2. Radboud opent de poorten

Onderzoekers kraken de crypto van de Mifare Classic

Deze zaak is in meerdere opzichten een klassieker. De Mifare Classic chip werd in 2008 gebruikt in miljarden toegangs- en betaalsystemen, waaronder ook de OV-chipkaart en toegangspassen tot overheidsgebouwen. De onderzoekers die de chip wisten te kraken, ontketenden een grote maatschappelijke controverse. De rechtszaak die erop volgde, biedt interessante jurisprudentie voor komende zaken. We zien ook hoe beveiliging bepaald wordt door bedrijfseconomische afwegingen: zolang de schade meevalt, loont het niet over te stappen op een duurder systeem. Maar bovenal is dit een zaak die bepalend is geweest voor hoe we nu in Nederland denken over verantwoorde onthullingen.

Hier ontmoeten we ook iemand die we in dit boek nog vaker zullen tegenkomen: professor Bart Jacobs van de Digital Security Group. De eerste keer dat ik Jacobs sprak was in 2004. Ik was toen onderzoeker bij RAND en deed met een collega interviews voor een overzicht van de Nederlandse R&D in informatiebeveiliging. We waren natuurlijk eerst naar de technische universiteiten geweest. En oh ja, iemand had gezegd dat we ook nog even langs een professor van de Radboud moesten, want die 'deed iets' met smartcards. Toen we twee uur later buiten stonden realiseerden we ons dat hier in Nijmegen iets bijzonders ging gebeuren. De kersverse hoogleraar Security & Software Correctness had zojuist elf promotieplaatsen gecreëerd voor onderzoek naar de beveiliging van smartcards. Daarnaast was hij met de andere universiteiten een hele opleiding aan het optuigen voor computer security-onderzoekers: het Kerckhoffs Instituut, vernoemd naar de 19^{e}eeuwse cryptograaf.

Als ik hem op 11 september 2013 weer bezoek, gaat net het nieuwe studiejaar van start. Overal zie ik posters en vlaggen met K3rckhoffs 1nst1tute. Er is nu naast de masteropleiding Digital Security ook een bachelor opleiding, waar zich zeventig studenten hebben aangemeld. Volgens de informatie op de site leren ze naast basisvakken als cryptografie, websecurity en netwerksecurity ook "als een aanvaller te denken door zelf kwetsbaarheden op te zoeken en ook te hacken". Bijvoorbeeld door 'social engineering', oftewel eerst het vertrouwen winnen van mensen om ze vervolgens geheimen te ontfutselen, zoals wachtwoorden. Krijgt hij nooit kritiek, omdat hij mensen opleidt tot hackers? Nee, daar wordt volgens Jacobs nooit moeilijk over gedaan. Bovendien krijgen de studenten ook juridische en ethische vakken.

Er is in de tussentijd veel gebeurd. Jacobs is uitgegroeid tot een bekende figuur in de media. Als er iets gehackt is of een systeem faalt, weten journalisten hem te vinden voor een goede quote. Jacobs is tegelijkertijd voorzitter van de raad van advies van Bits of Freedom en lid van de Cyber Security Raad van het Ministerie van Veiligheid en Justitie – actiegroep versus de overheid. Het is volgens hem ook typisch Nederlands om dissidenten te incorporeren: hackers worden aangenomen en actiegroepen mogen mee overleggen. Dat vindt hij een goede zaak. Maar bovenal hecht hij veel aan zijn onafhankelijke positie als hoogleraar. De universiteit laat hem ook vrij in zijn uitspraken en heeft hem twee keer beloond met een mediaprijs. Hij is ook benoemd tot Officier in de Orde van Oranje-Nassau. En in 2012 ontving hij een prestigieuze Advanced Grant ter waarde van 2,5 miljoen euro van de Europese Onderzoeksraad.

