De granaatappel helpt een beetje
3

Beestjes zoeken voor de sjeik
7

Kennis

OV-chipkaart **Deskundigen zetten vraagtekens bij risico's van manipulatie en fraude met toegangspas**

Laat ze maar lekker kraken

Heibel over de OV-chipkaart: wat moeten we ermee als die zo makkelijk te kraken is? Twijfel alom. De Tweede Kamer schortte deze week zelfs een debat over de beveiliging op. Maar is het allemaal wel zo dramatisch?
Door **Michael Persson**

'Steeds vaker krijgen we de laatste tijd te horen dat internet en chipkaarten onveilig zijn. En inderdaad: er worden verschrikkelijke fouten gemaakt bij het vervaardigen van zulke systemen. Hoe is het dan mogelijk dat de maatschappij, ondanks al die *braindead*-ontwerpen, best aardig blijft functioneren?'

Het is een tegendraadse stelling die computergoeroe Andrew Odlyzko van de universiteit van Minnesota begin deze week verkondigde op een symposium van de Technische Universiteit Eindhoven over digitale veiligheid.

In het hol van de leeuw. Van twee leeuwen eigenlijk, met een publiek dat zowel uit computerbeveiligers als computerkrakers bestond. De eerste groep kreeg te horen dat ze prutswerk levert, de andere dat het ontmaskeren van dat prutswerk eigenlijk helemaal niet zo veel uitmaakt.

De tweedaagse bijeenkomst was georganiseerd ter ere van de op-

Kort

Erasmus MC vindt gen voor groeihormoon

SCHILDKLIER Het Erasmus MC in Rotterdam heeft samen met Franse en Britse ziekenhuizen een tot nu toe onbekende genafwijking gevonden die de productie van schildklierhormoon remt. Dat blijkt uit hun publicatie deze week in *The New England Journal of Medicine*. Het schildklierhormoon is bij baby's essentieel voor de groei van organen en de ontwikkeling van de hersenen. De genvondst kan de effectiviteit vergroten van de hielprik, suggereren de onderzoekers.

Kans op intelligent leven is minimaal

BUITENAARDS Volgens Andrew Watson van de universiteit van East Anglia is de kans op intelligent buitenaards leven gering, rekent hij voor in het tijdschrift *Astrobiology*. De kans dat bacteriën ontstaan, daarna complexe cellen die zich specialiseren, en uiteindelijk intelligent leven, is volgens hem minder dan 0,01 procent. Daarbij komt dat de leefbaarheid van een planeet afhankelijk is van de ster waar hij omheen draait. Verwacht wordt dat de zon over een miljard jaar zo heet is, dat er op aarde geen leven meer mogelijk is. De tijd dringt dus ook nog eens.

Hersens van de baas werken beetje anders

HIËRARCHIE Wanneer iemand een hogere of lagere plaats inneemt in een hiërarchie, worden verschillende gebieden in het brein geactiveerd. Dat blijkt uit fMRI-scans die onderzoekers van het National Institute of Mental Health hebben gemaakt, meldt *Science* deze week. Proefpersonen speelden een computerspelletje tegen een betere en een mindere tegenstander. Bij een betere werden gebiedjes geactiveerd die geassocieerd worden met emotionele pijn en frustratie. Was de proef-

stituut voor de Protectie van Systemen en Informatie (Eipsi), een nieuw samenwerkingsverband van cryptologen (van de faculteit wiskunde) en computerexperts (van informatica). Los van die aanleiding was de timing natuurlijk perfect. Midden in de storm die OV-chipkaart heet.

Dus zitten ze allemaal in de zaal: de beveiligingsanalisten uit Nijmegen die de kaart begin deze maand dood hebben verklaard, de mensen van TNO en van OV-chipkaart-eigenaar Trans Link Systems die er gewoon mee willen doorgaan, en ambtenaren van het ministerie van Verkeer en Waterstaat die het allemaal niet meer weten. De onzekerheid was deze week ook in Den Haag merkbaar: woensdag werd het beveiligingsdeel van het Kamerdebat over de OV-chipkaart een maand uitgesteld.

