BERNER ZEITUNG BZ

18. April 2009

Darum gehts beim umstrittenen Pass wirklich

Kriminelle könnten die biometrischen Daten des neuen Passes unbemerkt lesen und die Reisen des Passinhabers verfolgen, wird behauptet. Doch tatsächlich lassen die technischen Möglichkeiten des Passes dies nicht zu.

Im neuen biometrischen Pass (Pass 10), über den das Volk am 17.Mai abstimmt, löst vor allem der mit Sender und Antenne ausgestattete RFID-Chip Ängste aus. Im Abstimmungskampf kursieren diffuse Befürchtungen über die technischen Möglichkeiten, die bis hin zur totalen Überwachung des Passinhabers gehen. Der schon erhältliche Pass 06 ist auch mit einem solchen Chip ausgerüstet – hier gab es diese Befürchtungen nicht. Der Chip im neuen Pass enthält allerdings zusätzlich Fingerabdrücke und ist besser geschützt, ansonsten gibt es kaum Unterschiede. Auch äusserlich sehen die beiden Pässe gleich aus.

RFID ist die Abkürzung für «Radio Frequency Identification», auf Deutsch heisst das: Identifikation mittels elektromagnetischen Wellen. Im biometrischen Pass wird ein passiver RFID-Chip zwischen zusammengeklebten Kunststoffseiten im Deckel eingebaut. Passiv bedeutet, dass der Chip nicht durch eine eigene Batterie betrieben wird. Aktivieren lässt er sich mit einem Lesegerät, das über ein externes Magnetfeld verfügt. Dies ist auch bei geschlossenem Pass möglich. Doch der etwa fingernagelgrosse Chip, der von einer rechteckigen, deutlich grösseren Funkantenne umgeben wird, kann nur aus einer geringen Distanz von maximal 20 Zentimetern aktiviert und gelesen werden. «In der Praxis beträgt die Distanz eher 10 Zentimeter», sagt Markus Waldner, Projektleiter Biometrie, beim Bundesamt für Polizei (fedpol). Es ist also nicht möglich, die persönlichen Daten aus grosser Distanz unbemerkt abzurufen.

Wenn der RFID-Chip über einen Magnetfeldleser zum Leben erweckt wird, sendet er zur Begrüssung von Mal zu Mal eine neue Nummer aus. Dann wartet er jeweils auf eine Antwort. Erst wenn er den passenden Schlüssel erhält, beginnt der Chip im sogenannten Basic-Access-Control-Verfahren (BAC) zu kommunizieren. Nach dem Überwinden dieser Hürde gibt der Chip nur jene Daten frei, die ohnehin im Pass lesbar sind.

Komplexer Schlüssel

Der BAC-Schlüssel lässt sich allerdings nicht einfach überwinden. Er setzt sich zusammen aus einer siebenstelligen Passnummer, dem Geburtsdatum und dem Ablaufdatum des Passes. Selbst bei einer einigermassen genauen Schätzung von Alter des Inhabers und Ablaufdatum kann dieser Code laut Waldner erst nach etlichen Jahren ununterbrochener Versuche geknackt werden, und der Angreifer erhielte dann lediglich die erwähnten Daten, die ohnehin auf der Personalienseite des Passes stehen. Das lässt die Befürchtungen eines solchen Datenklaus realitätsfern erscheinen. Denn wer auf wenige Zentimeter an den Pass herankommt, wird die Angaben eher kopieren oder mit dem Handy eine Foto machen, als versuchen, den Code zu knacken.

Drei Datengruppen

Die Daten sind im neuen biometrischen Pass in drei verschiedenen Gruppen abgelegt. Die erste Gruppe enthält alle Angaben, die im Pass lesbar sind – mit Ausnahme der Foto und der Fingerabdrücke. In der zweiten Gruppe wird die Foto in der gleichen Grösse wie die Originalfoto gespeichert. Die dritte Gruppe enthält zwei Fingerabdrücke. In der Regel sind dies die Abdrücke der beiden Zeigefinger. Stets sind flache Abdrücke gespeichert. Die Polizei verwendet hingegen gerollte Fingerabdrücke von allen zehn Fingern, um eine zuverlässigere Identifikation zu ermöglichen. Für Fahndungszwecke wären diese Daten deshalb nur bedingt tauglich. Weitere Angaben wie beispielsweise zum Reiseverhalten des Passinhabers werden im Chip des neuen biometrischen Passes nicht gespeichert.

Schwieriger ist der Zugriff auf die gespeicherten Fingerabdrücke. Im neuen Pass kommt hier das Extended-Access-Control-Verfahren (EAC) zur Anwendung. Damit der RFID-Chip diese Daten frei gibt, muss das Lesegerät einen weiteren Code senden. Dabei handelt es sich um ein Zertifikat, das an ausgewählte Länder vergeben und in Abständen von zwei Wochen bis maximal drei Monaten erneuert wird. Die Schweiz kann also den Zugriff auf die Fingerabdrücke stoppen, indem sie Zertifikate für bestimmte Länder nicht mehr erneuert.

