Bits&Chips

Interview

‘Wij maken het niet kapot, nee, het is kapot en wij laten dat zien’

16 mei 2008

Onder zijn leiding brak de Radboud Universiteit onlangs de beveiliging van Mifare Classic, NXP’s smartcardtechnologie voor de ov-chipkaart en een leger aan toegangspasjes. Daarmee zette Bart Jacobs’ onderzoeksgroep de ov-chipkaart op losse schroeven. Voor het elektronisch stemmen en het biometrisch paspoort bracht de hoogleraar zijn advies uit. Hoe onderzoek naar correctheid van software een witte hoed kreeg.

‘Nog even voor de duidelijkheid, ik mag het interview nog wel inzien van tevoren voor de gevoelige informatie, hè? Jullie mogen me verder best als een clown afschilderen, maar er spelen hier miljardenbelangen mee.’ Het is waar. Bart Jacobs’ Digital Security-onderzoeksgroep aan de Nijmeegse Radboud Universiteit weet hoe de beveiliging van Mifare Classic te omzeilen, de chipkaarttechnologie die wereldwijd wordt gebruikt in toepassingen uiteenlopend van de ov-chipkaart tot aan beveiliging van gebouwen en installaties. Daarmee omgaan is dus op eieren lopen. Niet dat het nog lang een geheim zal blijven overigens: in oktober brengen Jacobs en zijn medewerkers de details naar buiten. Maar tot die tijd mogen gebruikers zich nog even voorbereiden.

De ontmanteling heeft behoorlijk wat losgemaakt in de politiek en de media. Na de eerste interne demonstratie - met een toegangspasje van de universiteit - op een vrijdagmiddag in maart ging er een telefoontje naar het ministerie van Binnenlandse Zaken. Een paar uur later hing de AIVD al aan de lijn. Of ze gelijk konden langskomen om over de gebroken beveiliging te praten. Maandagochtend wisten alle ministeries al dat hun gebouwbeveiliging lek is.

Even voor de duidelijkheid: Jacobs’ groep is niet de enige die claimt Mifare te hebben gekraakt. Eind december kondigden Duitse hackers aan dat ze via analyse van de chiplay-out de beveiliging hadden weten te achterhalen. Vanwege veiligheidsredenen wilden ze nog geen details onthullen. Jacobs’ groep was toen al een jaar bezig met de ov-chipkaart, via meer traditionele cryptologietechnieken. In januari onthulde student Roel Verdult dat de onbeveiligde wegwerpkaart te emuleren was. Door de Duitse aankondiging kwam de analyse van Mifare Classic in een stroomversnelling. Dat was de aanleiding om een werkgroep op poten te zetten in Nijmegen. ‘Wij hebben het op een andere manier gedaan dan de Duitse collega’s en zijn in zekere zin ook wat verder gegaan, omdat we concrete aanvallen hebben kunnen demonstreren.’ Met relatief eenvoudige middelen kunnen de onderzoekers nu de geheime sleutels uit de kaarten peuteren, waarmee ze vervolgens de gegevens kunnen lezen en schrijven.

Wat dreef Jacobs en zijn groep eigenlijk tot deze vandalistische daad? ‘In de media ontstaat soms het beeld dat we hier in Nijmegen alles kapotmaken. Maar wij zien dat als een wetenschappelijke analyse. Kijk, dat Mifare Classic is een zwak systeem, en wij hebben aangetoond dat het zwak is. Vergelijk het maar met een fabrikant die een auto op de markt brengt en universitair onderzoek toont daarvan aan dat de remmen helemaal niet goed functioneren. Dan zal iedereen zeggen: ‘Goed gedaan jongens! Fijn dat jullie dat hebben laten zien.’ Bij Mifare is dat vergelijkbaar. Wij maken het niet kapot, nee, het is kapot en wij laten dat zien. Ik denk dat het publiek wel het recht heeft om over dit soort dingen goed geïnformeerd te zijn.’

