M0170 Kryptografie

Bezpečnost elektronických pasů

Richard Nossek

Obsah

- Úvod
- Elektronické pasy
- Bezpečnostní mechanizmy
- Útoky
- Závěr

Úvod

- Problémů se starými pasy je několik
- Kontrola je pomalá a často dochází k chybám při přepisování údajů
- Jediná forma automatizace byla strojově čitelná zóna
  - Pouze 2 digitalizované řádky (88 znaků)
  - Bezpečnostní kód jedinným ochranným prvkem
- Použití pasu fyzicky podobnou osobou
  - Jednoduchý podvod
  - Obtížně detekovatelné

Úvod

- Padělky
  - Výroba padělků a modifikace pravých dokumentů je v současnosti obtížná
  - Mnoho ochranných prvků
- Řešení – elektronické pasy
  - Bezkontaktní čipové karty
  - Biometriky

Elektronické pasy

- Pasy vybavené bezkontaktním čipem
- Standard zpracován mezinárodní organizací pro civilní letectví (ICAO Doc 9303)
- Bezkontaktní čipové karty
  - Čip s anténou je integrován v papírovém obalu pasu
  - Několik desítek kB EEPROM paměti
  - Kryptografické koprocesory
  - Pasivní RFID zařízení (přenos dat pomocí elmag. pole)

Elektronické pasy

- Komunikace se čtecím zařízením na vzdálenost 0-10 cm (ISO 14443)
- Data jsou uložena jako soubory v jednom adresáři
- Označovány jako DG1 až DG16
  - DG1 obsahuje data ze strojově čitelné zóny
  - DG2 až DG4 obsahují biometrická data
  - DG5 a výše obsahují dodatečné údaje o držiteli, vydávající instituci a pase
- Dva soubory s metadaty

Elektronické pasy

- Biometrická data jsou uložena ve formátu JPEG nebo JPEG2000
  - Tvář držitele (povinné, DG2)
  - Otisky prstů (povinné od roku 2009, DG3)
  - Oční duhovka (volitelné, DG4)

Bezpečnostní mechanizmy

- Elektronický pas obsahuje několik povinných a volitelných bezpečnostních prvků
- Integritu dat zajišťuje digitální podpis - tzv. pasivní autentizace (PA)
  - Klasická CMS struktura
  - Obsahuje podepsané hashe všech DG souborů
  - Jednoúrovňová hierarchie PKI
  - Každý stát má svou certifikační autoritu
  - CA vydává certifikáty jednotlivým subjektům, které vydávají pasy

Bezpečnostní mechanizmy

- Pro ověření je potřeba CVCA certifikát příslušné země a certifikát subjektu (bývá v pase)
- Několik podpisových schémat
  - RSA
  - DSA
  - ECDSA
  - Hashovací funkce SHA-1 až SHA-512
- Jednotlivé země mají povinnost vydávat CRL minimálně každých 90 dnů

Bezpečnostní mechanizmy

- Pasivní autentizace nebraní vytvoření kopie dat
- Zabránit klonování dat lze použitím aktivní autentizace (AA)
  - Narozdíl od veřejného klíče (uložen v DG15), privátní klíč nelze z čipu získat
  - Algoritmem výzva-odpověď lze zjistit, zda čip má přístup k privátnímu klíči
- Algoritmus založen na ISO 9796-2
  - Čtečka generuje 8 bytovou výzvu

Bezpečnostní mechanizmy

- Algoritmus (pokr.)
  - Výzva je odeslána s příkazem INTERNAL AUTHENTICATE
  - Čip generuje druhou část, obě zahashuje
  - Podepíše svoji část a hash, odešle čtečce
- AA není povinnou součástí, mnoho zemí neimplementuje (USA, Japonsko, Německo, …)
- Komplikované rozdílnými implementacemi čipu
- Jestliže odpověď není dle ISO 9796-2 schématu 1, autentizace selže

Bezpečnostní mechanizmy

- Bezkontaktní čip nese riziko neautorizovaného čtení
- Čtečku je relativně jednoduche skrýt
- Na druhou stranu je nutné umožnit snadné čtení na hraničních přechodech
- Kompromis – základní řízení přístupu (BAC)
  - Ten kdo má přístup k údajům vytištěným uvnitř pasu, může číst i data z čipu
  - Povinné v zemích EU
- Data z pasu nelze číst bez autentizačních klíčů
- Klíče jsou odvozené z dat ve strojově čitelné zóně

Bezpečnostní mechanizmy

- Konkrétně jde o druhý řádek čtecí zóny
  - Číslo dokumentu, datum narození, datum konce platnosti pasu
  - Tyto údaje mají kontrolní čislici
- Údaje se zřetězí a výsledek se hashuje (SHA-1)
- Z výsledného haše se odvodí 112ti bitové 3DES klíče
- Při pokusu o čtení čtečka zašle příkaz GET CHALLENGE
- Následně proběhne vzájemná autentizace (příkaz MUTUAL AUTHENTICATE)

