Marc Witteman

witteman@riscure.com

Attacks on Digital Passports

July 28, 2005, WhatTheHack

Contents

- **Introduction**
- Digital passports
- Privacy attack
- Cloning attack
- Conclusion

Legacy

Problems with legacy passports

- **Forgery**
  - Illegal document creation or modification
  - Very difficult today due to good quality of documents
- **Look-alike fraud**
  - Use passport of someone else
  - E.g. family member, or occasional match from large collection
  - Simple fraud, difficult to combat with traditional means

Moving to digital passports

- Accelerated by 9/11
- Provide better proof of passport holder identity

Threats to authorities

- Illegal migration

Threats to citizens

- Loss of privacy
- Identity theft

Contents

- Introduction
- **Digital passports**
- Privacy attack
- Cloning attack
- Conclusion

Technology for digital passport

Smart Cards

- Secure container
- Protected access
- Java OS
- Cryptography & PKI
- RFID (contactless)

Biometry

- Use physical personal properties
- E.g. facial scan, fingerprint, hand geometry, iris scan
- No absolute verification, error rate ≈ 5%

Security principles

- Security Object with identification and biometric data stored in RFID
- Authentication
  - Passive: static signed personal data
  - Active: dynamic challenge signing
- Confidentiality
  - Basic Access Control using MRZ data
  - Extended Access Control

Authentication

Passive

- Security Object contains a certificate
- Certificate signed by national governments
- Verification through PKI
- No protection against cloning!

Active

- Reader gets passport public key
- Passport signs challenge with RSA private key
- Reader verifies challenge
- Secret private key protects against cloning

Access Control

PASSPORT
PASSEPORT
PASAPORTE

UTOPIA

Type / Type / Tipo
P
Code / Code / Código
UTO
Passport No. / No. du Passeport / No. de Pasaporte
L898902C
Surname / Nom / Apellidos
ERIKSSON
Given names / Prénoms / Nombres
ANNA MARIA
Nationality / Nationalité / Nacionalidad
UTOPIAN
Date of birth / Date de naissance / Fecha de nacimiento
06 Aug 1969
Personal no / no personnel
ZE184226B
Sex / Dexe / Sexo
F
Place of birth / Lieu de naissance / Lugar de nacimiento
ZENITH, UTOPIA
Date of Issue / Date de délivrance / Fecha de expedición
24 Jun 1989
Authority / Autorité / Autoridad
Passport Office
Date of expiration / Date d' expiration / Fecha de caducidad
23 Jun 1994
Ammendments / Modifications / Enmiendas
See Page 24

P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<
L898902C<3UTO6908061F9406236ZE184226B<<<<<14

Basic Access Control

- Reader reads MRZ data
- Static access keys are derived from MRZ data
- Encrypted channel opened
- Passport can only be read by whom you show it to!

Extended access control

- Reader authentication to protect confidentiality

Key derivation

- Compute static encryption and protection keys by hashing (SHA-1) relevant MRZ data:
  - Date of birth
  - Date of expiry
  - Passport number
- Compute session keys by exchange of (Triple DES encrypted) session data.

Contents

- Introduction
- Digital passports
- **Privacy attack**
- Cloning attack
- Conclusion