In 2004 had ik geen flauw idee wat de professor van plan was met de smartcards, maar inmiddels weet ik beter. Na RAND ging ik werken bij het Rathenau Instituut, onder andere aan het dossier RFID: Radio Frequency Identitification, oftewel chips die communiceren via radiogolven. Als socioloog en elektricien zag ik meteen hoe deze kleine chipjes een belangrijke sleutel zullen worden tussen menselijke en digitale netwerken. Pasjes, poortjes, scanners en tags; alles krijgt een nummer en we gaan leven in een internet van dingen. In ons onderzoek was de OV-chipkaart een bijzonder vruchtbaar onderwerp. Vele interviews, kamerstukken, bijeenkomsten en krantenartikelen verder begreep ik hoe ingewikkeld het is om een elektronisch kaartje in te voeren in het Nederlandse polderlandschap. Met dus wat meer kennis van zaken zit ik nu weer tegenover professor Jacobs.

Zijn onderzoeksgroep, de Digital Security Group kent inmiddels veertig leden. Een van hen is Roel Verdult. Eind 2006 is hij op zoek naar een afstudeerproject. Begeleider Flavio Garcia zet hem aan het werk met de zogenaamde 'Ghost'. Dit is een apparaat dat een RFID-smartcard kan nadoen. Het ding was al sinds het begin van de groep in gebruik, maar werkte niet goed door diverse bugs. De

student gaat aan de slag en een half jaar later heeft hij de Ghost aan de praat. Om dit ook te demonstreren geeft Garcia hem een opdracht: “Probeer hier op het terrein gratis te parkeren.”

Het toenmalige parkeerterrein van de Radboud Universiteit werkte namelijk met een smartcard-systeem gebaseerd op RFID. Dat werkt als volgt. Bezoekers krijgen een pasje met daarin een chipje dat een antenne heeft in de vorm van een spoeltje. Naast de slagboom staat een leesapparaat dat telkens een signaal uitzendt van 13.56 MHz. Houd je het pasje erbij, dan wekt die straling in het spoeltje voldoende stroom op om het chipje aan de praat te krijgen en informatie heen en weer te sturen. Die informatie blijkt bij dit systeem relatief simpel: een nummer zonder enige cryptografische bewerking. Verdult weet de Ghost een geloofwaardig nummer te laten produceren en de poort gaat open.

Als in mei 2007 student Gerhard de Koning Gans op zoek is naar een afstudeeronderwerp, wordt hij ook op het project gezet. Hij komt met een alternatief voor de Ghost: de Proxmark III. Die kan niet alleen de kaart nadoen, maar ook het apparaat dat de chip uitleest. Nadeel is echter dat het niet dezelfde taal spreekt als de chips die ze onderzoeken. Ze moeten dus het hele ding herprogrammeren en gaan samen aan de slag. Jacobs hoort van de vorderingen en weet nog wel een betere target: de OV-chipkaart. Die werkt namelijk met dezelfde soort chips: de Mifare van NXP. Hij had de uitgever van de kaart, Translink Systems, al eens benaderd voor een test. Maar die reageerde volgens de professor in de trant van “Sodemieter op, alles is veilig”. Nu kan hij de twee studenten erop zetten om te kijken of dat ook werkelijk zo is.

In de OV-chipkaart worden twee type chips gebruikt. In de wegwerpkaart zit een Mifare Ultralight. Net als de parkeerkaart geeft die gewoon een nummer af dat door de lezer bij het OV-poortje wordt herkend. Die lezer geeft dan een signaal terug aan de chip waarmee hij zichzelf uitzet en niet nog een keer gebruikt kan worden. Roel zet de Ghost aan het werk als wegwerpkaart. Die doet het. Hij kan het apparaat bovendien zo programmeren dat hij zichzelf niet uitzet na gebruik. Hiermee kan hij dus oneindig vaak gratis reizen. Iets dergelijks was al eens eerder gedemonstreerd, dus niet zo spannend.

