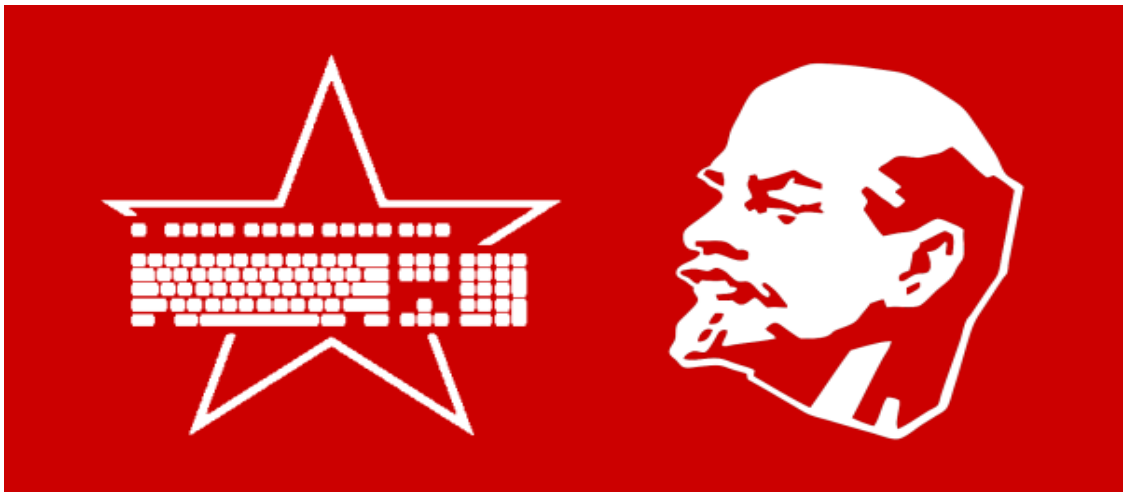
Vortrag – “Round Table 31”, 18.Nov.2008, Hotel Steigenberger, Zürich, Schweiz



“Vertrauen ist schlecht, Kontrolle ist unmöglich!”

Wie sollten wir mit Technik umgehen, die wir nicht oder nur teilweise verstehen können?
Warum sollte dabei Ge-Wissen wichtiger sein als Fach-Wissen?

Referent: **Bernd Fix**, Hacker-Veteran des Chaos Computer Clubs
Vorstandsmitglied der Wau-Holland-Stiftung

Zur Person:

- Jahrgang 1962 in Norddeutschland
- Studium Physik und Philosophie (Göttingen, Heidelberg)
- seit 1986 im Chaos Computer Club aktiv
- 1987 erste dokumentierte Viren-Bekämpfung
- 1988 Firma für Verschlüsselungs-Software (PC-DES)
- 1991 Firma im Bereich VR (CAD, 3D-Visualisierung)
- 1998 AG-Gründung in der Schweiz (Dornach)
- seit 2003 Mitglied der Wau-Holland-Stiftung
- 2004 jetzige Firma aspector GmbH

Ich arbeite im Bereich Computersicherheit mit den Schwerpunkten Kryptologie, Smartcards und Netzwerk-Sicherheit als Enterprise Security Architect für verschiedene Unternehmen, vornehmlich aus dem Bankensektor.

Einführung

Seit einigen Jahren beobachten vor allem kleine Gemeinden ein interessantes Problem: Von Jahr zu Jahr steigt die Anzahl der schweren Lastfahrzeuge, die unter Brücken oder in engen Ortsdurchfahrten oder Waldwegen einfach stecken bleiben – oft genug werden dabei Strassen, Brücken und sogar Häuser beschädigt. Nun, warum passiert das?

Eine naheliegende Erklärung gibt es ja: Last-Chauffeure stehen unter steigendem Druck, fahren oft länger als erlaubt und machen dann einfach solche Fehler. Eine logische Erklärung – aber leider nicht der wirkliche Grund!