Focus

En dat terwijl Jacobs zelf eigenlijk helemaal geen beveiligingsachtergrond heeft. De Nijmeegse hoogleraar, momenteel ook een dag per week gedetacheerd bij de TU in Eindhoven, heeft zijn wortels bij correctheid van software, een onderwerp waar de groep ook nog steeds aan werkt. ‘Je hebt een heel spectrum aan methoden om te bewijzen dat software correct is. Dat begint bij simpel testen en strekt zich uit tot asserties die je interactief moet bewijzen met een *theorem prover*. Ik heb me een aantal jaren beziggehouden met dat uiterste einde van het spectrum. Dat is wetenschappelijk een grote uitdaging, maar praktisch nog niet heel relevant gebleken. We hebben daarin wel de grenzen wat verschoven, maar het blijft nog steeds zo dat je dat hooguit op een paar duizend regels code kunt toepassen.’ Het verificatiewerk voor Jacobs zelf staat op dit moment op een laag pitje. Hij werkt alleen met een promovendus aan het genereren van code vanuit een logische systeemrepresentatie.

De groep in Nijmegen specialiseert zich met name in het gebied tussen softwarecorrectheid en -veiligheid. Er is een logische connectie tussen die twee, legt Jacobs uit. ‘Met name in een taal als C heb je wel eens last van *buffer overflows* die je kunt misbruiken. Je kunt je afvragen of dat nou een correctheidsprobleem is of een security-probleem. Het is beide. Als je naar de taal kijkt en de semantiek ervan, dan is het een correctheidsprobleem. Maar het misbruik ervan is vooral in de security-sector van belang.’

Die connectie kwam rond de millenniumwisseling aan het licht, toen Nijmegen het Verificard-programma coördineerde. ‘Een groot Europees project dat was gericht op smartcards, met name Java-smartcards. Daar draaien gewoon kleine Java-programmaatjes op die je op een hoog niveau kunt programmeren. Wij keken vooral naar de correctheid daarvan. Maar in die context hebben we redelijk wat industriële contacten gehad, met name in Frankrijk. Natuurlijk willen die bedrijven dat hun programmaatjes correct zijn, maar we merkten dat ze voornamelijk breder geïnteresseerd zijn in de security-issues. Dat leidde bij ons tot een focusverschuiving in zekere zin: we zijn daarnaar gaan kijken en dat bleek een razend interessant vakgebied te zijn voor ons.’ Zie daar ook de keuze voor de Mifare-smartcard bij Jacobs’ groep: de digitale kaarten zijn vanwege deze historische achtergrond altijd een belangrijk aandachtspunt gebleven.

Vertrouw ons maar

Bart Jacobs moet weinig hebben van geheimhouding bij het ontwikkelen van goede beveiliging. ‘Wie vertrouw je het meeste?’, brengt de hoogleraar een van zijn stokpaardjes in stelling. ‘Een slotenmaker die zegt: ‘Ik heb hier een fantastisch slot, maar hoe het werkt, is bedrijfsgeheim. Maar vertrouwt u het maar’, of eentje die zegt: ‘Kijk, het werkt op die manier, het is gepubliceerd en alle experts hebben ernaar kunnen kijken en de beveiliging hangt af van de kwaliteit van de sleutels’?’

Jacobs wijst fijntjes op de beveiligingen van dvd, Blu-ray en gsm. Ook die gingen uit van geheime beveiligingsmethoden, maar zijn gebroken – dvd en Blu-ray zelfs binnen maanden. ‘Ik kijk dan ook erg sceptisch aan tegen de cultuur van NDA’s, de *non-disclosure agreements*. TLS, de organisatie die de ov-chipkaart ontwikkelt, heeft redelijk wat kritische signalen gekregen door de jaren heen. Maar daar is niet adequaat mee omgegaan. En als je een NDA getekend hebt en je ziet dat het fout gaat, kun je dat misschien tegen je baas zeggen, maar als die er vervolgens niets mee doet, is het afgelopen.’ Jacobs ging na het openbaar maken van de ontmanteling dan ook niet in op een aanbod van Mifare-producent NXP om intensiever samen te werken onder een geheimhoudingsplicht.

Hij constateert een vergelijkbare situatie bij het elektronisch stemmen. ‘De software voor de stemmachines werd geleverd door het bedrijf Groenendaal. Dat maakt ook de software voor de Kiesraad om stemmen te tellen en daar een zetelverdeling uit te halen. Er heeft nooit ook maar één onafhankelijke partij gekeken naar hoe die telling werd uitgevoerd. Dat is natuurlijk van de gekke. Er waren drie programmeurs in Nederland die

wisten hoe de uitslag van de verkiezingen werd bepaald, verder wist niemand dat. Het is closed-source software. Groenendaal zegt dat het bedrijfsgeheim is en dat niemand het mag zien. Dat wereldje van producenten die zeggen: ‘Vertrouw ons maar, het zit goed’, dat werkt toch niet al te best. Dat is rond de ov-chipkaart ook altijd gezegd: ‘Vertrouw ons maar, het zit goed in elkaar, maar het is zo gevoelig dat we niet kunnen zeggen hoe het is beveiligd.’ Dat werkt een beetje als een rode lap op ons.’

