Med storebror i byxfickan

Från snokande kläder till människokartor – integritetsrisker med RFID-chips

PÄR STRÖM

OBS! Förbjudet att programmera om detta chip till exempelvis busskort eller nyckel.

Med storebror i byxfickan

PÄR STRÖM

Med storebror i byxfickan

Från snokande kläder till människokartor – integritetsrisker med RFID-chips

Den Nya Välfärden

den nya välfärden

Box 5625, 114 86 Stockholm

08-545 038 10 | www.dnv.se

Utgivet av Den Nya Välfärden

Roligt värre *(2006)*
Med storbror i uppfinnarverkstan
– ny digital övervakning från automatiska öron till internetdammsugare (2006)
Med storebror i baksätet
– digital övervakning av dina bilfärder (2006)
Nya Beska droppar
– korta kritiska krönikor (2006)
Första hjälpen
Om dina anställda blir sjuka – en liten handbok (2006, 2007)
Var tredje får inte vara med
– en studie om arbetslösheten bland invandrare (2006)
Hur hög är arbetslösheten, egentligen? *(2006)*
Ole, dole, arbetslös
– nästan 3 av 10 ungdomar 16-24 år saknar jobb (2006)
Ge de arbetslösa en chans
– 150 000 nya jobb genom halverade arbetsgivaravgifter (2006)
Så lyckas du som företagare
– de bästa tipsen från svenska entreprenörer (2005)
Bakom skurkar och skandaler *(2004)*
Värsta krånglet *(2004)*
Jobbet är att mata puman
– hur och varför försäkringskassorna slarvar bort 40 miljarder om året av skattebetalarnas pengar (2004)
Tankebok för entreprenörer
– 222 citat från Aristoteles till Ingvar Kamprad (2003)
Entreprenören bakom allt
– 101 svenska succéer från ABBA till ölburkar (2002)
Beska Droppar
– korta kritiska krönikor (2002)
Skärp dig, Svensson
– med deklarationen om medborgerliga skyldigheter (2002)
Personvalsparti
– bot för trötta partier (1999)
Berättelsen om jobben *(1996)*
Baksmällan
– förutsättningar för politisk tillnyktring (1995)
Molnstoden
– en vision för svenska folket (1994)

Den Nya Välfärden har även givit ut Medborgarnas offentliga utredningar

MOU 2000:1 Sveriges två gränser – om invandrarpolitiken
MOU 1999:1 För Sverige – på tiden!
MOU 1998:1 Samhällsmoral i praktiken
MOU 1997:1 Entreprenören i högsätet
MOU 1996:2 Kommunala företag – hot mot demokrati
MOU 1996:1 Den nya arbetsrätten – ett förslag
MOU 1995:3 Järntrianglar – förnyelsens fiende nummer ett
MOU 1995:2 Irrfärdens slut – för sunda statsfinanser
MOU 1995:1 När folkhemmets barn blivit vuxna
MOU 1994:1 HSF-modellen – patientmakt och kvalitet
MOU 1993:2 Charta Nova – politik för entreprenörskap
MOU 1993:1 Barnomsorg enligt kundvalsmodellen
MOU 1992:2 Hälso- och sjukvård för 2000-talet
MOU 1992:1 Eget val i äldreomsorgen – handledning
MOU 1991:6 Hur man säljer allmännyttehus – handledning
MOU 1991:5 På egna ben – reformera organisationsstödet
MOU 1991:4 Skolpeng hösten 92 – en handlingsplan
MOU 1991:3 Självständiga kommuner
MOU 1991:2 Sänkta skatter för en ny välfärd
MOU 1991:1 Företagsamhetens förutsättningar
MOU 1990:3 En marknad för bostäder åt alla
MOU 1990:2 Medborgarnas miljömanifest
MOU 1990:1 Minska statsskulden – sälj tillgångar
MOU 1989:1 Sänkt skatt för alla
MOU 1988:1 En ny grundlag – ett förslag

Innehållsförteckning

Förord

RFID-chips, även kallade radioetiketter eller smarta etiketter, är en sorts radiosändare som är platta som ett papper. Det är en alldeles utmärkt teknologi, som i likhet med telefonen har en väldig potential att bli till nytta för mänskligheten på mängder av områden. I de allra flesta fall är det problemfritt.

Det finns dock ett undantag. Så snart RFID-chips hamnar på människor – antingen direkt eller indirekt via föremål som människor har med sig – blir det känsligt. Då finns nämligen risken att människorna blir avlästa, spårade och kartlagda av bara farten när föremålen blir det. I värsta fall kan spårning och övervakning av människor till och med vara själva syftet – legalt eller illegalt.

Denna rapport är ingen teknikfientlig skrift. Den är däremot fientlig mot kränkande nyfikenhet och klåfingrighet rörande känsliga personuppgifter. Låt oss följa EU:s IT-kommissionär Viviane Redings uppmaning att ta RFID till våra hjärtan – men låt oss göra det med respekt för människors personliga integritet!

Jag vill rikta ett tack till Electrona-Sievert AB i Stockholm som välvilligt ställt upp med RFID-chips att klistra på omslaget till denna rapport.

Pär Ström i juni 2007

Finns som PDF och talbok

Denna skrift kan laddas ned gratis som PDF-dokument och som talbok i mp3-format från www.dnv.se. Skriften får i alla sina former kopieras och spridas fritt om det görs icke-kommersiellt. Den får också citeras fritt om källan anges.

Tidigare rapporter

”Med storebror i byxfickan” är den tredje i en serie rapporter om personlig integritet och övervakningssamhället som givits ut av Integritetsombudsmannen/Den Nya Välfärden. Under 2006 utgavs ”Med storebror i baksätet” (om bilövervakning) och ”Med storebror i uppfinnarverkstan” (om nya avancerade övervakningsteknologier). Dessa kan beställas på papper från www.dnv.se eller laddas ned som PDF- eller mp3-fil.

RFID i ett nötskal

- Platta ”radiosändare” som inte behöver batteri
- Kan avläsas med antenn genom olika slags barriärer
- Räckvidd från några centimeter till flera meter
- Kostar under 1 krona i stora serier (sjunkande pris)
- Används redan idag i exempelvis kläder, passerkort och djur
- Finns i en mängd utföranden avseende t.ex frekvens, storlek och intelligens
- RFID-chippet på omslaget av denna rapport är riktigt

1. Vad är RFID och hur fungerar det?

Vi har fått ett samhällsklimat där det blivit politiskt acceptabelt – till och med nödvändigt – att övervaka medborgarna in i minsta detalj. Det är mot den bakgrunden man ska se på integritetsriskerna med de RFID-chips (även kallade radioetiketter eller smarta etiketter) som snart kan finnas i var mans ficka och väska.

Men även om staten är en viktig potentiell ”storebror” är det inte den enda. Butiker och andra företag kommer att frestas att använda RFID för att i smyg skaffa sig information om kunder, och bedragare av olika slag kan komma att missbruka RFID-försedda kort och tillhörigheter.

Låt oss börja från början. En så kryptisk beteckning som RFID tarvar en förklaring. Bokstavskombinationen utgör en akronym för ”radio frequency identification”, vilket enklast översätts som ”identifiering med radiovågor”. Ett RFID-chip ”sover” tills det känner av en signal från en apparat kallad RFID-läsare, som med radiovågor skickar ut frågan ”vilka RFID-chips finns här?”. Då svarar alla närvarande chips genom att skicka sitt nummer. En RFID-läsare skickar ut sådana frågor hela tiden, och klarar ofta att genomföra 100-150 läsningar per sekund.

Numret från RFID-chippet används sedan av ett datasystem för att identifiera det föremål (eller djur, eller i vär-

sta fall människa) som bär chippet. I en databas ligger sedan information om föremålet. Ett visst nummer kan exempelvis betyda ”Coca Cola light, 33 cl, burkexemplar nr 21328564” eller ”Skjorta från Stenström, vit med bruna vertikala ränder, strykfri bomull, storlek 42, krage med snibbar, exemplar nummer 456777” eller ”730217-1754” (alltså ett personnummer, här påhittat).

I en del fall kan informationen om föremålet ligga lagrat i själva RFID-chippet, men det är mindre vanligt eftersom chips med stort minne är dyra. Eftersom den oftast förekommande typen av RFID-chips (som kallas passiva) hämtar sin energi från RFID-läsarens radiovågor behövs inget batteri – och därmed får chippet obegränsad livslängd.