Schuld ist etwas, was eigentlich als Hilfe für jeden Chauffeur gedacht war und ihm das Leben leichter machen sollte: das Navigationsgerät – liebevoll von vielen auch kurz als “NAVI” bezeichnet. Es soll Untersuchungen geben, nach der mehr Männer auf ihr NAVI hören als auf ihre eigene Frau – obwohl beide weibliche Stimmen haben.

Noch einen Schritt weiter geht es offenbar aber bei manchen Last-Chauffeuren: sie hören sogar eher auf das NAVI als auf ihren eigenen, gesunden Menschenverstand. Sie fahren, wohin ihr NAVI sie schickt – bis es (mit den bekannten Folgen) zu spät für eigenes Denken und Handeln ist.

Natürlich gibt es spezielle Navis für LKWs, beiden denen solche Missgeschicke nicht so häufig auftreten, aber die sind ungleich teurer als die normalen Navigationsgeräte für PKWs. Und solange die Spediteure ihr Navi vom Media-, ähm Massen-Markt holen, wird das Problem bestehen bleiben. Deshalb hat man mancherorts schon offiziell reagiert und wie in England ein neues Verkehrsschild eingeführt, das man wohl nur als “Höre nicht auf Dein Navi” verstehen kann. Nun, vielleicht würde es auch helfen, die weibliche Stimme im Navi durch eine Alpha-Tier Kommando-Stimme zu ersetzen, um das Vertrauen des Fahrers in diese quasselnde Blechbüchse zu erschüttern. Das könnte bei so manchem Fahrer dazu führen, dass er nach einem lauten “Halt' die Klappe, ich weiss selber was ich tue, Du Blödmann” anfängt, wieder selbst nachzudenken.

Und genau deshalb bin ich heute abend hier: Ich bin hier, um ihren Glauben und ihr Vertrauen in die Computertechnik zu erschüttern – nach bestem Wissen und Gewissen. Nicht nur in Bezug auf Navis, sondern in allen Bereichen, in denen sie mit Computern in Berührung kommen – also praktisch immer und überall. Ich denke, sie sollten einem Computer nicht weiter trauen als sie ihn werfen können – es sei denn, ihr Vertrauen basiert auf fundiertem technischem Verständnis.

Ich sehe es schon in ihren Gesichtern, dass sie jetzt denken: “Und jetzt wird uns dieser politisierende Technik-Hippie bestimmt gleich erzählen, dass wir Computertechnik einfach nur genauso gut kennen müssen wie er – und schon wird alles gut!”

Interessanter Ansatz – aber wenn alle Hacker werden, wer baut dann unsere Häuser, backt unsere Brötchen oder fährt unsere Banken an die Wand?

Nein, im Gegenteil: Ich denke nicht, das jeder von uns jede Computertechnik, mit der in Berührung kommt, vollkommen verstehen muss. Aber wir sollten von jeder Technik – speziell der, der wir vertrauen sollen – einige Dinge wissen:

- Was sind die **Genzen** dieser Technik?
- Was sind die **Möglichkeiten** dieser Technik?
- Was ist der **Nutzen** dieser Technik?
- Was sind die **Gefahren** dieser Technik?

Diese eigentlich nicht-technischen Punkte müssen wir bewerten – und der Bewertungs-massstab (vor allem für die letzten beiden Punkte!) ist nicht unser Fach-Wissen, sondern unser Ge-Wissen und unsere moralischen Werte. Es braucht zwar technisches Wissen, um diese Punkte in ihrer Vollständigkeit zu ergründen, aber jeder von uns kann und muss trotzdem die Ergebnisse selbst beurteilen und eigene Schlüsse ziehen. Wie wir in unseren Beispielen sehen werden, können die Bereiche unterschiedlich ausgeprägt sein – das hängt einfach davon ab, was wir uns genauer anschauen.

Am Ende der Beispiele sollte sich dann die Frage nach dem Vertrauen in Technik auch nicht mehr stellen; es wird klar, dass wir höchstens den Menschen vertrauen, die diese Technik entwerfen, herstellen, kontrollieren und nutzen.