Over het feit dat de kaart, in zijn drie verschijningsvormen, nu definitief is gekraakt, zijn alle partijen het inmiddels eens. Sinds Duitse hackers eind december lieten zien dat ze de Mifare Classic-chip grotendeels hadden ontleed, is de werking van het geheime algoritme op de chip in drie stappen achterhaald. Eind maart bleek die rekenformule zelfs zo eenvoudig, dat onderzoekers van de Radboud Universiteit in Nijmegen konden laten zien dat alle sleutels van één chip met een laptop in een paar seconden konden worden ontraadseld. Op die manier is elke OV-chipkaart te manipuleren.

Iedereen heeft een laptop, dus iedereen kan nu frauderen, was de impliciete boodschap. Maar wat betekent zo'n *proof-of-concept* in de praktijk? Hoe makkelijk kan een willekeurige treinreiziger straks frauderen met de OV-chipkaart?

Afluisteren

Allereerst de benodigdheden. Om te beginnen heeft de zwartrijder een kaart nodig die lijkt op een legale kaart.

Dan zijn er twee scenario's. De eerste mogelijkheid is om een eigen oplaadbare kaart te kopen en daar bijvoorbeeld 40 euro op te zetten. Je luistert één keer een transactie met een toegangspoortje af, en zet die informatie op je laptop. Vervolgens kun je die transactie omkeren, en het saldo op je zolderkamer steeds eigenhandig aanvullen tot dat oorspronkelijke bedrag van 40 euro.

De tweede mogelijkheid is wildvreemde kaarten af te afluisteren. Daartoe moet je in een stationshal de communicatie uitlezen tussen de OV-chippoortjes en de kaarten van bonafide reizigers. Met die informatie zijn steeds nieuwe kaarten te gebruiken, met het bijbehorende saldo.

Benodigd in beide gevallen: een laptop en een afluisterantenne die de 13,56 MHz-signalen opvangt, een blanco chipkaart (een zogeheten emulator), een kaartlezer en -schrijver, en, natuurlijk, niet triviaal: een stuk software.

In een eerste analyse van de frauduleuze mogelijkheden van de OV-chipkaart rekende TNO uit dat de benodigde investering zo'n 9 duizend dollar bedraagt, vandaag de dag ongeveer 5500 euro. Die kosten blijken echter schromelijk overdreven, zo is te zien op internet. De emulator kost vooralsnog rond honderd euro, en voor 22 dollar en 36 cent koop je een lezer/schrijver bij China Card Master Electronics in Shenzhen (wordt opgestuurd in cadeauverpakking). Daar komt dan nog wel de laptop bij, voor wie die nog niet heeft.

Maar zullen gewone consumenten dan ook straks zelf hun kaart gaan fabriceren? Niet zo heel veel, is de verwachting. In een vorige week verschenen analyse van de Royal Holloway University of London (RHUL) staat dat pas 'als de aanvalstechnieken eenvoudig genoeg worden, sommige kaarthouders in de verleiding zullen komen als amateurhacker hun reiskosten te reduceren'. De Nijmeegse aanval, hoe snel en simpel ook, is kennelijk nog niet eenvoudig genoeg voor grote aantallen particuliere fraudeurs.

We zullen het eerder moeten hebben van criminele tussenpersonen. TNO en RHUL hebben een aantal mogelijke scenario's bekeken, maar houden die geheim ('We vertellen ook niet hoe je bommen moet maken'). Het zal erop neerkomen dat criminelen kant- en-klare kaarten gaan verkopen (via belwinkels of via internet), of de gekopieerde kaartsleutels en bijbehorende software via internet proberen te slijten.

Illustratie Yvonne Kroese

> 'Een burger loopt meer financieel risico bij betalingen op internet en via de telefoon'

Consumenten zouden die data vervolgens kunnen downloaden en ze zelf op een eigen kaart kunnen schrijven. Al is de vraag of consumenten voor die service via internet zouden willen betalen, aan een digi-crimineel.

Verdiensten

Hoeveel valt er met deze zaken te verdienen? Stel dat straks 10 procent van de reizigers gaat frauderen. Dat lijkt een redelijke schatting: toen er nog geen controle was in Amsterdamse trams, reisde 20 procent van de passagiers zwart. Volgens het CBS (cijfers van 2005) wordt in Nederland jaarlijkse iets meer dan 20 miljard kilometer met het openbaar vervoer gereisd. Met een OV-chipkaart-kilometerprijs van ongeveer 15 cent resulteert dat in een totale 'winst' voor zwartreizigers van zeker 300 miljoen euro.