Ett RFID-chip kan vara oerhört litet, de minsta är ungefär som ett sandkorn. Emellertid kan de inte fungera utan en antenn, en spiral som normalt är mycket större än chippet (men platt). Chip plus antenn kallas tillsammans för ”tag”. Hittills har jag i denna rapport av enkelhetsskäl använt termen ”chip” för denna helhet, vilket alltså egentligen är fel. Från och med nu används benämningen ”tag” för helheten. En RFID-tag är alltså en komplett radioetikett.

Ju större antennen är, desto längre blir det avstånd på vilket taggen kan läsas av. Storleken för hela taggen ligger ofta mellan några centimeter och en decimeter.

Läsavståndet är en viktig faktor, och det varierar mycket. Vissa typer av RFID-taggar har bara några millimeters räckvidd, medan andra kan läsas av på ett par meters avstånd. Avgörande är inte bara storleken på taggens antenn, utan även storleken på RFID-läsarens antenn, vilken styrka (uteffekt) som RFID-läsaren har och hur miljön påverkar radiovågornas utbredning. Det innebär att för en och samma tag kan det maximala läsavståndet variera en hel del. Det är

värt att notera att lagen sätter en (ganska låg) gräns för hur stor uteffekt en RFID-läsare får ha. En illegitim RFID-läsare från en obehörig kan naturligtvis ha konstruerats för en större uteffekt, vilket väsentligt kan öka läsavståndet.

Nämnas bör att det också finns RFID-taggar med inbyggt batteri. Dessa kallas aktiva, och kan läsas av på tiotals meters avstånd. Aktiva RFID-taggar är mycket större och dyrare än passiva. De kallas ofta transpondrar, och förekom bland annat i den första versionen av Stockholms biltullar.

Eftersom RFID-tekniken använder sig av radiovågor behövs inte fri siktlinje. En tag kan därför avläsas genom många material, exempelvis papp och trä. Dock kan radiovågor inte passera genom metall, vilket gör att metall skärmar av RFID-taggar. Blotta närvaron av metall kan ibland ställa till med problem för RFID-tekniken, liksom närvaron av vätska.

Det är en myt att RFID-taggar kan läsas av via satellit. RFID har inte heller någonting med GPS-positionering att göra. RFID-taggar kan bara läsas när de befinner sig nära en RFID-läsare.

1.1 Hur används RFID?

Man kan se på RFID som en ersättare för streckkoder. Så fort man vill ha kontroll på något, med möjlighet att läsa av dess läge eller förflyttningar, kan RFID användas (under förutsättning att man har placerat ut RFID-läsare som täcker det aktuella området).

RFID kommer sannolikt att få en mycket bred användning i samhället. Många tror att RFID imorgon är lika självklart och välspritt som telefonen är idag. RFID förekommer redan idag i Sverige i vissa landstingskläder (för att underlätta sorteringen i tvätteriet), på soptunnor, i skidåkares

liftkort, i pass, inopererat i husdjur, i spån och flis som flyter genom en tillverkningsprocess, i arbetsplatsers passerkort, i kollektivtrafikens resekort, på fiskar för att forskare ska kunna följa deras rörelser, på verktyg i verkstäder och på biblioteksböcker. Och på många andra ställen.

Vissa landsting har numera börjat märka sina kläder med RFID-taggar

I de allra flesta fall är RFID en utmärkt teknologi som inte medför några risker för den personliga integriteten. Denna rapports författare vill därför ta avstånd från de försök att demonisera RFID som vissa aktivister driver. Dock är det så att så snart RFID-taggar hamnar på människor – direkt eller indirekt – blir det känsligt eftersom människan kan bli utsatt för dold spårning, avläsning och kartläggning. Vi ska nu titta på några exempel, genomförda eller föreslagna, där RFID utgör en integritetsrisk.

2. Harry Potters magiska karta i verkligheten

2.1 Människokartor på flygplatser

I Harry Potter-böckerna och –filmerna förekommer en magisk karta, som sekund för sekund visar var på slottet Hogwarts varje människa befinner sig. Sådana människokartor håller på att förverkligas, med RFID-tekniken som möjliggörare. Flera initiativ har tagits där sådana provas eller erbjuds till försäljning. Bland annat ger EU ekonomiskt stöd till utveckling av ett system för människokartor som i huvudsak är avsett för flygplatser – låt oss studera det.

Så här är det tänkt. Vid incheckningen på flygplatsen ska varje passagerare förses med en RFID-tag. Exakt hur det ska ske är inte bestämt, den kan komma att sättas i boardingcardet, eller också på passageraren genom en rem om halsen eller handleden. Ett nätverk av RFID-läsare kommer sedan att kartlägga varje persons läge ungefär en gång i sekunden med en noggrannhet av cirka 1 meter.

I ett datasystem läggs den informationen samman med bilder från ”smarta” övervakningskameror av panoramatyp. Människornas rörelser på flygplatsen syns sedan som gröna prickar som rör sig, inlagda på videobilderna från övervakningskamerorna. Varje människoprick har ett num-

mer eller annan identifikation som gör att övervakaren vet vem som är vem.

Teknologin utvecklas av ett konsortium bestående av bland annat Centre for Security and Crime Science vid University College of London (UCL), Telecommunications Systems Institute i Grekland och Debrecen-flygplatsen i Ungern. En testversion ska tas i drift på Debrecen-flygplatsen, och enligt de involverade institutionerna och företagen ska systemet göras tillgängligt för andra flygplatser år 2008.

Harry Potter-kartorna ska inte bara följa varje människas rörelser, de ska också tolka flygpassagerarnas beteende. Vid ”onormalt” beteende ska detta analyseras och lagras. I ett senare skede finns planer på att komplettera systemet med biometriska data. I första hand nämns ansiktsdata, att användas för att möjliggöra automatisk ansiktsigenkänning i övervakningskamerorna.

Här skulle vi ha visat människokartan, men konsortiet nekade publicering när de anade temat för denna rapport. *"This is one of the rare occasions when I have to refuse permission to use our images"*, skrev de i sitt svar.

Se bilden på:
www.optag-consortium.com

Huvudsyftet med människokartorna är inte oväntat att identifiera människor som kan misstänkas planerara terrordåd, men konsortiet ser även andra tillämpningar. Exempelvis för de samtal med flygplanstillverkaren Airbus, som håller på att utveckla ett så stort flygplan (700 passagerare) att ombordstigningen kan ta så lång tid att förseningar kan uppstå. Därför finns tankar på att använda människokartorna till att strax före ombordstigningstid titta efter var alla som ska med på den aktuella flighten befinner sig och sedan skicka ut ”springare” (mänsklig personal) som hämtar eventuella passagerare som befinner sig långt bort från den rätta utgången.

En talesman för utvecklingsprojektet, associate professor Paul Brennan vid University College of London, ser i förlängningen möjligheter att använda Harry Potter-kartorna även på andra platser än flygplatser. ”Tillämpningar finns överallt där det finns många människor”, säger han till nyhetstjänsten ZDnet. Här osar det alltså katt ur ett integritetsperspektiv (ändamålsglidning på gång!).

Ett annat projekt syftande till att utveckla människokartor för flygplatser har startats i den brittiska staden Manchester. Där är syftet kommersiellt – informationen om människors position och förflyttningar ska användas för att öka försäljningen i flygplatsens butiker. Undersökningar sägs visa att passagerare på flygplatsen gör av med drygt en krona per minut, och då är det förstås intressant att veta exakt var dessa vandrande plånböcker befinner sig. Ett pilotprojekt har redan genomförts, RFID-taggarna hängdes då om halsen på plånböckerna – förlåt, människorna. Nu ska man gå vidare med en annan och kostnadseffektivare typ av RFID-taggar.

”Tillämpningar finns överallt där det finns människor”

Associate professor Paul Brennan, University College of London, om breddad användning av människokartor

2.2 Barns rörelser i skolan registreras

En amerikansk skola har provat ett system som via RFID-märkning av eleverna registrerar när dessa går in i ett klassrum eller på toaletten. Efter protester från en del av föräldrarna har systemet dock stängts av.

