Tages-Anzeiger

31. März 2009

Neuer Pass: «Eine Frage der Zeit, bis ein Leck auftaucht»

Vor der Abstimmung am 17. Mai: Mikroelektronik-Professor Marcel Jacomet kritisiert die Technologie für biometrische Pässe und die zentrale Speicherung von Fingerabdrücken.

Herr Jacomet, am 17. Mai stimmen wir über die Einführung von biometrischen Pässen ab. Was bringt der neue Schweizer Pass Ihrer Ansicht nach?

Durch die Einführung von neuen biometrischen Merkmalen wird prinzipiell eine bessere Überprüfung des Passinhabers möglich.

Im Pass werden Daten wie Foto und Fingerabdrücke gespeichert. Kritiker befürchten, dass diese Informationen auf Distanz gelesen werden können. Ist das möglich?

Ist der Pass zugeklappt, so kann er nicht aus Distanz gelesen werden. Öffnet sich hingegen der Pass - wie dies in der Reisetasche durchaus vorkommen kann - so können gewisse Daten des Passinhabers aus der Distanz gelesen werden, wie Namen, Nationalität, Alter, Photo.

Das ist möglich, einfach so?

Wenn der Angreifer den elektronischen Schlüssel kennt: Ja. Diesen kann man aus der so genannten MRZ-Textzeile berechnen, welche im Pass sichtbar ist. MRZ steht für «machine readable zone». Besser geschützt sind die im Pass gespeicherten sensitiven biometrischen Daten. Diese können ohne Insiderwissen nicht gelesen werden.

In allen Pässen werden sämtliche Daten digital auf einem RFID-Chip gespeichert. Was steckt hinter dieser Technologie?

RFID steht für Radio Frequenzy Identification Device. Im neuen Pass 10 ist ein winziger RFID-Chip inklusive Antenne unter der roten Aussenhülle platziert. Die Funktionsweise der RFID-Technologie, wie sie im Pass 10 verwendet wird, ist sehr simpel: Das Lesegerät der Zollbehörde sendet dem RFID-Chip im Pass die notwendige Energie per Funk zu. Dadurch benötigt der RFID-Chip keine Batterie, um funktionsfähig zu sein. Nun können der RFID-Chip im Pass und das Lesegerät per Funk miteinander kommunizieren.

Wir begegnen heute der RFID Technologie auf Schritt und Tritt.

Richtig: In Warenhäusern werden Produkte markiert, damit sie nicht unbemerkt entwendet werden können. Bei manchen öffentlichen Bus- oder Trambetrieben wird mittels einer RFID-Chip-Karte das Billet gelöst. Und gewisse Produkte werden mit RFID-Chips versehen, um Originale von Nachahmern zu unterscheiden. Technologien müssen so eingesetzt werden, dass der Nutzen möglichst gross ist und negative Aspekte oder Missbräuche so weit als möglich ausgeschlossen werden können.

Und? Ist der Einsatz von RFID-Technologie im Schweizer Pass sinnvoll?

Nein. Weshalb soll ein Pass aus Distanz gelesen werden können? Will der Zöllner den Pass und Inhaber überprüfen, so muss er den Pass auf kurze Distanz (ein paar Zentimeter) zum Lesegerät hinhalten. Hätte man einen kontaktbasierten Chip eingebaut - wie dies bei der Bancomat-Karte der Fall ist - so müsste die Handbewegung des Zöllners nur ein paar Zentimeter weiter gehen, um den Pass lesen zu können. Ich kann mir nicht vorstellen, dass der Entscheid für die RFID-Technologie aufgrund einer Arbeitserleichterung der Zollstellen gefällt wurde. Hingegen öffnet die RFID-Technologie beim Einsatz im Pass Tür und Tor zu Missbräuchen. Ist das Passbüchlein einmal aufgeschlagen, können fremde Lesegeräte ohne weiteres aus Distanzen bis zu zwei Metern den Datenaustausch zwischen Pass und dem Lesegerät der Zollbehörde abfangen. Leider ist dies nicht die einzige Schwachstelle.

Sie sind dagegen, dass Fingerabdrücke in einer zentrale Datenbank gespeichert werden.

Natürlich. Wieso um alles in der Welt will der Bund das Informationssystem für Ausweisschriften (ISA) um die sensiblen Fingerabdrücke erweitern? Sämtliche Begründungen des Bundes dazu auf seiner Homepage sind nicht nachvollziehbar. Es gibt nichts Gefährlicheres als eine zentrale Datenbank mit den Identitäten jedes einzelnen Bürgers. Ich möchte jedenfalls nicht in der Haut des technisch oder politisch Verantwortlichen dieser Datenbank stecken.

Was ist denn genau das Problem?