Steentje

Over elektronisch stemmen gesproken: aan de muur van zijn werkkamer prijkt een foto van de commissie-Korthals Altes in overheidsperscentrum Nieuwspoort. De Nijmeegse hoogleraar was een van de leden van deze groep, die vorig jaar de beveiligingsgaten rondom het elektronisch stemmen onderzocht. Zijn betrokkenheid bij de automatisering rondom stemmen is eigenlijk een erfenis van het correctheidswerk. Jacobs en zijn groep hebben in het verleden meegewerkt aan experimenten met stemmen via internet. ‘Dat is erg gevoelig. Vanuit de commissie-Korthals Altes is ook gezegd dat dat voorlopig nog niet aan de orde is. Maar er wordt in Nederland wel mee geëxperimenteerd, met name bij waterschapsverkiezingen. Het systeem dat daar wordt gebruikt, zit zo in elkaar dat iedereen achteraf de uitslag kan controleren. Dat is ook ingezet bij de laatste parlementsverkiezingen voor de Nederlanders die in het buitenland wonen. Toen anderhalf jaar geleden de crisis uitbrak rondom de stemmachines hebben we in die discussie een rol gespeeld en dat heeft erin geresulteerd dat ik lid ben geweest van de commissie. Daarna ben ik door het ministerie van Binnenlandse Zaken gevraagd een expertgroep voor te zitten die de adviezen van deze commissie verder uitwerkt. Dat is tegen de zomer afgelopen, daar komt binnenkort een brief over naar de Tweede Kamer.’

Jacobs’ groep speelde ook een rol bij het biometrische paspoort, dat in 2006 in Nederland is ingevoerd. ‘Daar hebben we de afgelopen jaren af en toe advies over uitgebracht en ook evaluaties gedaan. Het is een essentieel onderdeel van ons vakgebied om security-analyses uit te voeren, om te kijken of die beveiliging goed in elkaar steekt. Dat is dus niet alleen destructief.’

‘Ik durf wel te stellen dat het Nederlandse paspoort een van de best beveiligde van de wereld is. Het heeft goed uitgepakt dat er is samengewerkt met een aantal onderzoekers. Aanvallers verzinnen de meest maffe dingen om dat systeem onderuit te halen, dingen waar je nooit aan zou denken. En de mogelijkheden van de aanvallers veranderen ook door de tijd heen. Dus de enige manier om zo’n systeem goed te beveiligen, is door er zo veel mogelijk mensen kritisch naar te laten kijken alsof ze aanvallers zijn. Een paar maanden terug heeft het ministerie weer aan drie partijen gevraagd om opnieuw een evaluatie uit te voeren op het paspoort, onder wie ons. Nog een keer kijken met de kennis van nu, nog een keer die evaluaties doen. Dat moet je gewoon constant blijven doen. Je moet je systeem ook modulair opbouwen, zodat je een steentje uit de muur kunt halen en er een ander steentje voor in de plaats kunt zetten. Het zijn oude lessen uit de informatica die al tientallen jaren gelden. Bij de ov-chipkaart is een systeem uit Hongkong overgenomen, met de gedachte dat het daar werkt en dus hier ook wel zal werken. Ik heb de afgelopen jaren wel eens nagevraagd bij verschillende evaluatiebedrijfjes of ze de ov-chipkaart hebben bekeken. En niemand heeft dat gedaan. Dat was ook een reden om dat zelf maar eens een keer te doen.’

Geklooid

Jacobs vindt het opzoeken van de praktijk een verantwoordelijkheid voor de universiteit. ‘We doen zeker het onderzoek waarvan een hoop mensen zeggen: ‘Wat heb je daar in godsnaam aan?’ Maar dat is het aardige aan academisch onderzoek, dat je je dat kunt veroorloven en hopen dat het over tien jaar nuttig is. Maar in dat spectrum van theorie naar praktijk vraag ik ook altijd van mijn mensen dat ze enigszins bewegen, dus niet te flauw zijn om af en toe ook iets praktisch te doen of juist het theoretische aspect ervan uit te zoeken. Ik doe zelf meer met de overheid, maar er zijn hier ook mensen die meer contact hebben met de industrie.’

