C. Bezpečnost elektronických pasů

Zdeněk Říha, Masarykova Univerzita a JRC EC Ispra, (zriha@fi.muni.cz)

O nově zaváděných elektronických pasech můžeme slýchat jak ujišťování úřadů, že jsou zcela bezpečné, tak i výroky tzv. hackerů o řadě proveditelných nebo i provedených útoků. Problémy nejčastěji souvisí s detekovatelností pasu (například odpálení bomby) nebo čitelností dat z pasu (a s tím souvisejícím klonováním pasů). Pojďme se v tomto článku podívat na problematiku bezpečnosti elektronických pasů podrobněji. Hned na úvod ale uvedu, že řada útoků na pasy je známa již delší dobu a státy se rozhodly elektronické pasy zavést, neboť rizika s nimi spojená považují za akceptovatelná. To platí například pro útoky klonováním dat, které jsou popsány již v dokumentaci organizace, které je standardizací elektronických pasů pověřena. Přesto byla možnost klonování dat prezentována řadou periodik téměř jako revoluční novinka.

Technologie

Standardizaci pasů na celosvětové úrovni má na starost Mezinárodní organizace pro civilní letectví (ICAO), což je část OSN. Tato organizace vydává (v současné době již v šestém vydání) standard číslo 9303, který popisuje, jak má pas vypadat. Nedávno byly standardizovány i elektronické pasy (samotné vydávání elektronických pasů je však na celosvětové úrovni zatím zcela dobrovolné). Řada vlastností elektronických pasů je volitelných, někdy je možná volba z několika variant. Evropská Unie, která nařizuje členským zemím vydávat elektronické pasy nejpozději od 28. srpna 2006, dále upřesnila některé parametry těchto elektronických pasů vydávaných svými členskými zeměmi.

Elektronický pas se od pasu tradičního liší integrovaným bezkontaktním čipem a logem elektronického pasu na obalu. Čip s anténou bývá nejčastěji vložen buď do vnějších desek pasu nebo do stránky s datovými údaji, která z tohoto důvodu bývá zesílena. U českých pasů je čip vložen do stránky s datovými údaji, která bude přesunuta z posledního listu na začátek pasu a bude tvořena polykarbonátovou vrstvou, do které bude zalit čip a do níž bude také laserem gravitována černobílá fotografie držitele pasu. Čip v pase je bezkontaktní čipová karta splňující ISO 14443 (povolené jsou oba typy – A i B). Tato technologie je schopna přenášet data na vzdálenost 0-10 cm a umožňuje využití relativně komplexních kryptografických čipových karet s paměťovou kapacitou desítek kB. Tím se liší od jiných RFID technologií, které sice komunikují na delší vzdálenosti, neumožňují však o moc složitější operace než pouhé vyslání identifikačního čísla. Na vyšší úrovni se komunikuje klasickým protokolem čipových karet podle ISO 7816-4 (tj. SELECT AID, SELECT FILE a READ BINARY).

Data v elektronickém pase jsou soubory (v terminologii čipových karet elementární soubory) v jednom adresáři (v terminologii čipových karet dedikovaném souboru). Datových souborů je maximálně 16, jsou nazývány DG1 až DG16 (DG jako Data Group – datová skupina). DG1 obsahuje data ze strojově čitelné zóny (tj. jméno, příjmení, číslo dokumentu, vydávající stát, pohlaví, datum narození, datum vypršení platnosti a volitelná data, která v českém případě obsahují rodné číslo), DG2 obsahuje fotografii držitele pasu (ve formátu JPG nebo JPG2000 plus nějaká metadata). DG3 je určena pro otisky prsů, DG4 může obsahovat oční duhovku. Další datové skupiny obsahují dodatečné údaje o držiteli, vydávající instituci nebo pase. Kromě datových skupin obsahuje pas ještě dva soubory s metadaty. Soubor EF.COM obsahuje seznam přítomných datových skupin (plus údaje o použitých verzích) a EF:SOD

digitální podpis dat. Soubory EF.COM, EF.SOD, DG1 a DG2 jsou povinné pro všechny elektronické pasy. V Evropě bude nejpozději od 28. června 2009 povinně ukládána ještě datová skupina DG3. Všechny ostatní datové skupiny jsou volitelné.

