Budapest-Erklärung zu maschinenlesbaren Ausweis-Dokumenten (Machine Readable Travel Documents, MRTDs)

Zusammenfassung

Dadurch, dass eine angemessene Sicherheitsarchitektur nicht implementiert wurde, haben die europäischen Regierungen im Resultat ihre Bürger gezwungen, neue international maschinenlesbare Ausweis-Dokumente (Machine Readable Travel Documents, MRTDs) zu akzeptieren, die in erheblichem Ausmaß ihre Sicherheit und Privatsphäre gefährden sowie das Risiko eines Identitätsdiebstahls erhöhen. Einfach ausgedrückt verwendet die gegenwärtige Implementierung des europäischen Passes Techniken und Standards, die für diesen Verwendungszweck von ungenügender Eignung sind. In dieser Erklärung, verfasst auf einer Konferenz des FIDIS[1] (Future of Identity in the Information Society)-Exzellenznetzwerks im September 2006 in Budapest, fassen Forscher, die sich mit Identität und Identitätsmanagement beschäftigen, Erkenntnisse einer Analyse von MRTDs zusammen. Sie empfehlen korrigierende Maßnahmen, deren Übernahme durch die Verantwortlichen in Regierungen und Industrie nötig ist, um kritische Punkte zu verbessern.

Einführung

Neue MRTDs wie der europäische Reisepass sind grundsätzlich den gleichen Risiken ausgesetzt, wie die bisherigen rein papiergebundenen Pässe. In Ergänzung treten jedoch zusätzliche Gefährdungen der Passnutzer auf, unter denen wir insbesondere die folgenden herausstellen wollen:

- Im Unterschied zu traditionellen papiergebundenen Pässen können Daten aus den neuen MRTDS aus Entfernungen bis zu 10 m unbemerkt und ohne Einflussnahme (aus Sicht des Passinhabers) abgehört oder ausgelesen werden.[2] Die bestehende Zugriffssicherung kann gebrochen oder umgangen werden. Damit besteht das Risiko der automatisierten Überwachung (mittels Tracking) von Personen in Situationen, in denen sie MRTDs bei sich tragen, z.B. als Touristen im Ausland.
- Biometrische Referenzdaten können in der Form, in der sie in MRTDs gespeichert werden, ungehindert auch für andere als den vorgesehenen Zweck verwendet werden. Eine solche Zweckentfremdung verletzt europäisches Datenschutzrecht. Darüber hinaus beruht biometrische Identifizierung auf Wahrscheinlichkeiten – Fehlerkennungen und Fehlzurückweisungen sind unumgänglich und werden europäische Bürger täglich betreffen.

Der europäische Reisepass (ePass) basiert auf technischen Leitlinien und Standards der ICAO[3], die im Dokument 9303[4] festgelegt sind und die mit der Verordnung 2252/2004[5] in europäisches Recht übertragen wurden. Im Jahre 2005 begann die Ausgabe der neuen Pässe in Europa.

Diese Erklärung basiert auf den Ergebnissen einer Analyse der rechtlichen Grundlagen sowie der Technik-, Datenschutz- und Sicherheitskonzepte des ePasses. Dieses Positionspapier basiert auf einer Analyse, die vom FIDIS-Exzellenznetzwerk durchgeführt und in der Studie „D3.6 Study on ID

---

[1] www.fidis.net

[2] ISO 14443-kompatible RFID-Chips, wie sie im ePass benutzt werden, sind für ein Auslesen auf 10 bis 15 cm optimiert. Allerdings ist ein Auslesen sowie Abhören der Kommunikation zwischen Leser und Transponder aus größeren Entfernungen (2-10 m) möglich (siehe Finke, T., Kelter, H., Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems, Bonn 2004. Download: www.bsi.de/fachthem/rfid/Abh_RFID.pdf) und wurde kürzlich am Beispiel des Niederländischen Passes von Robroch demonstriert (siehe Robroch, H., ePassport Privacy Attack, 2006, www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf), der auch Distanzen für Auslese- und Abhörvorgänge listet.
Einige ePässe, z.B. in den USA, sind mit einem Faraday'schen Käfig versehen, der in Form eingelassener Metallfäden im Deckel des Passes realisiert ist. Kürzlich konnten Mahaffey und Hering zeigen, dass wenn sich der Pass nur einen Zentimeter öffnet, was leicht in einem Rucksack oder einer Brieftasche passieren kann, er aus 60 cm Entfernung ausgelesen werden kann (siehe www.flexilis.com/epassport.php).

