Verantwoorde onthullingen #6

Dismantling Megamos. Hoe Volkswagen de Radboud publicatie over gekraakte autosleutels tegenhield.

Toen de Radboud universiteit in 2008 de Mifare Classic RFID chip kraakte, spande chipfabrikant NXP een rechtszaak aan om publicatie tegen te gaan. Radboud won: een triomf voor academische vrijheid en Responsible Disclosure. Hoe anders verging het de academische security onderzoekers in 2013 in Engeland. Daar werd hun publicatie over een gekraakte elektronisch autosleutel door de rechter tegengehouden. Aanklager was niet de maker van de chip of het algoritme, maar een gebruiker: Volkswagen. Hoe was dit mogelijk?

Al meer dan tien jaar zet de Digital Security Group zich onder leiding van professor Bart Jacobs in voor verantwoorde onthullingen. Onder de inmiddels veertig onderzoekers bevinden zich veel specialisten in RFID systemen. Dit zijn chips die middels elektromagnetische golven op afstand zijn uit te lezen, zoals de Mifare classic die wordt gebruikt in toegangspassen en de OV-chipkaart. Vanuit academische interesse en maatschappelijk belang, zijn al veel smartcards, tokens en e-readers onder hun handen geopend. Eind 2012 is het elektronische auto slot aan de beurt.

Zo'n slot werkt als volgt. Als je de fysieke sleutel in het slot steekt, stuurt een lezer in dat slot een signaal naar een chip in de autosleutel. Eerst gaan er wat nummers heen en weer om te kijken of de chip en lezer echt zijn, vervolgens geven ze elk een nummer dat uniek is voor dat specifieke slot en die sleutel van die auto. Klopt alles, dan kan de auto gestart worden. Draden lostrekken en starten, zoals in de film, kan dan niet meer. Hoe deze berekeningen worden uitgevoerd is geheim.

Roel Verdult – die ook de Mifare classic kraakte – richtte zich op de Megamos Crypto chip. Die wordt gebruikt in de sloten van Porsche, Audi, Bentley, Lamborghini en alle Volkswagens. Op internet kocht hij een Tango Programmer. Met dit apparaat kun je sleutel en slot programmeren. Het bevat het geheime algoritme waarmee de berekeningen worden uitgevoerd. Door steeds de input en output te variëren en te kijken wat er gebeurde - reverse enginering - kwam hij achter het algoritme.

Nu kon hij elke elektronisch sleutel van auto's met Megamos startonderbrekers namaken. Maar dat was natuurlijk niet zijn doel. Hij wilde zijn bevindingen samen met collega Barış Ege en Flavio Garcia van Birmingham University publiceren op de aanstaande USENIX computer security conferentie. Die was pas in augustus 2013, dus er was genoeg tijd om de eigenaar van het systeem in te lichten zodat die tijdig maatregelen kon nemen.

Alleen, wie is die eigenaar? Het algoritme is van het bedrijf Thales. Die heeft een ander bedrijf - EM - toestemming gegeven het te gebruiken in hun RFID chips. Weer een ander bedrijf - Delphi - gebruikt deze chips in hun sloten en sleutels en verkoopt dit systeem aan de fabrikanten die het in de auto's installeren. De onderzoekers gingen voor de chipleverancier en benaderde EM in november 2012. Ondertussen gingen ze schrijven aan hun artikel "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer". Deadline voor de Usenix conferentie: 25 juni.

EM reageerde pas in februari en op 6 juni was er dan eindelijk een meeting. Delphi was er ook bij. De leveranciers van de chips en de sloten vroegen de onderzoekers of zij bepaalde delen van het algoritme niet wilden publiceren. Op zich lastig, want zo konden ze niet precies laten zien wat het probleem was, en bewijzen dat ze het algoritme ook werkelijk hadden achterhaald, maar ze wilden het in het belang van deze bedrijven wel overwegen. Aan het eind van de meeting kregen de onderzoekers een e-mail van een advocaat van Volkswagen. De autofabrikant heeft de High Court of England and Wales gevraagd een rechtelijk bevel uit te voeren en publicatie tegen te gaan. Dat verzoek is de dag ervoor ingewilligd.

De zitting is 25 juni, de dag van de deadline van hun artikel. De aanklager beroept zich op de Human Rights Act. In artikel 12, over de vrijheid van meningsuiting, staat namelijk dat een rechter een publicatie mag tegenhouden als je daar overtuigende argumenten voor hebt. Hij stelt dat het algoritme vertrouwelijke informatie is. Het onthullen ervan schaadt de vertrouwelijkheid en faciliteert diefstal van miljoenen Volkswagens. Het algoritme moet onrechtmatig verkregen zijn door de maker van de Tango Programmer. Wie de Bulgaarse site van de verkoper Scorpio bezoekt, ziet meteen dat dit illegale software is, aldus de advocaat van Volkswagen.