Ich möchte das Ganze an zwei aktuellen Beispielen mit Ihnen zusammen mal durchspielen; die Beispiele sind so gewählt, dass wir alle davon über kurz oder lang betroffen sein werden:

- **Wahlcomputer**
- **Biometrischer Reisepass**

Wahlcomputer

“Es ist wichtiger, Begriffe zu besetzen als Häuser”, sagte einst Heiner Geisler über die Hausbesetzer-Szene – damals prominent in der Hamburger Hafenstrasse. Von den Jesuiten lernen heisst siegen lernen, werden sich die Befürworter von Wahlcomputern denken und verwenden deshalb konsequent den Begriff “Wahlmaschine”.

Was wie eine zulässige Bezeichnung aussieht, die doch dasselbe wie “Wahlcomputer” aussagt, ist in Wirklichkeit eine geschickte Realitäts-Manipulation, denn es gibt einen entscheidenden Unterschied zwischen einer Maschine und einem Computer:

- Eine Maschine hat eine definierte Funktion, die nur in engen Rahmen alternativ für etwas anderes verwendet werden kann. So kann ich mit einer Kaffemaschine auch Hühnerbrühe herstellen, wenn ich den Kaffee weglasse und in der Tasse Brühwürfel sind – aber der Funktionsbereich “Flüssigkeit erhitzen und wahlweise durch eine Substanz in ein Behältnis leiten” wird dabei nicht verlassen – das ist ein

wesentliches Kennzeichen einer Maschine.

Natürlich gibt es Ausnahmefälle: Mit der Maschine “Elektro-Herd”, einem Topfdeckel und einer Gabel war es an einigen Stellen in Hamburg möglich, NDR-Radio zu hören – aber Ausnahmen bestätigen ja die Regel. Das Thema “Komplexität als Mutter der Möglichkeiten” wäre ein ganz eigener Vortrag.

- Ein Computer hingegen ist eine Universalmaschine, die alle berechenbaren Verfahren als Funktion ausführen kann. Die Funktionen des Computers sind nur begrenzt durch die Möglichkeiten der Hardware – also wie das Programm mit der realen Welt interagieren kann.

Wenn das Gerät über das wir hier reden, eine Wahlmaschine ist, dann würde das heissen: feste und enge Grenzen, wenig Möglichkeiten (verschiedene Wahlzettel), nur einen Nutzen (Stimmzählung) und keine Gefahren. Und das die Maschine auch wirklich das tut, was sie tuen soll, wird in einer “offiziellen Typenprüfung” durch staatliche Stellen kontrolliert. Das ist alles so ganz im Sinne der Befürworter.

Wenn es aber ein Wahlcomputer ist, dann ist die Situation völlig anders: weite Grenzen, viele Möglichkeiten, viele Nutzen und viele potentielle Gefahren!

Um der Öffentlichkeit deutlich zu machen, dass es sich um einen Wahlcomputer handelt, haben Hacker sich einen gekauft (ganz offiziell von einer Gemeinde, in der zwei Wahlbezirke zusammen gelegt wurden und die dadurch ein Gerät “übrig” hatten). Um zu beweisen, dass es sich um einen Computer handelt, der noch ganz andere Dinge als “Stimmen zählen” kann, wurde der Wahlcomputer komplett zerlegt und die Software aus dem EEPROM ausgelesen. Das anschliessende Reverse Engineering der Hard- und Software hat einige Zeit in Anspruch genommen – das war streckenweise sogar Arbeit und nicht nur Spass.

Aber anschliessend konnten die Hacker neue Software für das Gerät schreiben – was immer sie wollten. Aber was sollte man wollen: Es musste etwas sein, das mit “Wahlen” oder “Stimmen zählen” absolut nichts zu tun hat. Gleichzeitig sollte es die “Intelligenz” des Gerätes demonstrieren und damit die vielen anderen Möglichkeiten erahnen lassen. Ich halte die dann getroffene Wahl für einen Genie-Streich, denn die Hacker entschlossen sich, dem Wahlcomputer das Schachspielen beizubringen.