[3] ICAO = International Civil Aviation Organization, www.icao.int

[4] Informationen dazu via www.icao.int/MRTD/Home/Index.cfm

[5] Siehe http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf

Documents“[6] dokumentiert wurde. In Ergänzung zu den in dieser Studie genannten Quellen wurden noch die folgenden Unterlagen ausgewertet:

- Protection Profiles for Biometric Verification Mechanisms and MRTDs including Basic Access Control (BAC)[7] zertifiziert vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Technical Guideline V1.0 for Extended Access Control (EAC) herausgegeben vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) im August 2006[8].

Zusammenfassung der Ergebnisse

Bisher ist kein ganzheitliches Sicherheitskonzept für MRTDs für die Öffentlichkeit oder interessierte Experten zugänglich. Öffentlich zugängliche Dokumente wie Protection Profiles oder Technische Leitlinien decken nur Teilbereiche eines solchen Konzeptes ab. Während Basic Access Control (BAC) ursprünglich als wirksame Zugriffssicherung präsentiert wurde, wurde kürzlich Extended Access Control (EAC) als verbesserte Version vorgestellt. Beide sind (als Zugriffsschutz für die Nutzer) in zahlreichen Situationen einfach unzureichend.[9]

Eine Reihe theoretischer und wissenschaftlich gezeigter Bedrohungen und konzeptioneller Schwächen des ePasses wurden bereits publiziert. Diese werden bislang von Protection Profiles, Technischen Leitlinien oder bestehenden ePässen nicht behoben. Unter diesen Schwächen sind am gravierendsten:

- Biometrische Informationen in MRTDs können derzeit nicht widerrufen werden. Da physische Merkmale wie das Gesicht oder Fingerkuppen nicht einfach geändert werden können, können einmal „gestohlene“ biometrische Merkmale lange Zeit missbraucht werden.
- Das Schlüsselmanagement bei BAC ist unzureichend. Der Schlüssel für den Zugang zum RFID-Chip ist auf dem Pass selbst gespeichert und kann maschinell sowie von Personen gelesen werden. Dies bedeutet, dass jeder, der berechtigt oder unberechtigt den ePass in den Zugriff bekommt, den Schlüssel kopieren, speichern und für den Zugriff auf die Daten im RFID-Chip nutzen kann.
- Die Kommunikation zwischen Leser und RFID-Chip kann abgehört und BAC mittels so genannter „Brute-Force-Attacken“ unter Nutzung bekannter kryptografischer Schwächen gehackt werden.[10]
- RFID-Chips in MRTDs konnten bereits kopiert (geklont) werden.[11]
- Die Lesbarkeit der RFID-Chips in Pässen aus der Entfernung könnte genutzt werden, um z.B. personenspezifisch Bomben auszulösen.

Die Kombination dieser Lücken und konzeptionellen Schwächen gefährdet Sicherheit und personenbezogene Daten europäischer Bürger erheblich. Dies gilt insbesondere unter dem Gesichtspunkt, dass die ePässe weltweit und über einen langen Zeitraum (Gültigkeit bis zu 10 Jahren) eingesetzt werden.

Empfehlungen für die Verantwortlichen in Europa

Basierend auf diesen Ergebnissen empfehlen wir Verantwortlichen in Politik, Verwaltung, Forschung und Wirtschaft:

1. Da der Reisepass mit seinen inhärenten Schwächen bereits eingeführt wurde und unweigerlich weiter benutzt werden wird, schlagen wir zur Minderung der Risiken von

---

[6] Verfügbar unter www.fidis.net/fidis-del/period-2-20052006/#c961
[7] Protection Profile BSI-PP-0016-2005 und BSI-PP-0017-2005, verfügbar via www.bsi.de/zertifiz/zert/report.htm
[8] Angekündigt unter www.bsi.bund.de/fachthem/epass/eac.htm
[9] Extended Access Control (EAC) z.B. wird nur auf bestimmte als besonders schutzwürdig eingestufte Informationen im ePass, etwa den Fingerabdruck, angewandt. Andere personenbezogene Daten wie auch das digitale, für biometrische Authentisierung optimierte Foto, Name, Geburtsdatum etc. werden dadurch nicht geschützt. Die Verwendung von EAC kann international nicht durchgesetzt werden, da EAC kein ICAO-Standard ist. In nichteuropäischen Ländern wird BAC mit seinem sehr viel geringeren technischen Sicherheitsstandard also weiter Verwendung finden.
[10] Die Schlüssellänge von BAC kann in bestimmten Fällen, etwa wenn die Passnummer vom Ausstellungsdatum abhängt, was beim niederländischen und deutschen Pass der Fall ist, auf 35 oder gar 28 Bit sinken. [Referenz: Beel, J., Gipp, B., ePass - der neue biometrische Reisepass, Shaker Verlag, Aachen 2005. Download des Kap. 6 "Fazit": www.beel.org/epass/epass-kapitel6-fazit.pdf]
[11] Siehe z.B. www.wired.com/news/technology/1,71521-0.html