Přístup k datům

V základní verzi nejsou data v elektronických pasech z hlediska důvěrnosti nijak chráněna. Na nižší úrovni (ISO 14443) získáme seznam dostupných čipů, jeden z nich vybereme jako aktivní a s tím komunikujeme. Data z pasu získáme výše uvedenými příkazy (SELECT FILE, READ BINARY) bez autentizace. Komunikace není nijak šifrována, takže možný je i odposlech probíhající komunikace.

Takové pasy však vyvolávají řadu debat. Jedním z možných vylepšení je stínění pasu (jeho zabalení do kovového obalu, např. do hliníkového přebalu). Stínění pasu využívají například americké pasy. Takto je možné zabránit nevědomé komunikaci s čipem (např. v kapse). Stínění ale nezabrání odposlechu, jakmile je pas otevřen a komunikace legitimně probíhá. Stínění navíc ztěžuje legitimní komunikaci a při mírném otevření pasu již není účinné.

Jinou možností obrany vůči neautorizovanému čtení je autentizace čtečky[1] a následná šifrovaná komunikace. To poskytuje obranu také vůči odposlechu přenášených dat. Vyřešit je však potřeba skutečnost, že pas musí být čitelný pohraničníky všech zemí světa. Autentizační údaje jim tedy musí být nějak přístupné. Řešení se našlo takové, že autentizační údaje jsou získány hašováním určitých údajů ve strojově čitelné zóně. Takto může přistupovat k datům v pase kdokoliv, kdo otevře pas na stránce s datovými údaji. Předpokládá se tedy, že kdokoliv, kdo má pas v ruce a může v něm číst data, má přístup i k údajům na čipu. Řeší se tak přístup k datům v zavřeném pase v kapse neznámého člověka, ale přístup k datům není omezen pouze na pohraničníky, ale číst data mohou například i hoteliéři apod. Tento způsob ochrany dat v pasech se nazývá základní řízení přístupu (basic access control – BAC) a celosvětově je volitelným ochranným prvkem. Pasy členských zemí EU však musí BAC implementovat povinně. Tedy i české pasy jsou chráněny pomocí BAC.

Základní řízení přístupu brání jak neautorizovanému čtení, tak odposlechu, nevýhodou však je malá entropie dat, ze kterých se odvozují autentizační údaje (viz dále). Základní řízení přístupu také nemůže zabránit detekovatelnosti čipu.

Pokud není čip stíněn, je možné jej detekovat. Nižší komunikační vrstvy podle ISO 14443 nám umožňují získat minimálně identifikátor čipu. Identifikátor čipu je buď náhodně vygenerován při každém resetu (u všech čipů typu B a u některých čipů typy A) nebo fixní po celou dobu života čipu (u některých čipů typu A). V případě fixních identifikátorů je možné sledovat čip (např. jeho pohyb) i v případech, kdy nejsme schopni z čipu získat další data. Identifikátor může prozradit i nějaké další údaje o čipu, příkladem může být samotná délka identifikátoru, ta totiž není jednotná (standard umožňuje několik variant (4, 7 nebo 10 bajtů), ty jsou však u výrobců různě oblíbené).

[1] Nejedná se o klasickou autentizaci čtečky, protože autentizační data nejsou tajná. Jedná se spíše jen o informaci, že čtečka zná určité informace vytištěné v pase. To by mělo prokázat možnost fyzického přístupu k pasu.

Integrita dat a autenticita čipu

Integrita dat je zajištěna digitálním podpisem dat. Digitální podpis je umístěn v souboru EF.SOD a jedná se o klasickou CMS strukturu typu SignedData. Hierarchie PKI je jednoúrovňová. Každý stát má svoji CA (tzv. CSCA – Country Signing CA), která vydává certifikáty složkám, které vydávají pasy (řekněme krajům, to záleží na rozhodnutí každé země) – jedná se o tzv. podepisovače dokumentů (Document Signers). Samotná data v pase jsou podepsána těmito podepisovači dokumentů.

Pro ověření podpisu musíme mít certifikát CVCA příslušné země, ten musíme získat důvěryhodnou cestou od dané země a certifikát konkrétního podepisovače dokumentů, ten se buď nachází přímo v pase (v části certifikátů struktury SignedData) a to je doporučený postup nebo jej musíme získat přímo od dané země podobně jako certifikát CSCA.