Skolan heter Brittan Elementary School och ligger i staden Sutter i Kalifornien. Där går barn från förskoleåldern upp till klass nio, men det var bara barn i åttonde och nionde klass som fick radiosändare och loggades. Systemet, som heter InClass och kommer från företaget InCom Corporation, marknadsförs nu brett mot skolor i hela USA. Så här fungerar det:

Varje barn får en RFID-försedd namnbricka (”badge”) att bära om halsen. RFID-läsare sätts ovanför de dörrar man vill bevaka. Dessa känner av varje passage och lagrar information i en databas om var och när varje barn har passerat, inklusive automatiska noteringar om eventuell sen ankomst. Lärarna får vid varje lektions början en närvarolista trådlöst sänd till sin handdator, vilket sägs underlätta närvarokontrollen. Den centrala databasen med barnens passager ska också hjälpa till att ”stävja skolk, vandalisering och förbättra barnens säkerhet” enligt den officiella motiveringen.

I installationen på Brittan Elementary School sattes avläsare även upp ovanför dörrarna till toaletterna i skolmatsalen. Syftet med det är inte känt. Måhända ingick det i stävjandet av vandalisering.

Många föräldrar reagerade negativt på förflyttningsloggningen och protesterade till skolledningen. Andra föräldrar, däremot, uppskattade systemet. Efter en tid blev trycket på skolledningen för hårt och systemet stängdes av.

En skola i Texas har också satt RFID-brickor på eleverna och loggar när de går på och av skolbussarna. Polis och skolledning har tillgång till informationen. Flera skolor i Japan har satt RFID på lågstadiebarn, och läsare i dörrarna loggar när de kommer till skolan respektive lämnar den. Vid vissa japanska skolor skickas automatiskt ett SMS- eller epostmeddelande till föräldrarna vid varje ankomst respektive hemgång. Syftet är ökad säkerhet.

En skola i den japanska staden Wakayama går ett steg längre. Tillsammans med Ministeriet för telekommunikationer planerar de att utöver RFID-läsarna i skolans dörrar skapa ett system med RFID-läsare på ”farliga platser” runtom i staden. Om ett RFID-märkt barn kommer i närheten av en sådan skickas genast ett epostmeddelande till föräldrarna. Automatisk RFID-baserad kontroll ska också ske av att barnen går av bussen vid rätt hållplats.

2.3 Personals och kunders läge övervakas

- Alla anställda som flygbolaget Finnair har på flygplatsen Vantaa utanför Helsingfors blir ständigt geografiskt loggade. De har nämligen försetts med en mobiltelefon med inbyggd RFID-tag, vilken hela tiden pejlas av ett nätverk med RFID-läsare.

- Alla anställda, underentreprenörer och besökare på oljebolaget BP:s raffinaderi i Cherry Point i den amerikanska delstaten Washington har försetts med en RFID-bricka, och pejlas därmed på samma sätt. Detta system kallas ”Location aware safety system”, och syftar till att ge kännedom om de anställdas exakta position i händelse av en olycka.

- I den japanska staden Yokohama har mobiloperatören DoCoMo testat ett system för marknadsföring i butiksmiljö. I varuhuset Takashimaya har 150 RFID-taggar placerats ut, och 90 kunder har försetts med en mobiltelefon med inbyggd RFID-läsare. När kunderna rör sig i butiken känner telefonen av vilken RFID-tag de är närmast, och därmed registreras deras exakta läge. Den informationen skickas kontinuerligt till en databas. En programvara tolkar varje kunds beteende och försöker lista ut vad kunden söker efter. Därefter skickas erbjudanden till kundens mobil, baserat på vederbörandes förmodade avsikter. Man kan anta att en kund som stannar till och tittar lite på herrskor, exempelvis, strax får ett erbjudande rörande just herrskor.

Länkar:
Flygplats: www.optag-consortium.com
Skolsystemet:www.incomcorporation.com

3. Resenärer som pejlas på åtta meters avstånd

En försmak av ett kommande RFID-samhälle kan erhållas genom att studera vad det amerikanska Department of Homeland Security (”Säkerhetsdepartementet”) planerar. De har begärt in anbud från näringslivet på tekniska lösningar för att göra ”resedokument” (bör rimligtvis tolkas som pass) trådlöst avläsningsbara på åtta meters avstånd. Utan att resenärerna vidtar några åtgärder, eller ens vet om det, ska deras RFID-märkta resedokument kunna avläsas av myndigheterna.

Detta framgår av en så kallad Request for Information som säkerhetsdepartementet i USA har utfärdat. I dokumentet vänder man sig till näringslivet med uppmaning att föreslå användbara tekniska lösningar. Syftet är att automatiskt kunna avläsa människors passager vid olika typer av gränsövergångar.

Det man begär är en lösning som i förlängningen skulle möjliggöra en mycket långtgående övervakning av individers förflyttningar. Här följer några översatta utdrag ur dokumentet (som i sitt originalutförande finns tillgängligt via länken nedan):

”Myndigheterna begär att identiteten ska kunna avläsas i alla situationer, inklusive om enheten bärs i en ficka, hand-

väska, plånbok, i resenärens kläder, eller vid resa i fortskaffningsmedel (såsom i bil, lastbil eller buss).”

”Resenären ska inte behöva göra någonting för att enheten ska bli avläst”

”Avläsare är placerade i dörrar och i filer för fotgängare och fordon”

”Den presenterade lösningen måste känna av den datainfångande teknologin för en gående person på 25 fots [8 meters] avstånd. Den presenterade lösningen måste känna av alla enheter som bärs av resande i en bil, lastbil eller buss på ett avstånd upp till 25 fot medan fordonet rör sig i hastigheter upp till 55 miles per timme [88 km/h]. För busstrafik måste lösningen kunna känna av upp till 55 enheter.”

Säkerhetsdepartementets förhoppning är att den valda tekniska lösningen ska utvecklas till en internationell standard. Man skriver: ”Informationen kan också komma att användas för att etablera internationella standarder avseende gränskontroll, passagerarhantering och reseunderlättande system”. Lyckligtvis har säkerhetsdepartementet tänkt på den personliga integriteten. ”Resenärernas integritet ska inte kränkas”, står det mot slutet av upphandlingsunderlaget.

Om den ovan beskrivna teknologin införskaffas och tas i drift av amerikanska myndigheter skulle det bli mycket lätt för myndigheterna att även övervaka människors förflyttningar inom landet. Ett avläsningsavstånd på åtta meter är ju tillräckligt för de flesta avläsningsmiljöer, såsom på gator och torg, längs trafikleder, vid järnvägsstationer, i shoppingcentra och liknande. Det skulle också bli lätt för poliser att via handhållen utrustning identifiera människor i exempelvis en demonstration.

Länk:
Upphandlingsdokument:www.dnv.se/travelsurveillance.pdf

”Myndigheterna begär att identiteten ska kunna avläsas i alla situationer, inklusive om enheten bärs i en ficka, handväska, plånbok, i resenärens kläder, eller vid resa i fortskaffningsmedel (såsom i bil, lastbil eller buss)”

Amerikanska Department of Homeland Security i ett förfrågningsunderlag rörande teknologi för fjärravläsbara resehandlingar

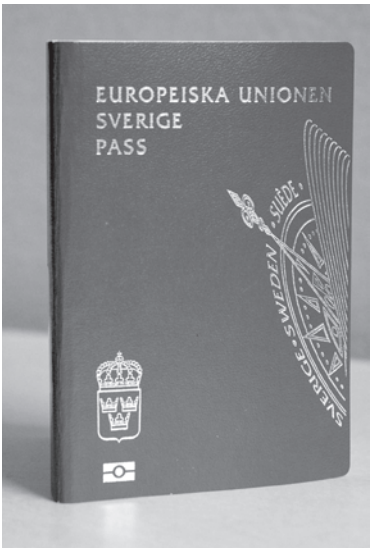
4. Pass i Sverige och andra EU-länder

Sedan hösten 2005 är alla pass som utfärdas i Sverige försedda med en RFID-tag. För att kunna läsa av den krävs två saker:

1. En RFID-läsare som är programmerad med ett särskilt protokoll (kommunikationsspråk) och en krypteringsalgoritm. Såväl läsaren, protokollet som krypteringsalgoritmen är tillgängliga för vem som helst på den öppna marknaden.
2. En digital nyckel, unik för varje pass, som består av en nummerkod. Den är hemlig men står skriven på passet.