Es ist nur eine Frage der Zeit, bis in solchen zentralen Datenbanken ein Leck auftaucht. Dies könnte ein Hacker sein - wenn nicht mit der heutigen, dann vielleicht mit der morgigen Technologie. Neben allen technisch möglichen Sicherheitsbarrieren, die der Bund aufgebaut hat um diese sensible Datenbank zu schützen, darf man den menschlichen Faktor nicht vergessen, lesen Sie die Berichte zu den Datenlecks in England. Ein interner technischer Mitarbeiter könnte durch einen Fehler oder aber auch durch physischen oder psychischen Druck zum Sicherheitsrisiko werden.

Einige IT-Experten gehen davon aus, dass Hacker die Daten auf dem Chip des Passes fälschen können. Also könnte man manipulierte Daten auf den Chip bringen und den Pass als echt verkaufen. Worst case: Hacker errechnen den Hauptschlüssel der Zertifizierungsstelle des Landes. Dann könnten sie eigene Pässe herausgeben und Lesegeräte einbauen. Ein realistisches Szenario?

Der Hauptschlüssel der Zertifizierungsstelle ist mit den heutigen Technologien kaum zu knacken. Prophezeihungen in die Zukunft sind da schon etwas gewagter, aber ich gehe davon aus, dass dies bei den verwendeten Schlüssellängen nicht so rasch zu bewerkstelligen ist. Viel gefährlicher ist der oben erwähnte menschliche Faktor.

Nach Ihren Ausführungen muss man davon ausgehen, dass Sie die Einführung des E-Passes ablehnen.

Trotz aller Bedenken, ich befürworte die Einführung des E-Passes in der Schweiz. Der weltweite Trend geht eindeutig in Richtung elektronisch basierter biometrischer Pässe - und zwar unabhängig davon, ob wir Schweizer dabei mitmachen oder nicht. Blieben wir aussen vor, so würde uns dies das Reisen doch erheblich erschweren.

Was raten Sie Inhabern von E-Pässen?

Sollte unbefugtes Lesen von E-Pässen aus Distanz zu einem Problem werden, so könnte dies jeder Bürger selber einfach unterbinden. Eine simple Alu-Folie zwischen den Passseiten oder ein dünnes Metallcouvert als Passhülle würde bereits genügen. Auf jeden Fall sollten Sie den E-Pass Unberechtigten nicht aushändigen, auch in Hotels nicht.

Wollen Sie damit sagen, dass der jetzige Pass sicherer ist als der biometrische Pass?

Es ist ein Einfaches, den RFID-Chip im biometrischen Pass innert Minuten zu kopieren - im Vergleich zum alten Papierpass ist das also keine Verbesserung. Anleitungen und Software zum Pass-Klonen kann jederman aus dem Internet gratis herunterladen, passende Programmiergeräte sind günstig zu kaufen. Hingegen sollte es nicht möglich sein, einen kopierten Pass zu verändern (indem zum Beispiel Photo oder Fingerabdrücke ausgetauscht werden), denn diese Daten sollten mit einer Signatur der ausgebenden Behörde vor Veränderungen geschützt sein und künftig hoffentlich von allen Zollbehörden auch darauf kontrolliert werden. Der alte Pass konnte beim Kopieren verändert werden, beim Neuen ist dies zum Glück kaum mehr möglich.

Also keine Angst vor Big Brother?

Werden die biometrischen Daten nur für die Authentifizierung der Bürger und auch in Zukunft nicht für andere Zwecke gebraucht, sehe ich keine Gefahr. Gläsern macht sich die heutige Generation bereits freiwillig. Denken sie nur an die Cumulus- oder Supercards von Migros und Coop. Noch extremer scheinen mir die freiwilligen und intimen Veröffentlichungen der jüngeren Generation im Facebook und ähnlichen sozialen Netzen.

Die jüngere Generation hat George Orwell vergessen.

Ja, das ist so. Wir hinterlassen bewusst aber auch unbewusst eine extreme Datenspur. Ich bin gespannt, wie lange es dauert, bis hier wirklich professionelles Profiling im grossen Stil gemacht wird und sich eine entsprechende Industrie etabliert. Solange die Migros per Brief die gekaufte Ananasbüchse wegen eines Produktionsfehlers zurückruft, mag dies ja noch als sinnvoller Einsatz der Technologie erscheinen.

Was darf bei der Erfassung von biometrischen Daten nie erlaubt sein?

Das Sammeln von biometrische Daten, welche Rückschlüsse auf genetische Eigenschaften oder Krankeiten geben, sind für mich absolut tabu. Damit könnten Nachteile für den Passinhaber entstehen – dies ohne dass er es selber erfahren würde oder beeinflussen könnte.