ePassports reloaded

Jeroen van Beek

BlackHat Asia 2008, Tokyo

Where will we go today?

- Technology overview
- Attacks
- Root causes
- Solutions
- The future(?|!)
- Questions

Technology overview

- An ePassport contains a chip
- The chip contains data about the passport holder
  - Name, date of birth, passport number, etc.
  - Biometrics (picture, finger prints, iris scan)
- Chip content is based on a standard by the International Civil Aviation Organization (ICAO)
  - See http://www.csca-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf for details
- *Chip content is accessible using a wireless interface (RFID)*
- ePassports are enrolled on a global scale
- Not widely used for real-life applications (yet)

Technology overview, ct.

- So what does it look like? Self scan setup at Amsterdam Airport, The Netherlands:

Technology overview, ct.

- So what does it look like? Portugal:

The ICAO standard: chip content

- Chip contains files (“Elementary Files”, EFs):
  - EF.DG1: personal information (required)
  - EF.DG2: picture, JPG/JPG2000 (required)
  - EF.DG[3-14,16]: finger prints, iris scans and other files for future use (optional)
  - EF.DG15: anti-cloning crypto (optional)
  - EF.SOD: safeguarding integrity of DGs (required)
  - EF.COM: index of available files (required)
  - **Demo!**

The ICAO standard: security

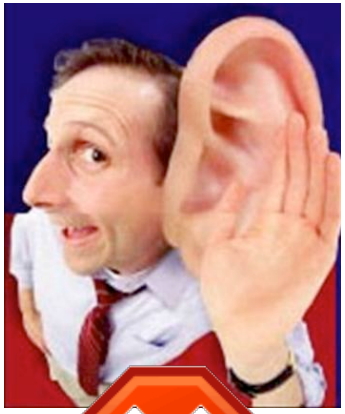
- Relevant security mechanisms in current chips:
  - Passive authentication (PA) (required):
    - Safeguard integrity of data → detect changes
    - EF.SOD stores hashes of EF.DG[1-16] and a public key, hashes are digitally signed with a private key
  - Basic Access Authentication (BAC) (optional):
    - Safeguard confidentiality of data → prevent eavesdropping
    - Authentication using key is required before reading files
    - KEY = DOCUMENT NUMBER + DATE OF BIRTH + DATE OF EXPIRY
    - After authentication data is encrypted (3DES) and messages contain MACs (MAC8)
  - Active Authentication (AA) (optional):
    - Prevent cloning and → detect copies
    - EF.DG15 contains a public key. The private key of this key pair is in inaccessible chip memory. Authenticity of the chip can be checked by letting the chip sign a reader's challenge and verifying the result with the public key

Passive Authentication (PA)

=

=

Basic Access Control (BAC)



Active Authentication (AA)

=

=

Grandmother flies to Canary Islands on her husband's passport

A grandmother flew to the Canary Islands using her husband's passport by accident.

Last Updated: 12:50AM BST 25 Jul 2008

Andrea Cole picked up the wrong passport when leaving her Cardiff home for the week-long holiday with her mother, and did not realise her mistake until minutes before their flight was due to leave.

The mother-of-three had already passed through two sets of checks at Cardiff International Airport - and was then allowed through immigration at Fuerteventura without the error being spotted.

Mrs Cole, a self-employed computer technician, said: "I just couldn't believe what had happened. You would expect people to double check in this day and age."