Klonen nicht möglich

Lesbare Daten können auch kopiert werden. Diese Regel ist im Bereich der Ausweisfälschung von Bedeutung: Mit einmal gelesenen Daten lassen sich demnach neue Pässe mit anderen Fotos herstellen. Der neue biometrische Pass verhindere einen solchen Missbrauch, versichert Waldner. Der Grund: «Der Chip enthält einen weiteren geheimen Schlüssel, der nicht kopierbar ist.» Ohne diesen Code wird bei einer Kontrolle festgestellt, dass mit dem Ausweis etwas nicht in Ordnung ist.

Zusätzlich sind die Daten im Chip elektronisch signiert, sodass auch eine Veränderung bemerkt würde. Hinzu kommt schliesslich, dass für einen Missbrauch auch das Passbüchlein, in welches der Chip eingebaut werden soll, gefälscht werden müsste.
(Bernhard Kislig/bz)

Erstellt: 18.04.2009, 10:07 Uhr

80 KOMMENTARE (9 zustimmend (11,5%))

Sándor Zlinszky
12:04 Uhr
ich habe kein Bedenken, wer nichts zu verbergen hat, hat nichts zu befürchten! Jedoch eine Frage ist bei mir aufgetaucht? Warum nur CH-Bürger? Ich denke, dass jeder in der Schweiz angemeldeter Person sollte sich biometrisch ausweisen können!!!!! Es wäre dann keine diskrimination-

S. Flüge
09:48 Uhr
Erstaunlich wie Naiv der Autor ist und ohne Recherche einfach die von der Industrie gelieferten Unwahrheiten reproduziert. RFID kann problemlos bis 50m gelesen werden. Jeder mit kenntnissen der EDV bzw. Verschlüsselungstechnik weiss das es keine Sicherheit gibt. Die grösste Gefahr liegt nicht beim Pass selber sonder bei der Zentralendatenbank auch im Hinblick was der Staat mit diesen Daten macht.

Tom Schneider
09:46 Uhr
Dieser Artikel strotzt nur von absolutisierenden Begriffen wie "nicht möglich", "nicht kopierbar" etc. Zum Vergleich: Die "absolut sicheren" Schutzmechanismen von US-Wahlmaschinen konnten überlistet werden durch das Aufbrechen eines billigen Schlosses und dem Einschieben einer Datenkarte mit präpariertem Betriebssystem. Auch da führten all die beeindruckenden Sicherheitsdiagramme nur in die Irre.

Frank Tester
09:39 Uhr
Trotz der Versicherung durch die Fedpol kann ich dem nicht zustimmen. Bereits vor 2 Jahren hat die CCC (Computer Chaos Club) bewiesen, dass das entsprechend RFID Chips mit analoger Sicherheit durchaus auslesbar sind. RFID Chips lassen sich im übrigen druch bekannte Verfahren durchaus auf grössere Distanzen wie 10 cm auslesen. Dazu kommt, dass gemäss Gesetz auch "Private" den Pass auslesen dürfen.

Luca Cartoffoli
07:12 Uhr
Die Überschrift ist total irreführend! Dass man den e-Pass trotz RFID Technik so sicher als möglich machen wird ist ja ok. Es geht doch nur darum, dass der Staat uns alle wie Verbrecher behandelt und unsere Fingerabdrücke zentral speichern will (ob gerollt oder flach). Sämtliche Argumente für diese DB kann ich nicht nachvollziehen & sind vollkommen übertrieben (siehe Datenschützer). Stimmt NEIN!

Christoph Meyer
06:04 Uhr
Drittens gibt es keinen Grund, die Daten der Passinhaber (eigentlich ist es noch schlimmer: der Passantragssteller) zentral bei der FedPol zu speichern, ausser dass es für die Hacker damit extrem einfach wird, an die GESAMTEN Daten aller CH-Passanstragssteller heranzukommen. Es gilt eine einzige Datenbank zu knacken, resp. einen Mitarbeiter zu bearbeiten. Ein vernünftiger Bürger sagt NEIN!

Christoph Meyer
06:02 Uhr
Zweitens hat der Pass keine Uhr eingebaut, d.h. der Pass ist ohne Hilfe von aussen gar nicht in der Lage, das genaue Datum und die exakte Zeit festzustellen. Damit kann der ach so intelligente Chip im Pass auch nicht feststellen, ob ein Zertifikat, das zum Auslesen der Daten präsentiert ist, noch gültig ist oder nicht (CRS!). Also kann jeder die Daten auslesen, der je ein Zertifikat hatte.

Christoph Meyer
05:59 Uhr
Erstens gibt es absolut KEINEN Grund, die Fingerabdrücke im Pass selbst zu speichern - ein Hash würde ausreichen, um sicherzustellen, dass der Vorweiser des Passes die gleichen Fingerabdrücke hat wie die Person, für die der Pass ausgestellt wurde. KEIN vernünftiger Kryptologe würde vorschlagen, Passwörter (= Fingerabdrücke) zu speichern, nur den Hash darf man speichern.

Armin B Schweizer
05:34 Uhr
Die vor Volksabstimmungen immer ueblichere einseitig tendenzioese Volksmeinungs-verbildung durch die gleichgeschalteten Massengrossmedien ist einmal mehr angelaufen....

Christian Stutz
05:32 Uhr
Wieder typisch, das Thema schön reden, damit die Abstimmungsvorlage alglatt durch kommt!!!