Statt des Wahlzettels gibt es ein druck-empfindliches Schachbrett mit Figuren. Der eigene Zug wird so vom Computer erkannt und der Computer-Gegenzug im Display angezeigt – bewegen muss man die Computerfigur aber schon noch selbst. Neben Knöpfen für “Spiel starten” und Sondersituationen wie “Bauerndurchmarsch” braucht es nichts weiter – ausser natürlich dem Schachprogramm für den Wahlcomputer. Das könnte für einige Wahlbezirke, in denen nicht so viel passiert, bestimmt eine interessante Alternativnutzung für gelangweilte Wahlhelfer sein. Das Programm ist selbstverständlich Open Source…

Schachspielen ist natürlich keine Gefahr für die Demokratie, also musste noch eine zweite Software her: eine manipulierte Wahl-Software. Diese sollte drei Grundanforderungen genügen:

1. sich exakt so zu verhalten wie das Original, damit die Manipulation nicht erkennbar ist und während der Wahl auffällt.
2. eine “offizielle Typenprüfung” erfolgreich zu bestehen, so dass sogar “ab Werk” ein manipuliertes Gerät eingeschleust werden könnte
3. gezielt Wahlergebnisse manipulieren

Schach ist komplexer, also war die neue Aufgabe nicht zu schwer und eine “verbesserte” Software für den Wahlcomputer schnell fertig. Wer jetzt denkt, “Ja, auf ihrem eigenen Gerät können sie ja rumprokeln wie sie wollen – aber bei einem echten Wahlcomputer können sie doch niemals unbemerkt die Manipulation vornehmen.”, ist auf dem Holzweg. Um zu beweisen, dass Hacker nur 60 Sekunden alleine mit dem Gerät sein müssen, um die Software zu tauschen, habe ich einen kleinen Film mitgebracht:

Wenn sie vorher noch Vertrauen in Wahlcomputer hatten – wie steht es jetzt damit? Vertrauen sie in die Sicherheit und Korrektheit des Hersteller der Wahlcomputer? (Kennen sie die Firma eigentlich?) Vertrauen sie allen Leute, die mehr oder weniger offiziell Zugang zu Wahlcomputern in den Wahlbezirken haben? Wissen sie eigentlich, wie viele Leute das so sind? Seit einigen Jahren setzt der Chaos Computer Club in deutschen Wahlen eigene Wahlbeobachter ein, um das Handling mit den Wahlcomputern zu beobachten – mit zum Teil haarsträubenden Vorfällen, die einem jedes Vertrauen nehmen, dass noch übrig ist.

Wenn wir aber irgendwo ein Vertrauensproblem haben, wie in aller Welt sollen wir dann dem Wahlergebnis trauen, dass dieses Gerät am Ende des Tages ausdruckt? Nachzählung – wie denn ohne Wahlzettel?

Dürfen wir in einer solchen Situation überhaupt Wahlcomputer einsetzen? Oder verletzen wir dabei unsere demokratischen Grundwerte? Hierbei geht es nicht um Abwägung zwischen Nutzen und Risiko: Jede mögliche Wahlmanipulation sollte Grund genug sein, den Einsatz nicht zuzulassen – zumal der Nutzen (Effizient und kostengünstig) auch nicht wirklich erfüllt wird.

Die Niederlande ist das erste Land in Europa, das den Einsatz von Wahlcomputern ganz offiziell gesetzlich verboten hat – nachdem es eines der ersten war, in dem Wahlcomputer überhaupt flächendeckend eingesetzt wurden und auch der Hersteller der Wahlcomputer von dort stammt. Aber Holland war eben schon immer ein progressives Land, das aus seinen Fehlern lernen konnte – schade, dass es bald untergeht.

Biometrischer Reisepass

Mein zweites Beispiel ist der biometrische Reisepass – vielleicht gibt es hier sogar den einen oder anderen, der schon einen hat – wohlgemerkt: weil er ihn wollte, denn einen Zwang gibt es hier in der Schweiz diesbezüglich noch nicht.