Podepsaná data tvoří speciální strukturu obsahující haše všech přítomných DG souborů v pase. Tímto způsobem je možné ověřit integritu každého souboru samostatně (tj. ověříme digitální podpis souboru EF.SOD a na základě zde uvedených hašů kontrolujeme integritu jednotlivých souborů).

Podpisové mechanismy použitelné v elektronických pasech jsou RSA (ve variantách RSASSA-PSS a RSASSA-PKCS1_v15, viz RFC 3447), DSA (viz FIPS 186-2, díky krátkým klíčům nyní nepoužitelné, čeká se na standardizaci algoritmu pro delší klíče) a ECDSA (viz X.62). Použitelné hašovací funkce jsou SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512.

Digitální podpis dat v pase je jedním z klíčových bezpečnostních prvků elektronických pasů, ne-li přímo ten nejdůležitější. Při podepisování dat si země může vybrat podpisové schéma, které jí vyhovuje z hlediska implementace (všechny komponenty však musí používat jen jediné schéma). Při ověřování podpisu je pochopitelně nutné podporovat všechny varianty. Ověřování podpisu je relativně bezproblémová věc, komplikacemi může být velké množství algoritmů, které je třeba implementovat, získávání správných kořenových certifikátů (CSCA) všech zemí (ICAO plánuje adresářové služby pro tento účel), CRL (země musí vydávat minimálně jednou za 90 dnů) a datové skupiny, u nichž jsou možné legitimní změny (typicky DG16 obsahující adresy příbuzných pro případ informování o nehodě držitele) – takové datové skupiny se nepodepisují.

Je zřejmé, že digitální podpis nemůže zabránit vytváření identických kopií dat (včetně souboru EF.SOD s digitálním podpisem). Z toho důvodu není možné spoléhat pouze na data z čipu, ale je třeba při kontrole cestovního dokladu věnovat pozornost i klasickým ochranným mechanismům (bezpečnostní tisk, vodoznak apod.) a souladu vytištěných dat s daty uvedenými v čipu. Zabránit kopírování (klonování) dat však můžeme i za pomoci kryptografie a odolnosti vůči narušení. V takovém případě je v pase uložen asymetrický pár klíčů. Zatímco veřejný klíč je volně čitelný (uložen v DG15 a jako u každé jiné datové skupiny je jeho haš digitálně podepsán), soukromý klíč není z čipu získatelný a je pouze možné ověřit (pomoci algoritmu výzva-odpověď), zda jej má čip k dispozici. Tento postup se nazývá aktivní autentizace a je volitelným prvkem elektronických pasů. Ani EU nestanoví povinnost implementace AA. České pasy však AA implementují (například německé ne).

Dostupnost dat

Zničit čip je možné nejen neúmyslně (teprve praxe spolehlivě ukáže, zda čip opravdu vydrží 10 let platnosti pasu), ale také úmyslně. Čip je možné spolehlivě zničit například v mikrovlnné troubě, ta je však značně výkonná a může pas viditelně poškodit. Na Internetu existují návody, jak vyrobit zařízení, které má dostatečný výkon ke zničení čipu, ale zbytek pasu neponičí [4]. Elektronický pas s nefunkčním čipem by neměl být důvodem přímo k neplatnosti pasu, ale spíše jen signálem k důkladnější kontrole. Konkrétní postup v takovém případě je však věcí státu, který provádí kontrolu. Důvodem k záměrnému zničení čipu může být obava ze vzdálené čitelnosti dat nebo snaha podvodníka s ukradeným pasem o znemožnění využití dat z čipu (například k biometrické verifikaci). Znemožnit čtení dat z čipu je možné také rušením patřičného signálu čtečky.

Základní řízení přístupu (basic access control - BAC)

Základní řízení přístupu je mechanismus bránící čtení dat z čipu bez znalosti autentizačních klíčů. Tyto autentizační klíče jsou odvozeny z dat vytištěných ve strojově čitelné zóně. Konkrétně se jedná o číslo dokumentu, datum narození držitele a datum vypršení platnosti pasu. Všechny tyto údaje se nacházejí na druhém řádku čtecí zóny. Nebyly vybrány zcela náhodně, jsou to právě ty údaje, které obsahují kontrolní číslici (rozpoznání OCR znaků bývá chybové, z tohoto důvodu je preference polí s kontrolní číslici pochopitelná). Tyto tři údaje se v ASCII formě zřetězí (včetně příslušných kontrolních číslic) a hašují algoritmem SHA-1. Z tohoto haše se dalším hašováním odvodí (112 bitové 3DES) klíče pro šifrování a autentizaci MAC. Následně se příkazem GET CHALLENGE získá výzva od čipu a příkazem MUTUAL AUTHENTICATE se čtečka a čip vzájemně autentizují. Dojde k ustavení sdíleného klíče sezení a následná komunikace je zabezpečena Secure Messagingem.