Privacy attack principles

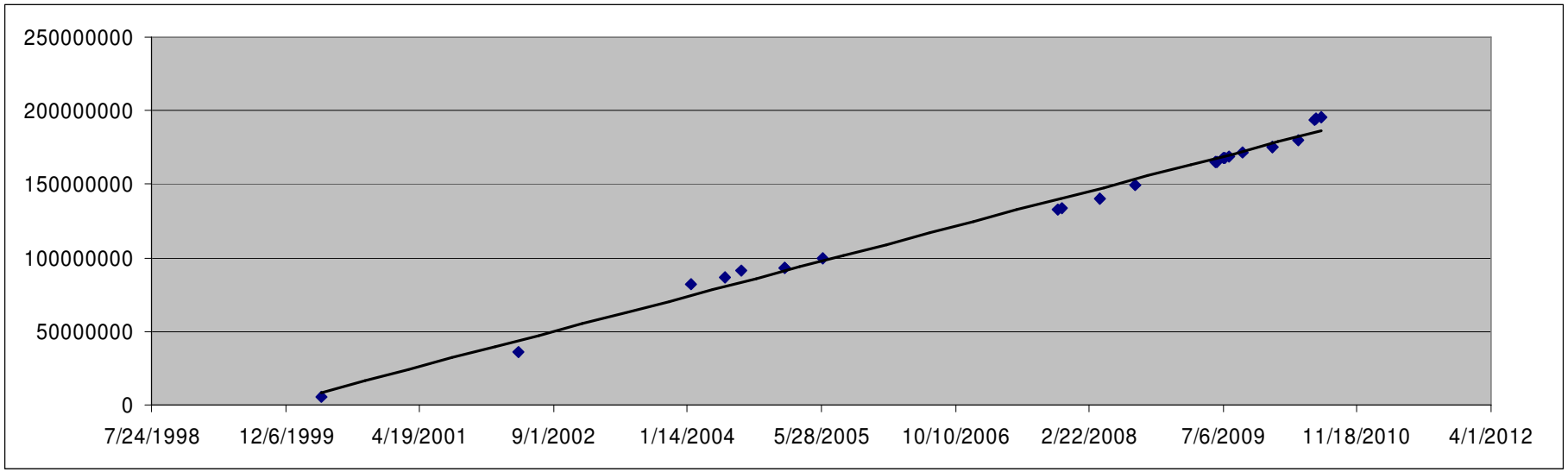
- Legacy passport can only be read by anyone who has physical access to your passport. (generally with consent of holder)
- Digital passport can be read by:
  - anyone who **knows your MRZ data** and is within short distance (< 0.5 meter)
  - Anyone who can **eavesdrop your authentication protocol** from medium distance (<10 meter) and can decrypt your static keys

Strength of static keys

- First analysis:
  - expiry date within 5 years: 5*365 = 1825 values
  - Birth date can be guessed: 10*365 = 3650 values
  - 8 digits passport number (Dutch)
  - Entropy ≈ 50 bits: ≈ 10^{15} possible values
- Static key guessing requires testing every key candidate: 2 * SHA-1, 4 * Triple-DES, can be done in 1 µs on standard PC
- Guessing seems unfeasible for low-end attacker (>35 years) -> **moderate privacy**

Analysis of passport number

- We collected a few Dutch passport numbers
- It appears that they are issued sequentially...
- Increase about 50,000 per day...



More passport number observations

- Dutch passport numbers generally consist of a static letter ‘N’ followed by another character and 7 digits, e.g. NF3858053
- Increase in passport number about 100M in 5 years -> 10 faster than expected, considering 15M Dutch nationals

BREAKING NEWS

We discovered last digit is only checksum, so the actual number space is 10 times smaller!

Checksum in passport number

- Many numbers use checksums for integrity checking, e.g. credit card or sofi number
- Formula for passport number discovered:
  - Replace character after 'N' by digit:
    A=7, B=8, C=9, D=0, E=1, etc
  - 8 digits called $x_1..x_8$
  - Check
    $(\mathbf{7}*x_1 + \mathbf{9}*x_2 + \mathbf{3}*x_3 + \mathbf{7}*x_4 + \mathbf{9}*x_5 + \mathbf{3}*x_6 + \mathbf{7}*x_7 + \mathbf{1}*x_8) \bmod 10 = 0$

Passport number predictability

- Daily increase of issued passport numbers: 50K
- Last digit is redundant and can be computed
- Attackers need only consider 5K passport numbers per expiry day
- Total entropy may be reduced to 35 bits
- Static keys can be broken in one or two computing hours on standard PC

Your privacy is void

Contents

- Introduction
- Digital passports
- Privacy attack
- **Cloning attack**
- Conclusion

