Fingerprinting Passports

Henning Richter
Wojciech Mostowski*
Erik Poll

Digital Security Group
Radboud University Nijmegen

*supported by Sentinels (NWO, STW, and Ministry of Economic Affairs)

deVerdieping
Trouw
dinsdag 8 april 2008
66ste jaargang nr 19447
www.trouw.nl

• Legio criminele toepassingen

Na ov-chip nu ook lek in paspoort

De chip in het nieuwe Nederlandse paspoort en andere passen is 'lek'. Dieven kunnen snel zien of iemand een paspoort bij zich heeft en uit welk land hij komt.

Vincent Dekker

Moderne paspoorten in tassen of binnenzakken verraden draadloos hun aanwezigheid én uit welk land ze komen. Onderzoekers van de Radboud Universiteit in Nijmegen hebben een beveiligingslek ontdekt in de chip die de pas juist veiliger moet maken.

„We hebben op de universiteit studenten van tien nationaliteiten en bij allen kunnen we ongezien zeggen uit welk land hun pas komt", aldus Erik Poll, die samen met Wojciech Mostowski en Henning Richter het beveiligingsprobleem ontdekte. In ieder geval paspoorten uit Nederland, Australië, België, Duitsland en nog zes Europese landen zijn voortaan ongemerkt te traceren en te herkennen. Poll denkt dat dit voor bijna alle moderne paspoorten geldt.

Het lek is des te opmerkelijker omdat de chips voldoen aan de zwaarste eisen van de Icao, de luchtvaartorganisatie van de Verenigde Naties. De passen zijn voorzien van een beveiliging die de gegevens in de chip, zoals naam, adres en een foto van de houder, tegen ongeoorloofd uitlezen beschermen. Dat lukt, maar bij die beveiliging is een andere, simpele kwestie over het hoofd gezien.

Poll: „We hoeven alleen maar een foute code naar een paspoort te sturen. In de Icao-regels staat precies hoe een chip in het paspoort moet antwoorden op elke correcte vraag van een officieel leesapparaat, zoals bij de douane. Maar men is vergeten dat ook te regelen voor antwoorden op verkeerde vragen. In de praktijk blijkt dat elk land een eigen manier heeft bedacht om met foute codes om te gaan. Analyseer de foutmelding die je terugkrijgt na het bewust versturen van een verkeerde code en je weet uit welk land het paspoort komt."

Foutmeldingen verraden veel over de werking van computers en zijn al vaak gebruikt om systemen te kraken. Daar heeft de Icao echter niet genoeg bij stilgestaan, blijkt nu.

De chip in het paspoort werkt, net als die in bijvoorbeeld de gekraakte OV-chipkaart en toegangspasjes, met de draadloze rfid-technologie. Daardoor is een rfid-lezer van een paar tientjes genoeg om de paspoorten te herkennen. Om ze geschikt te maken om op afstanden van 25 centimeter te werken, in plaats van de standaard van enkele centimeters, hoeft er alleen maar een grotere antenne aan te worden gekoppeld.

Poll en zijn twee collega's zullen hun ontdekking volgende maand tijdens een congres over beveiliging demonstreren en er meer details over bekend maken. In hun artikel voor dat congres waarschuwen zij ervoor dat terroristen een 'paspoortbom' zouden kunnen maken die alleen afgaat als een paspoort uit een bepaald land langskomt.

Minder spectaculair maar mogelijk realistischer, zo schrijven zij, is de dief die eerst vaststelt of iemand een paspoort bij zich heeft, waar die zit (in jas, tas of broekzak) en of het een pas van de gewenste nationaliteit is, waarna een zeer gerichte beroving mogelijk wordt.

Olympische fakkeltocht wacht in San Francisco volgend protest

Na Londen ontaardde ook in Parijs de olympische fakkeltocht door Tibetprotesten in chaos. De volgende steden maken hun borst al nat.