De gewone OV-chipkaart is een stuk spannender. Die heeft namelijk een zwaardere chip: de Mifare Classic. Die geeft niet zomaar een nummer af, maar doet cryptografische bewerkingen met het zogenaamde Crypto-1 algoritme. De lezer geeft de chip een nummer, waar hij zijn geheime algoritme op loslaat en pas als die het juiste nummer teruggeeft kan de communicatie starten. Hier schiet de Ghost te kort. Maar De Koning Gans heeft zijn Proxmark inmiddels zover dat deze ook de taal van de chip verstaat. Nu kunnen ze zowel de chip als de lezer nabootsen, die eindeloos met elkaar laten communiceren en zo kijken naar patronen. Elke dag komen ze dichter bij het vinden van het geheime algoritme.

Hier staat meer op het spel dan alleen het kunnen kraken van een chip, het gaat ook om het bevestigen van Kerckhoffs principe. Auguste Kerckhoff, de man naar wie het instituut is vernoemd, stelde namelijk in 1883 dat een systeem van versleuteling even veilig moet zijn, als alles behalve de sleutel publiek bekend is. Te vaak gaan mensen er namelijk van uit dat als anderen niet weten hoe het systeem werkt, ze het ook niet kunnen kraken. De meeste cryptografen zijn het niet mee eens met deze ‘Security by obscurity’. De werking moet openbaar zijn, zodat die getest kan worden. Het geheim moet in de sleutel zitten: die moet zoveel mogelijkheden hebben, dat die niet binnen redelijke tijd te raden is. Pas dan is een systeem veilig.

Hun project krijgt steeds meer interesse van de rest van de groep. Er hangt iets in de lucht. Jacobs: “Dat heeft zijn eigen dynamiek en daar ga ik niet in sturen. Maar ik werd me er wel snel bewust van hoe gevoelig het was. Die chip zat niet alleen in de OV-chipkaart, maar ook in de pas die toegang geeft tot ministeries.” NXP heeft in die tijd wereldwijd al meer dan een miljard chips verkocht voor allerhande toegangssystemen. Hij besluit daarom alle betrokken onderzoekers samen in één kamer te zetten. Naast Verdult, De Koning Gans en hun begeleider Garcia ook Jaap-Henk Hoepman, Ravindra Kali, Vinesh Kali, Ruben Muijrers, Peter van Rossum en Wouter Teepe. Iedereen kan de universiteit binnenlopen en er mag niets gelekt worden. Online communicatie wordt versleuteld. “We konden pas naar buiten komen als we echt resultaten hebben, dus: kopiëren, saldo veranderen, dat soort dingen”, aldus Jacobs.

Terwijl de onderzoekers druk aan het puzzelen zijn in hun geheime kamer, gaat Nederland langzaam maar zeker over op de OV-chipkaart. Steeds meer stations en voertuigen worden voorzien van

leesapparatuur waarmee reizigers kunnen in- en uitchecken. Rotterdam loopt voorop, met als eerste volledige dekking in metro en trams. In Amsterdam starten de eerste proeven. De ambitie is dat binnen een paar jaar iedereen met één kaart door het hele openbare vervoer kan. De regie wordt ondergebracht in een consortium van de vervoersbedrijven onder de naam Trans Link Systems, want de kaart moet het niet alleen de reizigers makkelijker maken, maar vooral ook de vervoerders. Zo hebben ze een meer realistisch overzicht van waar er gereisd wordt, zodat ze het aanbod kunnen aanpassen en de verschillen in kosten en inkomsten beter verdelen. En als je dan zo makkelijk een kaartje kunt kopen, waarom niet ook een broodje? Dit wordt het nieuwe betalen.

