Überwachung abschirmen

Der Siegeszug der RFID-Chips

An sich ist RFID nichts Neues: Seit Jahrzehnten schon gibt es die kleinen PickerIn an Klamotten und Juwelen, die beim unbefugten Verlassen eines Konsumtempels den Kaufhausdetektiv herbeirufen. RFID begann als Überwachungstechnik für die Errungenschaften des Freien Marktes. In den letzten Jahren nun hat die Technik die Kaufhäuser verlassen und schickt sich an, den Freien Markt selbst zu schützen: Der Sicherheits- und Überwachungswahn hat seine neuen Stars.

RFID steht für Radio Frequency Identification, und das sagt schon, worum es geht: Über Radiowellen rauskriegen, welche Käsepackungen auf einer Palette oder welche Menschen in einem Stadion stehen, ob das Buch, das gerade die Bibliothek verlässt, auch entliehen wurde oder ob ein Preisschild eine Kasse gesehen hat oder nicht.

Dabei braucht es zwei Beteiligte: Einen Transponder (gerne auch Tag genannt) und ein Lesegerät. Der Transponder ist ein Computerchip mit einer Antenne. Normalerweise hat er keinen Strom hat und ist also abgeschaltet. Er erwacht, wenn seine Antenne passende Radiowellen auffängt, aus denen er üblicherweise auch gleich seinen Strom gewinnt, was den Vorteil hat, dass keine Batterie die Lebensdauer des Transponders beschränkt, was für die hier interessanten Anwendungen ja schade wäre. Mit ein paar Tricks meldet der Chip sich bei der Quelle der Radiowellen -- das ist das Lesegerät -- und kann mit dieser zuvor in ihm gespeicherte oder auch frisch berechnete Daten austauschen.

Der entscheidende Punkt dabei: Dieser Datenaustausch braucht keine Zustimmung des/der TrägerIn des Transponders, der/die davon normalerweise nicht einmal etwas merken wird.

Was soll's?

Dies ist ein entscheidender Knackpunkt für die Beurteilung von RFID als Überwachungstechnologie: Anders als bei der klassischen Personenkontrolle merkt der/die Überwachte nichts von der Überwachung. Dies wiegt um so schwerer, als die Daten von vorneherein digital vorliegen und damit beliebig gespeichert, übertragen und zusammengeführt werden können -- im Rahmen der Datenschutzbestimmungen. Diese verbieten im Augenblick natürlich fast alle schicken Anwendungen, aber soweit das überhaupt wen kümmert, werden die Hürden wohl so schnell fallen wie die Verbote, mit Toll Collect „Verbrecher" zu fangen.

Welche Daten kommen nun aus so einem Transponder heraus? Im Prinzip ist viel denkbar. Moderne Transponder übertragen häufig eine eine Art Seriennummer, die den Transponder und damit etwa den Pullover, in den er eingenäht ist, global eindeutig identifiziert. Das allein reicht eigentlich schon, denn diese Seriennummer kann oft genug eindeutig einer Person zugeordnet werden, etwa wenn beim Kauf einer Ware eine Kunden- oder Kreditkarte im Spiel war. Allerdings weiß auch in diesem Fall bis zur nächsten Rasterfahndung nur der Händler, wer den Transponder hat.

Wer die Zuordnung von Seriennummer zu Person hat, muss nur noch ausreichend Lesegeräte aufstellen und kann sehr detaillierte Bewegungsprofile erstellen. Das geht so weit, dass in den diversen Future Stores aufgrund von RFID-Transpondern auf Kundenkarten gemessen werden soll, wie lang welcheR KundIn vor welchem Regal verweilt. Realität in Hi-Tech-Gebäuden ist bereits, dass mit RFID-Transpondern versehene Badges erlauben, festzustellen, welche Personen in welchen Räumen sind (Betriebsräte müssten sowas natürlich verhindern, aber die gibts nun mal nicht überall, und manchmal sitzen da auch ziemliche Pfeifen drin). Pläne, über implantierte RFID-Chips PatientInnen in Krankenhäusern zu identifizieren, sind

unterdessen erstmal auf Eis -- stattdessen bekommen „Nutztiere“ die Chips inijziert, um rechtzeitig vor dem Schlachttermin comuptergesteuert ihre Antibiotika abzusetzen.