Ett problem ur säkerhets- och integritetsperspektiv är att nyckeln i Sverige är ganska lätt att härleda. Den består av födelsedata, passnummer och passets utgångsdatum, och har man en del av detta kan resten ofta erhållas genom ett telefonsamtal till polisen. Den som har nyckeln till en viss persons pass kan läsa av detta pass med en RFID-läsare.

I praktiken innebär detta att det lyckligtvis inte är möjligt för en obehörig att sätta upp en RFID-läsare och sedan identifiera okända passbärande personer som går förbi. Om den nyfikne vet vem han eller hon är intresserad av, däremot, kan passnyckeln ofta härledas och därmed blir det möjligt att sätta upp en RFID-läsare som automatiskt slår



larm när vederbörande kommer nära. Om den nyfikne får fysisk tillgång till passet i några sekunder kan förstås nyckeln avläsas i klartext.

Officiellt sägs att RFID-taggen i passet inte ska kunna läsas av på längre avstånd än några centimeter, men forskare i Nederländerna har visat att detta avstånd kan tänjas till 50 centimeter. Det gäller när en obehörig RFID-läsare går direkt på källan och läser av en persons pass. Den som har möjlighet att avlyssna kommunikationen mellan ett pass och en legitim RFID-läsare, exempelvis på en flygplats, kan göra det på upp till 5 meters avstånd (eftersom den legitima RFID-läsaren står för strömförsörjningen av taggen).

Ytterligare en svaghet med RFID-passen i hela Europa ur ett säkerhetsperspektiv är att den elektroniska delen är relativt lätt att klona. Flera forskare har lyckats läsa av ett pass och programmera ett chip så att det nya chippet blir en exakt kopia av det legitima passet. Därmed blir det möjligt för en obehörig att passera under en stulen identitet (så länge bara elektronisk avläsning av passet görs, papperspasset är betydligt svårare att klona). Däremot har försöken att ändra informationen i passtaggen hittills misslyckats.

Det är värt att notera att de europeiska RFID-passen snabbinfördes efter amerikanska påtryckningar under tiden efter den 11 september 2001.

5. Spårning av människor via chippade kläder

Många RFID-kritiker skjuter in sig på risken för att taggar i kläder och andra produkter som vi bär på oss kan komma att användas för att registrera människors förflyttningar. Även om en sådan situation är avlägsen idag och riskerna inte ska överdrivas är farhågorna inte gripna ur luften. Tunga aktörer runtom vårt klot lägger ned stora resurser på att förverkliga en värld där de flesta av våra vardagsvaror – alltifrån matvaror till kläder – är chippade. Vissa producenter och detaljister har redan genomfört pilottester med chippade klädesplagg, och experimentbutiken Metro Future Store i Tyskland har provat RFID-chippade matvaror.

Ett bra sätt att förklara skräckvisionen är att redovisa tankarna i ett patent som tre anställda vid dataföretaget IBM har lämnat in till det amerikanska patentverket. Meningen är, enligt detta, att vi konsumenter ska identifieras och få våra förflyttningar kartlagda med hjälp av just RFID-taggar i kläder och tillhörigheter. Det ska ske med hjälp av RFID-läsare utplacerade i butiker och andra offentliga platser, till och med på toaletter.

Patentansökan lämnades in år 2002, och ännu finns inga konkreta tecken på att idéerna håller på att förverkligas någonstans, men ansökan visar ändå hur tankegångarna går i marknadsföringskretsar. Så här inleds dokumentet, som bär

”När en person som bär med sig eller har på sig föremål som är RFID-märkta går in i butiken eller ett annat område scannar en RFID-läsare av RFID-taggarna på den personen. [...] Baserat på resultatet av detta går det att fastställa personens exakta identitet, alternativt vissa av personens egenskaper. Den informationen används sedan för att spåra/följa personens förflyttningar genom butiken eller andra områden.”

Tre IBM-anställda i en patentansökan rörande ett RFID-baserat övervakningssystem för butiksmiljö

titeln ”Identification and tracking of persons using RFID-tagged items” (översatt till svenska):

”En metod och ett system för att identifiera och spåra/följa personer med hjälp av RFID-försedda föremål som bärs av personerna. Tidigare inköpshistorik för varje person som handlar i en butik samlas in genom terminaler vid kassorna och lagras i en transaktionsdatabas. När en person som bär med sig eller har på sig föremål som är RFID-märkta går in i butiken eller ett annat område scannar en RFID-läsare av RFID-taggarna på den personen. Informationen på RFID-taggarna samkörs med informationen i transaktionsdatabasen enligt kända korrelationsalgoritmer. Baserat på resultatet av detta går det att fastställa personens exakta identitet, alternativt vissa av personens egenskaper. Den informationen används sedan för att spåra/följa personens förflyttningar genom butiken eller andra områden.”

Så här kan det bli: En RFID-läsare vid exempelvis en butiksdörr noterar att en viss passerande person bär med sig:

- En gul fleecetröja storlek 38 av ett visst märke
- Ett par röda bomullstrosor med broderad ros i en viss skärning i storlek 38
- Ett par solglasögon av en viss modell, svarta
- Ett läppstift av ett visst märke i en viss kulör.
- En tub med salva mot fotsvamp av ett visst märke i en viss storlek

Blixtsnabbt går en programvara igenom databasen över tidigare inköp i butiken och upptäcker att tre av dessa fem varor faktiskt inhandlats relativt nyligen av, säg, en kund vid namn Eva Larsson. Alltså är det med mycket stor sannolikhet just hon som kommer här. Identifieringen möjlig-

görs av att varje exemplar av en vara har ett unikt nummer. Två exakt likadana varor har alltså olika nummer i RFID-taggen.

Kännedomen om kundens identitet ska sedan bland annat användas för att visa personligt anpassad reklam på olika displayer som hon passerar. Genom att använda RFID-läsare utplacerade på många platser i butiken registreras även hennes rörelser. Stannar hon exempelvis två minuter vid krukväxterna dras slutsatsen att hon är växtintresserad, vilket föranleder en uppdatering av kundprofilen i butikens databas. Det kan också ligga till grund för senare utskick av direktreklam, och för att kundens namn och adress tillsammans med andra växtintresserades namn säljs till exempelvis en blomsteraffär eller en trädgårdsmästare.

Så här står det i patentansökan: ”Vilket föremål som helst kan vara RFID-märkt, det kan vara en hatt, ett armbandsur, en livrem, ett par skor, en scarf, en handväska eller plånbok, kläder, portfölj, smycken, eller vilket annat föremål som helst”.

Nu kan det ju tänkas att personen inte kan identifieras, exempelvis på grund av att vederbörande inte köpt tillräckligt många av sina tillhörigheter i den aktuella butiken. I så fall går IBM:arnas tänkta system in i sitt sekundära läge: De burna kläderna och tillhörigheterna används för att automatiskt dra så mycket slutsatser som möjligt om personen. Så här står det i patentansökan:

”I ett annat utförande, istället för att fastslå personens exakta identitet, kan egenskaper såsom demografi (t.ex. ålder, ras, kön etc) bestämmas med hjälp av förbestämd statistisk information. Exempelvis, om personen bär föremål av exklusiva varumärken, såsom en Rolex-klocka, kan den personen klassificeras såsom hemmahörande i den över med-

elklassen. I ett annat exempel, ifall föremålen som bärs av personen är typiskt kvinnliga, såsom en handväska, scarf, ett par strumpbyxor, så kan könet på personen fastställas som kvinnligt.”

Nu är det inte bara i butiker som de tre IBM-anställda tänker sig att vi konsumenter ska bli avlästa. I patentansökan står det att systemet ”kan tillämpas på andra platser, såsom gallerior, flygplatser, järnvägsstationer, bussterminaler, hissar, tåg, flygplan, toaletter, sportarenor, bibliotek, teatrar, muséer etc.”.

Vidare ska spårningen inte bara ske i marknadsföringssyfte. Så här står det i patentansökan: ”Den föreliggande uppfinningen har ett brett tillämpningsområde. Exempelvis kan den användas för att spåra och följa en viss brottsmisstänkt person genom offentliga platser.”

Man kan konstatera att en sådan spårning naturligtvis skulle kräva att alla människors förflyttningar läses av.