De eerste gebruikersonderzoeken in Rotterdam zijn positief. Reizigers vinden de kaart makkelijker dan de strippenkaart en zien de voordelen van de poortjes: zo houden we die vervelende junks en zwervers uit het OV. Maar er is ook kritiek. In Amsterdam wordt het Gemeentelijk Vervoersbedrijf op de vingers getikt door het College Bescherming Persoonsgegevens. De vervoerder wil namelijk reclame gaan koppelen aan reisgedrag, zonder toestemming van de reiziger. Bovendien zijn die gegevens niet echt veilig opgeslagen volgens het CBP. Bekijken we de nieuwsberichten uit die periode, dan zien we vooral journalisten die bij de poortjes wachten tot iemand problemen heeft met in- en uitchecken: microfoon erbij en je hebt een leuk item. Partij Groen Links blijkt kritisch en zet een site op: ov-chipklacht.nl. De partij die zich van oudsher inzet voor goed openbaar vervoer, krijgt al snel vijfduizend klachten binnen en roert zich steeds vaker in Kamerdebatten over de kaart.

Dan is er nieuws uit Duitsland. Karsten Nohl van de universiteit van Virginia en Henryk Plotz van de Hamboldt universiteit in Berlijn beweren dat ze de Mifare Classic hebben gekraakt. Ze hebben het heel anders gedaan dan de jongens uit Nijmegen: namelijk met chip-slicing. Door de kaart laagje voor laagje af te schrapen worden delen van de schakeling zichtbaar. Hier zouden ze het verborgen algoritme uit hebben afgeleid. In december 2007 presenteren ze hun bevindingen tijdens de jaarlijkse bijeenkomst van de Computer Chaos Club. Niet alles, want ze zijn bang voor een rechtszaak. Het is ze nog niet gelukt zelf een kaart te maken, maar de zaak wordt breed uitgemeten in de media. Nu wordt het wel erg moeilijk voor de onderzoekers van de Digital Security Group om stil te blijven.

Jacobs wordt gevraagd om een reactie op de Duitse kraak. Verdult wil zijn bevindingen eigenlijk pas publiceren bij zijn afstuderen, maar nu moet hij wel iets onthullen. Zij kunnen immers wel een functionerende kaart produceren, de Duitsers niet. Jacobs besluit Koen de Regt van RTL een primeur te geven: de Ghost die werkt als wegwerpkaart. Verdult mag het zelf demonstreren in de metro van Rotterdam. Jacobs raadt hem wel aan zich niet te laten verleiden tot politieke of andere verreikende uitspraken. “Blijf bij je expertise”, zegt hij tegen de jonge onderzoeker.

Het RTL-nieuws van maandag 14 januari 2008 opent met ‘Gratis metro met gehackte OV-chipkaart’. De Regt heeft er een mooi item van gemaakt van maar liefst acht minuten. We zien Verdult bij de poortjes in- en uitchecken. Met zijn laptop past hij steeds weer het saldo van zijn Ghost aan. Dan zien we een interview met Jannemiek Zandee van Trans Link Systems die beweert dat de kaart toch echt veilig is. Op de achtergrond blijft Verdult rondjes lopen door de poortjes die nog steeds geen foutmelding geven. Een sterk staaltje journalistieke beeldretoriek.

Het item leidt tot Kamervragen. De woensdag erop wordt een hoorzitting belegd met diverse beveiligingsexperts, waaronder ook Verdult en Teepe. Een debat over de kaart stond al gepland op donderdag en nu richt alle aandacht zich op staatsecretaris Tineke Huizinga. Ze gaat dan weliswaar niet over Trans Link Systems - een onafhankelijk consortium van de vervoersbedrijven - maar er is zoveel subsidie ingegaan, dat de staat wel wat mag eisen. Bovendien is een goed openbaar vervoer van landsbelang en als er zoveel partijen bij betrokken zijn, zal toch iemand de regie op zich moeten nemen. De oppositie vindt dat zij dat moet doen.