Van onze redactie buitenland

De olympische vlam verliet gisteravond Parijs, op weg naar de volgende bestemming: San Francisco. Maar sommige officials beginnen zich vanwege alle Tibetprotesten af te vragen of de estafette wel door moet gaan.

De route van de vlam door Parijs werd gisteren ingekort. De protesten tegen het Chinese ingrijpen in Tibet veroorzaakten dermate veel chaos dat de fakkel liefst vijfmaal gedoofd moest worden – volgens de organisatoren één keer vanwege een defect en vier keer uit voorzorg. De olympische vlam bleef volgens hen wel permanent branden in een busje. Maar de chaos werd zo groot dat de route moest worden verlegd en een bezoek aan het Parijse stadhuis helemaal werd afgeblazen.

Rond tien uur vertrok het vliegtuig uit Parijs. In San Francisco stonden de volgende demonstranten al klaar om de Chinese omgang met Tibet aan de kaak te stellen. Gisteren klommen er alvast drie langs de kabels de Golden Gate Bridge omhoog, waarna ze een spandoek ontrolden met 'Bevrijd Tibet' erop. En presidentskandidate Hillary Clinton riep president Bush op de opening van de Spelen te boycotten vanwege Tibet.

De vlam is bezig aan een 137.000 kilometer lange tocht over de aardbol die in augustus in de Chinese hoofdstad Peking moet eindigen. Maar het aanpakken van betogers in Tibet vorige maand, heeft de schijnwerpers gezet op Pekings omgang met deze en andere mensenrechtenkwesties. Volgens Tibetaanse leiders zouden meer dan 150 mensen om het leven zijn gekomen, de Chinese overheid houdt het op twintig.

Voorzitter Jacques Rogge van het Internationaal Olympisch Comité (IOC), die lange tijd weinig commentaar wilde geven over de kwestie, riep gisteren China op de problemen rond de onrust in Tibet snel en vreedzaam op te lossen. „Wat ook de reden

Een ranger aan de voet van de Golden Gate bridge bij San Francisco. Drie activisten zijn langs de kabels van de brug omhoog geklommen en hebben een spandoek 'Bevrijd Tibet' opgehangen. De olympische vlam komt vandaag aan in San Francisco. Net als in Londen en Parijs zullen veel pro-Tibetbetogers de tocht van de vlam door de stad willen verstoren. FOTO AP

Wereldreis olympische vlam tot China

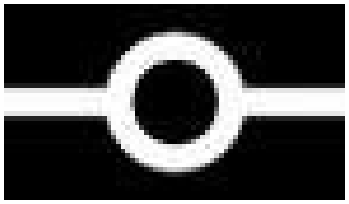
This talk

- e-passports
- passive and
  active attacks
- Basic Access Control
- fingerprinting
  passports

e-passports

- e-passport contains RFID chip / contactless smartcard
- chip stores digitally signed information:
  - initially just photos
  - later also fingerprints
- international standard by ICAO (International Civil Aviation Organization)

- chip much more advanced than MIFARE
  - no CRYPTO1, but RSA and 3DES

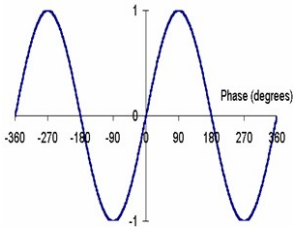


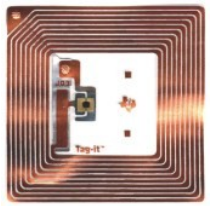
e-passport logo

Protocols & standards

ISO 14443

- defines physical communication for RFIDs





ISO 7816

- originally developed for contact smartcards
- defines byte format for commands & responses, in so-called APDUs

ICAO standard for e-passports

- defines specific ISO 7816 commands and responses for passports

passive vs active attacks on RFID

passive attacks

- eavesdropping on communication between passport & reader
- possible from several meters

active attacks

- unauthorised access to passport without owner's knowledge
- possible up to ≈25 cm
  - activating RFID tag requires powerful field!