De verdediging stelt dat de onderzoekers het algoritme hebben achterhaald middels legale apparatuur en methoden: reverse enginering. Onthulling van het beveiligingslek is juist wel in het publieke belang: als criminelen het kunnen weten, moet ook het publiek er van op de hoogte zijn. Geheel volgens de Leidraad Responsible Disclosure van het NCSC hebben de onderzoekers EM zes maanden de tijd gegeven er iets aan te doen. Het is niet de schuld van de onderzoekers dat Volkswagen niet is ingelicht. Bovendien: hoe kan het dat Volkswagen hen aanklaagt? Zij zijn immers niet de eigenaar van het algoritme.

Rechter Justice Birss vindt dat Volkswagen zeker gezien kan worden als aanklager en wijst op jurisprudentie. Uit de zogenaamde Cream Holdings zaak kwam namelijk naar voren dat als de oorspronkelijk gedupeerde van een publicatie – in dit geval Thales - een sterke zaak heeft, een ander ook in diens plek kan aanklagen als dat nodig is. Maar eigenlijk is Volkswagen volgens hem ook gedupeerde: “Their products depend on the secrecy of the Megamos Crypto algorithm.”

Aan de rechter het oordeel of deze onthulling verantwoord is. Hij vindt van niet, want met deze publicatie wordt een nieuwe manier om auto’s te stelen publiekelijk bekend. Hij vindt academische vrijheid een groot goed, maar “I think the defendants' mantra of "responsible disclosure" is no such thing. It is a self-justification by defendants for the conduct they have already decided to undertake and it is not the action of responsible academics.” Hij verbiedt de onderzoekers hun artikel te publiceren.

Verdult, Garcia en Ege kunnen het artikel ook niet meer aanpassen, want de deadline is die dag en het kan niet nog een keer door de peer review. Typisch voor cryptografen publiceren ze in plaats daarvan de hashfunctie van hun tekst, die het artikel terugbrengt tot een unieke code van 128 tekens. Mocht later nog eens iemand de Megamos kraken, dan kunnen zij aantonen hoe zij dat al eerder hebben gedaan.

Twee maanden later verschijnt Verdult toch op de USENIX Security Conference. Zonder artikel, maar wel met een presentatie die is gecheckt door juristen en begint met disclaimers. Hij mag geen technische details geven en geen vragen beantwoorden. Zijn verhaal gaat over hoe ze andere elektronische autosleutels hadden gekraakt, Responsible Disclosure en reverse engineering. Tussendoor zegt hij dat het met Megamos net zo ging. Op de laatste slide staat “Historical claim” met de hash van het artikel dat hij daar had willen presenteren.

```
9d05ba88740499eecea3d8609174b444
43683da139f78b783666954ccc605da8
4601888134bf0c23ba46fb4a88c056bf
bbb629e1ddffcf60fa91880b4d5b4aca
```

SHA-512 hash van het artikel

We zijn inmiddels alweer een half jaar verder. Het artikel is nog steeds niet gepubliceerd en ik ben benieuwd of Volkswagen inmiddels iets heeft gedaan met het gratis advies. Ik benader de Nederlandse afdeling en kom uit bij pr manager Ralf Dennissen. Wat vindt hij van het bovenstaande artikel? En zijn er nog concrete maatregelen genomen, zoals het terugroepen van auto’s naar de garage om hun slot te vervangen? Na wat heen- en weer mailen krijg ik het volgende antwoord:

“Aan Volkswagen en Thales is een voorlopige gerechtelijke bevel toegewezen dat publicatie verbiedt van het betreffende algoritme en wat andere informatie. Deze zaak loopt nog altijd en er zal door de rechtbank een definitief oordeel geveld worden als de betrokken partijen er voor die tijd niet onderling uitkomen.” Maar kan ik hieruit afleiden dat er geen concrete veiligheidsmaatregelen zijn genomen? Helaas, meer dan dit kan hij mij niet zeggen. Security by obscurity. Zucht…

Chris van ’t Hof (www.cvth.nl)

Bronnen:

[1] Uitspraak gerechtshof: http://www.bailii.org/ew/cases/EWHC/Ch/2013/1832.html
[2] Presentatie Verdult: https://www.usenix.org/conference/usenixsecurity13/dismantling-megamos-crypto-wirelessly-lockpicking-vehicle-immobilizer