Huizinga is dan nog niet zo lang staatsecretaris van Verkeer. Ze was na een moeizame kabinetsformatie in 2007 door de Christen Unie dankzij voorkeursstemmen naar voren geschoven. Eigenlijk weet ze vrij weinig van technologie en vervoer en nu krijgt ze dit hoofdpijndossier. Huizinga vraagt daarom voorafgaand aan het Kamerdebat de Radboudonderzoekers om raad. Hun advies: “Laat een onafhankelijke contra-expertise uitvoeren. Je hoeft ons niet te geloven, hoor…”.

In het Kamerdebat van 17 januari belooft de staatssecretaris een “aanvalsplan” om “het beschadigde beeld van de OV-chipkaart te herstellen”. In het plan komen afspraken met de betrokken partijen over beveiliging, privacy, tarieven, distributie, reisgemak en “de wijze waarop de regie op de voortgang van het invoeren van de OV-chipkaart blijvend wordt georganiseerd”. De vervoerders en

consumentenorganisaties onderschrijven de inhoud van dit plan en presenteren het gezamenlijk op 29 februari. Daarnaast wordt onderzoek gestart naar de veiligheid van de kaart, oftewel de contra-expertise. Dit wordt uitgevoerd door TNO.

TNO komt binnen een paar weken tot de conclusie dat de wegwerpkaart weliswaar is na te maken, maar fraude uiteindelijk zal worden ontdekt door de achterliggende administratie die dan de kaart blokkeert. Oftewel: voor elk ritje een nieuwe kaart maken, is niet echt een criminele business case. Bovendien zijn daar geavanceerde middelen voor nodig. Er is volgens de onderzoekers dus niets te vrezen. Dan maar nog een onderzoek, dit keer van de Engelse Information Security Group, Royal Halloway, van University of London. Die komt tot dezelfde conclusie. Bovendien hebben de onderzoekers daar al langer ervaring met de Oystercard. Die werkt met hetzelfde systeem en daar is ook niet mee gefraudeerd. Mocht er dan toch gefraudeerd worden, dan moeten de vervoersbedrijven een plan hebben om over te stappen naar een nieuwe chip, aldus de contra-expertise.

De kamer blijft echter kritisch naar Huizinga. In de tweede week van maart staat een hoorzitting gepland, waarin Huizinga de resultaten van het onderzoek mag toelichten. Die zitting komt er echter niet, want ze mag zich dan weer tegenover de Kamer verantwoorden. Het is de Digital Security Group namelijk vrijdagmiddag 7 maart gelukt de Mifare Classic en dus ook de gewone OV-chipkaart te kraken en ze willen ermee naar buiten komen. De bewindsvrouw heeft slechts een dag om zich voor te bereiden.

Wat was er gebeurd in de geheime kamer aan de Radboud Universiteit? Verdult en zijn collega's hebben met hun zelfgemaakte kaartlezer en kaart eindeloos in- en uitgecheckt. De enen en nullen gaan heen en weer en worden steeds weer bewerkt volgens het geheime Crypto 1 algoritme. Ze hebben al ontdekt dat ze zelf een sleutel in een blanco kaart kunnen zetten en daarmee allerlei variaties kunnen uitproberen: eerst een sleutel van alleen nullen, daarna een met alleen maar enen en vervolgens allerlei variaties daar tussenin. Dit is reverse engineering: door het gedrag van een apparaat na te bootsen erachter komen hoe het werkt.

Verdult houdt steeds de in- en output bij in een tabel. Als ze alle mogelijkheden willen proberen moeten ze 2^{48} keer de sleutel veranderen. Dat zou volgens hun eigen berekening 44.627 jaar kosten. De Koning Gans ontdekt echter dat de random generator geen willekeurig getallen genereert, maar telkens op dezelfde manier opstart en dan in twee uur een rondje langs dezelfde getallen maakt. Zo kunnen ze het aantal mogelijke sleutels drastisch terugbrengen tot 2^{16}, oftewel 65.536 keer. Dan kan het in een paar uur. En zo komen ze er op 3 maart achter welke berekening de chip op de sleutel loslaat. Ze hebben het achterliggende algoritme gevonden dat dan al vijftien jaar geheim is gehouden. Om dit te kunnen demonstreren, maken ze zelf een eigen OV-chipkaart. Op 7 maart 2008 is deze af.