Wat doe je eigenlijk als je - gevraagd of ongevraagd - zo’n fout vindt? ‘Stel, je vindt een fout in Windows’, begint Jacobs. ‘Dat kun je netjes aan Microsoft melden. Maar als je dat gewoon vertrouwelijk vertelt, is de praktijkervaring dat er dan bijna niks mee gebeurt. Dus, binnenskamers melden heeft niet zo veel effect. Het andere extreem is meteen de fout op het web zetten, dus voordat je Microsoft inlicht. Tja, dan reageren ze meestal wel, dus het is wel een effectief middel om het snel gerepareerd te krijgen, maar het is niet zo heel netjes. Wat ontstaan is in de gemeenschap als de min of meer standaard manier om dit te doen, is *responsible disclosure*. Je licht de betrokkenen in, maar zegt erbij dat ze een of twee weken de tijd hebben voordat het publiek wordt.’

Bij Mifare ligt de situatie iets anders. Om dat op te lossen, is natuurlijk wat meer nodig dan een simpele softwarepatch en er zijn ook nationale veiligheidsbelangen mee gemoeid. Maatregelen om de onderzoeksgegevens te beveiligen, waren dus wel op hun plaats. Zo werd alle onderlinge e-mail versleuteld en ging de deur van de werkgroep altijd op slot. En de periode waarin Mifaregebruikers zich kunnen voorbereiden, is een stuk langer. ‘In oktober, als we de resultaten publiceren, is het mogelijk dat nog niet alles is vervangen, maar dit soort dingen vijf jaar lang stilhouden is ook geen optie. Naar ik begrepen heb, vindt NXP dit kort.’

Wat is er eigenlijk zo erg aan dat de ov-chipkaart is gekraakt? ‘Een van de ergere dingen is dat je op kosten van iemand anders kunt reizen. Als abonnementhouder word je er dan niet blij van dat die kosten bij jou worden afgeschreven. In principe is het mogelijk dat deze kaarten worden gekloond. In de backoffice is wel te zien - na een dag, want die checks worden ’s nachts gedraaid - dat er geklooid wordt met die kaart. Het enige wat ze kunnen doen, is die kaart blokkeren. Maar dan blokkeren ze zowel het origineel als de kloon, dus de abonnementhouder die ’s ochtends in de trein wil stappen, komt niet door het poortje. Dan kun je wel gaan klagen en wordt het hersteld, maar als er een paar duizend van dit soort gevallen zijn, dan krijgt de organisatie die dit opzet toch een probleem. Om hoeveel gevallen het gaat, is natuurlijk een risico-inschatting. Ik ben daar niet in gespecialiseerd en ik heb ook nooit geclaimd dat ik dit soort brede risico’s kan inschatten. Wij gaan over de beveiligingsaspecten en daarover hebben wij een hele duidelijke waarschuwing gegeven.’

Ecotechnologie

Al met al is Nederland best goed vertegenwoordigd in de security-gemeenschap, schat Jacobs. Hoewel we niet veel zelf maken. ‘NXP heeft wel die chips, maar andere partijen leveren weer de software. We hebben meer een evaluatiesector, die de beveiliging test. Brightsight, een vroegere groep van TNO, doet dit soort security-evaluaties. Maar er zijn meer bedrijfjes in Nederland die dit goed kunnen doen, zoals Collis en Riscure. Wat de laatste jaren is gebleken, is dat Nederland toch een heel kritische security-gemeenschap heeft. Daar spelen ook mensen als Rop Gonggrijp een belangrijke rol in.’ Gonggrijp, medeoprichter van XS4All en bekend in hackerkringen, was een van de drijvende krachten achter de Stichting Wij Vertrouwen Stemcomputers Niet.

‘Maar ik denk ook de academische wereld. Er wordt wel eens negatief op gereageerd. Je kunt dat zien als lastig, maar ook als een kans. Ik vergelijk het graag met de milieusector. Twintig, dertig jaar geleden had je grote milieurampen in Nederland en mensen die daarop begonnen te wijzen, werden in eerste instantie ook wel eens als lastig gezien. Dat is totaal omgeslagen en nu exporteert Nederland ecotechnologie. Wij zijn daarin erg ver gevorderd. Zo moet je dat misschien ook met security zien. Het is nu even lastig, maar je kunt het ook als kans zien. En zelf als argument gebruiken: ‘Onze producten blijven zelfs in Nederland overeind.’

Pieter Edelman

Terug naar overzicht