Budapestdeklarationen över maskinläsbara resehandlingar (Machine Readable Travel Documents (MRTD))

Sammanfattning

Genom att inte implementera en passande säkerhetsarkitektur har, i princip, de europeiska staterna tvingat sina medborgare att använda nya internationella maskinläsbara resehandlingar (MRTDs) som dramatiskt minskar deras säkerhet och personliga integritet och ökar risken för identitetsstöld. Med andra ord, den nuvarande implementationen av det nya europeiska passet använder teknologier och standarder som inte är helt lämpade för sitt syfte. Med denna deklaration, skapad vid ett arbetsmöte i Budapest i September 2006, presenterar forskare från FIDIS[1], ett europeiskt så kallat ”Network of Excellence” för frågor inom elektronisk identitetshantering, sin utvärdering av MRTDs och sina rekommendationer för vilka förbättringar som så väl industri som myndigheter bör genomföra.

Inledning

Maskinläsbara resehandlingar adderar ett antal nya hot och är samtidigt som de traditionella riskerna associerade med ID-handlingar fortfarande finns kvar.

- Tvärtemot traditionella ID-dokument kan data lagrat i ett MRTD fjäravläsas eller avlyssnas på ett för passägaren osynligt och icke-interaktivt sätt på ett avstånd av upp till 10 meter[2]. Detta faktum förvärras av att den åtkomstkontroll som används är möjlig att kringgå eller ”hacka” vilket kan leda till en generell och icke observerbar accessrätt till data lagrat i MRTDs både för auktoriserade och icke-auktoriserade utomstående. Detta i sin tur gör det möjligt att spåra och övervaka personer med pass, till exempel när de besöker främmande länder.
- Biometrisk data som lagrats i ID-handlingar kan användas av såväl publika som privata intressen för andra ändamål än de avsedda och bryter därmed med europeiska principer för personlig integritet. Eftersom biometri i sig självt är baserat på sannolikheter är möjligheten för felaktig ID-verifiering ofrånkomlig och kommer potentiellt att påverka många Europeiska medborgare dagligen.

Implementationen av det Europeiska passet (epass) som ett internationellt MRTD startade under 2005 och är baserat på en internationell teknisk standard från ICAO[3] beskriven i dokument 9303[4] och i enlighet med EU förordningen EC 2252/2004[5]. Denna deklaration bygger på en analys av de legala grunderna för MRTD samt den använda tekniken och det sätt på vilken dataskydd och säkerhet har

---

1 FIDIS - “Future of Identity in the Information Society”. Se http://www.fidis.net

2 ISO 14443 den typ av chips som används i MRTDs är optimerade för att fungera tillsammans med respektive avläsningsutrustning inom en area på 10 till 15 cm. Men avlysning av konversationen mellan denna typ a pass är möjliga på längre avstånd (2-10 m) (se 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) och har nyligen demonstrerats av Robroch på ett Nederländskt pass (se Robroch, H., ePassport Privacy Attack, 2006, www.riscure.com/2_news/200604%20CardsAsiaSing%20ePassport%20Privacy.pdf), han listar också avstånd för läsning och avlysning.
Vissa MRTDs omslag är utrustade med avskärmningsmöjligheter, t.ex., Är US pass utrustade med en metallväv inbäddad i omslaget. Men, Mahaffey och Hering har visat att om bara passet öppnar sig en halv inch – något som är fullt möjligt I en handväska eller en ryggsäck- så kan det avslöja sig självt för en läsare som befinner sig åtminstone två fot bort. (se www.flexilis.com/epassport.php).

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

4 Information tillgänglig via www.icao.int/MRTD/Home/Index.cfm

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

implementerats. Analysen har gjorts av FIDIS och finns dokumenterad i FIDIS rapport D3.6 ”Study on ID Documents”[6]. Dessutom har följande material används för denna deklaration:

- P Protection Profiles for Biometric Verification Mechanisms and MRTDs including Basic Access Control (BAC)[7] certified certifierad av deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Technical Guideline V1.0 for Extended Access Control (EAC) utgiven av deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) i augusti 2006[8].