Email this article

Print this article

Share this article

Related Content

The Sophie Butler report: Losing a passport

Known attacks

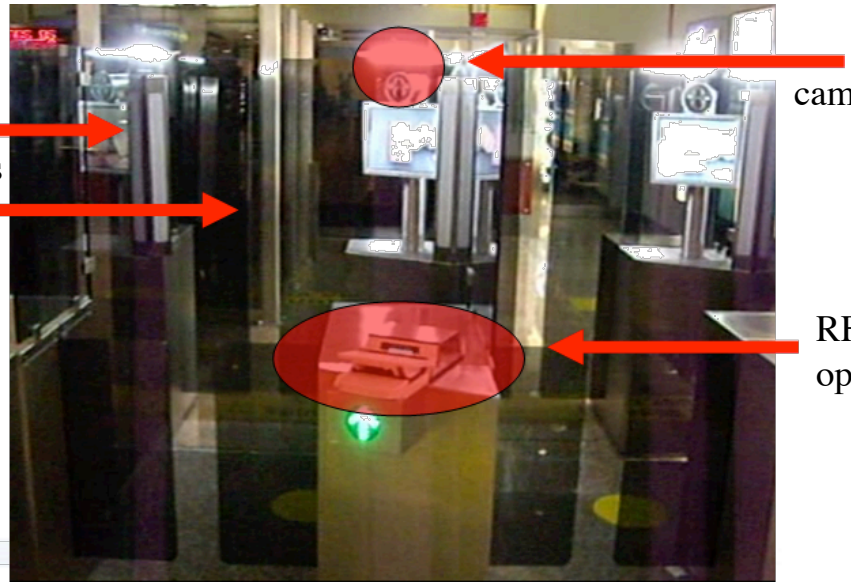
- Real life attacks, the past:
  - Cloning ePassports without Active Authentication
    - Lukas Grunwald @ BlackHat, USA, 2006
    - http://www.wired.com/science/discoveries/news/2006/08/71521
    - Bit by bit copy of content in a self-written ePassport emulator
    - Can be prevented by using Active Authentication
  - Retrieving secret ePassport key data
    - Marc Witteman @ What The Hack, The Netherlands, 2005
    - http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf
    - Using power analysis to retrieve AA private key
    - Can be prevented by using proper hardware

Known attacks, ct.

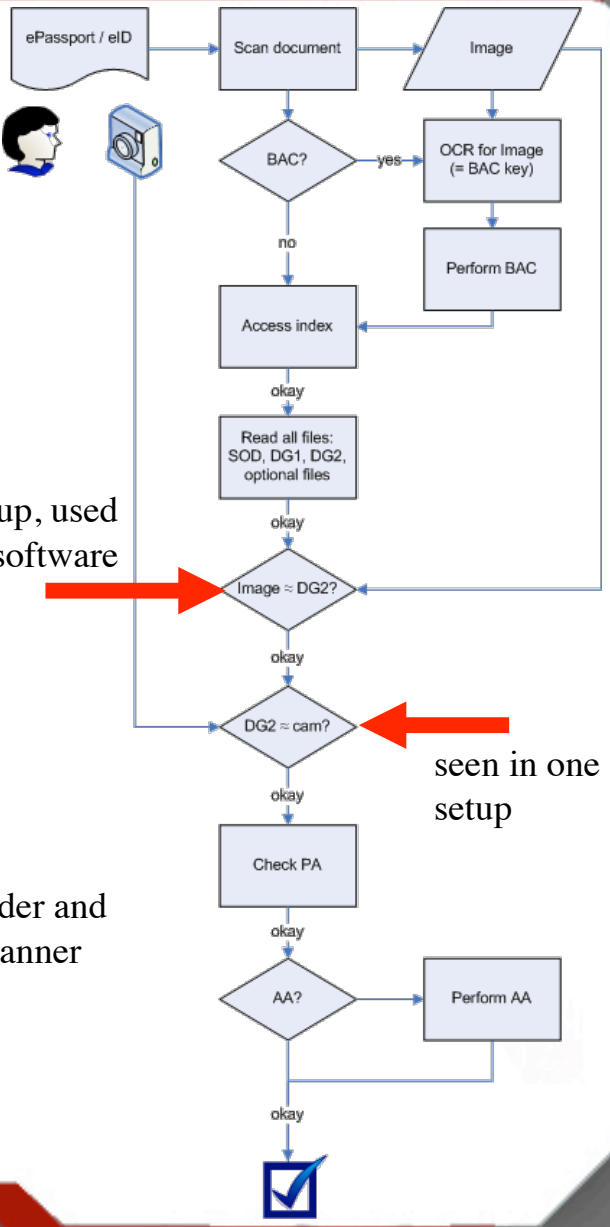
- Real life attacks, the past:
  - Read ePassports with predictable document numbers
    - Adam Laurie reads BAC protected UK ePassport of a Guardian reporter, UK, 2006
    - http://www.computerweekly.com/Articles/2006/11/21/219995/expert-cracks-biometric-passport-data.htm
    - An educated guess (sequential document numbers), also see Witteman's slides
    - Can be prevented by using non-sequential document numbers (though effective key length is still only ~72 out of 128 bits)
  - Fingerprint ePassports without authenticating
    - Radboud University / Lausitz University team @ NLUUG, The Netherlands, 2008
    - http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf
    - Characteristics of APDU responses show the origin of the applet
    - Can be prevented by using standard response codes ("status words")