Matthias Bürcher
03:12 Uhr
Im Artikel werden ein Dinge behauptet, die nicht Sinn machen (aus Platzgründen hier nur 2): - Distanz des RFID-Chips: niemand behauptet, dass jemand im Nebenzimmer den Pass ausliest. Der Pass gelangt aber an vielen Orten (z.B. Hotel) in fremde Hände. - Wenn der Chip keine Batterie hat, hat er auch keine Uhr und kann die richtige Zeit gar nicht wissen. Das Lesegerät kann ein Datum vortäuschen.

Philippe Schnyder
02:51 Uhr
Das echte Problem ist nicht der RFID der jedoch wirklich sehr fälschungsunsicher ist, sonder die zentrale Datenbank! Der kurze BAC Schlüssel ist jedoch mit heutiger Technik sehr einfach zu knacken. Die Feststellung, dass es wegen dem RFID-Chip im Pass 06 zu keiner oder wenig Kritik kam, ist korrekt, jedoch gabs es mit diesem Pass auch noch keinen RFID-Zwang! Autoren: Informiert euch bitte besser!

Ruedi Bliban
01:58 Uhr
@Tagi bitte hört auf solchen unsinnigen Propaganda Mist 1:1 abzudrucken. Alles was hier geschrieben wird, wurde innerhalb der EU schon einige dutzend Male wiederlegt. Ich bin entsetzt, dass man die Stimmbrüger wirklich für so bescheuert hält.

Gero Rubli
01:51 Uhr
Ein schönes Propagandastück. "Darum" geht es aber bei der umstrittenen Vorlage wirklich nicht: Den biometrischen Pass gibt es schon. Wer Orwells 1984 gelesen hat, will aber weder eine per Funk lesbare biometrische ID, noch Fingerabdruck-Fichen von jedermann, noch Zugang aller möglichen "Transportunternehmen" auf biometrische Daten. Das alles erlaubt dieses Gesetz, darum: NEIN.

Sapere Aude
00:46 Uhr
Bernhard Kislig ist ein Kurzdenker / Kurzschreiber, wenn er grossspurig sein Artikel mit "Darum gehts beim umstrittenen Pass wirklich" ueberschreibt. Selbstverstaendlich geht es auch um andere Punkte, welche bei den CH Stimmbuergern zu recht Unbehagen ausloesen. Meiner Meinung ist die zunehmende Tendez mit naiver Begeisterung (Ueberwachungs-) Technologien anzuwenden der Hauptgrund NEIN zu stimmen!

Dani Meier
00:13 Uhr
Wenn es die «Kriminellen» nicht schaffen, dann schafft es sicher der Staat diese Daten zu MISS-Brauchen! Ferner muss man bei Beantragung eines Passes wie ein Krimineller antraben, zwecks Erfassung der Daten. Teuer wird der Pass auch noch. Also wer's braucht, der muss später nicht fluchen.

wisi jori
00:08 Uhr
die meisten mitglieder "der jungparteien", welche gegen den neuen pass sind, sind auf youtoube, facebook registriert, benutzen cumulus und wie sonst noch heissen karten, und haben angst, dass ihre daten bekannt werden! das ist gestört. dafür werden alle leute bestraft, welche viel reisen, sei es geschäftlich oder zum vergnügen! auch die svp, , torpediert jede erneuerung!

Lorenz Amstutz
18.04.2009, 23:37 Uhr
Wer im Zusammenhang mit elektronischen Daten von absoluter Sicherheit spricht, kann problemlos der Irreführung bezichtigt werden. Alle Daten können, mit zum Teil erheblichem Aufwand versteht sich, kopiert und oder geknackt werden. Das gilt auch für die im Pass gespeicherten Daten. Alle anderen Behauptungen sind schlicht falsch und werden täglich durch gegenteilige Meldungen aus der IT widerlegt.

Jordan Keller
18.04.2009, 23:17 Uhr
Wenn heute in Sachen Verschlüsselung seitens Staaten behauptet wird "unsere Methode ist Sicher" kann ich es nicht glauben. Die meisten staatlichen "Experten" hinken weit hinter den echten Profis her. Und diese Profis beziehen meistens ihre Gehälter entweder von "Sicherheits und beraterfirmen" oder direkt von verbrecherischen Organisationen.

J. Kapp
18.04.2009, 23:00 Uhr
Die schönen Worte hör ich wohl...und wie war es damals mit der "hochgeheimen" ENIGMA? Die Crux liegt in den Zertifikaten- die können minütlich oder alle Jahre ändern - der Chip muss ja die Gültigkeit erkennen. Zudem müssen diese an bis zu 200Nationen verteilt werden. Zudem: hat die NSA sicher schon alle diese Schlüssel. - sie verhinderte vor 10Jahren die "sichere" Verschlüsselung,schon vergessen?

Armin Schaller
18.04.2009, 22:41 Uhr
Ein Beispiel: Es ist das Jahr 2012. Ein rechtschaffener ehemaliger Assistent aus der UBS wurde im Jahr 2009 Arbeitslos und fand keinen Job mehr. Seit 2 Jahren lebt er von der Fürsorge. Jetzt wird er von einem Freund fürs Wochenende an den Gardasee eingeladen. Die Behörden sehen, dass der fürs Weekend nach Italien ging, fragen sich, wie er sich das leisten kann und streichen die Fürsorge. Willkür!