- aka virtual pickpocketing
- variant: relay attack

active attack on Mifare Classic RFID application
(our university access cards)

Basic Access Control (BAC)

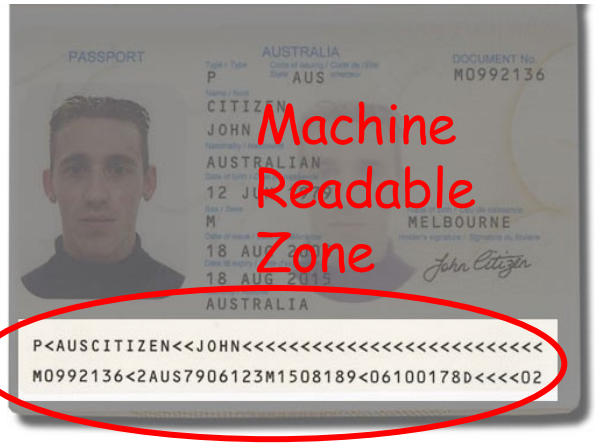
protects against unauthorised access and eavesdropping

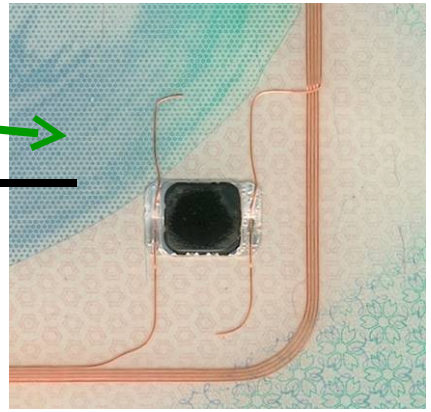
optically read MRZ

send MRZ

receive additional info

encrypted





Basic Access Control (BAC)

- Protects against
  - unauthorised access
    - access only after reading MRZ
  - eavesdropping
    - all communication encrypted

  using key printed in the passport (MRZ)
- Known problem
  - not enough entropy in random key to prevent brute force attack [Marc Witteman & Harko Robroch, 2006]
- We look at another issue
  - what can we find out *before* BAC?

Errors can leak information

```
An Error Has Occurred.
Error Message:
System.Data.OleDb.OleDbException: Syntax error
(missing operator) in query expression
'username ''' and password = 'g''.
System.Data.OleDb.OleDbCommand.ExecuteCommandTextE
   rrorHandling (Int32 hr) at
System.Data.OleDb.OleDbCommand.ExecuteCommandTextF
   orSingleResult (tagDBPARAMS dbParams, Object&
   executeResult) at
```

Fingerprinting passports

- All e-passports react the same to correct protocol runs....
- but what about *incorrect* ones? Eg
  - commands out of sequence
    - eg B0 (READ BINARY) *before* completing BAC
  - commands not in the ICAO specs at all
    - eg 44 (REHABILITATE CHV)
  - commands with silly parameters

Example commands & responses

Commands sent to card include 1 instruction byte, eg

- A4 SELECT FILE
- B0 READ BINARY
- 84 GET CHALLENGE
- 82 EXTERNAL AUTHENTICATE
- …

Responses from card include 2 bytes status word, eg

- 9000 No error
- 6D00 Instruction not supported
- 6986 Command Not Allowed
- 6700 Wrong Length
- …

Defined in ISO7816, re-used in ICAO specs

Example responses to B0 instruction

B0 means "read binary", and is only allowed after BAC

	response (status word)	meaning
Belgian	6986	not allowed
Dutch	6982	security status not satisfied
French	6F00	no precise diagnosis
Italian	6D00	not supported
German	6700	wrong length

255 other instructions to try,
and we can try different parameters ...

