“De maffia zal de RFID-chip kraken”

“Het is de evolutie van de computer: mainframe, desktop, pda, sensor, microchip. De computer wordt steeds kleiner.” Melanie Rieback, universitair docent Informatica aan de Vrije Universiteit in Amsterdam, doet onderzoek naar privacygevoeligheid rondom RFID-tags - chips die op afstand uitleesbaar zijn middels radiogolven.

Tekst: Eric van den Berg

Fotografie: Friso Keuris

>> Je moet het weten, anders zie je 'm niet: de ultrakleine microchip. Een minispeldenkop. Hij zit verstopt in het boek dat je net hebt gekocht, in het KLM-label om het handvat van je koffer en bij een enkeling al in de arm. Daar haalde een paar jaar geleden de Baja Beach Club in Rotterdam het nieuws mee. Vaste gasten kregen een chip vlak onder de huid ingeplant, een elektronische portemonnee. "Ach, dat was louter een publiciteitsstunt", zegt dr. Melanie Rieback, universitair docent Informatica aan de Vrije Universiteit in Amsterdam. "Volgens mij gebruikt nagenoeg niemand dat meer. Het was even hip, lekker controversieel en daarna was het weer over."

Wie weet wordt het de toekomst, maar wat Rieback vooral wil benadrukken: we zouden bijna vergeten wat zo'n ding in je arm of in het oor van een schaap of in de OV-chipkaart en het paspoort werkelijk is. Hoe klein en onschuldig het ook lijkt, het is een minicomputer met een geheugen waarin informatie is opgeslagen. Formeel met de naam RFID, Radio Frequentie Identificatie. De RFID-tag is een microchip die met behulp van radiogolven op afstand kan worden uitgelezen.

Privacygevoelig

"Sommige mensen zien de tag slechts als een radiografische streepjescode. Maar het is meer dan dat. De tag is de computer van de toekomst", zegt Rieback, die al jaren onderzoek doet naar hoe onveilig en privacygevoelig de microchip is. Twee jaar geleden promoveerde ze op dit onderwerp. "Het is de evolutie van de computer: mainframe, desktop, pda, sensor, microchip. De computer wordt steeds kleiner. De sensor heeft nog de beperking dat er een batterij in moet, bij RFID is dat niet meer nodig. En toch is het gewoon een chip met geheugen."

"We zijn dus zo ver dat we in feite een computer hebben met draadloze stroom. Dat is echt een van de grootste uitvindingen van de laatste tijd. De tag heeft een antenne die reageert op het leesapparaat. Eigenlijk wordt de chip gewoon wakkergemaakt. Geen snoeren, geen batterij, geweldig toch? Vergelijk het met een mobieltje dat je in een inductie-oplader zet of een elektrische tandenborstel die je oplaadt.

De RFID-tag zit in veel meer dingen dan de meeste mensen weten. We kennen natuurlijk de OV-chipkaart, het paspoort, toegangspasjes bij bedrijven, de antidiefstalstrips in de winkels. Elk boek in de openbare bibliotheek in Amsterdam heeft een RFID en ook boekhandel Selexyz is er al mee bezig – ze kunnen precies bijhouden hoeveel boeken waar zijn. Ook Ahold en C1000 proberen RFID al in de magazijnen en de bevoorrading uit. Schapen hebben een chip in hun oren, zelfs vissen zijn te identificeren met een RFID."

Criminelen

"In Japan zijn ze natuurlijk weer veel verder, daar zijn ze gek op technologie. Je ziet de chip daar ook vaak terug in rare en ludieke toepassingen. Doe een chip in je horloge en je kunt met je horloge betalen. Of een chip in een filmposter op straat: ga er langs met je mobiel en je krijgt extra informatie of wordt naar de juiste website gestuurd. Japanners maken zich minder druk om privacy en veiligheid dan wij hier doen. Ze vinden het snel allemaal wel goed.

"We hebben een aanval geopend op de chip. Zie het als hacken in een proefopstelling"

Melanie Rieback (1978, Ohio) is universitair docent/assistent-hoogleraar bij de vakgroep Informatica aan de Vrij Univeriteit in Amsterdam. In 2008 promoveerde ze met het proefschrift Security and Privacy of Radio Frequency Identification. Ze doet doorlopend onderzoek naar de veiligheids- en privacyaspecten van de RFID-technologie. Rieback is initiatiefneemster van het Girl Geek Dinner, een netwerk voor vrouwen in de wetenschap.

Ik heb eigenlijk geen specifieke bezwaren tegen de RFID-technologie. Het is gewoon het nieuwste in de technologie, iets heel moois en handigs. Maar je moet het op dezelfde manier behandelen als elke andere computertechnologie. Dus je moet opletten en beveiligen. En daar schort het nu aan. Er bestaat geen standaardtechnologie die de radiochips beschermt tegen aanvallen. Bedrijven houden zich er eigenlijk niet mee bezig. Het is recessie, ze hebben andere dingen aan hun hoofd, een firewall voor RFID staat dan niet hoog op het lijstje. Misschien komt het doordat er nog geen heel concrete voorbeelden van misbruik zijn te melden. Als er écht iets gebeurt, zal men schrikken. We hebben het idee dat criminelen er nog niet echt mee aan de haal zijn gegaan. Dat is een kwestie van tijd: een RFID-tag is een computer en een computer is te kraken. Studenten en Duitse hackers hebben de chip op de OV-kaart gekraakt; zij wilden daar verder geen kwaad mee. Maar er komt een moment dat de Chinese of Russische maffia het lukt. Er valt namelijk geld te verdienen."

Istanbul of Hawaii?