Zuerst einmal bleibt festzuhalten, dass wir diese Technik nicht den Holländern verdanken, sondern den Amerikanern – genauer vielleicht 9/11, obwohl sich notfalls bestimmt auch ein anderer Grund gefunden hätte. Die Einreisebestimmungen in die USA verlangen seitdem von anderen Staaten, die Pässe ihrer Bürger mit biometrischen Daten auszustatten und in maschinenlesbarer Form bereit zu stellen.

Wie das passiert, ist etwas komplexer als beim Wahlcomputer, von dem wir ja nur wissen mussten, dass er ein Computer ist. Deshalb ein kurze Einführung in die Technik:

Technik

Hardware

Im Umschlag des Passes befindet sich ein RFID-Chip, auf dem die Daten gespeichert sind. Ein entsprechendes Lesegerät kann über kurze Entfernungen (Zentimeter-Bereich) die Daten auslesen. Der Chip im Pass wird dabei durch Radiowellen mit Energie versorgt; die Übertragung der Daten geschieht ebenfalls über die gleichen Wellen.

Software

Nicht eine spezielle Software als vielmehr die verwendeten Krypto-Verfahren und das generelle Design der Lösung sind hier interessant – weniger das Betriebssystem der RFID-Chips oder der entsprechenden Lesegräte, die dem Beamten die Daten anzeigen.

Das wichtigste aber sind zuerst mal die gespeicherten Daten auf dem Chip. Dies sind – vereinfacht gesagt – alle Informationen, die auch im Pass gedruckt sind und das digitalisierte Passbild. Optional können weitere biometrische Merkmale wie Fingerabdrücke, Irisabbilder, Netzhaut-Scans oder ähnliches gespeichert werden.

Diese Daten sind gegen Manipulation und unberechtigte Einsichtnahme geschützt, wobei der Standard mehrere Sicherheitsmerkmale spezifiziert:

Sicherheits-Merkmale:

- Geschützt durch digitale Signatur (Klonen möglich)
- Persönliche Daten nur lesbar mit Kenntnis optischer Merkmale (Klonen erschwert)
- Mit eigenem privaten Schlüssel (Klonen nicht möglich)
- Zugriffsrechte auf sensible Daten (Auslesen bestimmter Daten geschützt)

Zwingend muss nur das Schutzmerkmal “Signatur” implementiert sein. damit die Integrität der digitalen Passdaten geprüft werden kann.

Für die Pass-Signatur muss jedes Land seine eigene PK-Infrastruktur betreiben; diese muss mindestens zweistufig sein und unterliegt definierten Regeln. Da es keine übergeordnete Autorisierungs-Instanz gibt, ist jedes Land souverän in Bezug auf seine eigenen Schlüssel.

Grenzen und Möglichkeiten

Wer sich jetzt fragt, ob Hacker auch auf dem Reisepass Schach spielen können – die Antwort ist definitiv “Nein”. Die Technik steckt enge Grenzen, was man mit dem RFID-Chip machen kann und so sind die Möglichkeiten der alternativen Nutzung reichlich beschränkt – also leider auch kein Radio-hören mit dem Pass, auch wenn die RFID-Technik auf Radiowellen basiert.

Wir konzentrieren uns also auf den Nutzen und die Gefahren des biometrischen Reise-passes:

Nutzen: fälschungssichere Ausweis-Dokumente

Ziel des ganzen Unternehmens ist es, die Fälschung von Reisedokumenten unmöglich zu machen und so Terroristen die Einreise zu verwehren. Es gibt zwar keine Anhaltspunkte, dass jemals gefälschte Einreisedokumente bei irgendeinem Terror-Anschlag verwendet wurden; aber was soll's. Merkwürdig ist allerdings schon, dass das ganze Projekt bereits Mitte der 90'er in den USA gestartet worden ist...