Verification process

- Two steps seem to be optional:
  - Scannend image versus chip image
  - Chip image versus camera image



seen in one setup, used in non-public software



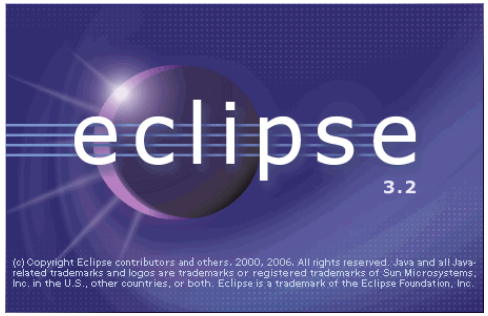
Verification process, ct.

- Dutch immigration seems to use (test) software which uses scan↔chip checks
  - And the minister of justice proudly shares his passport data on the net :)

Finding new flaws

- First we need a test platform

RFID reader, ~ $75



Eclipse & JCOP plug-in, ~ $0

All-in-one printer, ~$75

laptop computer, ~ $750

JCOP41 smartcard, ~$20

Finding new flaws, ct.

- Then we need code that emulates the ePassport
  - Just follow the specs, check ICAO's "worked example"
  - Add function to write data to the emulator
- Your emulator can be tested quite easily
  - Perform a read-out of a real chip with Adam Laurie's excellent RFIDIOt tools http://rfidiot.org/ and store it (= <chip>)
  - Change both mrpkey's and your emulator's code to make Debian style random number generators
  - Copy the original chip content to your emulator
  - Perform a read-out of the emulator with RFIDIOt (= <emulator>)
  - diff <chip> <emulator>
  - Fix bugs :)
  - **Code snippets!**

Finding new flaws, ct.

- If the emulator is up and running we need to:
  - Get reference implementations:
    - Golden Reader Tool, referenced in ICAO documentation
    - Real-life test setups
  - Successfully attack optical scanners
  - Successfully attack PA
  - Successfully attack AA
    (enabled on e.g. Dutch documents)

Attacking optical scanners

- Get OCR-B fonts for MRZ (= BAC key)
- Copy / paste the picture and MRZ in the right place
- *Advanced equipment is on the market*
  - *IR scans*
  - *UV scans*
  - *Systems are as strong as the weakest link*
- **Demo included later on!**

News Front Page

Africa

Americas

Asia-Pacific

Europe

Middle East

South Asia

UK

England

Northern Ireland

Scotland

Wales

UK Politics

Education

Magazine

Business

Health

Science/Nature

Technology

Entertainment

Country Profiles

Special Reports

Page last updated at 09:37 GMT, Tuesday, 29 July 2008 10:37 UK

E-mail this to a friend

Printable version

3,000 passports and visas stolen

Greater Manchester Police has launched an investigation into the theft of 3,000 blank passports and visas.

The documents were in a van which was targeted on 28 July.

The Foreign Office admitted a serious breach of security over the loss of the passports and visa stickers, which were being sent to embassies overseas.

The Foreign Office has admitted a serious breach of security

A former Scotland Yard fraud officer said the passports may be worth £1,700 each and could be used to set up bank accounts or get employment.

The theft is the latest in a series of security breaches but Labour's deputy leader, Harriet Harman, has denied

> **"I don't think that it necessarily shows a sloppy attitude"**

The passport service said the stolen documents could not be used by thieves because of their hi-tech embedded chip security features.

apprehend the offenders."