Active authentication with RSA

RSA is used for active authentication
(prevent cloning fraud):

- Reader reads signed passport public key
- Reader sends challenge to passport
- Passport encrypts challenge with secret RSA key
- Reader gets encrypted response from passport
- Reader verifies response with public key

RSA algorithm and implementation

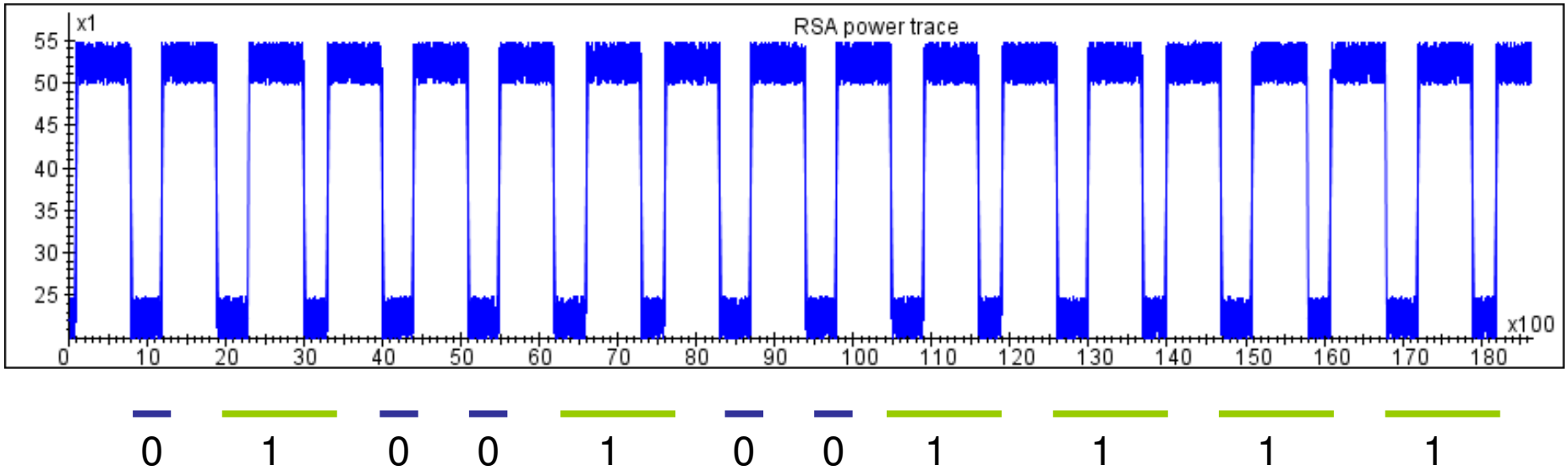
- RSA uses exponentiation for signing/verification: $C = M^{ks} \bmod N, \quad M = C^{kp} \bmod N$
- Exponentiation can be implemented in various ways, for example binary exponentiation:
  - C := 1
  - For each key bit k_i do:
    - C := C * C
    - If $k_i = 1$, then C := M*C

Side-channel attacks

Side-channels provide unintended means to analyze or manipulate the behavior of cryptographic implementations:

- **Time analysis**
  use process duration to reveal secrets
- **Power Analysis**
  use power consumption to reveal secrets
- **Electro-Magnetic analysis**
  Use EM radiation to reveal secrets
- **Power glitching**
  use power interruptions to inject computational faults

Time-Power Analysis of RSA



- Analyze RSA trace, and note the distance variations between higher and lower parts
- Key can be derived from a single observation!