Om vi får ett samhälle där våra vardagsföremål är RFID-chippade är det inte bara företag och statsmakt som utgör hot mot den personliga integriteten. Det gör även privatpersoner. Med en bärbar RFID-läsare skulle vi kunna bli avlästa av en främling i tunnelbanan, exempelvis, eller på andra platser där trängsel råder. Kvinnor som går på nattklubb och liknande etablissemang skulle kunna bli avlästa av män som de växlar några ord med – och sedan bli utsatta för så kallad stalking (förföljelse).

Här måste påpekas att det inte är sannolikt att information om en persons namn eller andra identifierande data kommer att lagras i klartext i själva RFID-taggen. Riktigt så illa är det inte. Den som läser av numret på en tröja, exempelvis, kommer att behöva tillgång till den databas där tröjans

nummer knyts till en viss person (om en sådan finns) för att få reda på vem personen är.

De flesta personer har naturligtvis inte sådan tillgång. Men en del har, och sedan tillkommer risken för intrång i databaser utifrån (hackning). Även om riskerna inte ska överdrivas finns därför ändå en reell risk för att människor blir identifierade av främlingar via RFID, om vi får en värld där ”allt” är chippat.

Dessutom kan integritetsintrång komma att ske via RFID-märkta varor även om bäraren inte kan identifieras av den nyfikne. Numret i en vara må vara intetsägande, men fungerar ändå som ett osynligt kännetecken som med radiovågor säger att ”här kommer denna person igen”. Det skulle gå att bygga en apparat som placeras på ett strategiskt ställe och på lämpligt sätt slår larm när den utvalda personen passerar (förutsatt att hon eller han en gång tidigare blivit avläst). Även detta skulle kunna användas av stalkers, men även av nyfikna arbetsgivare, grannar eller tjuvar. Det är över huvud taget svårt att i förväg förutse alla sätt på vilka RFID-märkning av produkter som bärs av människor kan komma att skada individerna.

Några producenter av konsumentartiklar har som nämnts redan börjat med RFID-märkning av sina varor. Exempelvis har ett av Europas största skoföretag, Reno, börjat chippa sina skor. Kedjan har 700 butiker i 15 länder. Sportskotillverkaren Nike har utvecklat en skomodell, Nike+, med inbyggd RFID-tag. Jeanstillverkaren Levi Strauss har genomfört ett pilottest där byxor som levererades till tre butiker i USA och Mexico var chippade. Den stora nederländska bokhandelskedjan Selexyz har i minst två av sina butiker infört RFID-märkning av alla böcker (där inaktiveras taggarna när betalning sker, av integritetsskäl).

Länkar:
RFID-standard för konsumentvaror:
www.epcglobalinc.org
Patentansökan: www.dnv.se/ibm-patent.pdf
Nike-skor: www.nike.com/nikeplus/

6. RFID-tag opereras in i människor

Ett amerikanskt företag vid namn VeriChip Corporation har utvecklat en RFID-tag avsedd att opereras in i människor. Den är något större än ett riskorn, och skjuts in under huden i överarmen med ett vaccinationsliknande förfarande. Därefter är människan chippad, och kan avläsas trådlöst med RFID-läsare.

Det har gått trögt med att få hela mänskligheten att låta chippa sig, vilket var VeriChip Corporations ursprungliga ambition, men en del framgångar har företaget haft. Mest omskrivet är kanske Baja Beach Club i Barcelona, en nattklubb som erbjuder sina stamgäster (”VIP-kunder”) att chippa sig med VeriChip. Därefter får de tillgång till särskilda VIP-områden på nattklubben, och de kan betala för sig i baren genom att hålla fram armen. VeriChip Corporation har nämligen utvecklat en betalningslösning till sin tag som heter VeriPay.

Så här säger Conrad K Chase, som är chef på nattklubben, till internationella medier: ”Chippningsevenemanget var en enorm succé. Alla blev förtjusta i den elektroniska betalningsmöjligheten. Mina kunder gillar det faktum att de slipper ha med sig kontokort eller legitimation. Med VeriPay-systemet behöver de inte längre vara oroliga för att deras kontokort ska tappas bort eller stjälas.”

”Chippningsevenemanget var en enorm succé. […] Med VeriPay-systemet behöver de inte längre vara oroliga för att deras kontokort ska tappas bort eller stjälas”

Conrad K Chase, chef på nattklubben Baja Beach Club i Barcelona, som börjat operera in RFID-taggar i sina stamgäster.

En annan uppmärksammad VeriChip-kund är det mexikanska riksåklagarämbetet. Riksåklagaren själv och ett antal av hans medarbetare har låtit chippa sig med VeriChip. Genom att få sin arm avläst blir de insläppta i arbetsplatsens entré och kan logga in i datasystemet.

VeriChip-taggen innehåller inte namn eller andra direkta identifieringsuppgifter, utan ett nummer som via databasen hos VeriChip Corporation kan knytas till en viss person. Det har också en mycket kort räckvidd. Ändå är det många som ser risker med ett eventuellt kommande samhälle där alla människor är RFID-chippade. Databaser kan läcka information, och i vissa situationer (såsom i kollektivtrafik i rusningstid) går det att komma en annan människa mycket nära.

Man kan också konstatera att forskare redan har lyckats med att klona ett VeriChip. Därvid kunde man skapa en digital dubbelgångare till en chippad människa.

VeriChip har på sina håll börjat användas i medicinska sammanhang. Exempelvis har det amerikanska försäkringsbolaget Horizon Blue Cross Blue Shield of New Jersey inlett ett tvåårigt test där taggarna opereras in i människor med kroniska sjukdomar. De ska sedan bli automatiskt avlästa varje gång de befinner sig på sjukhuset Hackansack Medical Center.

Bevakningsföretaget CityWatcher i den amerikanska staden Cincinnati kräver att de medarbetare som arbetar i företagets säkra datacenter låter operera in ett VeriChip i kroppen. Hittills har, såvitt känt, två väktare blivit chippade. Syftet är att säkert kunna identifiera dem.

I ett uppmärksammat uttalande i amerikansk TV föreslog koncernchefen för Applied Digital Solutions, som är VeriChip Corporations moderbolag, att amerikanska myn-

digheter skulle börja operera in RFID-taggar i alla invandrare.

Det finns en myt om att personer med VeriChip under huden kan spåras med hjälp av satelliter var än på jorden de befinner sig. Detta har ingen förankring i verkligheten. Kanske beror ryktet på en sammanblandning av teknologier. Sant är nämligen att moderbolaget till VeriChip Corporation, Applied Digital Solutions, har drivit utvecklingsarbete för att få fram en annan typ av inopererad apparat som faktiskt ska göra människor spårbara med GPS-positionering. Denna dosa har i prototypversion varit något större än en pacemaker, och innehåller teknik för GPS-positionering och utsändning av aktuell position via mobiltelefonnätet. Tanken är att potentiella kidnappningsoffer ska låta operera in en sådan dosa. Såvitt känt har utvecklingsarbetet ännu inte resulterat i någon färdigutvecklad produkt, och det är oklart om utvecklingen fortfarande pågår.

Länk:
VeriChip: www.verichipcorp.com

7. Andra exempel på känslig RFID-användning

7.1 RFID-märkta invånare i Ulricehamn

I Ulricehamn pågår ett försök där människor förses med en RFID-tag (dock inte inopererad). Tanken är att ifall en person medvetslös förs till sjukhus, exempelvis efter en olycka, ska sjukvårdspersonalen genom att läsa av taggen omedelbart få tillgång till patientens identitet och därigenom medicinska data om vederbörande. Systemet har utvecklats av företaget First Aid Profile. Deltagande är frivilligt. Den som vill vara med registrerar mot en avgift sina personuppgifter i en databas. Flera Ulricehamns-företag har i egenskap av arbetsgivare gått med i försöket, och erbjuder sina anställda medlemskap. Om projektet i Ulricehamn blir framgångsrikt tänker First Aid Profile lansera sin tjänst i andra svenska städer.

Länk:
www.firstaidprofile.se

7.2 Hotellgäster får radiosändare runt handleden

Ett så kallat resort-hotell i USA, Great Wolf Lodge i delstaten Ohio, ska införa RFID-armband för alla gäster. Arm-

bandet innehåller en tag som både bildligt och bokstavligt ska öppna alla dörrar under hotellvistelsen. Exempel: rumsdörren låses upp automatiskt när gästen närmar sig, inköp kan göras genom att hålla fram armen och poletter till spelautomater kan köpas i särskilda automater genom att hålla fram handleden. Taggen fungerar även vid bad i hotellets vattenland. Leverantör av armband och RFID-läsare är företaget Precision Dynamics.