Fingerprinting passports

- Response to strange inputs provides unique fingerprint for the ten nationalities we tested
  - Australian, Belgian, Dutch, French, German, Greek, Italian, Polish, Spanish, Swedish
- This fingerprint depends on implementation choices in the software
- If countries use the same implementation (ie. get passport from same supplier), the fingerprints would be identical

Detecting & distinguishing passports

- 4 commands suffices to distinguish between the 10 nationalities we tested
  - instruction byte 82 identifies Australian, Belgian, French, and Greek
  - A4 identifies Dutch and Italian
  - 88 identifies Polish and Swedish
  - 82 with different parameter identifies German and Spanish
- Code to do this is very simple & very fast

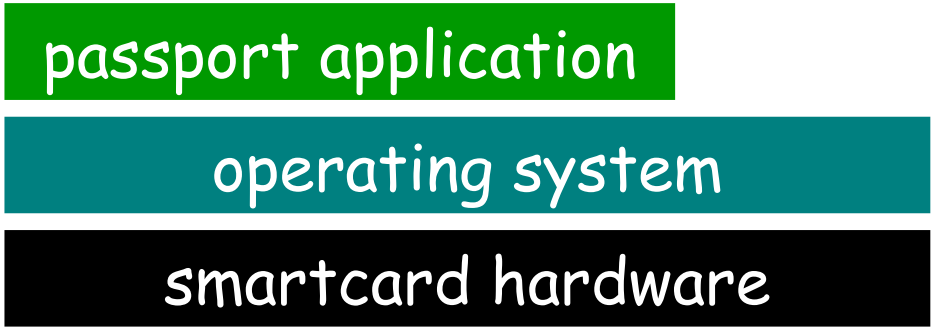
The small print in the specs

"A MRTD chip that supports Basic Access Control *must* respond to unauthenticated read attempts (including selection of (protected) field in the LDS) with 'Security Status not satisfied' (6982)"

[PKI for machine readable travel documents offering ICC read-only access, version 1.1. Technical report, ICAO, Oct 2004.]

but what constitutes a "read attempt"?

More fingerprinting possibilities



- Our approach fingerprints passport application
  - so upgrading hardware or OS won't affect fingerprint
- Fingerprinting may be possible at other levels, eg
  - OS
  - hardware

More fingerprinting possibilities

- UIDs used in anti-collision phase, if these are not random
  - *fixed* UID would provide unique fingerprint of a single passport, not nationality!
  - some countries reportedly use fixed UIDs

More fingerprinting possibilities

- ATS (Answer To Select)
  - sent by RFID on activation to indicate eg supported data rate, but also operating system version (in "historical bytes")
  - New Zealand passport sen
    IBM/NXP JCOP card, v
- Other OS behaviour
  - eg Dutch passport
    as it supports Glob
- Physical characteristi
  - power consumption

Remember this?

```
>telnet hera.cs.kun.nl
Trying 131.174.142.11
Connected to hera
Red Hat Linux 2.4.18
login:
```

Countermeasures

- better specs
  - clearly prescribing standard error responses
  - or, all countries could simply use a common open source implementation
    - eg our Java Card implemententation [http://jmrtd.sourceforge.net]

- metal shielding in passport cover (Faraday cage)
  - included in US passport
    - (initially *instead of* BAC?)
  - defence-in-depth

Abuse cases?

- Passport bomb triggered by a specific nationality
- Selection of potential victims by passport thieves

Fortunately, limited range for active attacks (25cm, maybe a bit more) reduces any serious threat

Also, there may be easier ways to detect nationality...

Conclusions

- Error responses to 'strange' inputs provides unique fingerprint per manufacturer
  - GIFO: garbage in, fingerprint out
- As usual, wireless has advantage for convenience, but disadvantage for security
- Lots of media attention about passport bomb, but central national database with fingerprints might be more of a security worry....

- Code for passport terminal and passport available at http://jmrtd.sourceforge.net

Questions?