Armin Schaller
18.04.2009, 22:34 Uhr
Die Ausstellugn des Passes und der Prozess sind belanglos! Es ist klar, dass am biometrischen Pass kein Weg vorbeiführt. Dennoch: Das Problem bei diesem Pass sind nicht die biometischen Daten an sich, sondern dass der Pass selbst quasi identifizierbar wird. Und jedes mal, wenn der Pass irgendwo eingelesen wird, wird das gespeichert. In irgendeiner Datenbank. Willkürlich vom Staat verwendbar.

Thomas Wirz
18.04.2009, 22:11 Uhr
2. geht es schlussendlich vor allem darum: die Kontrolle und Überwachung nimmt laufend zunimmt. In den USA werden RFID-Chips ersten Menschen bereits IMPLANTIERT. Es ist eine Frage der Zeit, bis dieser Standard ebenfalls von uns verlangt wird, wenn wir bei der

Einreise nicht schikaniert werden wollen. Ich wette, unsere Kinder werden eines Tages über diese Vorlage abstimmen: RFID-Implantat ja/nein.

Thomas Wirz
18.04.2009, 22:06 Uhr
1. Bankdaten sind ebenfalls absolut sicher, heisst es. Und plötzlich kursieren Daten herum, die gehackt wurden. Und etwas sicher nicht gehackt werden kann, dann das Pentagon, würde man meinen. Nun, auch das ist bereits passiert. Wie naiv muss man sein, um diese Story zu glauben? Selbst wenn es HEUTE schwierig möglich ist, was ist denn mit MORGEN?

Hans Walter
18.04.2009, 22:00 Uhr
Dank Schengen können nun auch international gesuchte Schwerverbrecher ohne Passkontrolle in die Schweiz einreisen. Weshalb sollen die überhaupt noch Pässe fälschen wollen?

peter spelt
18.04.2009, 20:49 Uhr
wenn jemand in die usa reist werden heute schon z.t. recht sensible daten aufgenommen und gespeichert und keiner weiss was genau damit passiert. um den pass optimal zu schützen kann man ihn in ein bleisack packen, die wurden verwendet um filme vor den röntgenstrahlen zu schützen. da kommt kein funksignal durch und die induktion funktioniert auch nicht. ha! ich mache ein bleisack-buisness auf!

Arturo Schäfer
18.04.2009, 20:42 Uhr
Nun ja - wie oft wurde schon behauptet, solche Dinge sind sicher und später stellte sich doch das Gegenteil heraus!

Salmo Fario
18.04.2009, 20:17 Uhr
Die Frage ist doch warum braucht es einen Zwang für so einen Pass? Jeder sollte selber wählen, ob er einen biometrischen Pass will oder nicht. Er kann dann vielleicht nicht mehr in alle Länder reisen, aber das ist doch jedem freigestellt. Warum eine zentrale Datenbank? Es dauert nicht lange und die Sicherheit ist überwunden. Und es wird auch nicht lange dauern bis der Staat die Daten missbraucht.

benedikt mei
18.04.2009, 20:06 Uhr
Als Informatiker kann ich zu diesem Bericht nur eines sagen: wer RFID-Chips verniedlicht, ist sich den technischen Möglichkeiten nicht bewusst. Ich verweise auf die Berichte des Chaos Computer Clubs (CCC).

Christian Suter
18.04.2009, 20:03 Uhr
Jede Technologie wurde irgend einmal eingeholt. Früher oder später ist der Pass kopierbar. Zudem finde ich das der normale Bürger immer mehr wie Verbrecher behandelt werden. Früher wurden nur Finger abdrücke von Verbrechern genommen. Dieser ganze Schwachsinn haben wir nur den USA zu verdanken!!

Christophe Bachmann
18.04.2009, 19:57 Uhr
Wissen ist gleich Macht und Macht korrumpiert! Damit der Chip aktiviert wird und seine Daten automatisch weiterleitet ohne dass der Inhaber etwas bemerken kann, würden Access (Control)-Points installiert werden (Ein- und Ausgänge, zBsp Banken, Vers., Restaurants). Unsere Daten können an einer Zentrale weiter geleitet werden, und somit würde die Ueberwachung des Bürgers ausgeweitet werden. NEIN!

Balz Ginsig
18.04.2009, 19:47 Uhr
Sicher ist nur, dass der Chip und die Software Hersteller an die Sicherheit des System's glauben. Der ganze Rest von der Produktion ueber die Datenverwaltung in der Schweiz und im Ausland ist nie sicher. Meine Frau beantrage Anfang 2009 einen neuen Ausweis und Ihre Daten gingen zwischen dem Migrationsamt ZH und dem Hersteller verloren. Ursache nicht nachvollziehbar, Verbleib der Daten unbekannt !

Dan Hostettler
18.04.2009, 19:45 Uhr
...alles kann gefaelscht werden. Sorry.

M. Forster
18.04.2009, 19:25 Uhr
Bla, bla, bla, das versucht man wieder, das Volk zu beschwichtigen und zu beruhigen. Dass die Daten zentral gespeichert werden wird mal wieder nicht erwähnt. Und so sicher wie es im Artikel dargestellt wird ist er auch nicht, wie zahlreiche Experten herausfanden. Im Netz findet man alle Beweise dazu, wenn man denn Interesse daran hat. Der gläserne Bürger wird uns wieder schmackhaft gemacht..

maurus candrian
18.04.2009, 19:24 Uhr
guter, sachlicher und informativer artikel. danke. werde ja stimmen.