Wenn Sie in die USA mit einem ePass einreisen, dann passiert folgendes: Mittels Lesegerät werden die Daten aus ihrem Pass ausgelesen und mit der digitalen Signatur auf Unver-sehrtheit geprüft. Schlägt diese Prüfung fehl, dann leuchten grosse rote Leuchten, heulen Sirenen und die Männer mit den automatischen Gewehren rücken an. Sie werden dann gute Argumente brauchen, wenn sie erklären sollen, warum sie versuchen, mit einem manipulierten Pass in die USA einzureisen.

Wenn die Daten positiv verifiziert sind, werden sie auf dem Bildschirm dem Beamten angezeigt. Der vergleicht jetzt die Angaben auf dem Bildschirm mit den Angaben im Pass, prüft ob die Passbilder gleich sind und ob sie auch wirklich so aussehen wie auf den Bildern. Ist alles O.K., dann erhalten Sie den Pass zurück und dürfen gehen. Ach ja, hätte ich fast vergessen: Alle Daten vom Pass und des Einreise-Vorgangs werden natürlich gespeichert – und zwar für verdammt lange Zeit.

Das ganze Konzept scheint auf den ersten Blick sicher – die Kryptoverfahren sind etabliert und anerkannt, die Schlüssellängen sind ausreichend und werden in kurzen Abständen gewechselt; zudem unterliegt der ganze Signiervorgang staatlicher Kontrolle und Hoheit.

Was soll da schon passieren? Nun, das alles ist nur graue Theorie – so richtig bunt und froh

wird es erst, wenn sich Hacker der Thematik annehmen. Dann kann es passieren, dass der Beamte bei der Einreise eines Hackers folgendes auf seinem Bildschirm sieht...

Das sieht zwar (absichtlich) so schräg aus, damit auch wirklich der schusseligste Beamte bemerkt, dass da was nicht stimmt – aber das entscheidende dabei ist: keine roten Lampen, keine Sirenen und auch keine Männer mit Gewehren! Die Software des Lesegerätes prüft die Daten und stellt fest, dass sie nicht manipuliert sind.

Wenn also statt dieser Demo ein richtiges Passbild, vernünftige Namen und Daten angegeben werden, so wäre die Fälschung gelungen – kein normaler Beamter in den USA würde Verdacht schöpfen.

Wie konnte das passieren? Haben die Hacker einen Schlüssel geknackt oder wie konnten sie die Daten so signieren, dass es dem Lesegerät nicht auffällt?

Die Lösung ist ganz einfach – wenn man sie kennt. Der Clou liegt wie immer nur darin, etwas “anders” zu denken als die Leute, die das System entworfen haben. In Abwandlung des Mottos aus “Raumschiff Enterprise” gilt für Hacker: “To boldly think what no man has ever thought before!”

Jeder von Ihnen hat eigentlich schon genug Informationen, um selber auf die Lösung zu kommen. Ich gebe ein Bier aus, wenn mir jemand sagt, wie es geht...

Des Rätsels Lösung: Wie erwähnt hat jedes Land die Hoheit über seine Schlüssel und es gibt auch keine übergeordnete Instanz, die die Länderschlüssel autorisiert. Wenn man sich jetzt also entschliesst, ein eigenes Land zu gründen, dann darf man auch selbst Pässe mit eigenen Schlüsseln ausstellen, die nach Systemspezifikation gültig sind und als solche bei der Einreise in die USA erkannt werden.

Das klingt zwar utopisch, als Bürger eines eigenen Landes in die USA einreisen zu wollen – aber wir dürfen natürlich nicht vergessen, dass Geographie noch nie die Stärke der Amerikaner war: es dürfte nicht viele Beamte geben, die einem Bürger aus “Holland” die Einreise verweigern würden. Der Hacker, der das alles gemacht hat, ist übrigens Holländer und hat einen niederländischen Pass – kein Scherz.

Interessant an diesem Beispiel ist, dass nicht die Technik versagt hat, sondern der Fehler im Design verankert ist. Multilaterale Übereinkommen sind vermutlich nur möglich, wenn die Souvernität der einzelnen Staaten nicht angestastet wird – so entstehen aber Probleme durch falsche Requirements.