The Conservatives regard the theft as another example of lax

SEE ALSO

- Previous cases of missing data
  15 Jun 08 | UK
- MoD admits another laptop stolen
  20 Jul 08 | UK
- MoD admits loss of secret files
  18 Jul 08 | UK

RELATED INTERNET LINKS

- Foreign and Commonwealth Office
- Identity and Passport Service

TOP UK STORIES

- Mortgage loans reach 'record low'
- Six held over honeymoon killing
- Sikh girl wins bangle law battle

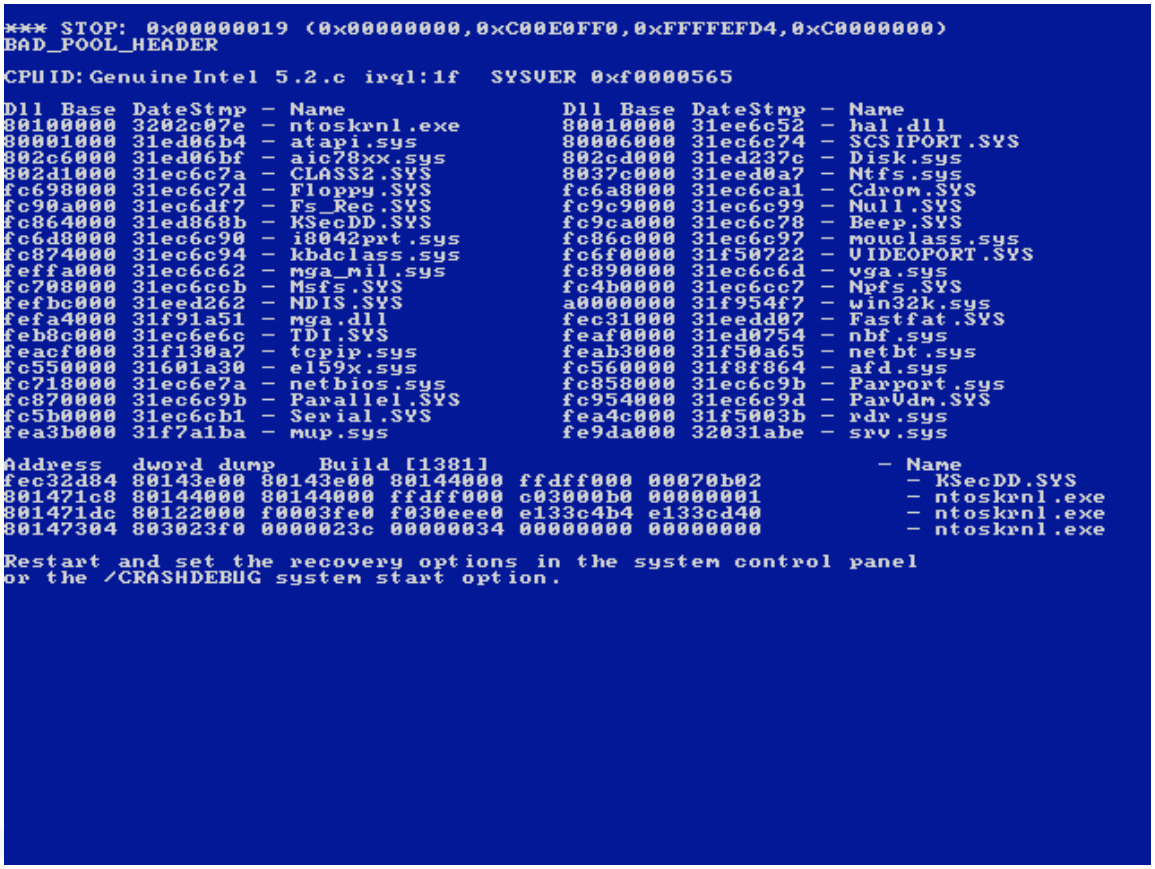
1 Hour's exercise 'to lose weight'

2 Russia claims world-record dive

Attacking PA: warning or error?

Attacking PA: warning or error?

Attacking PA: warning or error?



Attacking PA: warning or error?

Attacking PA: warning or error?

- The signature value is incorrect
  - A) Do nothing
  - B) Warning
  - C) Non-critical error
  - D) Critical error

