Elektronický cestovní pas

Zdeněk Junek

Úvod do kryptologie

Fakulta jaderná a fyzikálně inženýrská

24. dubna 2014

Zabezpečení cestovního pasu

- Ochranné prvky proti padělkům

Zabezpečení cestovního pasu

- Ochranné prvky proti padělkům
- Identifikace držitele

Zabezpečení cestovního pasu

- Ochranné prvky proti padělkům
- Identifikace držitele
- Porovnání s databází (automaticky)

"Starý" pas

- Ochranné prvky

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV
  - Ochranný kovový proužek

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV
  - Ochranný kovový proužek
- Identifikace

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV
  - Ochranný kovový proužek
- Identifikace
  - Fotografie

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV
  - Ochranný kovový proužek
- Identifikace
  - Fotografie
- Automatizace

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV
  - Ochranný kovový proužek
- Identifikace
  - Fotografie
- Automatizace
  - Strojově čitelná zóna

"Starý" pas

- Ochranné prvky
  - Speciální papír a barvy
  - Vodoznak
  - Prvky viditelné pouze pod UV
  - Ochranný kovový proužek
- Identifikace
  - Fotografie
- Automatizace
  - Strojově čitelná zóna
  - 2 řádky s osobními údaji - 88 znaků

Elektronický pas

- Přidání čipu RFID

Elektronický pas

- Přidání čipu RFID
- Standardy udává ICAO

Elektronický pas

- Přidání čipu RFID
- Standardy udává ICAO
- V EU povinné od 28. 8. 2006, od 28. 6. 2009 i s otisky prstů

Čip RFID

- RFID čip (Radio Frequency Identification)

Čip RFID

- RFID čip (Radio Frequency Identification)
- Bezkontaktní (do cca 10 cm)

Čip RFID

- RFID čip (Radio Frequency Identification)
- Bezkontaktní (do cca 10 cm)
- Bez napájení

Čip RFID

- RFID čip (Radio Frequency Identification)
- Bezkontaktní (do cca 10 cm)
- Bez napájení
- Vnitřní paměť v desítkách kB, rychlé procesory (včetně kryptografických koprocesorů)

Čip RFID

- RFID čip (Radio Frequency Identification)
- Bezkontaktní (do cca 10 cm)
- Bez napájení
- Vnitřní paměť v desítkách kB, rychlé procesory (včetně kryptografických koprocesorů)
- Obsahuje osobní údaje, fotografii, novější i otisky prstů

Čip RFID

- RFID čip (Radio Frequency Identification)
- Bezkontaktní (do cca 10 cm)
- Bez napájení
- Vnitřní paměť v desítkách kB, rychlé procesory (včetně kryptografických koprocesorů)
- Obsahuje osobní údaje, fotografii, novější i otisky prstů
- Obsahuje soubor pro metadata, soubor se zabezpečením; ostatní soubory uloženy do DG, např. osobní údaje v DG1, v DG2-7 biometrické údaje, DG15 veřejný klíč pro aktivní autentizaci

Zabezpečení

- Digitální podpis

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí
  - Mají povinně všechny pasy

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí
  - Mají povinně všechny pasy

  $=>$ Nemožné vytvořit dokonalý padělek (díky soukromému klíči)- tzv. pasivní autentizace

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí
  - Mají povinně všechny pasy

  $=>$ Nemožné vytvořit dokonalý padělek (díky soukromému klíči)- tzv. pasivní autentizace
  - Nezabrání přesným kopiím (tzv. klonování)

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí
  - Mají povinně všechny pasy

  $=>$ Nemožné vytvořit dokonalý padělek (díky soukromému klíči)- tzv. pasivní autentizace
  - Nezabrání přesným kopiím (tzv. klonování)
  - Každý stát má vlastní certifikační agenturu, která podepisuje klíče vydávajících autorit - ty pak podepíší data v pasech

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí
  - Mají povinně všechny pasy

  $=>$ Nemožné vytvořit dokonalý padělek (díky soukromému klíči)- tzv. pasivní autentizace
  - Nezabrání přesným kopiím (tzv. klonování)
  - Každý stát má vlastní certifikační agenturu, která podepisuje klíče vydávajících autorit - ty pak podepíší data v pasech
  - U nás MV ČR $->$ Státní tiskárna cenin

Zabezpečení

- Digitální podpis
  - Digitálně podepsáno vydávající institucí
  - Mají povinně všechny pasy

  $=>$ Nemožné vytvořit dokonalý padělek (díky soukromému klíči)- tzv. pasivní autentizace
  - Nezabrání přesným kopiím (tzv. klonování)
  - Každý stát má vlastní certifikační agenturu, která podepisuje klíče vydávajících autorit - ty pak podepíší data v pasech
  - U nás MV ČR $->$ Státní tiskárna cenin
  - CRL - seznam odvolaných certifikátů - v případě prozrazení klíče je třeba CRL distribuovat do 2 dnů

