Nein zum neuen CH-Pass mit RFID

Erfasst am : 25. März 2009 20:59 | Erfasst von : Martin
Verknüpfte Kategorie(n): Beobachtungen

Derzeit wird über den neuen PASS für die Schweizer diskutiert. Er hat einen Chip mit dem Passfoto und den Fingerabdruckdaten gespeichert. Egal, was darauf gespeichert ist, das grosse Problem am Pass ist der RFID Chip, der von aussen unbemerkt abgefragt werden kann.

In der Schweiz herrscht - soviel ich weiss - noch keine Pflicht, einen Pass oder eine ID jederzeit auf sich zu tragen. Das ist gut so. Denn wenn dann auch mal noch die Identitätskarten einen RFID Chip drauf hat und man gezwungen ist, diese auf sich zu tragen, dann wird's brenzlig:

Denn wie gesagt, ein RFID Chip kann unbemerkt angesprochen und zur Herausgabe von Daten angefragt werden. Die Befürworter des Passes werden sicher sagen, dass kein Unbefugter Daten abrufen könnte - figura zeigt jedoch, dass es in der Welt genug "kriminelle" Genies gibt, die jede Art von Kopierschutz etc. knacken können. Das aktuelle Beispiel aus der IT ist die Aushebelung der Bluray-Kopierschutzes, dessen Verschlüsselungsmethodik eigentlich sehr klever ist. Dennoch war der Bluray-Schutz schon geknackt, bevor die Bluray hierzulande vom Boden abhob. Wer also ist so arrogant und behauptet, dass man die Daten eines RDIF Chips im Pass nicht auslesen kann? Reicht es eventuell dann einfach mal, dass man eine autorisierte Auslesestation nachahmen oder übernehmen kann?

In der BRD ist diese Diskussion ja schon durch: Eine verblüffend einfache Methode gegen das unbefugte Auslesen des RFID wäre, dass die Daten aus dem Chip in jedem Fall immer nur verschlüsselt mit einem asymmetrischen Verschlüsselunsalgorithmus rausgehen dürfen. Nun muss der Schlüssel, der den ausgesandten Datenstrom des Chips entschlüsseln kann, visuell im Pass aufgeszeichnet sein, auch maschinenlesbar, aber vor allem einfach auf dem Pass. Denn so kann man sicher sein, dass der Pass trotz strahlendem RFID aus der Hand gegeben werden muss, damit selbst eine autorisierte Auslesestation überhaupt was mit den Funkdaten des Chips anfangen kann.

Wenn man die derzeit aktuellen asymmetrischen Ciphers wie RSA und Elliptic Curves anschaut, so sind diese derzeit noch sicher gegen Brute Force Attacken - obwohl jeder, der zuhause eine Top-Grafikkarte im PC hat, bereits die technische Basis hat, mit Passwort-Knackprogrammen auf Passwörter bzw. deren Hash-Sequenzen los zu gehen.

Gelten also RSA und Co. noch als sicher, so kann das Public Key Verfahren folgendes lösen: Die Auslesestation muss sich ausweisen gegenüber dem Chip. So kann beispielsweise eine zuvor visuell vom Pass gelesene Textsequenz mit dem privaten Schlüssel der Auslesestation verschlüsselt und an den Chip übermittelt werden. Der kann sie mit dem öffentlichen Schlüssel der Auslesestation, die diesen ja durchaus andauernd ausstrahlen kann, entschlüsseln. Gelingt die Entschlüsselung, ist die Auslesestation autorisiert. Nun kann der Chip seinen Public Key verschlüsselt an die Auslesestaion übermitteln. Ab dann kann die Kommunikation mit der Auslesestation losgehen, weil diese nun den Datenstrom mit dem Schlüssel des Chips verschlüsselt an diesen funken kann. Es besteht dann die Möglichkeit, die Komunikation über das Schlüsselpaars des Chips oder der Auslesestation zu führen. Oder, was meistens passiert, man einigt sich auf ein symmetrisches Verschlüsselungsverfahren mit einem temporären Schlüssel.

Das ist alles schon erfunden, und wer PGP benutzt oder einmal schon im Internet eine Website mit https:// besucht hat, hat dieses ganze, eben beschriebene Spiel unbewusst wohl ausgelöst. Um genau

zu sein, es wird beim https:// derzeit verzichtet, dass der Browser sich gegenüber dem Webserver ausweisen muss - nur der Webserver weist sich gegenüber dem Browser aus.

Bei PGP und SSL ist es so, dass ich die Kommunikation anstosse. Besuche ich keine solche Website, schreibe ich keine verschlüsselte Mail, kann man mir auch nichts entlocken.

RFID Chips haben es aber an sich, dass sie eben angesprochen und zu Antworten gebracht werden können, ***ohne*** mein Einverständnis, ja ohne meine Kenntnis überhaupt.

Ein biometrischer Pass aus meiner Sicht, darf - ausreichend gut gesichert - von mir aus viel über mich gespeichert haben. **ABER ER DARF AUF KEINEN FALL OHNE MEINE EIGENE AUTORISIERENDE AKTIVITÄT AUTOMATISIERT ABGEFRAGT WERDEN KÖNNEN.**

Ich glaube keinem, der mir sagt, es sei 100% sicher. Es mag sein, dass ein System dort nicht geknackt werden kann, wo alle Profis und Begutachter den Hauptfokus drauf legten. Aber - wie das Knacken der Bluray zeigte - man kann ggf. das gesamte System an anderem Orte aushebeln. Und wenn man das kann, dann spielt es ja keine Rolle, ob die Daten in Austauschverfahren unknackbar waren oder nicht. Die Diskussion über Wählcomputer in der BRD zeigte ja, dass man dem Wählcomputer das Schachspiel beibracdhte, weil man ihn in die Hände bekam. Das System wurde also ganz anderswo ausgehebelt, als dort, wo die Experten gut planten.

Und wie gesagt, ich würde eben auch die missbräuchliche Verwendung eines geknackten RFID Systems nicht bemerken. Und ich denke, das ist die wahre Kriminalitätsgefahr: Das Internet brachte eine Gefehr hervor, die nicht gegen Leib und Leben geht, sondern gegen Identitäten. Und ob meine Identität missbraucht werden kann ... ich erführe es erst, wenn es zu spät ist. Das ist eben typisch für elektronische Kriminalität.

Also, ich will, dass es in der CH nie einen Zwang gibt, RFID bestücktes Ausweiszeug auf sich tragen zu müssen. Denn sonst muss ich halt aufrüsten und elektronische Abwehrmassnahmen treffen ... :-) ... gibt es übrigens auch schon alles ... für die Paranoiker.