read-out continues and successfully finishes after detection of invalid SOD

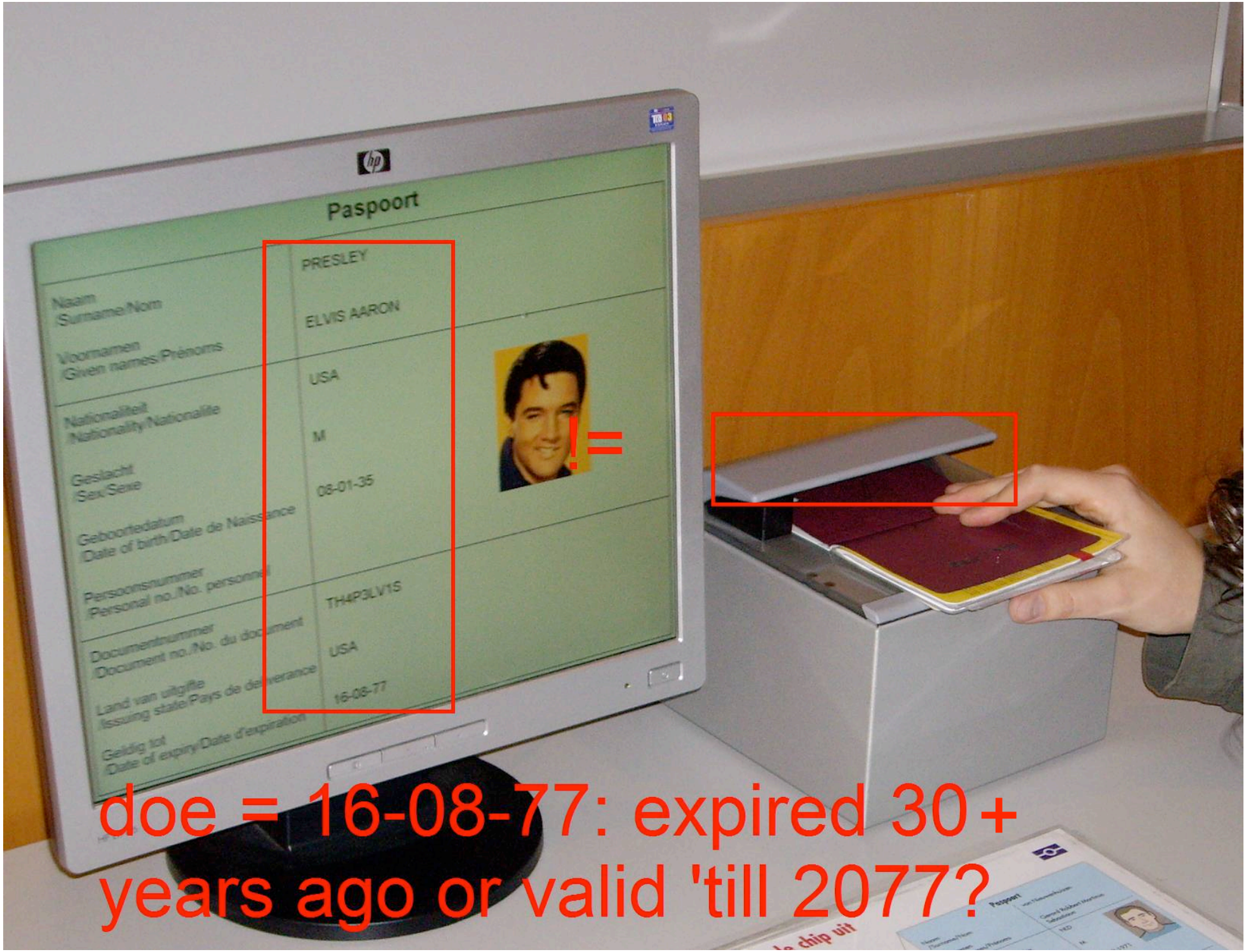
Attacking PA: warning or error?

- A hash value is incorrect
  - A) Do nothing
  - B) Warning
  - C) Non-critical error
  - D) Critical error

find the difference

Attacking Passive Authentication

- This is all very strange… If the reference implementation is not that strict, what about real test setups?
  - Let's try some publicly accessible test equipment
  - **Demo!**


Paspoort
PRESLEY
ELVIS AARON
USA
M
08-01-35
TH4P3LV1S
USA
16-06-77
!=
doe = 16-08-77: expired 30+ years ago or valid 'till 2077?