Sicherheitsmängeln und Identitätsdiebstahl die folgenden Maßnahmen zur sofortigen Umsetzung vor. Diese Empfehlungen enthalten auf Szenarien basierende Verfahren und technische Ansätze, die Entwicklungen und Übereinkünfte auf internationaler Ebene (d.h. ICAO) erfordern:

a. Organisatorische Einhaltung und Durchsetzung des Zweckbindungsgrundsatzes für biometrische Daten in MRTDs (bei denen der definierte Zweck die Authentifizierung international Reisender ist). Der Einsatz von MRTDs darf nicht auf Authentifizierung im privaten Sektor ausdehnbar sein.

b. Bürger müssen über die bestehenden Risiken bei der Benutzung von MRTDs und mögliche von ihnen zu treffende Vorbeugungsmaßnahmen informiert werden (z.B. Vermeidung der Weitergabe der Dokumente an private Organisationen wie Hotels etc.).

c. Verfügbare, aber derzeit noch nicht genutzte Sicherheitsmaßnahmen wie der Faraday'sche Käfig müssen von den europäischen Mitgliedsstaaten bei den derzeitigen MRTDs sofort integriert werden.

d. Organisatorische Maßnahmen sind erforderlich, um für das Versagen von biometrischer Authentifizierung durch Biometrie-inhärente Probleme einer fehlerhaften Nichterkennung (FRR) oder des Nichtfunktionierens bei bestimmten Personen Vorsorge zu treffen.

e. Es müssen bessere organisatorische und technische Maßnahmen getroffen werden, um den Missbrauch von Daten von MRTDs (insbesondere der biometrischen Daten) zu verhindern.

f. Es müssen organisatorische und technische Maßnahmen für den Fall eintretenden Identitätsdiebstahls durch Daten von MRTDs oder ganze MRTDs getroffen werden.

2. Mittelfristig (innerhalb der nächsten drei Jahre) ist die Entwicklung und Kommunikation eines neuen, überzeugenden und integrierten Sicherheitskonzepts für MRTDs und damit in Zusammenhang stehende Systeme erforderlich. Dies sollte insbesondere berücksichtigen:

   a. Geeignete Definition der Schutzbedarfe bzw. des Sicherheitsniveaus.

   b. Schutz personenbezogener Daten der europäischen Bürger (einschließlich biometrischer Daten, sofern diese denn noch verwendet werden).

   c. Berücksichtigung mehrseitiger technischer und organisatorischer Sicherheitsaspekte der Einführung von MRTDs, die die Belange unterschiedlicher Betreiber in unterschiedlichen Ländern und der MRTD-Nutzer berücksichtigen. (Zum Beispiel muss in diesem Kontext die Frage beantwortet werden: Wie kann der Missbrauch personenbezogener Daten im Ausland verhindert werden?)

   d. Risiken, die sich aus der Kombination unterschiedlicher Technik, die im MRTD-Bereich eingesetzt wird, ergeben, z.B. Biometrie, RFID und Sicherheitsmerkmale traditioneller Papierdokumente, müssen Berücksichtigung finden.

   e. Basierend auf der Definition des Sicherheitsniveaus und einer Risikoanalyse sollten die gesamten technischen Lösungen, die gegenwärtig bei MRTDs eingesetzt werden, neu konzipiert und neu evaluiert werden. Dabei ist zu überdenken, ob die derzeitig eingesetzte Technik, insbesondere RFID und Biometrie, wirklich benötigt wird oder ob nicht datenschutzfreundlichere Technik (wie z.B. kontaktgebundene Chipkarten statt kontaktloser Mechanismen) hinreichend ist. Möglichkeiten, wie die Umsetzung der gewählten Technik unter Datenschutz- und IT-Sicherheitsgesichtspunkten weiter optimiert werden kann (z.B. bei Biometrie durch Einsatz von on-card matching und on-card Sensoren), sind ebenfalls zu untersuchen.

   f. Auf europäischer Ebene sollte das resultierende Konzept von Datenschutz- und Datensicherheitsexperten öffentlich diskutiert werden.

3. Die entwickelten technischen und organisatorischen Maßnahmen sind zu standardisieren (ICAO), in eine neue Generation von MRTDs zu implementieren und weltweit zu auditieren.