Der RFID-Chip im elektronischen Pass hingegen denkt sich für jede Kommunikation eine neue Seriennummer aus, so dass es vermutlich unmöglich ist, den ePass zu diesen Zwecken zu verwenden. Das wäre auch gar nicht so interessant, weil die wenigsten ihren Pass immer dabei haben. Wie das bei den künfigen elektronischen Personalausweisen sein wird, bleibt natürlich abzuwarten.

Bei den WM-Tickets ist hingegen die Seriennummer das entscheidende Datum -- sie verknüpft das Ticket mit dem im Vorfeld erhobenen umfangreichen Datensatz (zwischen Geburtsdatum und Bankverbindung ist alles dabei), und vermutlich auch wenigstens mit Teilen der BKA-Datenbank INPOL.

ED-Misshandlung in der Jackentasche

Transponder haben häufig auch beschreibbaren Speicher für mindestens ein paar Bytes, in denen beispielsweise gespeichert werden kann, wann und wo ein Transponder zum letzten Mal Kontakt zu einem Lesegerät hatte (EC-Karten haben übrigens eine ähnliche Funktion, nur dass Magnetstreifen nicht ausgelesen werden können, ohne dass ihr es merkt). Natürlich lassen sich auch größere Datenmengen unterbringen. Auf den neuen Pässen liegt das Passfoto als JPEG-Datei, später werden auch JPEGs eurer Fingerabdrücke dort untergebracht.

Damit könnte, wer ein Lesegerät hat, von PassantInnen einfach einen einer ED-Behandlung entsprechenden Datensatz abgreifen, ohne dass diese auch nur etwas davon merken würden. Dieses Szenario war auch den Überwachungsfanatikern im Innenministerium vorläufig zu viel, und so haben sie die Daten verschlüsseln lassen, wobei Teile des Schlüssels auf dem Ausweis selbst aufgedruckt sind.

Dabei wird genutzt, dass die Transponder selbst kleine Computer sind, die allerlei vor allem kryptographische Rechnungen durchführen können. Im ePass kann der Chip so prüfen, ob das Lesegerät auch im Besitz des am Pass aufgedruckten Teilschlüssels ist, bevor er Daten rausrückt. Eigentlich sollte also niemand an die Daten am Transponder herankommen, ohne den Pass selbst gesehen zu haben (und das wäre schon mal nicht schlecht, weil mensch dann immerhin etwas von der Überwachung merkt).

Leider sind die Überwachungsfanatiker nach dem Kostensenkungsprinzip vorgegangen und haben dazu noch durch etwas ungeschickte Regelungen einiges an Datensicherheit verjuxt, so dass für niederländische Ausweise (die analog funktionieren) bereits demonstriert wurde, wie die Daten aus den Pässen rauszubekommen sind, ohne den Pass gesehen zu haben. Vorerst allerdings ist das sicher zu aufwändig, um es etwa zur kleinen Volkszählung bei einer Demo einzusetzen, zumal die niederländische Methode auch nur funktioniert, wenn eine „legitime“ Stelle mit dem Pass kommuniziert.

Volkszählung mit BMW

Das Szenario dahinter ist: An sich könnte es ausreichen, einmal mit einem mit Lesegerät ausgerüsteten Motorrad an einer Demo langzufahren, und presto! hat man eine komplette Liste der anwesenden Personen, mit Foto, Fingerabdruck und allem. Offenbar haben sich beim ePass DatenschützerInnen durchgesetzt, die ein Szenario dieser Art natürlich auch mit Horror erfüllt, und haben die erwähnten Hürden erzwungen -- technisch wäre sowas nämlich schon heute kaum mehr ein Problem.