Criminelen kunnen lang niet dat hele bedrag vragen voor hun diensten, want dan kan de zwartrijder net zo goed legaal reizen. Maar een markt van 50 tot 100 miljoen euro lijkt er wel te zijn.

Is dat een criminele *businesscase*, mede gelet op de benodigde eenmalige investering van zeker 100 euro ?

De meningen zijn daar verdeeld over. TNO concludeerde dat handel in valse OV-chipkaarten voor criminelen niet aantrekkelijk is. De RHUL houdt een paar slagen om de arm, maar verwacht van wel.

Veel kennis over dergelijke vormen van criminaliteit is er niet. Het Wetenschappelijk Onderzoeken Documentatie Centrum (WODC) van het ministerie van Justitie liet drie jaar geleden onderzoeken welke fraudevormen mogelijk zijn bij mobiel betalen, een techniek die in de verte vergelijkbaar is met de OV-chipkaart. De opstellers van dat rapport signaleerden 'goed georganiseerde fraude, gepleegd door grote bendes met internationale vertakkingen, die ook toegang weten te krijgen tot geavanceerde cryptologische kennis van werkloze Oost-Europese experts'. Maar hoe vaak en om hoeveel geld het gaat, staat er niet bij.

Bij eventueel verlies voor de vervoerbedrijven hebben de experts zich in elk geval neergelegd. Sommigen van hen denken dat de consument daar geen last van hoeft te hebben. 'Niets is helemaal veilig', zegt een woordvoerder van TNO, dat nog steeds vindt dat de chipkaart per januari 2009 kan worden ingevoerd. 'Ook pinnen niet. Per jaar verdienen criminelen 20 miljoen euro met het skimmen, het ongemerkt uitlezen van betaalkaarten. Durf je om die reden geen geld meer uit de muur te halen?'

Volgens Andrew Odlyzko van de universiteit van Minnesota is een zeker verlies inherent aan elk financiële systeem. 'En dan is het hacken van een OV-chipkaart niet de ergste vorm van misbruik. Neem Nick Leeson (1,4 miljard dollar), of die Fransman, Jérôme Kerviel, die 4,9 miljard euro aan zijn bank had onttrokken: ik heb nog nooit iets vergelijkbaars gehoord door toedoen van hackers.'

Hij noemt de mogelijke fraude met de OV-kaart *collateral damage*. 'Een gaatje in de dijk is geen lek. Zolang er water doorheen sijpelt, is er niets aan de hand. Je moet alleen oppassen dat het gat niet te groot wordt, en dan klaarstaan om het lek te dichten. De *bad guys* laten sporen achter, dus je kunt ze ook signaleren en bestrijden, en voorkomen dat het lek te groot wordt.'

Rammelende crypto is geen ramp, zegt hij. 'Een slecht slot zal geen professionele inbreker tegenhouden, maar wel de tiener uit de buurt. Dat scheelt al heel veel ellende.' Het verlies komt bovendien niet voor rekening van de gedupeerde, maar van het bedrijf, zeggen de meeste onderzoekers . 'Een burger loopt meer financieel risico bij betalingen op internet en via de telefoon', aldus het RHUL-rapport. Toch zullen ook legale OV-chipkaarthouders last hebben van illegale kopieën, bijvoorbeeld als de kaart wordt geblokkeerd doordat het systeem ontdekt dat er twee kaarten in omloop zijn met hetzelfde serienummer. Uit het RHUL-rapport: 'Zulke incidenten kunnen leiden tot een grote stijging in klachten, claims en vragen. Het kost een bedrijf enorm veel geld om die vragen te onderzoeken en te beantwoorden.'

Niet te kraken

Volgens Wouter Teepe, een van de Nijmeegse onderzoekers die de OV-kaart hebben ontmanteld, is de enige oplossing de chip te vervangen en het hele systeem daarachter te herzien: 'Er wordt nu gedaan alsof alles gekraakt kan worden. Dat is niet zo. Wij hebben ook het paspoort getest. We hebben toen suggesties gedaan voor een betere beveiliging – die zijn overgenomen, en nu is de chip niet meer te kraken.