Toto je klasická vzájemná autentizace, která je považována za bezpečnou, pokud jsou klíče tajné. V případě pasů nejde o tajnost klasickou, protože klíče jsou odvoditelné z dat napsaných v pase, nicméně i zde je vhodné zabránit náhodnému uhodnutí klíče. U pasů je však toto mírně problematické, protože data, ze kterých jsou klíče odvozeny, nemají příliš velkou entropii. Ačkoliv teoretické maximum je 58 bitů a v případě alfanumerického čísla dokumentu až 74 bitů, reálné hodnoty jsou o dost nižší. Pojďme se na jednotlivé položky podívat podrobněji:

- datum narození držitele: jeden rok mívá 365 až 366 dnů, teoretické maximum je 100 roků tj. asi 36524 dnů (15,16 bitu entropie). Reálně však můžeme věk držitele odhadnout s předností na 10 let (3652 dnů, 11,83 bitů entropie), často i přesněji.
- datum vypršení platnosti pasu: maximální délka platnosti pasu bývá 10 let (tedy podobně jako výše uvedených přibližně 3652 dnů, 11,83 bitů entropie). U dětí bývá platnost kratší (často 5 let). V nejbližší budoucnosti můžeme využít faktu, že elektronické pasy jsou vydávány jen krátkou dobu. První rok je entropie pod 8 bitů (pokud správně odhadneme, zda je platnost pasu 5 nebo 10 let).Využít je také možné skutečnosti, že pasy jsou vydávány jen v pracovní dny a datum vypršení platnosti přímo souvisí s datem vydání pasu (datum vypršení platnosti bývá určováno jako datum vydání plus X let platnosti). Pracovních dnů bývá v roce jen asi 2/3 kalendářních dnů.
- číslo dokumentu: na číslo dokumentu je ve čtecí zóně vyhrazeno 9 znaků. Pokud je číslo dokumentu kratší, doplní se znaky <, pokud je delší, patřičně se zkrátí. Pokud

číslo dokumentu uvažujeme pouze číselné (a znak <) získáváme 11^9 možností (31,13 bitu entropie), pokud je číslo alfanumerické, je možností až 37^9 (tedy 46,88 bitů entropie). Těchto hodnot bychom však dosáhli, jen pokud by čísla pasů byla zcela náhodná. A tak je tomu málokdy. Pokud však nevíme o číslování pasů dané země vůbec nic (a nebo ani netušíme, o jakou zemi se jedná), jsme v podobné situaci. Pokud však známe určité údaje o číslovacím plánu pasů dané země (nebo všechna platná čísla dokumentů), možností a tím entropie ubývá. Řada zemí čísluje své pasy sekvenčně. Známe-li datum vydání (nebo datum vypršení platnosti), možných čísel pasů není až tak moc. Například Česká republika vydává asi milion pasů ročně, známe-li rok vydání pasu a rozsah čísel pasů v tomto roce, zmenšuje se entropie na přibližně 20 bitů. Známe-li měsíc vydání a rozsah v tomto měsíci, je entropie asi 17 bitů. Podobně můžeme jít až k jednotlivým dnům. Takto detailně asi běžný člověk nebude znát číslování pasů, nicméně nejen insideři, ale například i hoteliéři mohou znát o číslování pasů dost (je možné, že dříve nebo později se podobné informace objeví například na Internetu). V praxi je odhad čísla pasů komplikován tím, že musíme nejprve odhadnout stát vydávající pas, případně ještě typ pasu, neboť různé typy pasů mohou být číslovány separátně.

- Každá z položek je ještě následována kontrolní číslicí. Algoritmus výpočtu kontrolní číslice je však veřejně znám, takže kontrolní číslice nepřináší žádnou novou informaci.