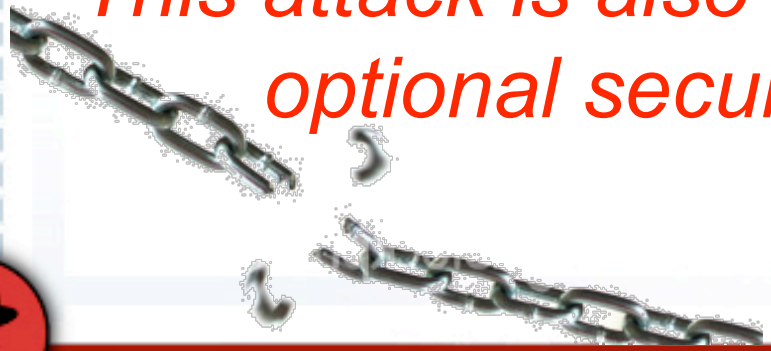
Attacking Passive Authentication, ct.

- Hashes of all data groups are stored
- Hashes are signed using a digital signature
  - Public key is in EF.SOD to check signature
  - Public key should be checked to see if it can be trusted
  - ICAO Public Key Directory (PKD) facilitates online check
    - Chips enrolled in 45(+) countries
    - ICAO, April 2006: PKD membership should be *"necessary...and not optional".*
    - ICAO, May 2008: *"The ICAO PKD has grown to nine participants"*
    - Fall-back mechanism: *"distributed by strictly secure diplomatic means"*
      - Manual process: store all public keys in inspection systems
      - What about e.g. key exchange Israel ↔ Iran?
- Create self-signed certificate and sign altered data
  - Create your own country!
  - Thanks to Peter Gutmann http://www.cs.auckland.ac.nz/~pgut001/


Golden Reader Tool
Picture
Facial Image
<
>
Personal Data
Name
ELVIS AARON
Surname
PRESLEY
Date of Birth (dd.mm.yy)
08.01.35
Nationality
United States
Sex
Male
Valid until (dd.mm.yy)
16.08.77
Document Number
TH4P3LV1S
Document Type
P
Issuer
United States
Optional Data
Printed MRZ
P<USAPRESLEY<<ELVIS<AARON<<<<<<<<<<<<<<<<<<<<
TH4P3LV1S1USA3501081M7708165<<<<<<<<<<<<<<04
Operation
Autodetect
Read
Read BAC / EAC
Read from Disk
Write to Disk
Reset Display
About...
Options
Configuration
Close
Access Control
BAC
Chip Authentication
EAC
Terminal Authentication
Active Authentication
Chip Data
UID
n/a
ATR/ATS
3b8a80014a434f503431563232317f
ISO-14443
n/a
Reading time
7.86
Seconds
Passive Authentication
DG1
DG16
Signature EF.SOD
Algorithm RSA / SHA256
Certificate-Chain
Revocation
Logging
7.75 : Size EF_DG2: 14302 Bytes.
7.75 : DG2 read successfully.
7.75 : Hash Datagroup 2 OK.
7.75 : CBEFF Format Type 0008
7.78 : Facial Image Type 0000
7.81 : Image data type: JPEG
7.86 : The overall size is 19633
7.88 : The average reading speed was 19.99 kpbs.

Attacking Active Authentication

- Not writing the file (DG15) doesn't work
- But what about manipulating EF.COM?
  - If a file is not there you cannot check it…
- **Demo!**
- *This attack is also applicable to all other optional security features!*



Attacking Active Authentication, ct.

- Removing AA from the index:

