

# RFID en veiligheid

Paul Goossens

**Zogenaamde RFID-tags worden op steeds meer plaatsen toegepast. Zo worden deze gebruikt in het betaalsysteem van het openbaar vervoer in diverse steden en als bibliotheekpas. In dit artikel kijken we hoe het gesteld is met de veiligheid en privacy rond deze RFID-tags.**

RFID-tags zijn speciale chips gecombineerd met een kleine antenne. Zodra zo'n tag in de buurt komt van een bijbehorend leesapparaat (reader), zal de RFID-chip gevoerd worden door de energie die de reader uitzendt. Via deze radiogolven kunnen de reader en chip in beide richtingen met elkaar communiceren. Het feit dat RFID-tags draadloos zijn, maakt dat ze voor veel doeleinden toepasbaar zijn. De tag hoeft nog niet eens zichtbaar te zijn om met de reader te kunnen communiceren. Dat levert ook enkele nadelen op. De eigenaar van zo'n RFID-tag merkt normaliter niet dat zijn RFID-tag wordt uitgelezen, of dat de communicatie tussen reader en zijn eigen tag door een derde partij onbemerkt wordt bespioneerd.

## Nadelen

Stel dat je in een winkel een biefstuk in je winkelwagen legt (met een eigen RFID-tag). Zodra je langs het wijnrek loopt, meldt je winkelwagen (voorzien van reader) welke wijn het beste bij die biefstuk past. Bovenstaand voorbeeld is nog aardig onschuldig, maar wat als derden de informatie op je paspoort ongemerkt kunnen uitlezen en kopiëren, of bij het afrekenen bij een benzinstation dit op jouw rekening plaatsen? In dergelijke situaties willen we toch niet ongemerkt ten prooi vallen aan kwaadwillende personen of bedrijven.

Op dit moment zijn al diverse groepen mensen bezig om deze gevaren wereldkundig te maken, om duidelijk te maken dat er voorzichtig met deze nieuwe technologie moet worden omgesprongen en dat veiligheid een zeer belangrijk aspect is waar de fabrikanten en organisaties rekening mee moeten houden.

Zo heeft een groep studenten het RFID-systeem 'Exxon Mobile Speed Pass' gekraakt, dat door Amerikaanse benzinestations van het merk Exxon als eigen betaalsysteem wordt gebruikt. De toegepaste RFID-tags zijn weliswaar voorzien van een cryptografisch systeem, maar dit heeft de studenten niet tegengehouden om toch met een zelf gekopieerde RFID-tag ongemerkt te kunnen afrekenen. Met een zelfgemaakt apparaat hebben ze de communicatie (op afstand, dus ongemerkt) tussen een RFID-betalpas en de bijbehorende reader kunnen ontvangen. Door deze communicatie te analyseren waren ze in staat de beveiliging te kraken en de RFID-betalpas te kopiëren. Bij wijze van experiment hebben ze vervolgens met succes geprobeerd benzine te tanken en automatisch met hun gekopieerde RFID-betalpas te betalen. Uiteraard hebben ze een eigen RFID-betalpas gebruikt om te kopiëren, zodat ze niet strafbaar zijn.

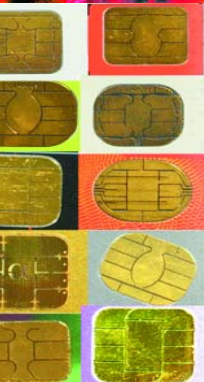
Ondertussen is er zelfs een eerste RFID-virus ontwikkeld door een medewerker van een onderzoeksgroep aan de Vrije Universiteit in Amsterdam. Dit virus is geschreven voor een eigen RFID-systeem, dus niet voor een systeem dat commercieel wordt toegepast. Desondanks maakt dit virus eens te meer duidelijk dat we toch zeker moeten stil staan bij de gevaren die de RFID-technologie met zich mee brengt.