Ueli Steiner
18.04.2009, 19:09 Uhr
Jede Sicherheitsvorkehrung kann auch umgangen werden. Und beim Computer dies meist noch einfacher. Dass sich Daten nicht über irgendwelche obskuren Sicherheitsschema einsperren lassen, hat inzwischen selbst die Unterhaltungsindustrie gemerkt.

Robert Mädler
18.04.2009, 19:05 Uhr
Jedes System hat Sicherheitslücken. Entweder sind Hacker geschickt genug, um alle Sperren zu überwinden, was dann im Internet veröffentlicht wird. Hacker haben schon das Pentagon und weitere geheime Dinge geknackt.. Oder die Geheimnisträger (wieviele in der Schweiz? 30, 50, oder mehr?) verkaufen ihr Wissen, oder sie werden zur Herausgabe gezwungen. Nein, ich schaue nicht zu viele Hollywoodfilme.

Olivier Kessler
18.04.2009, 19:00 Uhr
Offenbar ist der Autor dieses Artikels auf die unwahren Propaganda-Argumente der Befürworter hereingefallen. Wie die alte Fasnacht kommt er mit dem längst widerlegten Argument, dass man den Chip im Pass kaum haken könne und wenn, dann ginge das höchstens aus 20 cm. Diverse Experten haben bereits das Gegenteil bewiesen und den

Daten aus mehreren Metern Entfernung stehlen können. Sehr gefährlich!

Pierre Heri
18.04.2009, 18:52 Uhr
Ich reise viel und bin auf einen Pass angewiesen, der mir ohne Verzögerung und Probleme die Einreise in andere Länder ermöglicht. Ich verstehe die Aufregung nicht. Warum macht man nicht einfach neben dem biometrischen auch einen konventionellen Pass für jene, die den neuen Pass nicht haben möchten? Oder sie können ja auch mit der ID im Schengenraum reisen. Viele Grüsse in die Schweiz aus Bangkok.

Joe Grovel
18.04.2009, 18:39 Uhr
Sagt mal, wie naiv sind die Tagi-Redakteure eigentlich. Bisher ist noch bei jedem der bereits eingeführten Biometrischen Pässe eine Sicherheitslücke aufgetaucht. Warum sollte das in der Schweiz anders sein? Hört euch mal unter Informatikern um, da sind alle gegen die Einführung. Alle Datensicherheitsexperten stellen sich uniform gegen diese neue Technik. Das soll nicht bedenklich sein?

David Meili
18.04.2009, 18:36 Uhr
Entweder verfügen Herr Waldner oder der Journalist über in eher beschränktes Wissen bzgl. des RFID-Chip und Zertifikate. RFID-Scanner entwickeln sich sehr rasch und können bereits heute auf Distanz ablesen, sonst setzt sich die Technologie in der Warenlogistik nicht durch. Dass "ausgewählte Fluggesellschaften" Zertifikate erhalten werden, um meine biometrischen Daten zu lesen, macht nachdenklich

Herbert Selig
18.04.2009, 18:36 Uhr
Selten so viel Blödsinn gelesen. Es wurden schon Distanzen von 10 Metern demonstriert. Schlüsselstärken von 35bit können nach dem Abhören einer korrekten Verbindung innert Stunden geknackt werden, danach ist Personentracking etc. easy möglich. Zertifikatrevokierung bring nix, da der Pass keine Uhr mit Datum drin hat. Ich will nicht, dass der Staat meine Fingerabdrücke zentral speichert.

Sim Merki
18.04.2009, 18:21 Uhr
Wenn dies der Autor wirklich ehrlich meint, dann ist er: 1. Keine Fachperson 2. Naiv Ich möchte einmal einen Artikel vom zuständigen Prof. Basin der ETHZ lesen. Ziemlich sicher wird er für diesen Pass garantiert nicht die Hand ins Feuer legen.

Maximilian Blöchlinger
18.04.2009, 18:20 Uhr
Seit Monaten warte ich auf eine unvorbereitete Live-Vorführung wie ein E-Pass von nicht Berechtigten (den jungen Grünen) gelesen wird. Auch wenn er einmal gelesen wird, er ist internationaler Standard! Wenn die Schweiz nicht mitmacht, kommen wir auf die schwarze oder graue Liste und schiessen damit nur ein Eigengool.

Stefan Johner
18.04.2009, 18:07 Uhr
Mir ist es ein Rätsel, warum diese Sicherheitsmängel von vielen Leuten nicht ernst genommen werden. Informatiker aus der ganzen Welt warnen, dass Teile des Passes nicht genügend gesichert sind! Warum hört niemand auf diese Leute? Beim Hausbau nimmt

schliesslich auch jeder den Rat des Architekten an, aber in der Informatik denkt wohl jeder er sei selber genug Spezialist...

Kurt Wahren
18.04.2009, 18:06 Uhr
Es ist schon überraschend wie einige Leute bei der Fedpol die technischen Bedenken von weltweit angesehenen Wissenschaftlern und Physikern EPFL und ETH ignorieren. Richtig ist, dass der RFID (Basic Access Control) heute auf 10m Distanz problemlos gelesen werden kann. Das Material kostet ca. 2500 CHF und ist für jedermann zugänglich. Um den BAC zu knacken braucht man nicht Jahre sondern 4 Std !!!