De vondst kan een mooi artikel worden voor ESORICS, het European Symposium on Research in Computer Security in oktober dat jaar. Met een peer review procedure van zeker een half jaar is de deadline akelig dichtbij. Echt veel tijd voor een verantwoorde onthulling hebben ze dus niet. Dan ontdekken ze nog iets anders, wat nog veel alarmerender is: de toegangspassen voor de overheidsgebouwen zijn nog veel makkelijker na te maken. Waar elke OV-chipkaart nog een eigen sleutel heeft, wordt die bij deze passen nauwelijks gevarieerd. Sommige gebouwen hebben zelfs maar één sleutel voor alle passen. Met deze kennis kan iemand dus zomaar ongemerkt een militaire basis, bank of de Tweede Kamer binnenwandelen.

Jacobs belt daarom die vrijdag meteen met Roelof de Wijkerslooth, de voorzitter van het College van Bestuur van de universiteit en zegt: "Ik druk op de rode knop." Een vooraf afgestemd plan treedt in werking. De collegevoorzitter verschijnt binnen tien minuten op het lab, ziet hoe de onderzoekers met hun eigen pas een deur openen en neemt direct contact op met het Ministerie van Binnenlandse Zaken. De volgende dag, zaterdag, krijgt de Digital Security Group bezoek van het Nationale Bureau voor Verbindingsbeveiligingen. Dat zijn de rijkscryptografen van de AIVD. Ze zijn geschokt dat dit zomaar kan, maar ook gerustgesteld dat de bevindingen niet direct worden gepubliceerd. Zondag worden TLS en NXP ingelicht om tijdig maatregelen te nemen. Na de hetze rondom de wegwerpkaart hadden de onderzoekers de kaartuitgever en chipbouwer al betrokken in hun vorderingen. Nu moet er snel gehandeld worden. Hans de Jong van NXP komt die maandag kijken in Nijmegen en ziet met eigen ogen hoe de onderzoekers hun chip klonen. Die middag heeft hij een meeting bij TLS en informeert hen ook.

De onderzoekers schrijven een persverklaring die ze eerst voorleggen aan de betrokkenen. De AIVD is content. NXP is minder blij. De chipfabrikant vindt dat er teveel details worden vrijgegeven, maar is niet bij machte de perspublicatie tegen te gaan. Die woensdag krijgt de wereld te horen hoe slecht het is gesteld met de beveiliging van de Mifare Classic. Guusje ter Horst, die als minister van Binnenlandse zaken de coördinatie op zich heeft genomen, informeert die dag ook de Tweede Kamer. Pas dan krijgt ook de staatssecretaris Huizinga het te horen. Haar debat over de contraexpertise staat al de volgende dag gepland. Om zich daarop voor te bereiden worden Verdult en zijn collega's weer opgeroepen haar te adviseren.

De vrijdag daarop komt NXP weer naar de Radboud Universiteit om te praten over vervolgstappen. Directeur Rausch overhandigt Jacobs een fles wijn en feliciteert de onderzoekers met de resultaten. Hij stelt dat NXP graag met hen wil samenwerken om de chips veiliger te maken, maar dat moet dan wel onder een geheimhoudingsverklaring. Jacobs ziet niets in zo'n verklaring, want zo kunnen hij en zijn collega's er niet meer over publiceren. En dat is precies wat ze willen doen. De deadline voor ESORICS is 7 juli. NXP mag in de tussentijd ook het artikel lezen, maar dan moet Rausch zelf een geheimhoudingsverklaring tekenen. Zo heeft iedereen tot oktober de tijd om maatregelen te nemen. Zes maanden moet genoeg zijn bij een verantwoorde onthulling.