Länk:
www.pdcorp.com

7.3 Malaysia och Bermuda ska avläsa bilar via radiosändare

Regeringen i Malaysia har beslutat om ett successivt införande av bilnummerplåtar med inbyggd aktiv RFID-tag (transponder). Syftet är att bekämpa bilstölder. Eftersom transpondrarna kan avläsas på 100 meters avstånd blir det lätt att bygga upp avläsningsstationer i exempelvis gathörn. Som av en händelse får myndigheterna förstås även tillgång till detaljerad information om hur varje bil förflyttar sig. RFID-skyltarna levereras förmodligen från det brittiska företaget e-plate. Det svenska företaget Tagmaster har också utvecklat en RFID-försedd bilnummerplåt. Även regeringen i Bermuda har beslutat om RFID-märkning av alla bilar.

Länkar:
www.e-plate.com
www.tagmaster.com

7.4 Spårande casino-marker

Det amerikanska företaget Shuffle Master har köpt ett patent som möjliggör en slags intelligenta, RFID-försedda spelmarker. Dessa ska automatiskt kunna spåras hela tiden från att de köpes av en spelare tills de löses in. Syftet är att automatiskt kunna kartlägga varje spelares vanor och taktik.

Länk:
www.shufflemaster.com

7.5 Svensk kollektivtrafik

I Sverige håller kollektivtrafikföretagen på att införa RFID-försedda resekort. I bräschen går Storstockholms lokaltrafik (SL), Västtrafik och Skånetrafiken, men fler bolag lär följa efter. I samband med övergången till elektroniska kort

RFID-läsare i Stockholms kollektivtrafik (ovalen på spärren) ska tas i drift hösten 2007

kommer trafikföretagen att börja lagra information om varje genomförd resa på individnivå, vilket innebär ett stort hot mot den personliga integriteten, men det har egentligen ingenting med själva RFID-tekniken att göra (samma lagring skulle kunna genomföras om korten hade magnetremsa istället för RFID-baserad informationsöverföring).

7.6 Körkort och ID-kort

I USA förbereds en lag om ett standardiserat, federalt ID- och körkort kallat Real ID. Detta kan komma att utrustas med en RFID-tag (frågan är ännu inte avgjord). Oavsett hur det blir med den saken är sannolikheten stor att körkort och ID-kort i många länder inom en relativt nära framtid kommer att ha RFID.

8. RFID-hackning, kloning och annat missbruk

Integritets- och säkerhetsriskerna med RFID har tilldragit sig många teknikers och forskares intresse, varför en hel del experiment har genomförts i syfte att testa tekniken. I många fall har svagheter och risker mycket riktigt uppdagats. Här följer några exempel.

8.1 Forskare byggde under-jackan-avläsare

Två forskare i Israel har i demonstrationssyfte byggt en så kallad RFID-skimmer, alltså en bärbar apparat med vilken människors RFID-taggar i smyg kan läsas av. Den är kraftfull nog att läsa av en RFID-tag på minst 25 centimers avstånd – vilket är fullt tillräckligt för att läsa av främlingar i folksamlingar.

Apparaten är batteridriven och kan döljas under exempelvis en rock eller kappa. Den byggs med standardkomponenter som finns lättillgängliga för hobbyanvändning till en kostnad av runt 700 kr. Forskarna, Ilan Kirschenbaum och Avishai Wool, tror att konstruktionen kan finslipas så att avläsningsavståndet utökas. De skriver att apparaten förmodligen skulle kunna användas för att få tillgång till främmande människors kontokortsnummer för genomförande av bedrägerier (om korten har RFID – se nästa avsnitt).

När en RFID-tag av något slag kommunicerar med en legitim RFID-läsare (exempelvis vid en spärr i kollektivtrafiken eller en entré till en arbetsplats) kan datakommunikationen med hjälp av skimmern avlyssnas på större avstånd (flera meter) än det ovan angivna. Det beror på att den obehöriga RFID-läsaren i det fallet inte behöver strömförsörja RFID-taggen (som ju då får sin energi från den legitima RFID-läsaren).

En beskrivning av RFID-skimmern återfinns via länken:
www.eng.tau.ac.il/~yash/kw-usenix06/index.html

8.2 Amerikanska kreditkort kan avläsas genom handväskan

I USA har tiotals miljoner kreditkort redan försetts med RFID, en utveckling som säkerligen kan förväntas även i Sverige. Nu har en forskargrupp visat att vem som helst som kommer inom ett par decimeters avstånd kan läsa av ett kreditkort som en annan person bär i fickan eller handväskan - och därmed både identifiera vederbörande och komma över kortnumret. Kortet kan även läsas av genom kuvertet medan det befinner sig under postbefordran.

Försöket genomfördes av en institution som kallas Consortium for Security and Privacy vid det amerikanska universitetet Massachusetts Institute of Technology (MIT). Den nyfikne kan enkelt dölja sin utrustning under jackan, närma sig personer och i klartext läsa av information som namn, kontokortsnummer och giltighetstid på kort som han eller hon bär på sig. Den kod som är kopplad till kortet kan inte läsas av, men den avslöjade informationen räcker för att köpa varor med främlingens kortnummer i många nätbutiker.

”Trots de miljontals RFID-aktiverade konto-kort som redan används [...] så är alla kort vi testat mottagliga för [...] attacker”

En forskargrupp vid det amerikanska universitetet Massachusetts Institute of Technology (MIT), som testat kort från Visa, MasterCard och American Express.

Den apparat som forskarlaget satt ihop är inte större än ”ett par pocketböcker” och kostade motsvarande cirka 1.000 kronor. Forskarna säger att de förmodligen skulle kunna bygga en andra version som inte skulle behöva vara större än ett paket tuggummi och som bara skulle kosta 350 kr.

Risken att få kortnumret stulet och sedan råka ut för att tjuven köper varor med detta är inte det enda problemet. Bäraren av ett RFID-kort kan också bli identifierad av en främling utan att veta om det, exempelvis på tåg och bussar där det råder trängsel, i en hiss eller på en nattklubb. Mindre nogräknade butiker kan sätta en antenn under disken och registrera sina besökare i syfte att bygga ett kundregister. Brevbärare och annan postpersonal kan läsa av kreditkort som befinner sig under postbefordran. Och så vidare.

Forskargruppen på MIT, som leds av professor Kevin Fu, konstaterar att RFID-korten skulle kunna skyddas med kryptering men att kontokortsföretagen inte har gjort det. I marknadsföringen, däremot, hävdar kontokortsföretagen att korten är säkrade med mycket hög kryptering.

”Trots de miljontals RFID-aktiverade kontokort som redan används [...] så är alla kort vi testat mottagliga för [...] attacker”, skriver forskargruppen. Testerna har gjorts med 20 kort från Visa, MasterCard och American Express.

Kontokortsföretagen avvisar kritiken. ”Det här är ett intressant tekniskt experiment, men inte något reellt hot mot konsumenter”, säger Brian Triplett, en av Visas vice VD-ar. En av MasterCards högsta chefer, Art Kranzley, uttrycker saken så här: ”Det här är nästan som om någon står upp i en biosalong och skriker ’Det brinner!’ bara för att någon har tänt en cigarrett”.

John Pescatore, som är vice VD för internetsäkerhet på analysföretaget Gartner Group, kommenterar säkerhets-

avslöjandet så här: ”Det här är ett klassiskt ’Vi förlitar oss på säkerhet genom att mörka - vem kommer att titta?’ Sedan, ojdå! Så fort någon tittar så rullas säkerheten bort”.

Länkar:
TV-reportage: www.abcnews.go.com/Video/playerIndex?id=2602025
Forskargruppens rapport: www.rfid-cusp.org/blog/blog-23-10-2006.html

8.3 Hotelldörr öppnades med ost

En tysk säkerhetsexpert, Lukas Grunwald, har i demonstrationssyfte utvecklat en programvara som gör det lätt att både läsa av information från RFID-taggar och skriva information till dem. RFDump, som programvaran heter, ligger på internet tillgänglig för alla (www.rfdump.org). Grunwald berättar för tidskriften Wired om hur han befann sig på ett hotell som använde sig av RFID-försedda nyckelkort och fick lust att busa. Han tog fram sin dator, läste av nyckelkortets information med hjälp av RFDump och överförde sedan informationen till RFID-taggen på en förpackning gräddost inhandlad på Metro Future Store. Därefter gick det utmärkt att öppna hotelldörren med osten.