Bezpečnostní mechanizmy

- Rozšířené řízení přistupu (EAC) je v EU povinnou součástí od roku 2009
- Používá se spolu se základním řízením přístupu
- Chrání přístup k otiskům prstů a snímku duhovky
- Autentizuje se nejen čip, ale také čtečka
  - Autentizace čipu probíhá podobně jako u BAC
  - Bezpečnost ustanoveného kanálu je vyšší
- Čtečky se prokazují certifikátem (CVC)
  - Kratká platnost (1 den až 1 měsíc)

Bezpečnostní mechanizmy

- Nestopovatelné charakteristiky čipů
  - RFID čipy lze detekovat bez jakékoliv komunikace (antikolizní protokoly)
  - Čip odpovídá různými identifikačními čísly
- Stínění čipu
  - Brání neautorizovanému čtení
  - Tenká kovová síťka uvnitř obalu
  - Stíní čip když je pas zavřený
  - Používané v USA

Útoky

- Útoky na **základní řízení přístupu**
- Vzájemná autentizace je obvykle bezpečná
- BAC ovšem generuje klíče z dat, která mají relativně malou entropii
- Teoretická entropie je až 74 bitů pro pasy s alfanumericými čísly dokumentu
- Pro ostatní pasy je maximum 58 bitů
- Reálná entropie je značně nižší

Útoky

- Datum narození
  - Věk držitele je možné odhadnout s přesností na 10 let (3652 dnů = 11.8348 bitů entropie)
- Konec platnosti pasu
  - Platnost je pasu je obvykle 10 let (11.83 bitů entropie)
  - Elektronické pasy jsou vydávány něco přes pět let (10.9 bitů entropie)
  - Teoreticky lze dále snížit odebráním víkendů

Útoky

- Číslo dokumentu
  - Přesně 9 znaků (případně doplněno znaky <)
  - Pokud neznáme nic o číslování pasů dané země je entropie 31.13, resp. 46.88 bitů
  - Pasy jsou často číslovány sekvenčně
  - ČR vydá asi milion pasů ročně, známe-li rok vydání pasu a rozsah čísel pro daný rok entropie spadne ke 20 bitům
- Kontrolní číslice nepřináší žádnou novou informaci
- Celková entropie přes 40 bitů, lze ovšem dále snížit

Útoky

- Útok hrubou silou na klíčový prostor
- Online útok neefektivní
  - Zpomalován výpočty na straně čipu
  - 10-15 pokusů za sekundu
  - Projití celého prostoru klíčů by při entropii 40 bitů trvalo několik tisíc let
- Offline útok
  - Potřebujeme záznam úspěšné autentizace
  - Jsou potřeba dva výpočty SHA-1 a jedno dešifrování

Útoky

- Offline útok (pokr.)
  - Na průměrném PC lze výpočet provést za 1 mikrosekundu (cca milion pokusů za sekundu)
  - Projití klíčového prostoru:
    - Při entropii 50 bitů 30+ let
    - Při entropii 40 bitů 12.8 dne
    - Při entropii 35 bitů 9.5 hodiny
- Útok teoreticky proveditelný
- V praxi jen těžko
- Úspěšnost závislá na znalostech číslování pasů

Útoky

- Bylo provedeno několik úspěšných útoků na **aktivní autentizaci**
- AA má bránit kopírování obsahu čipu
- Čip a implementace RSA jsou nachýlné k útoku postraními kanály
  - Pomocí časové a odběrové analýzy lze získat privátní RSA klíč
- AA může rovněž sloužit k útoku na soukromí držitele pasu
- Pas podepíše po výzvě libovolná data

Útoky

- Místo náhodné výzvy lze pak pasu poslat například údaje o místě a času
- Tyto údaje by pak některé země mohli shromažďovat
- Malá vypovídající hodnota takto shromažďovaných informací
- Možnost tohoto útoku důvodem proč Německo aktivní autentizaci neimplementovalo
- Pasy bez aktivní autentizace je jednoduché zkopírovat

Útoky

- Vlastnosti RFID čipů mohou vést k útokům
- Různé implementace čipů mají různá chybová hlášení
- Na základě chybové hlášky je možné zjistit, kterým státem byl pas vydán (bez autentizace)
- Čip v pase je bez stínění snadno detekovatelný

Závěr

- Elektronické pasy jsou při správné implementaci všech bezpečnostních prvků relativně bezpečné
- Digitální podpis zvyšuje bezpečnost dokladu, představuje další překážku pro padělatele
- Přečtení obsahu schovaného pasu není pro útočníka jednoduché
  - Online útok je znemožněn malým výpočetním výkonem pasu
  - Offline útok je značně zkomplikován obtížností odposlechu komunikace

Závěr

- Útočník s fyzickým přístupem k pasu může číst data z čipu (s výjimkou citlivých biometrických dat)
- Ovšem nedozví se žádné užitečné informace
- Pas je těžší zneužít po krádeži
- Zneužitelnost ukradeného inspekčního systému je problém

Děkuji za pozornost!

Dotazy?

Zdroje

- Security and Privacy Issues in e-Passports, Ari Juels, David Monar, David Wagner
- Fingerprinting Passports, Henning Richter, Wojciech Mostowski, Erik Poll
- A Tracebility Attack Against e-Passports, Tom Chothia, Vitaliy Smirnov
- Biometric passport, Wikipedia
- Bezpečnost elektronických pasů, Zdeněk Říha – CryptoWorld 10/2006