Sammanfattning av gjorda observationer

Inget sammanhängande och integrerat säkerhets koncept för MRTD har presenterats varken för allmänheten eller för intresserade experter. De publikt tillgängliga dokumenten så som skyddsprofiler och tekniska riktlinjer täcker endast delar av ett sådant säkerhetskoncept[9]. BAC presenterades ursprungligen som en effektiv lösning för åtkomstkontroll och senare har EAC presenterats som en förbättrad version. Båda är emellertid otillräckliga (som dataåtkomstskydd för användaren) i många situationer.[10]

Ett antal teoretiska och vetenskapligt demonstrerade hot och konceptuella svagheter för MRTD har redan publicerats. Dessa adresseras inte ännu av säkerhetsprofiler, riktlinjer, standarder eller existerande implementationer. De mest framträdande hoten och svagheterna är:

- Biometri-information i MRTD kan inte återkallas och eftersom biometriska egenskaper hos användaren så som fingeravtryck och utseende är svåra att ändra kan ”stulen” biometri missbrukas under en lång tidsperiod.
- Nyckelhanteringen i BAC är otillräcklig: Nyckeln för att få tillgång till data som lagras på RFID - etiketten är lagrat i passet och kan läsas av så väl manuellt som maskinellt. Detta innebär att någon som har haft fysisk tillgång till passet kan kopiera nyckeln och senare använda den för att få tillgång till informationen på RFID-etiketten.
- Kommunikationen mellan RFID-etiketten och avläsaren kan avlyssnas och BAC kan knäckas genom att använda en så kallad ”Brute-Force-Attack” och kända kryptografiska svagheter.[11]
- Det är möjligt att klona RFID etiketterna i MRTDs.[12]
- Möjligheten att fjäravläsa RFID etiketter i pass kan missbrukas för till exempel personkänsliga utlösningsmekanismer för ”smarta bomber”.

---

[6] Tillgänglig via www.fidis.net/fidis-del/period-2-20052006/#c961
[7] Protection Profile BSI-PP-0016-2005 and BSI-PP-0017-2005, tillgänglig via www.bsi.de/zertifiz/zert/report.htm
[8] Tillkännagiven på www.bsi.bund.de/fachthem/epass/eac.htm
[9] Till exempel, Skyddsprofilerna (Protection Profiles) är endast riktlinjer för säkerhetsåtgärder med avseende på definierade produkter (tekniska komponenter) i ett MRTD kontext, I vilken omfattning de implementerats eller vilken kvalitet de har i existerande MRTDs så som epasset är inte beskrivet i texten. Dokumentation av existerande epass med avseende på implementationen av dessa skyddsprofiler verkar, I dagsläget, inte vara publikt tillgänglig. Existerande tekniska riktlinjer t.ex. riktlinjerna för Extended Access Control (EAC) täcker också endast delar av den tekniska säkerheten.
[10] Extended Access Control (EAC) kommer t.ex. endast att användas på valda element av den personliga data som lagras på epasset (särskilt data som kategoriseras som speciellt känslig så som biometrisk fingeravtrycksinformation), medan data så som det digitala fotot och andra personliga data som namn, födelsedatum etc. inte täcks. Krav på internationellt användandet av EAC är inte möjligt eftersom EAC inte är en internationell standard accepterad av ICAO. Detta betyder att endast BAC med en signifikant lägre säkerhetsnivå kommer att användas i icke-europeiska länder.
[11] Nyckelns effektiva styrka kan sjunka till 35 eller till och med 28 bitar om t.ex. passnummeret är beroende av annan data i passet (vilket är fallet I t.ex. Nederländerna och Tyskland). (Se Beel, J., Gipp, B., ePass - der neue biometrische Reisepass, Shaker Verlag, Aachen 2005. Download of chapter 6 "Fazit": www.beel.org/epass/epass-kapitel6-fazit.pdf).
[12] Se t.ex. www.wired.com/news/technology/1,71521-0.html

Kombinationen av dessa hot och svagheter hotar säkerheten och den personliga integriteten för europeiska medborgare på ett signifikant sätt. Speciellt när man betraktar den geografiska spridda användningen och den långa livstiden (up till 10 år) hos dagens MRTDs.