"We hebben hier op de VU de kwetsbaarheid van de systemen met microchips al aangetoond. Samen met mijn collega, professor Andy Tanenbaum, hebben we een aanval geopend op de chip. Zie het als hacken in een proefopstelling. Eigenlijk is dat niets nieuws, het is nu alleen bij een heel kleine computer. Je overlaadt het systeem bijvoorbeeld met data. We hebben bewezen dat je via de chip, hoe klein ook, een virus in het systeem kunt sturen. Daar was nooit zoveel aandacht aan besteed, omdat er te weinig geheugenruimte op zou zitten voor een virus.
Neem Schiphol. Het vliegveld maakt gebruik van een sorteersysteem voor koffers. Veel van die koffers hebben een tag met chip waarop staat naar welk vliegtuig hij moet. Maar, puur hypothetisch: nu vervangen wij de chip door een verkeerde chip, met veel meer nullen en enen. Het complete bagagesysteem kan erdoor van slag raken, kan de overflow van informatie niet aan. De koffer gaat de verkeerde kant op of de volgende koffer wordt verkeerd gelezen. De koffer die naar Istanbul moest, komt op Hawaii terecht, of andersom. En erger: koffers kunnen ongemerkt ergens aan boord komen.
Het kan nog dichter bij huis. Koop een pot pindakaas in de supermarkt die tags op zijn producten heeft. Ga langs de kassa, vervang thuis de chip door een verkeerde chip, ga terug naar de supermarkt en loop direct door naar de kassa. De tag-lezer brengt nu besmette informatie in het systeem. Misschien dat je zo de hele inventarisatie op hol kunt brengen of prijzen van producten kunt veranderen."

Samenwerking

"Er bestaat nog geen goede manier om deze systemen te testen. Daar wordt het wel tijd voor. Kijk naar de OV-chipkaart. Studenten in Nijmegen kunnen nu al een kopie maken van een jaarabonnement. Stel dat iedereen de beschikking heeft over dezelfde apparatuur waarmee je dat kunt doen. Dat is een nachtmerrie. Misschien dat gaat doordringen dat risico's op de loer liggen. Walmart, een Amerikaanse supermarkt, was al heel ver met tags op alle producten, maar is nu toch wat voorzichtiger geworden. Niet zozeer vanwege

>>

>> privacyproblemen, maar vanwege twijfels. Hoe kwetsbaar is het systeem en ook hoe nauwkeurig? Leest de scanner alle producten in het winkelwagentje? Als dat niet gebeurt, kan dat een hoop geld kosten."
"Soms worden we benaderd door bedrijven voor advies of hulp. Niet zozeer om hun systeem te testen. Ik ben best bereid samen te werken met bedrijven, maar ze moeten er wel voor betalen. Ik hoef het geld niet zelf, maar onze projecten zijn duur, we hebben investeerders nodig."

Onderbuikgevoel

"We zijn nu de RFID Guardian aan het ontwikkelen, een apparaat dat de tag en de lezer kan testen en het dataverkeer kan verstoren. Zie het als een *man in the middle*, een apparaat dat het verkeer regelt tussen de microchip en het leesapparaat. Je kunt ermee regelen wie wel en wie niet iets kan doen met de informatie van de tag. Ik wil bijvoorbeeld dat alleen de marechaussee mijn paspoort kan uitlezen en alleen de VU mijn toegangspasje, en dat alleen mijn eigen iPod is verbonden met de sensor in mijn Nike-schoen.
Ik hoop dat we binnen een jaar echt een versie op de markt kunnen brengen, voor zeg vijfhonderd à duizend euro. We mikken op bedrijven en systeemontwerpers. Die moeten dit gaan gebruiken. Ook particulieren kunnen het apparaat gebruiken, al verwacht ik niet echt dat iedereen zich op die manier met beveiliging en veiligheid gaat bezighouden.
Zelf zal ik me meer bewust zijn van privacykwesties dan de meeste mensen, maar ik ben door mijn werk niet neurotisch of technofoob geworden. Ik doe aan internetbankieren en koop spullen op het net met mijn creditcard. Ik kijk wel goed welke website of betaalsystemen ik wel en niet vertrouw. Google Checkout gebruik ik, die is bekend, en ook PayPal. Het is toch, net als bij andere mensen, een onderbuikgevoel: je wéét gewoon of het te vertrouwen is. Ik gebruik Facebook, omdat ik zo contact houd met mijn familie en vrienden in de States. Maar ik zet er nooit iets op wat ik niet in de openbaarheid zou willen gooien." ●

Deloitte en Cybersecurity
De digitale infrastructuur ondersteunt steeds meer kritieke functies en faciliteiten in ons dagelijks leven. Zo worden stroomvoorziening en kritische informatiesystemen in toenemende mate via internet aangestuurd.

**Vanwege de hoge opbrengsten en lage pakkans wordt de dreiging van cybercrime steeds groter, zowel voor het bedrijfsleven als voor de nationale veiligheid. Dit is ook een van de conclusies uit de TMT Global Security Study van Deloitte.
De Study is te downloaden via www.deloitte.nl/tmtsecuritystudy**

**Dick Berlijn, voormalig Commandant der Strijdkrachten van het Nederlandse leger, is sinds september 2009 senior board advisor bij Deloitte Nederland. Belangrijk onderdeel van zijn portefeuille is veiligheid. Hij houdt zich ook bezig met cybersecurity.
Contactpersoon bij Deloitte is Jacques Buith: jbuith@deloitte.nl**

De favoriete innovatie van Melanie Rieback: "De draadloze transfer van elektriciteit/energie. Zo zijn er al lampen die werken op basis van magnetische inductie. Geen snoeren nodig, geen batterijen."