveiligingsmechanismen zijn uiteindelijk hoe dan ook te omzeilen. Dus blijft als laatste bastion de versleuteling over. Aan de ene kant is dit het beveiligingstype met de grootste potentie, want de producenten hebben een hele reeks erkend veilige cryptoalgoritmes tot hun beschikking. Desondanks ontstaan er bij het combineren van de algoritmes tot een werkend cryptosysteem steeds weer kritieke fouten. Als het sleutelbeheer bijvoorbeeld halfslachtig is geïmplementeerd, kun je ook een veilige AES-256-versleuteling omzeilen.

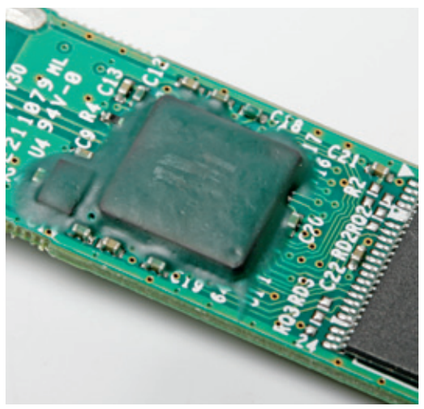
IC-producent Innmax ging bij zijn controller IM7206 wel heel drastisch te werk. De controller werd expliciet aangeprezen met 'AES-128-versleuteling'. Daarbij liet men echter heel handig in het midden wat de controller nou precies met AES versleutelt. Die wolk van geheimzinnigheid zorgde ervoor dat productontwikkelaars van usb-sticks die op de IM7206 gebaseerd waren, trots reclame maakten met AES-data-encryptie. Uiteindelijk bleek echter dat niet de gegevens zelf met AES werden versleuteld, maar alleen de opgeslagen toegangscode. De gegevens zelf werden met een zelfontwikkeld, op XOR gebaseerd algoritme versleuteld, wat wij binnen een paar uur konden kraken.

De koppeling van de toegangscode met het versleutelingsalgoritme alleen kan al op zeer uiteenlopende manieren verlopen en is van doorslaggevende invloed op de beveiliging van het hele systeem. Het zou voor de hand liggen om de toegangscode als key voor de versleuteling te gebruiken. Dit kan gedaan worden met een sleutelafleidingsalgoritme, waarmee uit het wachtwoord een voor het versleutelingsalgoritme geschikte sleutel van een bepaalde grootte berekend wordt.

Als je de afgeleide sleutel direct zou gebruiken om de data te versleutelen dan wel te ontsleutelen, zou de controller echter de complete flashinhoud opnieuw moeten versleutelen als je alleen je wachtwoord verandert. Om dit te voorkomen, is het gebruikelijk geworden om de data met een onveranderlijke masterkey te versleutelen en deze samen met het gebruikerswachtwoord versleuteld in de controller op te slaan.

Bij een onveilige variant van deze methode slaat de controller een vergelijkingskopie van de geheime toegangscode op en ontsleutelt bij een positief resultaat de gegevens met de in leesbare tekst opgeslagen masterkey. Met een – behoorlijk ingewikkelde en dure – chipanalyse kun je in zo'n geval het wachtwoord en de masterkey waarschijnlijk uitlezen en de flashdata ontsleutelen. Dat is dan alleen nog een kwestie van geld.





Selectief ingieten van veiligheidskritieke onderdelen – links de flashchip van de SafeStick, rechts de controller van de Kingston DataTraveler BlackBox – is een compromis tussen resistentie tegen hardwareaanvallen aan de ene kant en betere warmteafvoer en lagere productiekosten aan de andere kant.

Grote geheimen

Om de versleutelbeloftes tenminste met een steekproef aan de tand te voelen, hebben we datarecoverybedrijf Attingo (met vestigingen in Nederland, Duitsland en Oostenrijk) gevraagd om de flashinhoud uit te lezen van twee beveiligde usb-sticks, waarvan de chips relatief makkelijk los gesoldeerd konden worden. Dit zijn de oude versie van de Blockmaster SafeStick en de Verbatim USB Executive Se-

Een gietmassa van epoxyhars is bijzonder krachtig en bestand tegen oplosmiddelen. Maar met het juiste gereedschap kun je ook die verwijderen, zij het met veel moeite.

cure. Uit een korte analyse van de data bleek dat de inhoud bij beide met uitzondering van een gebied voor de operating data van de flashcontroller daadwerkelijk versleuteld waren. Met welk algoritme dat gebeurt, kan echter niet nader bepaald worden zonder omvangrijke analyses met meerdere identieke exemplaren en verschillende sets testdata.

Helaas staat geen van de producenten een blik achter de schermen van hun implementatie toe. Belangrijke beveiligingscertificeringen voor gebruik in de financiële sector en voor overheidsinstanties eisen zelfs uitdrukkelijk dat belangrijke delen van het cryptosysteem geheim moeten blijven. De versleuteling van usb-sticks blijft dus vooral een kwestie van vertrouwen.