Rekommendationer för intressenter i Europa

Vi har utvecklat ett antal rekommendationer för europeiska intressenter (politiker, näringsliv och forskare) inom MRTD området baserade på våra fynd.

1. Eftersom MRTDs med inneboende svagheter redan har introducerats och ofrånkomligen kommer att användas i framtiden rekommenderar vi att följande åtgärder omedelbart vidtas för att minska risken för säkerhetsluckor och identitetsstöld. Rekommendationerna innehåller scenariobaserade procedurer och tekniska ansatser som kräver överenskommelser och utvecklingsarbete på en internationell nivå (d.v.s. ICAO):
    a. Organisatoriskt införande och övervakning av syftesbindningprincipen. Speciellt för biometri som används i MRTD (där syftet är ID-verifiering av internationella resenärer). Användningen av MRTD bör inte utökas till att även omfatta ID-verifiering inom den privata sektorn.
    b. Medborgarna behöver informeras om de inneboende riskerna i att äga nya MRTD och de säkerhetsåtgärder de kan vidta (till exempel att undvika att lämna ifrån sig dokumenten till privata organisationer så som hotell).
    c. Tillgängliga men ännu inte införda säkerhetsåtgärder så som Faraday-burar bör omedelbart integreras i dagens MRTD av de europeiska medlemsstaterna.
    d. Organisatoriska åtgärder behövs för att ta hand om de fall då biometrisk ID-verifiering misslyckas på grund av inneboende biometriska svagheter så som felaktigt avvisande (FRR) och fel vid upptagningen av biometrisk data.
    e. Organisatoriska och tekniska åtgärder behövs för att förhindra missbruk av personlig information från MRTDs.
    f. Organisatoriska och tekniska åtgärder behövs för att hantera identitetsstöld där information från MRTDs eller kompletta MRTDs används.
2. Ett nytt övertygande och integrerat säkerhetskoncept som täcker MRTDs och angränsande system behöver utvecklas och presenteras i en nära framtid (inom de närmsta tre åren). Specifikt måste följande punkter adresseras:
    a. En definition av nödvändiga säkerhetsnivåer.
    b. Skydd av europeiska medborgares personliga data (inklusive biometri om det fortfarande används).
    c. Multilaterala tekniska och organisatoriska säkerhetsaspekter i samband med införandet av MRTD med hänsyn till olika operatörer i olika länder och med hänsyn till MRTD användaren. (Exempelfråga: Hur kan vi förhindra att aktörer i främmande länder missbrukar personliga data?).
    d. Risker och hot stammande från kombinationen av de olika tekniker som används inom MRTD så som RFID, biometri och säkerhetsåtgärder för pappersbaserade dokument.
    e. En komplett omvärdering och rekonstruktion av de tekniska lösningarna som används i dagens MRTD bör göras baserad på de definierade säkerhetsnivåerna och riskanalyser, speciellt vad gäller RFID och biometri. Man bör överväga om dessa teknologier verkligen är nödvändiga eller om teknologier som är säkrare och mer

integritetsbevarande (så som smartcards som kräver galvanisk kontakt i ställer för ”kontaktlösa” mekanismer) är tillräckliga. Förbättringsmöjligheter för använda tekniker bör också undersökas (t.ex ”on-card” matchning och ”on-card sensors” för biometri).

f. Säkerhetskoncepten runt MRTD bör debatteras offentligt på en europeisk nivå av experter på säkerhet och personlig integritet.

3. De tekniska och organisatoriska åtgärderna som utvecklas måste standardiseras (ICAO), införas i nästa generation av MRTDs och utsättas för en världsomspännande granskning.