Die nach ISO 14443 standardisierten Transponder (dazu gehört der ePass ebenso wie die WM-Tickets und viele der in Warenwirtschaftssystemen eingesetzten Transponder) sind als „Proximity coupling“, also „Kopplung in der Nähe“ konzipiert und sollten per Design nur größenordnungsmäßig 10 cm vom Lesegerät entfernt antworten. Mit einem Lesegerät aus dem Ramschladen nebenan ist diese Zahl durchaus zutreffend, zumal ja das Lesegerät den Transponder durch die Luft mit Strom versorgen soll.

Auf der anderen Seite kann man mit passenden Antennen auch deutlich größere Distanzen überwinden -- für ISO 14443-Transponder wurde schon deutlich über ein Meter öffentlich gezeigt, das physikalische Limit dürfte wegen der verwendeten induktiven Kopplung in der Größenordnung der verwendeten Wellenlänge (rund 20 Meter) liegen. Will man nur die Kommunikation eines Transponders mit einem Lesegerät

abhören, kommt man bereits mit einem Hula-Hup-Reifen und etwas Versandhaus-Elektronik auf zehn Meter und mehr, physikalische Beschränkungen gibt es dabei nicht.

Und jetzt stellt euch vor, welchen Spaß man als Überwacher haben kann, wenn man nicht nur Videobilder hat, sondern zu jeder Figur auf dem Videobild auch noch Name und Adresse, Fingerabdruck und Datenbankauszug.

Was tun?

Transponder sind empfindliche elektronische Geräte. Waschen werden sie meistens überstehen, doch können sie Mikrowellen in hoher Dosis überhaupt nicht ab. Wenn ihr glaubt, dass irgendwo ein Transponder drinsitzt, bruzzelt einfach ein paar Sekunden im Mikrowellenherd eures Vertrauens auf das Teil ein. Nur, damit ihr uns nicht verklagt: In empfindlichen Pullovern könnte das Spuren hinterlassen, CDs und erwünschte Elektronik überleben diese Behandlung nicht.

Im Fall von Pässen hilft das aber nicht so arg viel, denn die Pässe sind danach kaputt, und ein kaputter Pass ist nutzlos, was vor allem dann ärgerlich ist, wenn der Lappen schon 59 Euro gekostet hat (als Ausweisdokument wird er aber immer noch akzeptiert).

Beim ePass ist -- wie oben ausgeführt -- in dieser Hinsicht zunächst sowieso wenig Handlungsbedarf (sehr wohl aber, das nur nebenbei, im Hinblick darauf, dass zu seiner Produktion die gesamte Bevölkerung ED-behandelt wird). Da aber finstere Pläne in den Schubladen liegen, sollte erwähnt werden, dass sich RFID auch unterhalb der Zerstörung von Transpondern kontrollieren lässt, denn Transponder werden eben durch Radiowellen ausgelesen. Radiowellen werden beim Durchgang durch Metall massiv geschwächt. Häufig reicht schon großzügig eingesetzte Alufolie, von allen Seiten um das gute Stück rumgewickelt, die Profi-Lösung bedient sich einer kleine Blechschatulle. Solange der Pass oder die Karte in der Kiste ist, ist nichts mit Auslesen und nichts mit Vollüberwachung. Damit merkt ihr wenigstens weiter, wenn ihr euren (in Zukunft RFID-ausgestatteten) Personalausweis herzeigt.

Ansonsten gilt wie immer: Der beste Schutz ist aktiver Widerstand gegen die Einführung und Ausbreitung auch dieser Überwachungstechnologie. RFID begann als Ausdruck des Misstrauens von Kaufhäusern gegenüber ihren KundInnen. Der staatliche oder staatlich verordnete Einsatz ist dann einfach Ausdruck des Misstrauens des Staats gegenüber seinen BürgerInnen. Es hat eine gewisse Ironie, dass dieses Misstrauen schon lange nicht mehr so unbegründet war -- aber wer weiß schon, wie lange das so bleibt.

Datenschutzgruppe der Roten Hilfe Heidelberg

datenschutzgruppe@rotehilfe.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a

http://www.datenschmutz.de