Als de encryptie in orde is, zou je eigenlijk van een fysieke beveiliging van het inwendige van een beveiligde usb-stick kunnen afzien. Het is in het beste geval alleen met een behoorlijke financiële investering in de orde van grootte van meerdere 10.000 tot 100.000 euro mogelijk om met behulp van chip-reverse-engineering de geheime masterkey aan de controller te ontfutselen. Bij een veilig cryptosysteem is zelfs dat onmogelijk. Het loont voor criminelen dan eerder om het doelwit af te persen of zijn pc met een Trojaans paard te besmetten. Tenslotte zijn de gegevens op die pc gewoon uit te lezen als de juiste pin-code is ingevoerd.

Resistente behuizingen en ingegoten printplaten hebben dus zowel voor- als nadelen. Aan de ene kant verhogen ze de moeite die een aanvaller moet doen om de usb-kluis te kunnen kraken – als ze goed zijn gemaakt zelfs behoorlijk. Maar aan de andere kant maken ze het ook voor onafhankelijke experts moeilijker om de veiligheid te beoordelen. Deze missen zo misschien een zwakke plek die voor een aanvaller met meer tijd en geld bij wijze van spreken zonneklaar is. Hoe veilig een 'usb-safe' echt is, wordt door de geheime constructieplannen helaas pas bij een serieuze aanval duidelijk. (mja)

"Versleuteling is een uitdaging"

Bedrijven bieden het uitlezen van flashchips als een service aan klanten aan. In een gesprek met c't beoordeelt forensisch expert Robbert Brans van Attingo de veiligheid van usb-kluizen uit het oogpunt van datarecovery.

c't: Hoe moeilijk is het om gegevens van flashchips te benaderen?
Robbert Brans: Het is technisch niet bijzonder moeilijk om de gegevens van een chip uit te lezen. Daar zijn commerciële leesapparaten voor beschikbaar. Een potentieel probleem is wel dat er voor veel flashchips die in de handel zijn geen documentatie beschikbaar is. Wij hebben ook al chips gezien die als meerdere afzonderlijke chips in een gezamenlijke behuizing benaderd moeten worden. De benodigde parameters moesten we soms raden.

Er zitten echter meer verwerkingsstappen tussen de chipinhoud en de gegevens die de gebruiker weggeschreven heeft. De controller zorgt bijvoorbeeld voor een gelijkmatige belasting van alle memory pages, foutherkennings- en -correctieinformatie, en het beheren van defecte memory pages en de bijbehorende reserve-pages.

Bovendien verdeelt de controller de gegevens zomogelijk over meerdere chips om de leessnelheid te verhogen. Er zijn ook controllers die een dataversluierings- of encryptielaag toevoegen. Met al deze extra verwerkingsstappen moeten wij rekening houden om uit de datablokken in de flashchips het oorspronkelijke bestandssysteem te kunnen reconstrueren.

c't: Hoe schat je de veiligheidswinst door het gebruik van gietmateriaal in?
Brans: Ingieten biedt geen absolute beveiliging, aangezien het om 'security by obscurity' gaat. Tweecomponent-kunstharsen zijn moeilijk te verwijderen, materialen op basis van siliconen of rubber en thermoplasten eerder makkelijk. Met de nodige inspanning kun je echter elke schakeling vrijmaken. Wij gebruiken daar beproefde reverse-engineeringtechnieken voor. Het ingieten maakt het herstellen van de data wel een stuk duurder. Bovendien kun je bij deze geheugensticks meestal duidelijk zien dat ze open gemaakt zijn, waardoor het moeilijk wordt om ze onopgemerkt uit te lezen.

c't: In hoeverre vormt encryptie een probleem bij datarecovery?

Foto: Attingo Datarecovery, www.attingo.com

Brans: Versleuteling betekent altijd een extra uitdaging. Ook bij algoritmes die als veilig beschouwd worden, worden soms fouten gemaakt, maar als de implementatie en de passphrase veilig zijn, hebben wij geen kans. Dan kunnen we de gegevens hooguit uitlezen, maar niet ontsleutelen. Verrassend vaak zijn de privé-sleutels van de controllermodellen echter bekend, omdat ze voor de complete modelserie identiek zijn.

c't: Waar moet je bij een aankoop op letten?
Brans: Ik denk dat het praktisch onmogelijk is om als gewone klant de beveiliging van de aangeboden usb-safes te beoordelen. Ook experts moeten vaak enorme inspanningen verrichten om de veiligheid van een bepaald product te toetsen, omdat de aanbieder geen details over de werking prijsgeeft. Er zaten zelfs implementatiefouten in usb-safes van bekende producenten die volgens FIPS 140-2 Level 2 gecertificeerd waren. Bij het betreffende model hoefde de AES-encryptiehardware niet aangevallen te worden, omdat de code voor het vrijschakelen van de usb-stick altijd dezelfde was.

Ik zou een zorgvuldig opgebouwd systeem met volledige constructieplannen en onafhankelijk geteste, open sourcecode van alle hierop draaiende software het beste vinden, maar zo'n product ben ik nog niet tegengekomen. Deze situatie kun je op dit moment alleen bereiken met opensource softwareoplossingen zoals TrueCrypt in combinatie met gewone usb-sticks. Het beveiligingsniveau van zo'n combinatie is veel makkelijker in te schatten en beveiligingslekken kunnen achteraf worden gedicht. Wat gemak en platformonafhankelijkheid betreft, is een dergelijke oplossing natuurlijk niet te vergelijken met een usb-safe.

c't