

De verwachtingen rond RFID zijn hooggespannen. Als we de geluiden van leveranciers en analisten mogen geloven, dan is ons hele leven binnen een paar jaar vergeven van de tags. Privacy-organisaties en security-specialisten maken zich ondertussen zorgen over de maatschappelijke consequenties van deze technologie. Wil RFID inderdaad doorbreken, dan zal een balans moeten worden gevonden tussen commerciële en private belangen.

Door Aad Offerman

B140NL465856DF7243KL<<<<<<22HK564038475

LZZI<<HAMD<<<<<22HK56

65856DF724NLDJANSEN<<HENDRIK<<<<22H
5B724>>NLDJANSEN<<HENDRIK<<<<22H

NC43140NL465856

374462304997467>>NLDBOUALZZI<<HAMD<<<<

De grenzen van auto-ID

RFID en PRIVACY

Op een bijeenkomst van de Vereniging voor Informaticarecht Advocaten (VIRA) gingen onlangs voor- en tegenstanders van het gebruik van RFID-tags met elkaar in discussie. Gastheren van de discussie waren het AICC en Vanderlande Industries. Sjoera Nas van Bits of Freedom (BoF), een organisatie die opkomt voor digitale burgerrechten en Jeroen Terstegge, Corporate Privacy Officer bij Philips zetten de voors en tegens uiteen. Waar de een waarschuwt voor een te grote inbreuk op de privacy pleit de ander voor grootschalige “maar gecontroleerde” inzet van automatische informatiedragers.

De goedkoopste RFID-tags, die we straks het meest gebruikt zullen zien worden, bevatten slechts een minimale hoeveelheid intelligentie. Ze doen niet veel meer dan hun unieke nummer roepen als ze via hun inductie-antenne voldoende stroom toegevoerd krijgen. Dat nummer is op zichzelf absoluut niet interessant; pas binnen de context van een applicatie krijgt het betekenis.

In de opzet van EPCglobal, die de RFID-standaarden voor de Supply Chain ontwikkelt, met name de Electronic Product Code (EPC) en de Gen2-interface, is de RFID-tag niet meer dan een nummerbord, vergelijkbaar met de barcode. Alle intelligentie zit in hun EPCglobal Network. Dat is een gedistribueerd systeem van servers waar fabrikanten, vervoerders, distributeurs

en retailers informatie over de gelabelde producten kunnen opvragen. Het gaat dan bijvoorbeeld om de vraag waar in de keten een item zich precies bevindt, of om meer inhoudelijke informatie als “wat voor smaak heeft dat kokosbrood?” en “wat voor kleur heeft die sweater?”.

Toegangscontrole

Elke deelnemer slaat zijn eigen gegevens op in zijn eigen lokale systemen. Heeft hij meer nodig, dan kan hij daarvoor bij anderen terecht. Daarvoor wordt gebruik gemaakt van registries (Object Name Service, ONS) die systemen kunnen vertellen waar specifieke informatie precies te vinden is.

Voor deze uitwisseling via de zogenaamde EPV Information Services (EPCIS) heeft EPCglobal een laag voor autorisatie (wie mag wat?) en toegangscontrole (wie ben jij?) bedacht. Een retailer zal een fabrikant immers alleen informatie willen geven over producten die daar vandaan komen. Een transporteur zal een retailer alleen informatie willen geven over zijn specifieke levering. En transporteurs en retailers zullen een fabrikant alleen informatie over zijn eigen producten willen geven als deze bijvoorbeeld aangevuld of teruggehaald moeten worden.

Naast dit EPCglobal Network voor dynamische data, ligt het Global Data Synchronization Network (GDSN). Dat wordt gebruikt om statische gegevens als productinformatie te verspreiden.

Ondanks dat EPCglobal aangeeft dat dat belangrijke zaken zijn, worden veiligheid en privacy in hun Frequent Asked Questions en Public Policy and Privacy statement pas helemaal onderaan genoemd. Privacy-aspecten worden vooral gezien als een belemmering voor de snelle, grootschalige invoering van RFID. En over de beveiliging wordt niet meer gezegd dan dat ‘het een belangrijk onderdeel is van het EPCglobal Network, en dat van leden wordt verwacht dat zij passende maatregelen zullen nemen’. Dat de beveiliging van de databases die door de deelnemers in de keten gedeeld moeten worden te weinig aandacht krijgt, is ook een van de zorgen van de Amerikaanse Federal Trade Commission (FTC).