Peter Meier
18.04.2009, 18:04 Uhr
Einfach in Google mal eingeben "rfid long distance reader" und schon findet man Lösungen und Bauanleitungen für RFID-Leser, welche mehrere Meter Distanz überwinden können. Von wegen 10-20cm...

Sebastian Heinzinger
18.04.2009, 18:04 Uhr
Liebe Leserschaft, der Pass ist doch nie das Problem, sondern die zentrale Datenspeicherung. Dadurch wird Orwell leider langsam aber sicher Wirklichkeit. Schade, dass der Autor kein Wort darüber verliert. Manchmal frage ich mich, ob die Medien in unserem Land, dem schönsten Land der Erde, denn noch frei sind. Kritisch darüber wird kaum mehr berichtet. Müssen wir auch hier der EU klein beigeben?

Conradin Räber
18.04.2009, 17:52 Uhr
Es ist beschämend wie der Autor versucht dem Leser den biometrischen Pass schmackhaft zu machen. Als Krypografieingenieur muss ich dazu klar festhalten. Der Pass ist fälschbar, der RFID Chip ist nicht für sensible Daten entwickelt worden und die Möglichkeit etwas zu entschlüsseln steigt nicht linear sondern exponentiell. Was heute sicher ist, ist morgen geknackt und Fingerabdrücke sind ungeeignet!

Toni Müller
18.04.2009, 17:50 Uhr
Wie naiv ist das denn. Der biometrische Pass ist nicht nur ein Kontrolldokument für demokratische Staaten. Je mehr zentral abgespeicherte Daten, desto grösser die Missbrauchs-Möglichkeit durch jene, die zu diesen Daten Zugriff haben - und das sind nicht nur demokratische Staaten. Den Bürgern aller Völker sei empfohlen, sich der totalen Kontrolle durch Regierungen zu entziehen. Nein zu diesem Pass.

Max Muster
18.04.2009, 17:39 Uhr
Mag sein dass am Anfang ein Missbrauch fast unmöglich ist, aber wie bei anderen Techniken auch ist es nur eine Frage der Zeit bis man Zugriff hat, sprich die Daten missbraucht werden können! Desweiteren ergibt sich durch diesen Pass faktisch kein nennenswerter Sicherheitsgewinn für uns alle!!! Aber mit inszeniertem Terror soll uns der Überwachungsstaat weiter aufgeschwatzt werden! Sagen Sie NEIN!!

Werner N. Staub
18.04.2009, 17:37 Uhr
Einfach einen Pass kreieren, mit dem man überall hinreisen kann, ohne sich zusätzliche

Dokumente beschaffen zu müssen. Wieso immer diese Befürchtungen wegen einer angeblich totalen Ueberwachung? Da haben sich ja kuriose Seilschaften gebildet in der Bekämpfung des biometrischen Passes. Also JA für den neuen Pass!

georg hemmer
18.04.2009, 17:35 Uhr
das Problem ist weniger der Pass, sondern die unnötigen Datenbanken, die an das Passprojekt geknüpft wurden. Meine Daten möchte ich dieser Regierung sicher nie zur Verfügung stellen!

Tobias Frey
18.04.2009, 17:33 Uhr
Also ist ja alles in Ordnung, ausser der zentralen Datenspeicherung, richtig?

Werner Schadegg
18.04.2009, 17:32 Uhr
Der biometrische Pass sollte als Option erhätlich seinl. Schweizer welche nicht in die USA reisen, sollten weiterhin den Pass 06 erhalten können. Die Schweiz verlangt von USA Bürgern auch keinen biometrischen Pass, ja nicht einmal ein Visum.

Marco Tedaldi
18.04.2009, 17:28 Uhr
"Nach dem Überwinden dieser Hürde gibt der Chip nur jene Daten frei, die ohnehin im Pass lesbar sind", steht im Artikel. Dass diese Daten aber ausgelesen werden können, ohne dass der Inhaber es merkt, wird nicht erwähnt. 7-stellig Zahl = 10Mio Schlüssel. Das ist kryptografisch gesehen ein Witz. Die Daten können recht genau geschätzt werden. BAC ist ein Witz!

Peter Weierstrass
18.04.2009, 17:26 Uhr
All das ändert aber immer noch nichts daran, dass der biometrische Pass völlig überflüssig ist... fälschungssicher? Ist unser alter Pass sowieso schon, zumindest verglichen mit vielen anderen Ländern. Bessere Identifikation an der Grenze? Fingerabdrücke abgeben ist etwas, das ich eher mit Kriminellen assoziiere. Nein danke...

Peter Baumgartner
18.04.2009, 17:24 Uhr
Das Problem ist dass mit diesem Pass via Fingerabdruck nachher alles gemacht werden kann (automatische Passkontrolle). Dieser Pass verlässt isch auf den Fingerabdruck als eindeutig und unfälschbar. Leider kann man einen Fingerabdruck aber fälschen, sofern man einen originalen zur Verfügung hat. Apropos Datenbank: Vertauen sie jedem einzelnen Polizisten Europas? Manche Macht sollte niemand erhalten

Marco Tedaldi
18.04.2009, 17:24 Uhr
Mit verlaub. so eine Ansammlung von Blödsinn habe ich noch selten gelesen. Die Distanz, aus welcher ein RFID-Chip gelesen werden kann hängt von der Leistungsfähigkeit des Lesegerätes und der eingesetzten Antenne ab. In der Industrie werden ganze Paletten mit hunderten Ettiketten gleichzeitig über Distanzen von Metern ausgelesen! Markus Waldner ist entweder schlecht informiert oder ein Lügner!