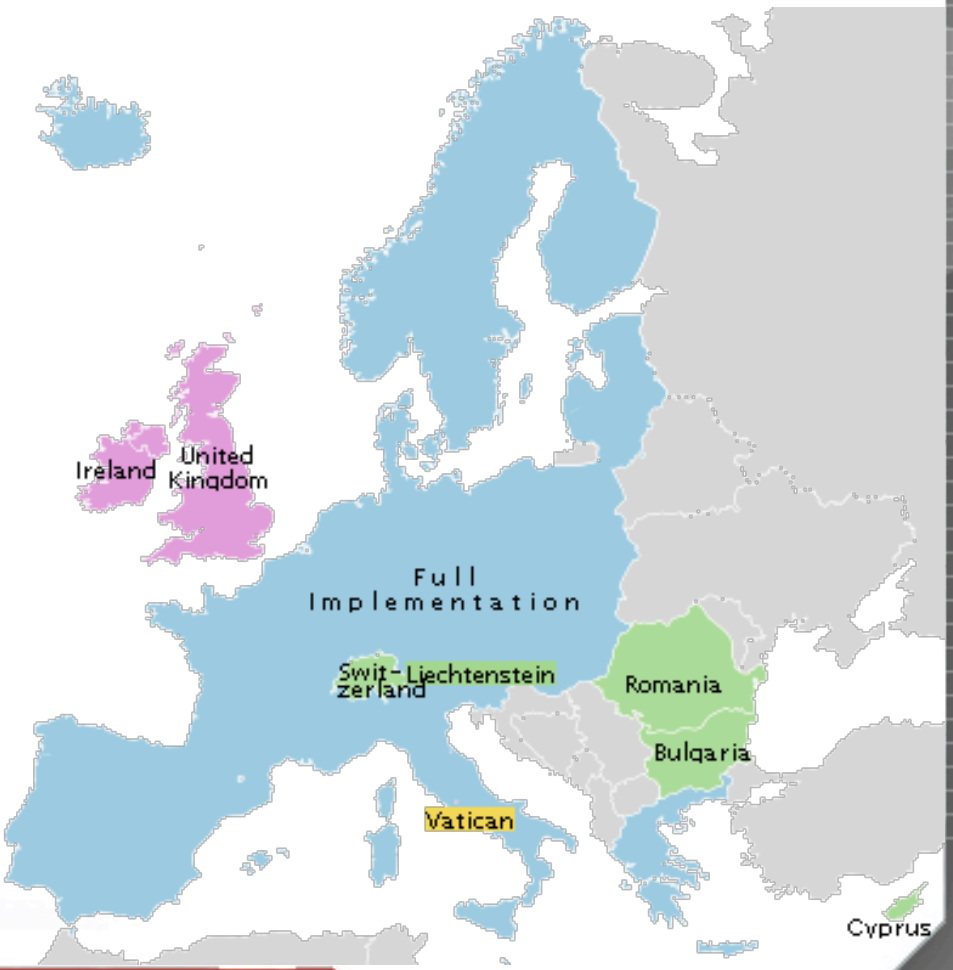
```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 60 15 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 ; `._..0107_6.0400
00000010h: 30 30 5C 03 61 75 6F                           ; 00\.auo
```

bytes - 1
tags
DG1 (required MRZ info)
DG2 (required picture)
DG15 (optional active authentication)

```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 60 14 5F 01 04 30 31 30 37 5F 36 06 30 34 30 30 ; `._..0107_6.0400
00000010h: 30 30 5C 02 61 75                              ; 00\.au
```

European Union

- Passport-free travel zone EU
- Are all implementations 100% secure?



Finding new flaws: summary

Test	Design ok	Impl. ok	Risk
Images scan = Image chip check	?	? / ✗	Illegally entering / leaving a country using low-tech scan and cloned chip
Incorrect hash values	✓	✗*	Identity theft / identity creation
Self-signed document	✓	✗	Identity theft / identity creation (okay if PKD is checked real-time)
Active Authentication	✓ / ✗**	✗*	Cloning cannot be prevented (use the weakest link)
Index manipulation	✗***	✗	Cloning cannot be prevented (use the weakest link)

* *Non-critical error in GRT, check not implemented(!) in examined test setups*

** *"When a MRTD with the OPTIONAL Data Group 15 is offered to the inspection system, the Active Authentication mechanism **MAY** be performed…"*