Het Massachusetts Institute of Technology heeft wel een site waarop ze aandacht zeggen te schenken aan privacy, maar ook daar komen vooral de mogelijkheden en voordelen van RFID aan bod. Dat is niet zo verwonderlijk als we weten dat EPCglobal een commerciële spin-off van dit onderzoeksinstituut is. Wel staan er links naar een aantal rapporten van anderen waarin duidelijk gemaakt wordt dat aan terechte privacy-bezwaren eerst tegemoet zal moeten worden gekomen, wil RFID inderdaad kunnen doorbreken en al die beloften kunnen waarmaken.

In Nederland kwam het RFID Platform Nederland, een samenwerkingsverband van RFID-leveranciers en een enkele gebruiker, tot dezelfde conclusie: voor de acceptatie is >

RFID-angsten



TRACKING:



tags kunnen in de winkel worden gebruikt om het gedrag van de shopper heel nauwkeurig, haast real-time, in kaart te brengen. Dit geldt ook voor werknemers, waarvan met een tag niet alleen hun locatie altijd precies bekend is, maar waarvan ook hun gedrag en opbrengsten precies zijn te kwantificeren.

PROFILING:



EPC-nummers zijn uniek, en kunnen bij aanschaf via een klant- of betaalpas aan een unieke klant worden gekoppeld. Die profielen kunnen worden gebruikt om dynamische marketing te bedrijven: zo willen vervoerders de reisgegevens die ze straks met de OV-chipcard verzamelen ook voor direct marketing kunnen gebruiken.

SKIMMING:



tags kunnen in principe door iedereen met een antenne worden uitgelezen.

FUNCTION CREEP:



gegevens die voor het ene doel worden verzameld, worden later ook voor andere doelen gebruikt (secundair gebruik).

THE INTERNET OF THINGS':



elk fysiek object op aarde zou op termijn met een tag uitgerust en gevolgd kunnen worden; tags zijn wel 'de verbinding van alle voorwerpen aan het internet' genoemd.

de steun van de consument essentieel.

Hoewel item level tagging (het op item-niveau taggen) nog jaren weg is, zijn veel consumenten bang dat deze technologie ernstige inbreuk zal maken op hun privacy. Jeff van Hek, directeur van AIDC Consultants en bestuurslid van de Association for Automatic Identification and Mobility, kan zich deze angst heel goed voorstellen. 'Je ziet het niet, en je ruikt het niet. Tags beginnen gewoon uit te zenden zodra je ermee in de buurt van een elektromagnetisch veld komt.' In de position paper van Bits of Freedom (BoF) kunnen we dan ook lezen dat 'het gebruik van RFID-labels op consumentengoederen in winkels verstreckende negatieve gevolgen kan hebben voor de privacy van consumenten. Een onjuist gebruik van RFID tast de anonimiteit van kopers aan en kan zelfs een bedreiging vormen voor de vrijheid van onze samenleving in het algemeen'.

Grenzen opgezocht

De belangrijkste angsten zijn hiernaast op een rijtje gezet. Deze zijn nog eens versterkt door de eerste pilots waarbij inderdaad de grenzen werden opgezocht.

Benetton en Gillette kwamen beide onder vuur van consumentenorganisaties te liggen omdat zij het gedrag van hun klanten wilden vastleggen. Wal-Mart heeft van zijn proef met Gillette geleerd en het gebruik van RFID in ieder geval voorlopig beperkt tot de Supply Chain en het voorraadbeheer.

Spraakmakend was de Baya Beach Club in Rotterdam die zijn VIP's een implantaat aanbiedt waarmee zij toegang kunnen krijgen en af kunnen rekenen.

En recent bleek dat voor sommige werknemers hun toegangspas niet meer aan een touwtje om hun nek hangt, maar wordt geïmplanteerd. Voor functies waarbij toegang tot een kluis of computersysteem nodig is, wordt alleen nog een implantaat gebruikt. Hoewel de suggestie wordt gewekt dat een werknemer hier niet toe verplicht kan worden, kan Sjoera Nas van BoF zich niet voorstellen dat een werknemer zal weigeren. Het nieuwe beleid betekent immers dat hij 'zijn taak niet

meer kan uitvoeren'. Hetzelfde geldt voor ziekenhuispatiënten. 'In het AMC loopt een proef waarbij medicijnen, patiënten en verplegers van RFID-tags zijn voorzien. Dan is het nog maar een kleine stap naar het injecteren van een implantaat.'