Silvio Suter
18.04.2009, 17:16 Uhr
Das Problem der biometrischen Pässen liegt wohl eher bei den Kosten für die Bürger und dem Sicherheitsrisiko bei der zentralen Datenspeicherung. Ist es nötig, dass der Pass und die Identitätskarte in einer Datenbank biometrisch zwangserfasst werden? Der biometrische Pass ist nicht notwendig für unsere Reisefreiheit - ein weiterer Risikofaktor für nichts? Es sollte doch jeder selbst wählen dürfen.

Daniel Wigger
18.04.2009, 17:10 Uhr
Endlich wird neutral informiert. Bravo! Die Contra-Argumente der unheiligen Allianz extrem rechts und links (auslandfeindliche SVP und fichenfürchtende Grüne und Sozialisten) sind an den Haaren herbeigezogen. Erreichen würden wir mit einem Nein höchstens, dass wir nur noch mit Visas reisen könnten, z.B. in die USA. Wer Angst vor Datenklau hat, soll doch einfach keinen Pass beantragen!

egon Stein
18.04.2009, 17:03 Uhr
Es gibt in der Schweiz auch heute Bürger die keinen Pass und keine ID-Karte haben, wer das nicht will der kann das selbst ändern. Wer nicht ins Ausland reist dem darf auch der Pass nicht aufgezwungen werden. Geschieht das dennoch per Gesetz, so ist das Beweis für den Polizeistaat dessen Besoldete die totale Bürgerkontrolle für eine Versklavung anstreben. Terrorgefahr droht von der Nomenklatur.

Claus Koch
18.04.2009, 16:52 Uhr
Der BAC/EAC-Code kann vielleicht mit der *heutigen* Hardware erst "nach etlichen Jahren ununterbrochener Versuche geknackt werden". Wie es in fünf Jahren aussieht weiss niemand. Keine Verschlüsselung ist 100%-ig perfekt. Wie schnell in der Vergangenheit auch aufwendige Verschlüsselungen geknackt wurden, lässt sich an DVD, Blueray, Nagravision, WEP, WPA usw. sehr schön illustrieren.

Francois Stocker
18.04.2009, 16:47 Uhr
Achtung! Den Staaten ist nicht zu trauen. Es wird keine Woche vergehen bevor der Staat die Daten für allgemeine Zwecke einsetzen und verkaufen wird. Wenn Waldner sagt dass kopieren nicht möglich ist hat er vergessen zu sagen dass der Staat, jeder Staat in Europa, die Daten automatisch bekommt und verkaufen kann.

Kurt Zerzawy
18.04.2009, 16:44 Uhr
mag ja alles sein. Aber das Hauptübel, dass uns die Schweizer Regierung gleichzeitig unterjubeln will, hat damit gar nichts zu tun. Das ist die völlig unnötige zentrale Speicherung. Diese Daten werden wahrscheinlich nur sehr kurz in der Schweiz bleiben und beim geringsten Druck von aussen an unseren grossen Bruder USA geschickt.

Petar Tirci
18.04.2009, 16:41 Uhr
Ich bin kein Krimineller, nur bescheidener Informatiker. Aber dass ein solch kompliziertes Verfahren schon rein systembedingt haufenweise Löcher haben muss, ist mir klar. Nur schon der Satz "Für Fahndungszwecke wären diese Daten deshalb nur bedingt tauglich.". Dazu, jemandem bei Bedarf etwas anzuhängen, reicht's. Nein, Leute, lasst Euch von einem Insider

sagen: Diese Vorlage muss verworfen werden.

Paul Müller
18.04.2009, 16:39 Uhr
Viel schlimmer als den RFID-Chip finde ich die Speicherung der Fingerabdrücke. Erst kürzlich hat der europäische Gerichtshof für Menschenrechte entschieden, dass ein Staat nicht das Recht hat, ohne begründeten Verdacht die Fingerabdrücke seiner Bürger zu speichern. Es kann doch nicht sein, dass unbescholtene Bürger/innen wie Verbrecher behandelt werden. Deshalb werde ich ein klares NEIN! einlegen!

Hans Grauer
18.04.2009, 16:34 Uhr
Leider trügt der Titel, den darum gehts beim umstrittenen Pass nicht. Es geht um die zentrale Datenbank, welche Fingerabdrücke speichert. Hat man dort ein Sicherheitsleck, kann jeder der dieses Leck ausnützt mit Fremden Fingerabdrücken Verbrechen begehen.

André Bisang
18.04.2009, 16:32 Uhr
Noch Fragen? Es zeigt sich wieder einmal, dass die politische Ecke, die gegen den neuen Pass polemisiert, einmal mehr mit Unwahrheiten, falschen Behauptungen und Ammenmärchen operiert. Wer hat Angst vor seinem Fingerabdruck?