*** *Issue documented in supplement 6, conclusion "rejected"*

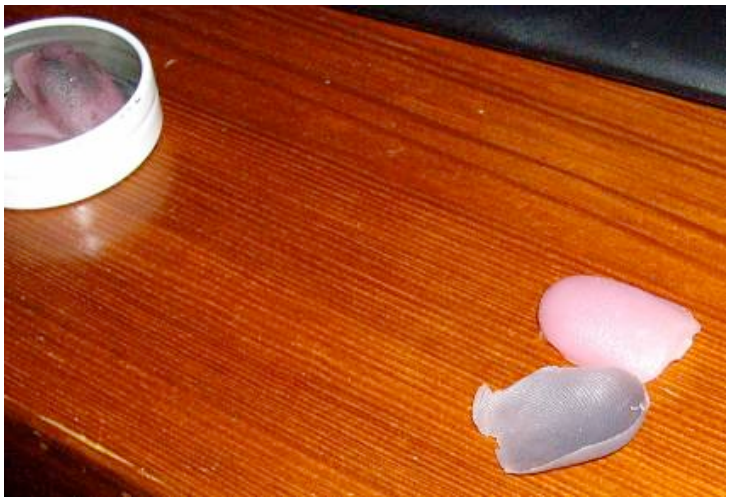
Root causes

- Design (ICAO standard):
  - *Some key security features are optional: if one party doesn't use a feature the security level of the entire system (globally!) depends on compensating measures*
  - PA does not protect against index manipulation
- Tested implementations:
  - *Do not follow the ICAO standard!*
  - Every country is reinventing the wheel
    - Reinventing the applet (fingerprinting nationalities)
    - Reinventing reader bugs (Elvis lives!)
    - Reintroducing hardware problems (DPA attacks etc.)

Solutions

- Design (ICAO standard):
  - *Require all security features including PKD by default*
  - Protect the integrity of *all* files
- Implementation:
  - Implement all security features by default
  - Use automated border control for chips with *all* security features enabled only
- Global coordination (e.g. ICAO or other UN body):
  - Provide standard implementation for ePassport applets and inspection systems
    - The more (black box) implementations, the higher the risk of a serious problem
    - *Open standards and implementations, no security by obscurity!*
  - Provide countries with a list of authorized hardware and hardware lifetimes
    - Think about the Mifare Classic chip family
    - History might repeat itself with ePassports: e.g. German ePassports are valid for 10 years. In 10 years the hardware is most probably outdated (DPA attacks etc.)
  - Enforce the use of a trusted PKI environment (PKD)
    - Automated real-time certificate & CRL checks

The future(?|!)



- More biometrics will be added:
  - June 2009: EU adds fingerprints
  - Later: Iris? DNA? Footprints?
- If implemented correctly (…), the system heavily relies on PKI
  - Let's take a job at customs!
  - Let's check their network security!
  - In my professional 'ethical hacker' career we've got a 100% hit rate on p0wning networks
  - I guess unethical hackers got a similar hit rate…
- In the end it's just another software product
  - Same bugs, same exploits. Exploit terminals to hop on to the backend systems
  - E.g. GRT uses CxImage for JPGs, spl0it writers, please contact me…
- Happy traveling :)

“Just trust us!”

The Dutch government responded to the findings (Dutch) and said that systems will be enrolled in 2009 that do perform Active Authentication and certificate checks. Though there is no standard available (yet?) documenting security features of the new system. So a system is being built now and will be enrolled in 2009 but there is no documented design available at this time. This is not a good idea. No safeguards. No independent third party reviews possible by e.g. universities and security researchers. And we are talking about a critical application called border control...

Entrust, which handles PKI security for ePassports, says that we should trust them. *"Governments' security experts aren't dummies and they aren't going to make those mistakes"*. No word about a safe design. Just trust the professionals. Yeah right :) Trust but verify:

- *"3,000 passports and visas stolen"*
- *"Grandmother flies to Canary Islands on her husband's passport"*
- *"MI5 computer stolen in burglary"*
- *"5,000 secret computer files on prison governors and staff vanish"*
- *"USB Stick Containing Classified NATO Info Lost in Sweden"*
- *"Passport applicant finds massive privacy breach"*
- *"Trojan horse captured data on 2,300 Oregon taxpayers"*
- To be continued…

Questions

Thank you!

jeroen@dexlab.nl

Further reading

- http://www.theregister.co.uk/2008/09/30/epassport_hack_description/
- http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece
- http://www.timesonline.co.uk/tol/news/uk/crime/article4467098.ece
- http://blog.wired.com/27bstroke6/2008/08/e-passports-cra.html
- https://www.os3.nl/2008-2009/epassport_eng
- http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx
- http://www.icao.int/icao/en/atb/meetings/2008/TagMRTD18/TagMrtd18_ip04.pdf
- http://www2.icao.int/en/MRTD/Downloads/Supplements%20to%20Doc%209303/Supplement_to_ICAO_Doc_9303_-_Release_6.pdf
- http://www.csca-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf
- http://news.bbc.co.uk/2/hi/uk_news/7530180.stm
- http://www.telegraph.co.uk/news/newstopics/howaboutthat/2456084/Grandmother-flies-to-Canary-Islands-on-her-husbands-passport.html