Controle

Inmiddels wordt ook hard nagedacht over manieren waarop een consument tegen dergelijke praktijken beschermd zou kunnen worden. Een deel daarvan is technisch, een ander deel beleidsmatig.

Volgens Jeroen Terstegge zouden consumenten de controle over de tag moeten krijgen na het point-of-sale. Hij is als Corporate Privacy Officer binnen het juristen-team van Philips onder andere gespecialiseerd in de privacy-aspecten van e-commerce. Dat bedrijf is de grootste fabrikant van RFID-tags ter wereld, en heeft, afhankelijk van het type, 40 tot 75 procent van de markt in handen. 'Over tien jaar verwachten we 1 triljoen tags te fabriceren. Deze markt is dan 25 tot 50 miljard dollar groot, waarvan een kwart zal worden uitgegeven aan chips en driekwart aan infrastructuur en diensten.' Hij maakt daarbij een belangrijk onderscheid tussen identificatie-technieken waarbij mensen aan informatie, entertainment en diensten worden gekoppeld, en de identificatie en het volgen van goederen.

Killen

'Een klant zou bijvoorbeeld de mogelijkheid kunnen krijgen de tags op zijn aankopen te "killen" voordat hij de winkel uitstapt', zegt Terstegge. 'Dat hoeft echter niet automatisch, want er er zijn ook toepassingen daarna die voor de consument interessant zijn. Zolang technologie een doel dient, moet die mogen.' Sjoera Nas voorspelt echter lange rijen voor de uitschakelkiosk. 'Uitschakelen van de tags zal door de winkeliers ontmoedigd worden, omdat er voor hun zulke interessante dingen mee te doen zijn. Voor hen is het uitschakelen een kostenpost.'

Behalve een expliciete kill-opdracht zou dit uitschakelen ook kunnen door de tag met rotzooi te overschrijven, door de tag simpelweg te verwijderen (removable tags), of

EPCGLOBAL PRIVACY-RICHTLIJNEN

EPCglobal is zich er sterk van bewust dat het rekening moet houden met de privacy van de consument als het RFID snel wil invoeren in de keten. De organisatie heeft daarom een viertal richtlijnen vastgesteld waar RFID-gebruikers zich aan zouden moeten houden.

Consumenten moeten duidelijk aan een product kunnen zien dat er een RFID-label op zit, bijvoorbeeld met behulp van een EPC-logo. De verantwoordelijkheid hiervoor ligt bij fabrikanten en retailers.

Consumenten moet duidelijk worden gemaakt dat zij de tag kunnen verwijderen of (in de toekomst) uitschakelen. Er wordt van uit gegaan dat de tags zich meestal in of op de verpakking zullen bevinden.

Consumenten moet uitgelegd worden wat EPC- en RFID-technologie precies is en waartoe het dient.

De EPC-organisatie verzamelt geen consumentengegevens; dat wordt gedaan door de afzonderlijke bedrijven die deze technologie gebruiken.



door de antenne kapot te maken (scratchable antenna). Alternatief is een "deep sleep" modus waarbij de tag later ook weer geactiveerd zou kunnen worden. Een andere tijdelijke oplossing zijn de blocker-tags van RSA Security. Deze verstoren het signaal van de eerste tag. Nog een hele praktische oplossing: Amerikaanse paspoorten met een tag zullen straks twee metaallagen bevatten (RF-shielding), zodat de tag alleen kan worden uitgelezen als het paspoort opengeslagen is.

Sowieso vindt Terstegge dat er nooit persoonsgegevens op een smart-tag opgeslagen mogen worden. 'Dat mag alleen in smartcards. Vanwege de prijs wil men wel steeds meer persoonsgegevens in labels en tags opslaan. Die zijn echter niet beveiligd.' Nas noemt het idee dat duurdere chips wel goed beveiligd zijn echter een mythe.

Regelgeving

Opvallend is dat de zorgen van consumenten geen van alle over de technologie op zich gaan, maar vooral over de informatie die ermee verzameld kan worden. Dat betekent dus dat gezocht moet worden naar een manier om deze technologie op een acceptabele manier te kunnen gebruiken.