Hans R. Leutwyler
18.04.2009, 16:31 Uhr
Der Bericht ist sehr technisch und für viele Leser schwer verständlich. Tatsache ist, dass Fedpol mehr (Schnüffel) Möglichkeiten in die neuen biometrischen Pässe einbauen will, als Schengen verlangt . Das halte ich im Hinblick auf sukzessiv schwindenden Datenschutz für die Bürger unklug. Dafür habe ich kein Verständnis und werde am 17.5. ein NEIN in die Urne werfen.

Marcel Baumann
18.04.2009, 16:18 Uhr
1. Was entwickelt wurde ist immer "clonebar". Nur eine Frage der Zeit und Profit. 2. Sicherlich versucht niemand den Chip aus Distanz zu lesen. Die Probleme sind die Passkontrollen der Ländern (spez. auch USA) wo Niemand weiss was mit den gescannten Daten passiert und wo diese gespeichert bleiben. 3. Scanners könnten auch in Hotels oder wo auch immer Passdaten *gelesen* werden vorhanden sein.

Urs Müller
18.04.2009, 16:12 Uhr
ja klar es geht ja auch nicht drum dass meine fingerabdrücke (als unbescholtener bürher wohlgemerkt) zentral erfasst und abgespeichert werden. Und ja klar RFID chips lassen sich nur aus 20cm entfernung auslesen (recherchiert hierzu mal ein bisschen). aber wenns der hersteller sagt muss es ja stimmen (sowas nennt sich journalismus?). Und ja der schlüssel ist sicher, laut hersteller, toll.

Peter Amrein
18.04.2009, 16:11 Uhr
Die alte Mär der absoluten Sicherheit. Nix ist absolut Sicher: Kein Schloss, kein Ausweis, kein Chip, kein Code etc.

Hans Meier
18.04.2009, 16:02 Uhr
Schön wärs! Erstens hat man bei britischen Pässen bereits etliche Sicherheitsmassnahmen überwunden. Zweitens gelten die beschriebenen Bedingungen nur in Ländern welche sich die Infrastruktur überhaupt leisten können. In allen anderen Staaten erleichtert der neue Pass das fälschen & Missbrauch massiv, weil die Zöllner annehmen, dass was der Chip sendet, meist stimmt. Es braucht keine zentrale DB!

Patrick Leu
18.04.2009, 15:57 Uhr
Ob ein Chip von 10cm oder 20cm oder von 5m aus aktviert werden kann, ist vermutlich von der Sendeleistung des Lesers abhängig. Es ist wie mit den Handys: Die Bluetoothreichweite ist im Durchschnitt bei 20-30m. Es gibt aber genügend Hardware, die einen Empfang über mehrere hundert Meter möglich machen. Der Missbrauch wird möglich sein, da bisher auch beinahe jede vVerschlüsselung geknackt wurde.

Dominik Ruf
18.04.2009, 15:55 Uhr
Ist hier ein Nutzen zu Gunsten der vertraulichen Sicherheit gegeben, oder mehr der beteiligten Industrie?! Defacto sind die verbauten Speichermedien nicht sicher gegen elektromagnetische Einflüsse und - es ist allenfalls eine Frage der Zeit - gegen willkürliche Manipulationen. Das wird bedeuten müssen: der Pass wird nur eine kurze Halbwertzeit haben können. Ist dies in der Sache wirklich Sinnvoll?

Christain Thommen
18.04.2009, 15:52 Uhr
Eine ziemlich billige Propaganda für die Abstimmung. Der Schlüssel ist nominal 56 bit, real nur 43 bit breit, völlig ungenügend und innert kurzer Zeit zu knacken. Die Daten können auch via die vielen autorisierten Leser (Flughäfen, Fluggesellschaften) an Dritte gelangen. Wenn man mit frontalen Fingerabdrücken nicht zweifelsfrei Personen identifizieren könnte, wären sie nicht im Pass.

Doris Kaufmann
18.04.2009, 15:46 Uhr
Interessante Argumentation "Der Pass ist besser geschützt" was heisst das denn? Gar nichts. Wer kann ihn denn alles auslesen? Antwort alle Staaten und jeder, der ein Lesegerät hat. Aussage "der Chip kann nicht kopiert werden". Antwort: Lüge jedes digitales Element und das ist der Chip kann kopiert werden! Interessant die Grafik oben, die Finberabdrücke sind also doch für die Polizei und Fahndung.

Rudolf Steiner
18.04.2009, 15:45 Uhr
Leider hat der Autor nicht im Ansatz begriffen, weshalb diese Vorlage umstritten ist. Es geht in erster Linie um die unnötige zentrale Datenbank, die Tatsache dass die gespeicherten Daten an private wie Flughafenbetreiber und Airlines weitergegeben werden können, und nicht zuletzt auch darum dass die rechtliche Grundlage geschaffen wird, den Biometrie-Zwang auf IDs auszuweiten. NEIN am 17. Mai !!

Manuela ManuelaMeier
18.04.2009, 15:40 Uhr
Der periodische Wechsel des Zertifikats ist leider nutzlos. Der Pass bezieht die Uhrzeit von aussen, da er keine eigene Stromversorgung für einen Taktgeber besitzt. Das grössere

Problem ist allerdings, dass auf der zentralen Datenbank die Fingerabdrücke nicht einwegverschlüsselt abgelegt sind, das öffnet Missbrauch Tür und Tor.