8.4 Virtuell nyckelstöld på arbetsplats

Den amerikanska tidskriften Wired arrangerade tillsammans med en universitetsstudent en virtuell nyckelstöld. Den arbetsplats som nyckeln avsåg hade passerkort med RFID istället för magnetremsa, vilket medför att nyckelkorten kan

avläsas trådlöst. Studenten såg till att kollidera med en anställd så att båda ramlade, medan han höll en hemmabyggd RFID-läsare dold i handen. I villervallan såg han till att RFID-läsaren kom tillräckligt nära den anställdes passerkort (kanske hängde det som en badge utanpå kläderna) för att en avläsning skulle ske. Därefter var det lätt för studenten att gå hem och programmera en egen RFID-tag med samma nummer som den anställdes passerkort. Studentens RFID-tag fungerade därefter som nyckel.

9. Skyddslösningar

Det finns olika slags lösningar utvecklade avsedda att hindra missbruk av RFID-taggar och skydda den personliga integriteten. Här redovisas några:

Skydd 1: inaktivering av tag

Efter påstötningar från integritetsförespråkare har den så kallade EPC-standarden (avsedd att bli världsstandard för RFID-taggar på konsumentvaror) försetts med ett så kallat ”kill command”. Det innebär att chippet permanent kan inaktiveras med hjälp av en viss signal från en RFID-läsare. Därmed blir det exempelvis möjligt för en butik att införa rutinen att alla taggar på alla sålda varor inaktiveras vid kassan. En nackdel med detta är att eventuell nytta med RFID-taggen efter köpet försvinner. Det har exempelvis talats om tvättmaskiner med inbyggd RFID-läsare som skulle känna av plaggen i trumman och slå larm om kombinationen är olämplig (kanske föreligger risk för att ett rött plagg färgar vita lakan rosa om tvätt sker tillsammans i 95 grader).

Skydd 2: RFID-blockerande plånbok

RFID-taggar avläses med radiovågor, som stoppas av metall. Ett sätt att skydda sig är därför att linda in sina RFID-

försedda kort och andra föremål i exempelvis aluminiumfolie. Det går också bra att köpa en särskild anti-RFID-plånbok som tillverkats med ett inbyggt metallskikt. Några leverantörer av sådana återfinns via länkarna nedan – den översta länken leder även till en videodemonstration.

Länkar:
www.difrwear.com/products.shtml
www.rpi-polymath.com/ducttape/RFIDWallet.php
www.thinkgeek.com/gadgets/security/8cdd/

Skydd 3: RFID-blockerande kuvert

En av världens största tillverkare av kuvert, National Envelope Corporation, har utvecklat ett kuvert med inbyggt RFID-skydd. Kuvertet, som kallas Smart Card Guard, har en tunn metallhinna som stoppar radiovågor och är tänkt för bland annat kreditkortsföretag.

Länk:
www.nationalenvelope.com/prod/SmartCardGuard Envelopes.htm

Skydd 4: bärbar brandvägg

Några forskare från Vrije-universitetet i Amsterdam har utvecklat prototypen till en bärbar brandvägg – en apparat avsedd att bära med sig för den som är orolig att bli obehörigen RFID-avläst. Brandväggen möjliggör vad forskarna kallar integritetsadministration i en kommande värld full av RFID-tillämpningar. Apparaten spärrar RFID-läsning i närmiljön genom att sända ut en störsignal, men eftersom

den kan kopplas ur får apparatens bärare makten att själv bestämma när hon eller han vill bli avläst.

Länkar:
Videodemo, hög bandbredd:
www.rfidguardian.org/videos/rfid-guardian-1000.wmv
Videodemo, låg bandbredd:
www.rfidguardian.org/videos/rfid-guardian-0250.wmv
Akademisk avhandling:
www.cs.vu.nl/~melanie/rfid_guardian/papers/lisa.06.pdf
Projektsajt: www.rfidguardian.org/

Skydd 5: aktiva skyddspåsar

En lösning som påminner en aning om ovanstående har presenterats av företaget RSA Security. De har utvecklat och patenterat en teknologi som bygger på ett särskilt chip som genom sin blotta närvaro stör RFID-läsare. Produkten kallas RSA Blocker Tag, men är såvitt känt ännu inte kommersialiserad (sannolikt på grund av att efterfrågan knappast finns innan RFID i konsumentvaror blivit vanligt). Det finns också en teknologi som kallas Soft Blocker, som består av en programvara som laddas i en vanlig RFID-tag och i allt väsentligt gör samma sak som en blocker tag.

Skydd 6: RFID-tag med rivflik

IBM har presenterat ett integritetsskydd för RFID som man kallar ”clipped tag”. Det innebär att taggens antenn är så utformad att den enkelt kan rivas bort, ungefär som när man drar bort en perforerad kupong. Därmed minskas kraftigt det avstånd på vilket taggen kan läsas av (men avläsning förhindras inte helt).

10. Lagreglering eller frivillig etisk kod?

I både USA och Europa är frågan om lagreglering av RFID-användning på tapeten. Det finns två huvudskolor som står emot varandra: De som kräver lagreglering, och de som anser att det räcker med frivilliga överenskommelser om att följa någon slags etisk kod. Här följer en genomgång av läget i USA och Europa som det såg ut när denna skrift gick till tryck (förändringar sker snabbt på det här området).

10.1 USA

I USA är såvitt känt ingen lag på federal nivå under beredning, men flera delstater har antagit RFID-lagar eller håller på att bereda sådana.

– Delstaten Wisconsin antog i början av 2007 en lag som förbjuder RFID-användning i ”amerikansk valuta” (varmed torde avses sedlar) och i ”dokument”. Tidigare har delstaten antagit en lag med förbud mot att tvinga på människor inopererade RFID-taggar.

– I Kalifornien bereds flera lagar som berör RFID-användning. Delstatens senator Joe Simitian ligger bakom dem (men guvernören Arnold Schwarzenegger är motståndare). Simitian föreslår bland annat stopp för RFID i körkort i tre år, införande av integritetsregler för RFID i andra ID-kort

(såsom studentkort och personalkort), förbud mot dold avläsning av RFID-taggar och förbud mot att tvinga på människor inopererade RFID-taggar.

– Delstaten North Dakota är på väg att anta en lag som förbjuder tvingande inoperering av RFID-taggar.

– Delstaten New Hampshire förbereder en lag som totalförbjuder användning av RFID i offenciella dokument såsom körkort, och reglerar näringslivets användning av tekniken. Bland annat krävs enligt lagtexten att butiker tydligt märker produkter som innehåller RFID-taggar. Dessutom förbjuds påtvingad inoperering av RFID i människor enligt lagförslaget.

– I delstaten Washington diskuteras en lag som skulle göra det obligatoriskt att inhämta konsumenters samtycke innan de får utsättas för RFID-avläsning. Lagförslaget attackeras dock hårt av lobbyister från näringslivet, och utgången är oviss.

10.2 Europa

På vår sida av Atlanten är skepsisen mot lagstiftning faktiskt större. Under våren 2006 initierade EU:s IT-kommissionär Viviane Reding en serie hearings för att skaffa beslutsunderlag i frågan om huruvida lagreglering av RFID behövs. I början av 2007 offentliggjorde hon sitt beslut. ”Det blir inga regleringar. Vi måste ge branschen möjligheterna att verkligen go for it”, sa hon till media.

Reding är såld på RFID-tekniken, och vill att Europa helhjärtat satsar på den. Hon säger sig ha etablerat ett nära samarbete med den amerikanska regeringen och säger sig föra samtal med bland andra Rysslands högsta ledning för att säkerställa att RFID-tekniken blir globalt användbar.

Emellertid tänker Viviane Reding sätta samman en intressegrupp som ska utarbeta en etisk kod för RFID-användning som blir frivillig att tillämpa. ”Ingen ska behöva bli föremål för RFID-avläsning utan vetskap eller mot sin vilja”, säger hon. Det kan tyckas finnas en motsättning mellan detta uttalande och beslutet att bara införa en frivillig etisk kod.