Statistical analysis of RSA (1)

- Encryption is alternation of square and multiply operations
- Squaring uses slightly more energy than multiplication:
  - Consider value set { 1, 2 }
  - Average multiplication of random values:

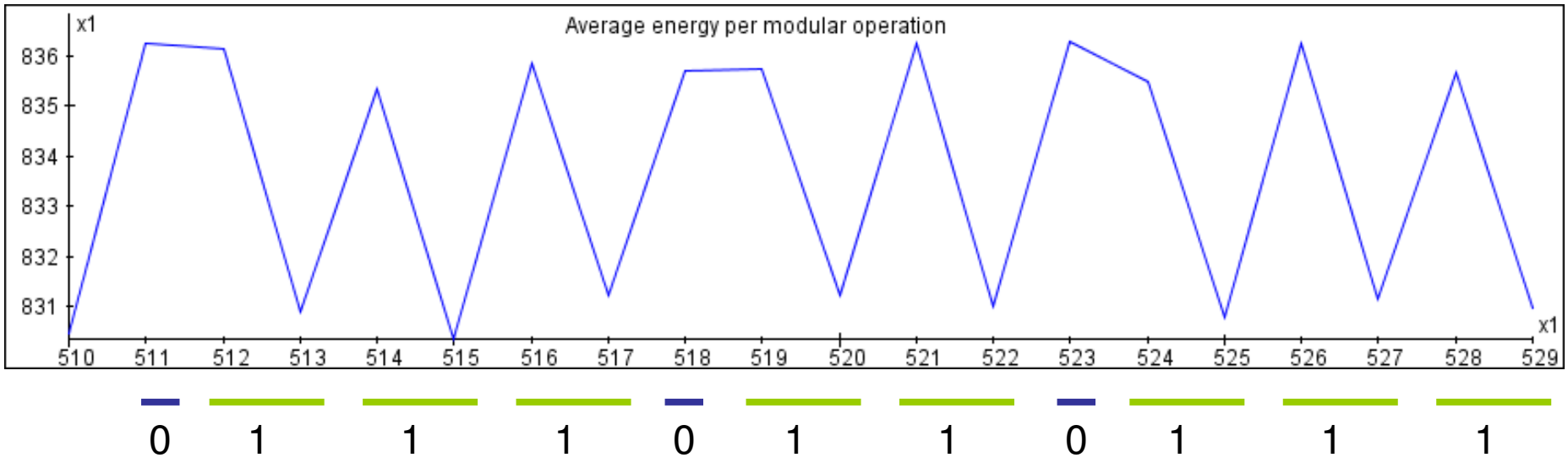
$$\frac{1\times1+1\times2+2\times1+2\times2}{4}=\frac{9}{4}=2.25$$

  - Average squaring of random values:

$$\frac{1\times1+2\times2}{2}=\frac{5}{2}=2.5$$

- Average energy distinguishes operations

Statistical power analysis of RSA (2)



- Collected many (>1000) RSA power traces
- Compute average energy per modular operation
- Small variations reveal key bits
- More advanced correlation analysis is possible...

Exploitation of authentication key

- Cloning requires physical access to victim passport
- First, read personal data
- Next, perform multiple active authentications (RSA)
- Retrieve private key by (statistical) analysis
- Load new chip with personal data and RSA keys
- Attach chip to passport document with same identity
- **Clone ready for use!**

Contents

- Introduction
- Digital passports
- Privacy attack
- Cloning attack
- **Conclusion**

Recommendations

What should authorities do to prevent cloning fraud?

- Evaluate for advanced side-channel vulnerabilities

What should authorities do to gain public trust?

- Apply sound design and evaluation strategies
- Re-establish privacy by introducing high-entropy unpredictable passport numbering scheme

What can citizens do to protect their privacy now?

- Get a deviating passport, e.g business passport or ask for shorter life time (e.g. 4 years).

Summary

- The digital passport complicates **look-alike fraud**
- Passport numbering system easy to **break**
- **Key space** protecting privacy much smaller than claimed
- **Privacy** poorly addressed in NL passport
- Advanced side-channel attacks may still allow **cloning fraud**; applies internationally

Any questions?

Thanks!

Riscure is a security lab specialised in smart card and mobile phone security

We're hiring!

We like to meet with you if you have exceptional technical qualities and share our passion for information security

Contact? -> witteman@riscure.com