De AIVD kan zich wel vinden in de termijn van een half jaar en heeft geen bezwaar tegen de publicatie. Sterker nog: dit zal de beveiliging van de Nederlandse gebouwen alleen maar ten goede komen. Govcert, het Computer Emergency Response Team van de overheid en voorloper van het NCSC, stuurt een waarschuwing uit met instructie hoe te handelen: 'Factsheet FS-2008-03. Kwetsbaarheden Mifare Classic chips in toegangspassen'. Hierin staat dat het Crypto1 algoritme is gekraakt, de passen nagemaakt kunnen worden en welke maatregelen genomen kunnen worden. Doe dat snel, want de details van de kwetsbaarheden worden binnen enkele maanden vrijgegeven. Case closed.

Staatsecretaris Huizinga is inmiddels alweer wat OV-chipdebatten verder. In het debat van 15 april 2008 neemt ze de contra-expertise van de universiteit van Londen als leidraad voor haar beleid. Daarin staat onder andere dat de vervoersbedrijven een migratieplan moeten hebben om over te stappen op een nieuwe chip als blijkt dat op grote schaal misbruik wordt gemaakt van de kaart. Ze waarschuwt vooral geen overhaaste beslissingen te nemen en "hibbel de dribbel op een nieuwe chip over te stappen".

Dan is de oppositie het zat. Op 16 april 2008 dienen ze een motie van wantrouwen in tegen Huizinga. Het initiatief komt van Groen Links Kamerlid Wijnand Duijvendak. Als ik hem een maand later spreek, vertelt hij me dat ze hier toen al maanden mee bezig waren. Hij verwijt haar geen leiding te nemen, terwijl zij de enige is die er wat aan kan doen. En die kraak, daar kun je op wachten. "Dit leidt tot chronische zakkenrollerij", aldus Duijvendak. De motie wordt gesteund door Groen Links, SP, VVD en PVV, maar haalt net geen meerderheid. De kraak was dan wel niet de oorzaak van de hetze, maar wel de katalysator van al het ongenoegen rondom de kaart en de staatssecretaris.

De jonge onderzoekers van de Radboud zijn op dat moment in London. Een van de argumenten in de contra-expertise is namelijk dat het wel mee zou vallen met de fraude want de London Oystercard is al langer in gebruik en daar wordt ook niet mee geknoeid. Proberen dus. Op een rustig stationnetje zetten ze de Ghost en Proxmark aan het werk. Ze checken in en uit en veranderen het saldo. Alles werkt en tevreden gaan ze terug naar de luchthaven. Daar zien ze een goededoelenbus: "Doe hier uw Oystercard in en steun een goed doel!". Ze zouden de kaart kunnen opwaarderen tot 100.000 Britse pond en hem in de bus te doen… Ze twijfelen en moeten nog hun vliegtuig halen… Toch maar niet doen.

Eenmaal thuis schrijven ze hun eerste concept van het artikel: 'Dismantling Mifare Classic'. Roel Verdult kan dan ook eindelijk afstuderen. Het voorwoord van zijn scriptie 'Security analysis of RFID tags' begint met "The process during my master thesis was an experience I will never forget". Gaat het hier over de commotie rondom de OV-chipkaart? Nee, het gaat om de moeizame relatie tussen hem en de Ghost. Over hoe zwaar het was dit apparaat aan de praat te krijgen en hoe blij hij was toen hij het werkelijk kon testen. In de rest van het stuk kunnen we lezen hoe hij en de Ghost diverse beveiligingsproblemen vinden in RFID-chips. Voor de problemen met de beveiliging van de Mifare Classic verwijst hij netjes naar het artikel dat hierover zal verschijnen bij ESORICS. Op 25 juni 2008 levert hij de definitieve versie van zijn scriptie in. De echte rel moet dan nog beginnen.

Jacobs ontvangt namelijk diezelfde dag een brief van NXP: ze starten een rechtszaak tegen de professor en zijn universiteit.

30 maart 2015