Problémy

- Možnost detekování čipu

Problémy

- Možnost detekování čipu
- Bez přístupu k samotným datům je možné zjistit nějaké informace o čipu

Problémy

- Možnost detekování čipu
- Bez přístupu k samotným datům je možné zjistit nějaké informace o čipu
  - Např. číslo a typ čipu, výrobce - a tím většinou i vydávající stát $\Longrightarrow$ hrozba teror. útoku

Problémy

- Možnost detekování čipu
- Bez přístupu k samotným datům je možné zjistit nějaké informace o čipu
  - Např. číslo a typ čipu, výrobce - a tím většinou i vydávající stát $\Longrightarrow$ hrozba teror. útoku
  - Obrana: Faradayova klec

Přístup k datům

- Údaje nemusí být šifrované

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - *Basic Acces Control*

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - *Basic Acces Control*
  - K přístupu k datům je třeba přečíst některé údaje z pasu

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - *Basic Acces Control*
  - K přístupu k datům je třeba přečíst některé údaje z pasu
  - Číslo pasu + datum narození + doba expirace $->$ SHA 1 $->$ získání dvou 3DES klíčů $->$ ustanovení společného klíče pro zajištění bezpečné komunikace

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - *Basic Acces Control*
  - K přístupu k datům je třeba přečíst některé údaje z pasu
  - Číslo pasu + datum narození + doba expirace $->$ SHA 1 $->$ získání dvou 3DES klíčů $->$ ustanovení společného klíče pro zajištění bezpečné komunikace
  - Takto je komunikace chráněna i proti odposlechu

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - *Basic Acces Control*
  - K přístupu k datům je třeba přečíst některé údaje z pasu
  - Číslo pasu + datum narození + doba expirace $->$ SHA 1 $->$ získání dvou 3DES klíčů $->$ ustanovení společného klíče pro zajištění bezpečné komunikace
  - Takto je komunikace chráněna i proti odposlechu
  - Povinné v EU

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - Problémy

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - Problémy
  - Malé množství kombinací údajů - entropie max. 56 bitů

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - Problémy
  - Malé množství kombinací údajů - entropie max. 56 bitů
  - V praxi ale méně kvůli malé "náhodnosti" čísel pasu a odhadu data narození $->$ entropie cca 35 bitů - možnost off-line útoku

Přístup k datům

- Údaje nemusí být šifrované
- Problém, jak zamezit neautorizovanému čtení dat
- **BAC** - Problémy
  - Malé množství kombinací údajů - entropie max. 56 bitů
  - V praxi ale méně kvůli malé "náhodnosti" čísel pasu a odhadu data narození $->$ entropie cca 35 bitů - možnost off-line útoku
  - Řešením je větší náhodnost při číslování pasů
  - **EAC** - *Extended Acces Control*

Aktivní autentizace

- Digitální podpis nezabrání kompletnímu "naklonování" čipu

Aktivní autentizace

- Digitální podpis nezabrání kompletnímu "naklonování" čipu
- Používá se ještě tzv. aktivní autentizace

Aktivní autentizace

- Digitální podpis nezabrání kompletnímu "naklonování" čipu
- Používá se ještě tzv. aktivní autentizace
  - V čipu je uložen soukromý asymetrický klíč - nedá se přečíst, jen se dá zjistit, zdali v čipu existuje

Aktivní autentizace

- Digitální podpis nezabrání kompletnímu "naklonování" čipu
- Používá se ještě tzv. aktivní autentizace
  - V čipu je uložen soukromý asymetrický klíč - nedá se přečíst, jen se dá zjistit, zdali v čipu existuje
  - Součástí dat na čipu je veřejný klíč (digitálně podepsaný)

Aktivní autentizace

- Digitální podpis nezabrání kompletnímu "naklonování" čipu
- Používá se ještě tzv. aktivní autentizace
  - V čipu je uložen soukromý asymetrický klíč - nedá se přečíst, jen se dá zjistit, zdali v čipu existuje
  - Součástí dat na čipu je veřejný klíč (digitálně podepsaný)
  - Snímač přečte veřejný klíč a ověří, zdali má čip soukromý klíč odpovídající veřejnému klíči

Aktivní autentizace

- Digitální podpis nezabrání kompletnímu "naklonování" čipu
- Používá se ještě tzv. aktivní autentizace
  - V čipu je uložen soukromý asymetrický klíč - nedá se přečíst, jen se dá zjistit, zdali v čipu existuje
  - Součástí dat na čipu je veřejný klíč (digitálně podepsaný)
  - Snímač přečte veřejný klíč a ověří, zdali má čip soukromý klíč odpovídající veřejnému klíči
  - Nelze tedy vytvořit přesnou kopii čipu