Abychom odhadli celkovou entropii dat můžeme entropii jednotlivých prvků sečíst. To je ovšem korektní jen v situaci, kdy jsou údaje zcela nezávislé. U data platnosti by se dalo diskutovat o tom, že si člověk požádá o doklad v 15 letech a pak jej pravidelně obnovuje. To je sice pravda u občanských průkazů, u pasů tomu tak ale asi moc nebude, takže tento vliv pravděpodobně můžeme zanedbat. Podobně bych neviděl souvislost mezi datem narození a číslem dokumentu. Mezi číslem dokumentu a datem vypršení platnosti však závislost typicky bude. Jen v případě zcela náhodných čísel dokumentů ne a pak můžeme entropii sčítat. U jiných číslovacích plánů už nějaká závislost bude a pak záleží kolik znalostí o tomto plánu máme. V případě značných znalostí může entropie čísla dokumentů značně klesnout. Teoreticky v případě sekvenčních čísel dokumentů, zemí o velikosti ČR, rovnoměrného vydávání pasů po celý rok a detailní znalosti čísel pasů vydávaných ten který den klesá entropie asi na 12 bitů. Celková entropie tak z teoretických 58/74 bitů klesá na přibližně 32 bitů.

Výpočtem entropie jsme se zabývali, abychom se nyní mohli věnovat možným útokům. Komunikace s elektronickým pasem začíná výběrem aplikace ePasu (SELECT AID), potom následuje autentizace a ustavení šifrovacího klíče. Autentizace začíná získáním 8bajtové výzvy z čipu (GET CHALLENGE) a pokračuje odesláním šifrované (a MAC kódem zajištěné) výzvy čtečky (obsahující také výzvu čipu). Pokud je MAC kód v pořádku (a výzva čipu je shodná), odpovídá čip podobně. Při autentizaci se používá statický šifrovací a MAC klíč, který je sdílený mezi čtečkou a čipem (tento je odvozený z dat ve strojově čitelné zóně). Na základě výzev je vypočítán klíč sezení (šifrovací a MAC). Všechny klíče jsou 112 bitové 3DES klíče (detaily viz ISO 7816 nebo [2], tam je příklad komunikace uveden od strany 47). Protože 112 bitů je příliš hodně na útok hrubou silou, můžeme s výhodou využít skutečnosti, že statické autentizační klíče jsou deterministicky odvozeny z informace v pase, která má mnohem menší entropii. Útok hrubou silou tedy můžeme provést s menším množstvím klíčů.

Typy útoků hrubou silou jsou v principu dva. Buďto odposlechneme úspěšnou komunikaci a tu se pak snažíme dešifrovat, nebo se snažíme úspěšně autentizovat vůči čipu a pak s ním komunikovat.

Výhodou odposlechu je možnost data si uložit a off-line je potom analyzovat. Pokud odposlechneme celou komunikaci, můžeme útokem získat všechna přenášená data. Nevýhodou je nesnadnost získání dat odposlechem existující komunikace (tj. komunikace musí probíhat a my ji musíme odposlechnout).

Nejprve získáme výzvu čipu, ta je přenášena nešifrovaně. Pak analyzujeme příkaz MUTUAL AUTHENTICATE zasílaný čtečkou čipu. Hrubou silou zkoušíme všechny smysluplné kombinace údajů ze strojově čitelné zóny, tyto hašujeme (dvakrát, viz detailní popis protokolu např. v [2]) abychom získali šifrovací klíč (MAC klíč nutně nepotřebujeme) a tímto zkoušíme dešifrovat datovou část příkazu a ověřujeme, zda se dešifrovaná výzva čipu (9.-16. bajt) shoduje s nešifrovaně poslanou výzvou (na toto nám stačí dešifrovat bajty 9-16 a xorovat s bajty 1-8 šifry (jedná se o CBC mód)). Pokud se výzva neshoduje, pokračujeme v prohledávání stavového prostoru, pokud se výzva shoduje, můžeme ještě pro kontrolu vypočítat MAC klíč a ověřit MAC příkazu, dále dešifrujeme odpověď čipu, abychom získali všechny výzvy a mohli tak vypočítat klíč sezení, pomocí kterého můžeme dešifrovat následnou komunikaci. Pro každý testovaný klíč musíme provést dvakrát SHA-1 hašování a jednou 3DES dešifrování. Alternativní útok může počítat MAC klíče a kontrolovat, zda má APDU příkaz odpovídající MAC kód. Pro každý testovaný klíč pak musíme provést dvakrát SHA-1 hašování, čtyřikrát DES šifrování a jedno 3DES šifrování[2]. Takový útok není rychlejší, ale může být výhodný v situaci, kdy máme k dispozici pouze odposlechnutá data ze čtečky (odposlouchávat čtečku je podstatně jednodušší, než odposlouchávat odpověď karty). V takovém případě můžeme získat statické klíče pouze na základě odchycených dat ze čtečky, pro přečtení dat se však musíme vrátit k pasu a data přečíst (klíče již k dispozici máme).