'Dat komt mede doordat het algoritme van het paspoort niet geheim is. Dat kan iedereen testen, en zolang het niet gebeurt, weet je dat het systeem veilig is. De OV-chipkaart met al zijn geheimen bewijst dat *security through obscurity* niet werkt.'

Maar goed, zelfs als Trans Link Systems straks door de bocht zou gaan en een geheel beveiligde OV-chipkaart zou leveren, dan nog houden hackers als Rop Gonggrijp hun twijfels. 'Ik vindt die heisa over misbruik helemaal niet interessant', zegt Gonggrijp. 'Wie een slecht systeem bouwt, moet op de blaren zitten. Verlies maar geld, als je dat zo graag wilt. Maar wat betekent al dit gestuntel voor de privacy? Kan straks iemand zo in de *backoffice* inbreken en de reisgegevens van half Nederland uit de databank halen? Of wat als een van de medewerkers straks een dvd'tje laat liggen met die gegevens erop? Daar moeten we ons veel meer zorgen over maken dan over de criminele *businesscase*.'

Wat er allemaal aan voorafging

- **Mei 2007: studenten van de Universiteit van Amsterdam kraken wegwerpversie OV-chipkaart. Trans Link Systems dicht het lek.**
- **November 2007: afstudeerder Roel Verdult van de Radboud Universiteit in Nijmegen kraakt wegwerpversie OV-chipkaart opnieuw. Lek wordt nu niet gedicht.**
- **December 2007: de Duitse hackers Karsten Nohl en Henryk Plötz laten onder luid applaus op een congres in Berlijn zien hoe zij de Mifare Classic-chip hebben ontleed.**
- **Januari 2008: het dringt tot Nederland door dat de Mifare Classic-chip onder meer op de oplaadbare versie van de OV-chipkaart zit.**
- **Januari: de tweede Nijmeegse kraak van de wegwerpkaart (uit november) wordt nu pas bekendgemaakt.**
- **Begin maart: Radboud-onderzoekers klonen toegangspasjes van de universiteit, die voorzien zijn van Mifare Classic-chips. Omdat vergelijkbare passen worden gebruikt door ambtenaren van ministeries, wordt de AIVD gewaarschuwd.**
- **Eind maart: de sleutels van de OV-chipkaart blijken met een laptop in zeer korte tijd te kunnen worden ontdekt. Ministerie van V&W gewaarschuwd.**

Flexibel werken is gezonder

ARBEID Werknemers die flexibeler gaan werken, zijn minder vaak ziek. Ze zijn bovendien loyaler. Dat blijkt uit onderzoek van de Amerikaanse Wake Forest University School of Medicine onder ruim drieduizend werknemers van een multinationaal bedrijf. De flexibiliteit betreft zowel de plaats waar gewerkt wordt (thuis of elders) als het aantal uren. De bevindingen zijn gepubliceerd in de *Psychologist-Manager Journal*.

Niet alle mensen worden steeds ouder

LEEFTIJD Mensen worden gemiddeld steeds ouder, maar niet iedereen profiteert daar evenredig, van, zeggen epidemiologen van Harvard School of Public Health in Boston. Bij 4 procent van de mannen en bij 19 procent van de vrouwen in Amerika is sinds begin jaren tachtig de levensverwachting zelfs dalende, aldus hun artikel in *PLoS Medicine*. Vermoedelijk komt dat doordat in bepaalde streken van de VS de gezondheidszorg minder adequaat is. In de VS is de gemiddelde levensverwachting bij geboorte voor mannen tussen 1961 en 1999 gestegen van 66,9 naar 74,1 jaar, en voor vrouwen van 73,5 naar 79,6 jaar.

Nu op vk.nl/wetenschap

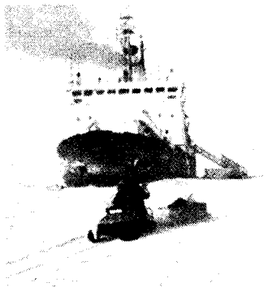

Foto CCG

Publicist **Bennie Mols** won een hoofdprijs in een internationale competitie van wetenschapsjournalisten: een poolreis met een Canadees onderzoeksschip. Vrijdag kreeg hij zijn hut, die hij twee weken deelt met de enige Inuit op het schip. Volg dagelijks zijn **poolblog** op de site van de Kennis-redactie.