Das war's dann erstmal mit dem Nutzen – auch wenn man sich sicherlich bemüht, das Problem so schnell als möglich komplett zu eliminieren. Aber ob es das letzte Problem ist, darf ernsthaft bezweifelt werden. Und wie sieht es mit den Gefahren aus?

Gefahren

Da es erstmal keine technischen Sicherheitsmassnahmen gibt, kann prinzipiell mal jeder, der ein RFID-Lesegerät sein Eigen nennt, Pässe auslesen. Inwieweit persönliche oder sensible Daten dabei zugänglich sind, hängt immer davon ab, welche optionalen Sicherheitsmerkmale ein Land implementiert – neben der digitalen Signatur natürlich.

Der Schutz dagegen ist vergleichsweise einfach: eine spezielle Pass-Tasche aus metallischem Material sorgt für eine ausreichende Abschirmung gegen unbemerktes Auslesen. Selbst der Chef der Bundesdruckerei – die stellen in Deutschland die Pässe her – soll angeblich so eine Hülle benutzen; klug wäre es auf jeden Fall.

Eine mehr generelle Gefahr ist die des Datenmissbrauchs: Unsere Erfahrung lehrt uns, dass überall dort, wo Daten erfasst und gesammelt werden, diese Daten auch missbraucht werden (Deutsche Telekom), verloren gehen (England) oder an den unmöglichsten Stellen auftauchen (deutsches Mautsystem). Vertrauen wir den Personen, die eine Technik kontrollieren, unsere Daten wirklich an? Was kann damit in Zukunft passieren?

Beim Beispiel des biometrischen Reisepasses muss sich jeder selbst überlegen, ob ihm der Nutzen (schnelle Einreise in die USA) wichtiger als die Gefahr ist. Aber diese Indiviual-entscheidung ist natürlich nur möglich, solange die Bürger die Wahl zwischen einem normalen und einem biometrischen Pass haben. Es wäre schön, die Schweiz würde beim momentanen Modell der Freiwilligkeit bleiben – dann hätten alle diese Wahlmöglichkeit.

Wenn ich allerdings einen biometrischen Pass erhalte (in zwei Jahren), dann kann ich nicht garantieren, dass mir dabei kein Missgeschick mit der Mikrowelle passiert... Zwar kann ich nicht verhindern, dass meine biometrischen Merkmale in einer Bundes-Datenbank gespeichert sind oder gar kontrollieren, was mit diesen Daten letzendlich alles geschieht, aber ich kann doch wenigstens entscheiden, ob der Reisepass funktioniert oder nicht.

Abspann

Dies waren zwei aktuelle Beispiele, die deutlich machen sollten, dass Fachwissen alleine nicht ausreicht, um Technik zu bewerten. Ich hätte auch andere Beispiele wählen können – ec-Karten, Vorratsdatenspeicherung, Online-Überwachung – you name it.

Wir haben es uns zu Angewohnheit gemacht, die Bewertung von Technik den Technikern (die sich nicht um Nutzen und Gefahren kümmern) oder den Politikern (die sich in der Technik und ihren Möglichkeiten auch nicht besser auskennen als wir selbst) zu überlassen. Ich denke, diese Bewertung ist aber zu wichtig, um sie einfach ohne Hinterfragen anderen zu überlassen – wir sind es schliesslich, die mit dieser Technik “leben” müssen. Die Abwägung zwischen Nutzen und Gefahren muss jeder für sich selbst treffen.

In diesem Sinne sind die Hacker ihre Verbündeten, denn wir sehen es auch als unsere Aufgabe an, die Grenzen und Möglichkeiten einer Technik auszuloten und ihnen unsere Entdeckungen nahezubringen – damit sie nicht selbst zum Technik-Freak werden müssen, um es zu verstehen. Aber ihre Schlüsse müssen sie schon selber ziehen – das ist ihre Verantwortung, mit der ich sie hiermit aus dem Vortrag entlasse...

Danke für Ihre Aufmerksamkeit.