10.3 Etisk kod för RFID-användning

I USA föreligger sedan flera år olika förslag från organisationer och integritetsaktivister på vad som skulle kunna ingå i en frivillig, etisk kod för RFID-användning. I huvudsak handlar det, i olika konstellationer, om nedanstående punkter:

1. RFID-taggen ska monteras på förpackningen, inte på själva varan, när så är möjligt. Det innebär att taggen inte längre följer med varan efter att denna packats upp.
2. RFID-taggar ska monteras så att de tydligt syns.
3. Konsumenterna ska informeras om att en vara är RFID-märkt.
4. RFID-taggar ska enkelt kunna inaktiveras av kunden, exempelvis vid en RFID-inaktiveringsapparat placerad utanför kassorna (en sådan lösning har installerats vid den tyska butiken Metro Future Store). Ett alternativ är att taggen automatiskt inaktiveras i kassan med hjälp av ett så kallat kill command.
5. Inga dolda RFID-läsare ska placeras ut i offentliga miljöer. RFID-avläsning ska vara tydligt utmärkt.
6. Ingen användning av RFID som eliminerar anonymitet ska förekomma. Det innebär exempelvis att RFID-

läsning i en butik inte får användas för att identifiera kunder genom att matcha en produkts RFID-nummer (exempelvis ett klädesplagg) mot information som tidigare lagrats i kundregistret (exempelvis när varan köptes).

11. Vilka är hoten – förslag på åtgärder

Att vi står inför en RFID-revolution råder det inget tvivel om, eftersom det finns så stora effektiviseringsvinster att hämta hem. Men hur ska vi betrakta tekniken ur ett integritetsperspektiv? Utgör RFID ett jättehot mot den personlig integriteten? Ska användningen begränsas i lag? Eller är sådana farhågor ogrundade och bara ett tecken på paranoia hos en klick teknikmotståndare?

För det första kan man konstatera att RFID har ett gigantiskt användningsområde, där de allra flesta tillämpningarna inte medför någon integritetsrisk. RFID på lastpallar, reservdelar till flygplan eller verktyg i verkstäder är helt okontroversiellt. Det är bara när taggarna direkt eller indirekt hamnar på människor som det blir känsligt. Precis som fallet är med nästan all ny teknik ska därför RFID rent principiellt bejakas, eftersom tekniken kan öka effektiviteten i näringsliv och offentlig sektor och därmed ytterst bidra till ett ökat välstånd och höjd livskvalitet.

När detta är sagt måste man konstatera att integritetsriskerna för vissa typer av applikationer är reella. När RFID-samhället är utbyggt kommer de flesta människor för det mesta att ha en eller flera RFID-taggar på sig eller med sig, och då – men först då – kan vi räkna med att problemen och farorna visar sig. Tre slags aktörer utgör hot: enskilda

personer (såsom bedragare, stalkers och allmänt nyfikna), företag och statsmakten.

När det gäller enskilda personer kommer vi säkerligen att få se ett antal fall av RFID-hackning och RFID-kloning, ungefär som vi idag lider av phishing på internet och hackade databaser. Å andra sidan kommer naturligtvis säkerhetsåtgärderna att skärpas när RFID-användningen blir utbredd och attackerna börjar komma. Sedan blir det, i vanlig ordning, en kapprustning mellan ”the bad guys” och ”the good guys”.

Företagen, å sin sida, kan komma att utnyttja människors okunnighet om riskerna och locka med förmåner för de kunder som accepterar trådlös avläsning. Därmed kan ett alltmer omfattande snokande komma att realiseras, baserat på frivillighet. Med tiden kan detta via en successiv glidning komma att bli normalförfarande för alla kunder. Ett annat företagsrelaterat hot är naturligtvis att mindre nogräknade näringsidkare helt utan accept i hemlighet börjar läsa av och registrera människor.

Riskerna för integritetskränkande RFID-avläsning av människor utförd av statsmakten är på sätt och vis svårast att hantera. Statsmakten har ju lagstiftningsmakten i sin hand, och om dagens övervakningsvänliga samhällsklimat håller i sig är risken uppenbar att även människors RFID-taggar med tiden inlemmas i samhällets övervakningsinfrastruktur.

I faktarutan på nästa sida sammanfattas riskerna.

Risker med RFID

Hot från enskilda

- Obehöriga personer med en bärbar RFID-läsare kan komma att identifiera människor i miljöer där trängsel råder
- Även om identifiering inte är möjlig kan obehöriga tänkas programmera apparatur till att ständigt vakta och automatiskt slå larm när en viss (tidigare avläst) person kommer förbi (detta kan alltså vara möjligt även om den avlästa taggen bara innehåller ett ”anonymt” nummer).
- Obehöriga kan tänkas avläsa vilka föremål vi har med oss, exempelvis i en väska eller på kroppen, något som ibland kan vara känslig information
- Identitetsstölder kan förekomma, exempelvis genom att ett RFID-baserat passerkort till en arbetsplats eller ett kollektivtrafikkort klonas av en obehörig

Hot från företag

- Butiker kan tänkas använda kundkort med RFID för att automatiskt registrera varje besök i butiken
- Butiker kan tänkas använda RFID-läsare för att automatiskt detektera när en kund kommer in som har ett plagg/föremål från den aktuella butiken på sig (samt detektera vilka plagg/föremål det rör sig om)
- Butiker kan tänkas montera RFID-läsare som identifierar kunder och/eller noterar och registrerar hur de rör sig.
- I många fall gäller ovanstående naturligtvis även andra näringsidkare än butiker

Hot från statsmakten

- Som ändamålsglidning kan det komma att byggas ut en infrastruktur av RFID-läsare på gator och torg och i andra offentliga miljöer som rutinmässigt identifierar människor och registrerar deras förflyttningar
- Polisen kan komma att utrustas med bärbara RFID-läsare som kan identifiera deltagare i exempelvis en demonstration, något som lätt skulle kunna missbrukas.

Avslutningsvis: Vi ska inte förfalla till teknikfientlighet. Vi ska säga ja till RFID, men se upp ordentligt när det gäller taggar som direkt eller indirekt bärs av människor. Det är klokt att vara skeptisk till åtgärder som sägs skydda integriteten där kontrollen över data ligger hos någon annan än den berörda människan (exempelvis ”vi krypterar all känslig information” eller ”det ligger bara ett kodnummer och inga personuppgifter i själva taggen”). Vi ska tänka på risken för ändamålsglidning, och inte ge ett finger till dem som snart kan tänkas ta hela handen.

Integritetsombudsmannen/Den Nya Välfärden hyser åsikten att uppmaningar att tillämpa en frivillig, etisk kod för RFID-avläsning *inte* utgör ett tillräckligt skydd för den personliga integriteten. Individer behöver skyddas i lag mot otillbörlig avläsning av deras RFID-tillhörigheter. En sådan lag bör reglera avläsning utförd av såväl enskilda, näringsidkare som samhället. RFID-användning som inte berör människor behöver dock inte regleras.

Vi får inte glömma att det är med personlig integritet som med syre – man uppskattar den först när den saknas.

Pär Ström
Integritetsombudsman, tankesmedjan Den Nya Välfärden
par.strom@dnv.se

RFID-chips är en sorts minimala radiosändare platta som papper. En utmärkt teknologi. Men så snart RFID hamnar på människor – direkt eller indirekt via tillhörigheter – finns risken att människorna blir avlästa, spårade och kartlagda i hemlighet. Myndigheter, företag och enskilda bedragare med en antenn under jackan hör till dem som kan hota vår personliga integritet.

Vi står inför en RFID-revolution, där de små chippen sannolikt hamnar i allt från kläder till matvaror. I Sverige finns de redan i bland annat pass, busskort och vissa landstingskläder. I Spanien, Mexico och USA har man börjat operera in RFID-chips i människor. RFID-övervakning planeras redan.

Pär Ström är integritetsombudsman vid Den Nya Välfärden. Läs även hans tidigare rapporter ”Med storebror i baksätet” och ”Med storebror i uppfinnarverkstan”.

den nya välfärden

Box 5625, 114 86 Stockholm | tel 08-545 038 10
www.dnv.se | integritetsombudsmannen@dnv.se