Jeden výpočet klíče z autentizačních dat, dešifrování dat a porovnání výzvy trvá na běžném počítači asi 1 mikrosekundu. Procházení prostoru autentizačních dat o velikosti 2^{32} tak zabere něco přes hodinu. Marc Witteman ve svém příspěvku [5] ukázal možnost provedení takového útoku vůči holandským pasům. Ve svém útoku využil dodatečných informací o závislosti čísla dokumentu na datu expirace a znalosti kontrolní číslice.

Jak již bylo zmíněno, odposlech existující komunikace není snadný. Zamýšlený dosah zařízení splňujících ISO 14443 je 0-10 cm. To sice neznamená, že odposlech na delší vzdálenost není možný, při odposlechu však útočník brzy narazí na problém poměru šumu a signálu. Zatímco signál čtečky je silný a zachytitelný na delší vzdálenosti, při odposlechu dat z čipu (přenášených pomocí zátěžové modulace) se bojuje o každý centimetr.

On-line útok vůči čipu prochází stavový prostor stejně, jedno ověření autentizačních dat však trvá déle, protože jednak musíme komunikovat s čipovou kartou, jednak je potřeba vždy vypočítat také MAC klíč a kód. Jedno ověření trvá u běžné komerční čtečky řádově dvě desítky milisekund, útok tak je asi 10 000 x pomalejší než off-line útok.

---

[2] Děkuji Marcu Wittemanovi za diskusi v této oblasti.

Autorův pokus o program pro off-line i on-line útoky můžete najít na http://www.fi.muni.cz/~zriha/bac . Program není speciálně optimalizovaný, test jednoho klíče trvá skutečně asi jednu mikrosekundu, režie programu pro generování správných kombinací dat a výpočtu kontrolní číslice je však významně vyšší. U off-line útoků program neřeší odposlech dat a očekává odchycená data v souborech.

Aktivní autentizace

Cílem aktivní autentizace je ověřit, zda je čip v pase autentický. Pomocí protokolu výzva odpověď se ověřuje, zda pas má k dispozici správný soukromý klíč. Asymetrický pár klíčů pro aktivní autentizaci je specifický pro každý pas. Protokol výzva-odpověď je založený na ISO 9796-2. Čtečka generuje 8 bajtovou výzvu a tu posílá čipu s příkazem INTERNAL AUTHENTICATE. Čip generuje další náhodnou část a obě části hašuje. Svoji náhodnou část a haš (spolu s hlavičkou a patičkou) podepíše svým soukromým klíče. Výsledek posílá čtečce. Ta digitální podpis ověří. Za předpokladu odolnosti vůči narušení čipu, správnosti implementace, odolnosti vůči útoků postranními kanály apod. je výsledkem bezpečné ověření autenticity čipu.

V praxi je aktivní autentizace komplikována faktem, že ne všechny implementace v čipu se drží faktu, že odpověď má být vytvořena podle ISO 9796-2 schématu 1. Může se pak stát, že odpověď není správně interpretována a autentizace selže.

Zajímavý je i útok vůči soukromí, kdy výzva, která se posílá k pasu k podepsání, není zcela náhodná, ale má určitou sémantiku, například kóduje čas a místo. Pak může nějaká země uchovávat výzvy a odpovědi jako důkaz o tom, že se daný člověk nacházel v daném čase na určitém místě. V praxi však takový důkaz musí čelit faktu, že pas podepíše kdekoliv a kdykoliv jakoukoliv výzvu a vypovídací hodnota odpovědí je tedy malá. I tak je ale existence tohoto útoku důvodem proč Německo ve svých pasech aktivní autentizaci neimplementovalo.