Een tweede belangrijke constatering is dat alle bezwaren zich richten op item level tagging en de koppeling met persoonlijke gegevens, niet op het gebruik van RFID in de Supply Chain. De waardeketen en voorraadbeheer zijn ook de plekken waar RFID ons de komende jaren het meest te bieden heeft.

Het gebruik van RFID op item-niveau en na de point-of-sale duurt nog jaren. Volgens sommigen komt het zover zelfs nooit. Bovendien wordt betwijfeld of er business modellen zijn waarbij bedrijven informatie over hun tags met elkaar gaan delen. Terstegge meent echter dat item level tagging breedschalig zal worden ingevoerd als de prijs per tag onder de dollarcent duikt. Volgens hem is het slechts een kwestie van tijd. 'Dat is waar de markt naar toe groeit.'

Op dit moment lijkt het er nog op dat het point-of-sale het natuurlijke punt is waarop tags vooralsnog gedeactiveerd zullen gaan worden. Er zijn partijen die de beperking tot de keten al willen vastleggen in wetgeving. Volgens anderen is het daarvoor nog te vroeg. In een aantal Amerikaanse staten zijn al wetsvoorstellen rond het gebruik van RFID ingediend. En ook op Europees niveau en in Azië wordt over de noodzaak van wetgeving nagedacht. In het rapport

'Privacyrechtelijke aspecten van RFID' zegt ECP.NL, dat nauw samenwerkt met het RFID Platform Nederland, dat aparte wetgeving voor RFID niet noodzakelijk is. Wel kan het nodig zijn de bestaande formuleringen in de privacy-wetgeving aan te passen. Zij spreken van de "noodzaak van een verantwoorde invoering van RFID in onze samenleving".

Wal-Mart en Procter & Gamble hebben gezegd zich aan de huidige richtlijnen te houden en geen tags uit te lezen op de winkelvloer. Marks & Spencer zegt het gebruik van tags te beperken tot de Supply Chain, en niet in de winkel. ECP.NL vindt dat RFID-tags wel in de winkel gebruikt mogen worden, zolang dat is om de winkel optimaal in te richten, niet om de klanten te kunnen volgen. Het precieze onderscheid is echter lastig aan het publiek uit te leggen.

Nieuwe richtlijnen

Terstegge meent dat op de lange termijn, hij spreekt dan over de "sensor age" waarin computers niet alleen meer nadenken maar ook waarnemen en reageren op hun omgeving, zeker nieuwe privacy-richtlijnen nodig zijn. 'De huidige principes zijn 25 jaar oud. Het wordt tijd voor nieuwe. Het gaat straks niet meer om persoonlijke

Privacy-aspecten worden vooral gezien als een belemmering voor de snelle, grootschalige invoering van RFID

gegevens maar om elektronische footprints. Deze zijn niet herleidbaar tot mijn persoon, maar hebben wel een impact op mijn leven.' Een ander probleem dat hij noemt is de consumer-to-consumer privacy. 'Het gaat niet meer alleen om Albert Heijn en de douanebeambte, maar ook om mijn burens en gezinsleden.'

Terstegge ziet twee manieren om de privacy te waarborgen. De eerste is privacy-by-design, waarbij de technologie beperkingen oplegt aan wat een system integrator ermee kan. De tweede is trust-but-verify, waarbij belangrijke zaken in regelgeving worden vastgelegd. 'Nadeel daarvan is wel dat deze maatregelen alleen achteraf

met behulp van audits gecontroleerd en gesanctioneerd kunnen worden.'

Alle rapporten wijzen erop dat de invoering en de opbrengsten van RFID zullen vertragen als er te veel van de consument gevraagd wordt. Er is met RFID in de Supply Chain al enorm veel te halen: het optimaliseren van de keten, vermindering van voorraden en vertraging, verhoging van de zichtbaarheid, vermindering van "shrinkage", minder fouten, fouten worden gecorrigeerd in het proces in plaats van achteraf, Tracking & Tracing, het gebruik van temperatuur- en schoksensoren, en het automatisch afprijzen van artikelen die tegen de datum aan zitten.

Er zijn zeker ook goede argumenten om tags nog na het point-of-sale geactiveerd te laten, zonder daarbij de privacy van de klant in de knel te brengen, bijvoorbeeld voor Product Lifecycle Management, en het afhandelen van retouren, garantie en callbacks. Op die manier kan verder worden geprofiteerd van al gedane investeringen.

Toch lijkt het erop dat deze laatste mogelijkheden voorlopig opgeofferd moeten worden om deze technologie überhaupt geaccepteerd te krijgen. De Information and Privacy Commissioner in Ontario, Canada, vat het in één zin samen: "Good privacy is good business".

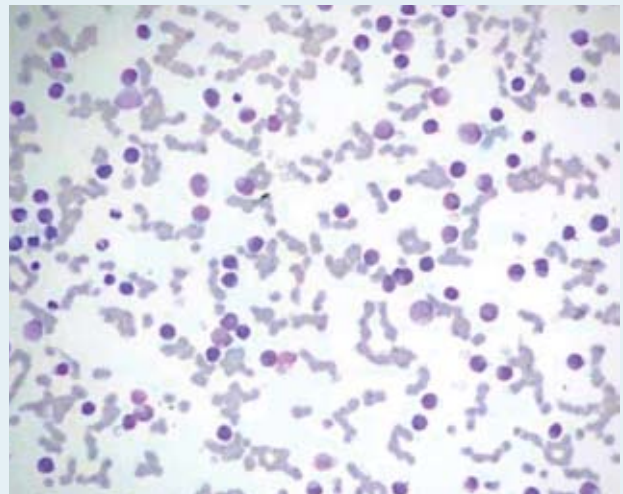
VIRUSSEN VIA RFID-TAGS

Onlangs kwamen onderzoekers van de Vrije Universiteit, waaronder de bekende operating system-specialist Andrew Tanenbaum, met een rapport waarin zij wijzen op het gevaar van virusbesmettingen via RFID-tags. In die publicatie beschrijft het team hoe een virus in een supermarkt, bij de dierenarts of op een luchthaven van de tag wordt gelezen, in de achterliggende systemen terecht komt en vervolgens verder verspreid wordt. In het laatste geval wordt een scenario geschetst waarbij binnen een dag honderden luchthavens worden besmet. Terroristen kunnen deze techniek gebruiken om infrastructures plat te leggen, en drugsmokkelaars om hun illegale waren ongemerkt te kunnen verplaatsen.

De methoden die Tanenbaum e.a. gebruiken zijn hele bekende: een **SQL injection attack**, waarbij met het uitlezen van de string ook een database-opdracht wordt meegegeven, de **buffer overflow-aanval**, waarbij gehoopt wordt dat via een niet goed afgeschermd buffer ook programma-code kan worden weggeschreven, en het **verbergen van JavaScript-code** in een string, die uitgevoerd wordt zodra een tag-waarde op een web-pagina wordt weergegeven.

Natuurlijk zijn er een heleboel mensen (en belanghebbenden) over Tanenbaum en zijn team heengevallen. Zijn voorbeelden werden geconstrueerd, vergezocht en onwaarschijnlijk genoemd. Dat is inderdaad zo voor de meest eenvoudige chips. De goedkopere stekers heel eenvoudig in elkaar: ze geven ze alleen hun unieke nummer - vergelijk de UPC-barcode. Naarmate de prijs van de tags lager wordt, zullen steeds intelligenter chips toegepast worden. Op de echt lange termijn wordt misschien zelfs de kloof gedicht met de contactless smartcards die nu nog enige tientallen dollars per stuk kosten.

Intelligenter chips betekenen meer complexiteit, en dat betekent meer gelegenheid voor programmeurs om fouten te maken, en meer



Virussen via RFID. Onnodige angst of realiteit?

gelegenheid voor kwaadwillenden om er rottiigheid mee uit te halen. Bruce Schneier, een bekend auteur in de security-wereld, noemde in BusinessWeek RFID-tags dan ook kleine draagbare computers zonder scherm en toetsenbord. "Het zou best kunnen dat RFID-tags niet worden gekraakt, maar dat zou dan de eerste keer ooit zijn dat een dergelijke, onkraakbare computer werd gemaakt..."

Hoewel de replicatie van RFID-virussen en -wormen door Tanenbaum niet goed is uitgewerkt en aannemelijk gemaakt, is het controleren van wat complexere invoer van buiten een reëel probleem. Ondanks dat dat hele bekende fouten zijn, wordt er nog steeds succesvol gerommeld met de parameters van URL's om via de applicatie de web- of database-server binnen te dringen, op precies dezelfde wijze die de onderzoekers in hun paper voor RFID schetsen.