## Melanie Rieback

De schrijfster van dit virus, Melanie Rieback, heeft dit virus geschreven om aandacht te vragen voor de problematiek rondom de veiligheid van RFID. Ze is van mening dat privacy-gevoeligheid en veiligheid niet alleen een probleem zijn voor de consument, maar ook voor de bedrijven die deze technologie willen inzetten. Gezien het aantal publicaties rond dit virus is dat zeer zeker gelukt. Naar aanleiding van deze aandacht is Melanie door een aantal bedrijven benaderd om ze te helpen hun RFID-software veiliger te maken. Helaas reageerden enkele bedrijven in RFID-technologie zeer negatief op dit virus en vonden dit een storm in een glas water. Naast het al eerder vermelde kraken van de 'Exxon Mobile Speed Pass' weet Melanie te melden dat ook het nieuwe Nederlandse paspoort niet geheel kraakvrij is. Het Delftse bedrijf 'Riscure' heeft aangetoond dat de voorgestelde RFID-technologie niet veilig genoeg is. De sleutel in zo'n paspoort was in een paar uur tijd gekraakt, waardoor men in staat was onopgemerkt de geboortedatum, pasfoto en vingerafdrukgegevens uit dit nieuwe paspoort te lezen. Naar aanleiding hiervan heeft het ministerie van Binnenlandse Zaken aangekondigd de beveiliging van deze technologie te verbeteren. Niet alleen het Nederlandse paspoort heeft nog problemen met de veiligheid van de RFID-tag, ook het Amerikaanse paspoort ligt onder vuur. Op een conferentie van 'Freedom and Privacy' heeft een lid van de 'Civil Liberties' gedemonstreerd dat het nieuwe Amerikaanse paspoort al op een meter afstand uit te lezen is, terwijl de fabrikanten melden dat dit alleen op enkele centimeters afstand mogelijk is.

## Bedenkelijk

Naar aanleiding van deze voorbeelden vraagt Melanie zich ook af of de industrie hier wel echt iets van heeft geleerd. "Auto's worden uitvoerig getest voordat ze de weg op mogen, waarom gebeurt dit niet voldoende met



# Virussen bedreigen RFID-tags

privacy-gevoelige technologie?". Hoe moeten de mensen deze ontwikkelingen nu kunnen vertrouwen en accepteren als blijkt dat deze niet serieus genoeg getest zijn? Tot nu toe zijn het nog onderzoekstellingen die RFID-technologie gekraakt hebben, maar wie vertelt ons dat kwaadwillende mensen dit niet ook doen of gaan doen? Als er maar genoeg RFID-systemen in gebruik worden genomen, is het niet meer dan een kwestie van tijd voor de enige echte test: de praktijktest. Helaas is het dan te laat. Zelfs RFID-chips ter vervanging van barcodes zijn al geschikt voor het verzamelen van privacy-gevoelige informatie. Iedere RFID met een ingebakken serienummer kan worden gebruikt om te traceren waar mensen zijn geweest, wat hun aankoopgedrag is, etc. Er zijn diverse organisaties die al jaren waarschuwen voor deze ongewenste effecten van RFID. De mening van de industrie t.a.v. dit soort berichten is dat deze berichten erop gericht zijn om RFID helemaal boycotten en ze nemen dit niet zo serieus.

## Oplossingen en barrières

Gelukkig zijn er ook methodes om deze gevaren het hoofd te bieden. Zo zijn er RFID-jammers ontwikkeld waarmee de communicatie tussen RFID-tag en RFID-reader verstoord kan worden. Indien iemand zo'n jammer bij zich heeft, is het niet mogelijk om RFID-tags in zijn directe omgeving uit te lezen. Melanie is in een onderzoeksgroep bezig om de RFID-Guardian te ontwikkelen. Dit apparaat werkt iets verfijnder dan een jammer. Met behulp van de RFID-Guardian is het mogelijk om zelf te kiezen welke RFID-tags wel en welke niet uitgelezen mogen worden. Het apparaat bezit de mogelijkheid om aanvragen van RFID-readers te analyseren en op basis hiervan de communicatie wel of niet toe te staan. Hierdoor wordt het mogelijk om bijvoorbeeld je toegangspas voor het openbaar vervoer wel gewoon te laten communiceren, maar alle andere RFID-tags niet. Dit systeem is vergelijkbaar met een Firewall in je computer.

## Een stem

Volgens Melanie is het belangrijk dat de consumenten van zich laten horen en dat zij een hogere mate van veiligheid eisen. Er zijn al tests gedaan met een uitgebreidere beveiliging in RFID-chips, maar dit zijn nog labopstellingen. Om deze verbeterde beveiliging op grote schaal toe te passen is veel geld nodig. Zolang de consument genoeg neemt met minder veiligheid, is het voor de fabrikanten wellicht minder interessant om veel geld uit te geven voor deze extra beveiliging.

Op dit moment zijn een aantal commissies bezig met het maken van standaarden voor RFID. Het is te hopen dat deze standaarden hogere eisen gaan stellen aan de veiligheid van RFID dan nu het geval is. Uiteraard zijn de fabrikanten van RFID-chips ook in deze commissies vertegenwoordigd. Deze zijn erop gebrand om hun huidige technologie te kunnen gebruiken, aangezien ze anders veel geld moeten investeren om hun producten te verbeteren.

## Weerwoord

Naar aanleiding van deze resultaten hebben we Philips gevraagd om hierop te reageren, een van de grootste RFID-fabrikanten ter wereld. Philips laat weten op de hoogte te zijn van de gevaren rond de RFID-technologie. Men vindt het belangrijk om dit soort ontwikkelingen te volgen en vindt het ook interessant om te zien aan welke gevaren de RFID-technologie bloot staat. Wel merkt Philips op dat het belangrijk is om te weten hoe het virus getest is en dat het in dit geval gaat om een systeem dat juist is opgezet om gekraakt te worden. Het gevaar bij dit soort berichtgeving is dat dit ook gelezen wordt door mensen die niet zo goed op de hoogte zijn van de toegepaste methode. Dit kan leiden tot een verkeerde interpretatie van de gegevens en een verkeerd beeld bij de consument opleveren.

Volgens Philips zijn de door deze firma ontwikkelde RFID-tags die in paspoorten en betaalsysteem worden gebruikt dusdanig goed beveiligd dat deze veiliger zijn dan betalingsverkeer via internet. Zo levert Philips RFID-tags aan o.a. Visa voor hun 'banking cards'. Bij Visa zijn deze tags terdege getest voordat ze werden toegelaten in hun betaalsystemen.

Welke beveiliging wordt toegepast in een systeem heeft ook alles te maken met het soort applicatie waarvoor RFID wordt ingezet. Zo heeft Philips al meer dan 500 miljoen Mifare RFID-chips geleverd sinds 1994, die o.a. gebruikt worden in een betalingssysteem voor openbaar vervoer. Tot nu toe is er nog geen geval bekend waarin deze RFID-chip is gekraakt.

## Conclusie

RFID-tags gaan een steeds grotere rol spelen in onze samenleving. In hoeverre dit voor veiligheidsproblemen zal gaan zorgen, is nog koffiedik kijken, maar het staat als een paal boven water dat dit beslist nog kritisch bekeken moet worden. Zeker indien we ook bankzaken, medische gegevens en andere gevoelige informatie op onze RFID-tags met ons meedragen, is het belangrijk om deze informatie af te schermen voor onbevoegden. Aan de ene zijde vinden we de RFID-fabrikanten die ons nog meer luxe en gemak beloven bij het gebruik van RFID. Aan de andere zijde zijn er groeperingen die menen dat de komst van RFID de vooraankondiging is van de Apocalyps. Wie van beide kampen zal gelijk krijgen? Zoals meestal zal de waarheid wel ergens in het midden liggen. Wij zullen bij Elektuur deze ontwikkelingen in elk geval scherp in de gaten houden!

(060174)

## Weblinks:

<http://rfidanalysis.org/>  
[www.rfidvirus.org/](http://www.rfidvirus.org/)  
[www.riscure.com/](http://www.riscure.com/)  
[www.rfidjournal.com](http://www.rfidjournal.com)