Brzy si zřejmě uvědomíme, že spolu s pasem jsme vlastně dostali i výkonnou čipovou kartu. Využití pro digitální podepisování dokumentů je však viditelně nebezpečné, neboť pas podepisuje vše bez dodatečné autentizace např. PINem (nehledě na fakt, že použitý protokol výzva-odpověď není vhodným podpisovým schématem). Využití pro autentizaci uživatele např. při přihlašování k počítači však už může být podstatně zajímavější.

Závěr

Ukázali jsme si, že elektronické pasy jsou vybaveny bezpečným nosičem dat, obsahujícím údaje o držiteli a vydávající instituci. V základní verzi jsou data chráněna „jen“ digitálním podpisem, volitelně je však možné chránit přístup k datům, případně zajistit autenticitu čipu.

Bez účinného stínění čipu je možné i s dodatečnými ochrannými mechanismy detekovat existenci čipu. To může vést k řadě útoků, reálně však budete podstatně snadněji vysledovatelní díky vašemu mobilnímu telefonu.

Ačkoliv entropie dat využitých pro odvození klíče je značně nižší než délka výsledného klíče, jsou v praxi realizovatelné útoky omezeny nesnadností získání odposlechnutých dat u offline útoků a pomalostí komunikace u on-line útoků. Předpokládáme-li, že při pohraniční kontrole

je typicky držitel pasu vzdálen asi 50 cm od pohraničního úředníka a ostatní osoby asi další 1 metr a vezmeme-li v úvahu velikost současných odposlouchávacích zařízení, nemusí být odposlech dat nejsnazším útokem pro získání dat uložených v čipu. Při on-line útocích nemusí být náročné dostat se do dostatečné vzdálenosti od pasu (s využitím velké antény ukryté v kufru to může být až 40 i 50 cm [3]), problémem však je pomalá rychlost komunikace, což omezuje počet pokusů o autentizaci, které můžeme v rozumném čase provést.

Je dobré si také uvědomit, že BAC neomezuje přístup k datům těm subjektům, kteří z něj mohou přečíst údaje ze strojově čitelné zóny. Necháte-li tedy pas na recepci hotelu nebo jiné instituce, BAC vaše data neochrání. Na druhou stranu se v elektronické části pasu zatím nenachází moc jiných informací, než které jsou tam tak jak tak vytištěné. O možnostech zneužití digitálně podepsaných dat a kvalitních fotografií ke krádežím identit se však již spekuluje…

Aktivní autentizace je protokol ověřující autenticitu čipu. Možné útoky vůči němu mohou směřovat proti odolnosti pasu vůči narušení nebo využívat postranních kanálů.

Na závěr je možné konstatovat, že elektronická část elektronického pasu sice má svá slabá místa, ale zcela perfektní není žádná technologie. Navíc je třeba si uvědomit, že bezpečnost pasu nezáleží jen na elektronické části, ale také na částech ostatních (tiskové a jiné bezpečnostní techniky). Elektronický podpis dat zcela jistě zvyšuje bezpečnost těchto cestovních dokladů. Otázkou je, zda tato dodatečná bezpečnost stojí za nutné náklady na zavedení této technologie do praxe. Na takovou otázku mi však odpovídat nepřísluší.

A co otisky prstů?

Zmínil jsem, že nejpozději od 28. června 2009 se budou v EU do pasů ukládat i otisky prstů (DG3). Tyto však budou chráněny zcela jiných mechanismem. O tomto tzv. „rozšířeném řízení přístupu“ si povíme příště.

Poznámka

Názory, zde uvedené, jsou soukromé názory autora a nemohou být považovány za oficiální stanovisko Evropské komise.

Odkazy

[1] ICAO TAG MRTD/NTWG: Biometrics Deployment of Machine Readable Travel Documents, version 2.0. Včetně příloh A-J, http://www.icao.int/mrtd/download/technical.cfm
[2] ICAO TAG MRTD/NTWG: PKI for Machine Readable Travel Documents offering ICC read-only access v1.1, http://www.icao.int/mrtd/download/technical.cfm
[3] Kirschenbaum, I., Wool, A. How to Build a Low-Cost, Extended-Range RFID Skimmer, http://www.eng.tau.ac.il/~yash/kw-usenix06/index.html
[4] MiniMe (pseudonym), Mahajivana (pseudonym): RFID-Zapper, http://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)
[5] Witteman, M. Attacks on Digital Passports, WhatTheHack, http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf