

# Smart Card Security Testing

Marc Witteman  
Riscure

31 March 2006

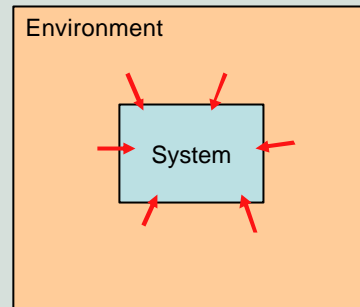
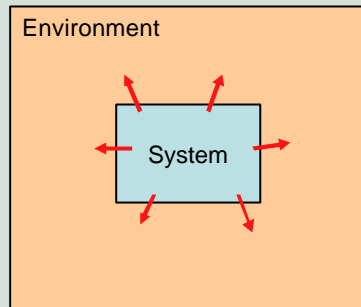
Security Testing

## Outline

- **Context**
- Introduction to smart cards
- Introduction to cryptography
- Attacks & tests
- Conclusion

Security Testing

# Safety and Security



Safety vs Security

Security Testing

# Security terminology

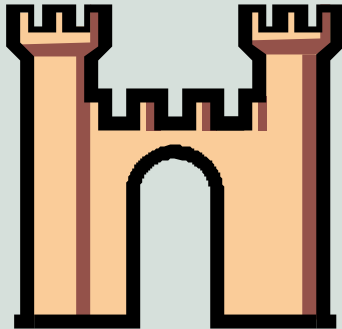


A somewhat militaristic jargon...

- Attack
- Defense
- Threat
- Vulnerability
- Exploit

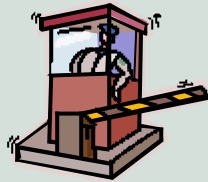
Security Testing

## What is Information Security?



Protection of data:

- Confidentiality
- Integrity
- Authentication
- Availability



How?

- Passwords / PIN codes
- Cryptography

Security Testing

## Outline



- Context
- **Introduction to smart cards**
- Introduction to cryptography
- Attacks & tests
- Conclusion

Security Testing

## What is a smart card?



A smart card

- can store data (e.g. personal, purse balance)
- provides cryptographic services
- is a microcomputer
- is small and personal
- is a *secure* device



Security Testing

## Smart card applications



### Financial

- Smart Credit / Debit
- E-Purses
- Loyalty programs



### Identification

- Passport
- Driving license
- Voting



### Mobile Communication

- Infotainment
- Business support
- Network optimizers

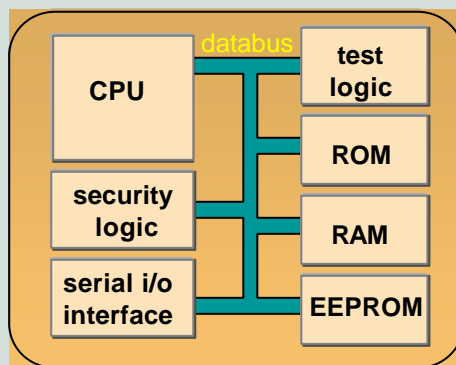
Security Testing

# Chip electrical contacts



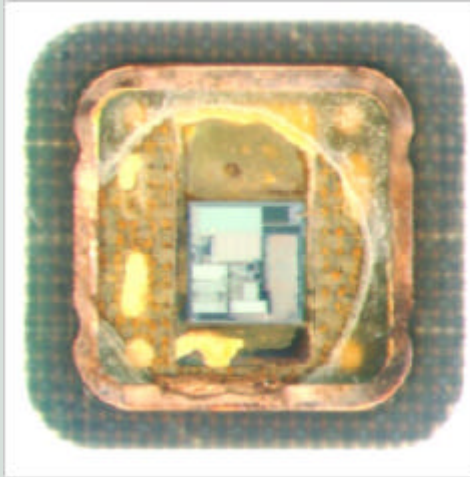
Security Testing

# Logic inside

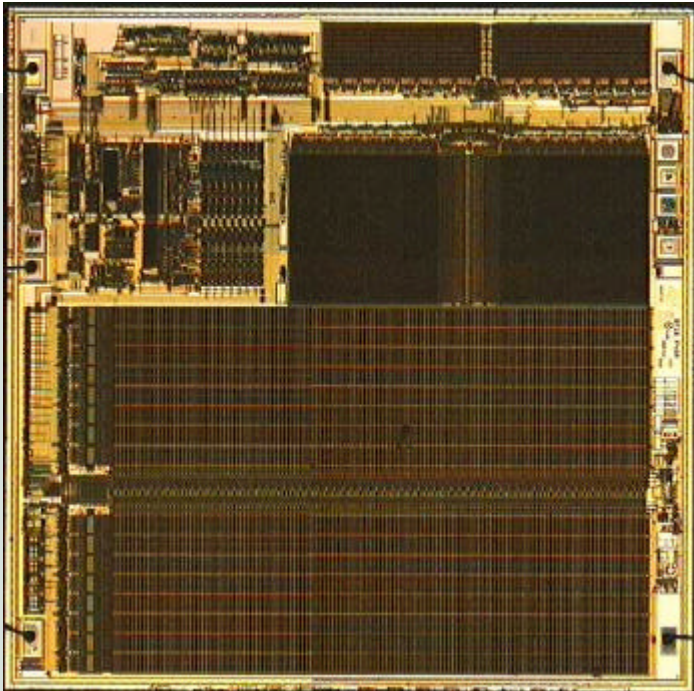


Security Testing

# Take off the lid...

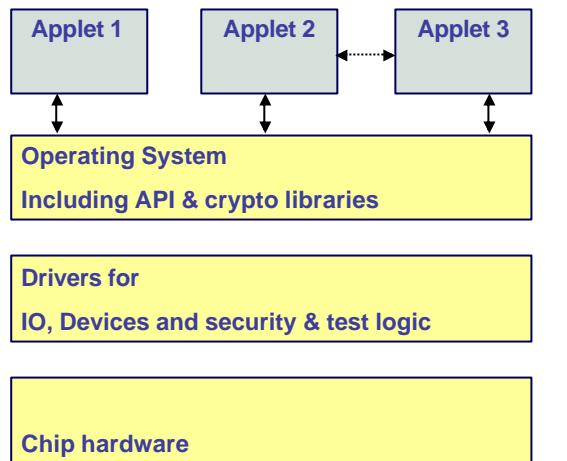


Security Testing



Inside the chip

# System architecture



Security Testing

# Outline



- Context
- Introduction to smart cards
- **Introduction to cryptography**
- Attacks & tests
- Conclusion

Security Testing

## Cryptography principle



Algorithm (= lock) + Key

- key secrecy
- strong algorithm
  - difficult to guess key from message/ciphertext pairs
  - sufficient key length (brute force)
  - strength should reside in secrecy of key, not in secrecy of algorithm

Security Testing

## Crypto protocol concepts

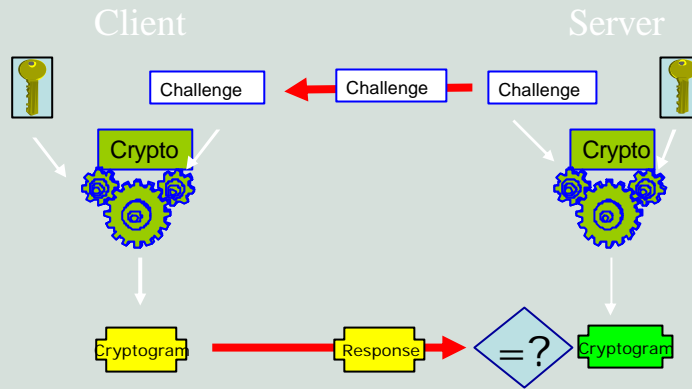


- Challenge / response
  - ✍ authentication
- Digital Signature
  - ✍ authentication & integrity
- Digital Envelope (Encryption)
  - ✍ Confidentiality

Security Testing

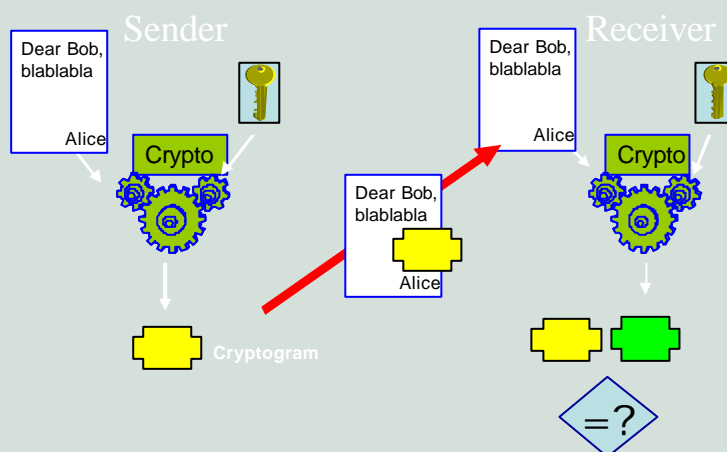


# Challenge / response



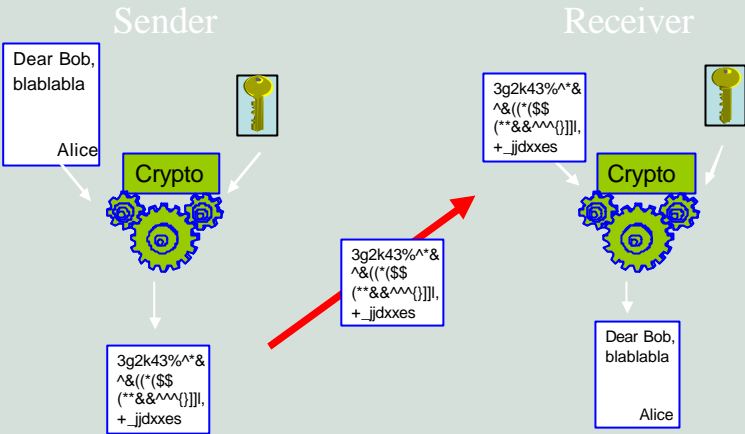
Security Testing

# Digital Signature



Security Testing

# Digital Envelope



Security Testing

# Classical Crypto systems



- transposition (mixing character sequence)
- substitution (changing characters)

⇒ easily broken, using language statistics

Security Testing

## Modern cryptography



Today two kinds of algorithms:

- Secret key (symmetric)  
repetitive transposition and substitution of bits
  - DES
  - AES
- Public key (asymmetric)  
based on hard mathematical problem
  - RSA
  - Elliptic curve

Security Testing

## Threats



- Brute force attacks
- Crypt-analysis
- Protocol attacks
- Vulnerability attacks
- Side-channel attacks

Security Testing

# Outline



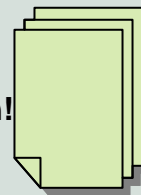
- Context
- Introduction to smart cards
- Introduction to cryptography
- **Attacks and tests**
  - Brute force attacks
  - Crypt-analysis
  - Protocol attacks
  - Vulnerability attacks
  - Side-channel attacks
- Conclusion

Security Testing

# Key size: how much is enough?



- Consider a key of 56 bits (DES)
- Number of possible keys:  $2^{56} = 7 \times 10^{16}$
- Write down all keys,  
...and get a stack of paper from here to the moon!
- Imagine a computer tries 1 million keys per sec  
... and wait 2283 years to try all keys
- But, DES is broken several times:
  - Distributed attack
  - Parallel array of FPGAs



Security Testing



## Static key derivation



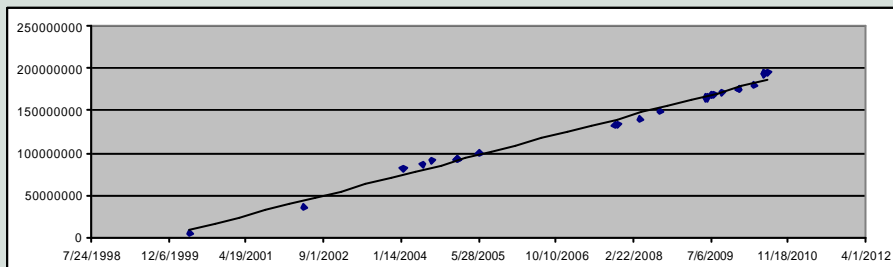
- Key is derived from these 3 numbers:
  - Date of birth
  - Date of expiry
  - Passport number
- Key strength:
  - Birth date can be guessed:  $10 \cdot 365 = 3650$  values
  - expiry date within 5 years:  $5 \cdot 365 = 1825$  values
  - 8 digits passport number (Dutch)
  - Entropy  $\sim 50$  bits:  $\sim 10^{15}$  possible values
- Static key guessing requires brute force testing of every possible key, which can be done in  $1 \mu\text{s}$  per key on a standard PC
- Guessing seems unfeasible for low-end attacker (>35 years) -> moderate privacy

Security Testing

## Passport number analysis



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



Security Testing

## Passport security



- Daily increase of issued passport numbers: 50K
- We discovered that the 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 key can be broken in few computing hours on standard PC: **Your privacy is void**
- After briefing by Riscure the Ministry of Internal affairs has initiated a revision of the standard

Security Testing

## Crypt-analysis



- Design flaw in algorithm
- Happens often to proprietary crypto
- Notorious example in GSM: COMP128
  - Original example algorithm for GSM authentication
  - More than 50% of operators used it
  - Algorithm has a compression flaw
  - Birthday attack using collisions published in 1998
  - Attack implementation downloadable in 2002
  - Operators massively surprised by cloning fraud...



Security Testing

## Cryptanalysis example: Clone your SIM



**Birthday attack on Comp128**

Round 2 left: 100.0% Key-value: 26 E2

Round 3 left: 100.0% Key-value: EA AA

Round 4 left: 100.0% Key-value: F4 60

Round 2 right: 100.0% Key-value: EA 68

Round 3 right: 100.0% Key-value: D8 63

Round 4 right: 100.0% Key-value: 46 AD

Time left: 00:00:00 Loop: 1

Key to find is: 26 E2 F4 60 EA AA 68 D8 63 46 AD 6F 18 50 80 2D  
Found subround 2 key after 25965 queries.  
Key is now: 26 00 00 00 00 00 00 00 63 00 00 00 00 00 00  
Found 4 sub round 3 collisions after 630 queries  
Found 5 sub round 3 collision(s) after 846 queries  
Key is now: 26 00 00 00 EA 00 00 00 63 00 00 00 18 00 00 00  
Found 12 sub round 4 collisions after 744 queries  
Key is now: 26 00 F4 00 EA 00 68 00 63 00 AD 00 18 00 80 00  
Found subround 2 key after 17225 queries.  
Key is now: 26 E2 F4 00 EA 00 68 00 63 46 AD 00 18 00 80 00  
Found 4 sub round 3 collisions after 1202 queries  
Key is now: 26 E2 F4 00 EA AA 68 00 63 46 AD 00 18 50 80 00  
Found 12 sub round 4 collisions after 2174 queries  
Key is now: 26 E2 F4 60 EA AA 68 D8 63 46 AD 6F 18 50 80 2D  
Ready in 146 seconds, used 48160 queries  
**HAPPY BIRTHDAY**

## Protocol attacks



Attacker abuses protocol design weaknesses:


- Replay attacks
- Relay attacks
- Man-in-the-middle
- Phishing



# Phishing example



## Example of a "phishing" e-mail



Dear customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information ( i.e.change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below:

<https://arribada.com/saw-cgi/eBay/SAP/dll?PlaceCInfo>

If your account information is not updated within **48 hours** then your ability to sell or bid will become restricted.

Thank you

The Billing Department .

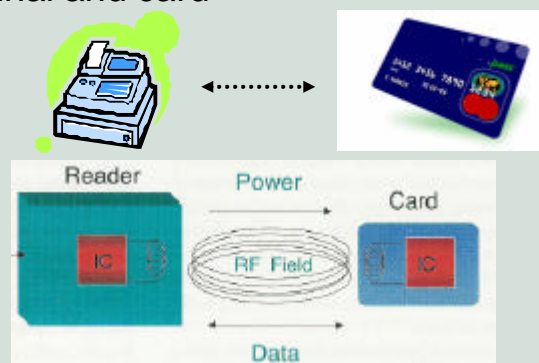
"Courtesy of Indiana University."

Security Testing

# Protocol attack



- Consider a contactless payment card
- A crypto-protocol runs between payment terminal and card



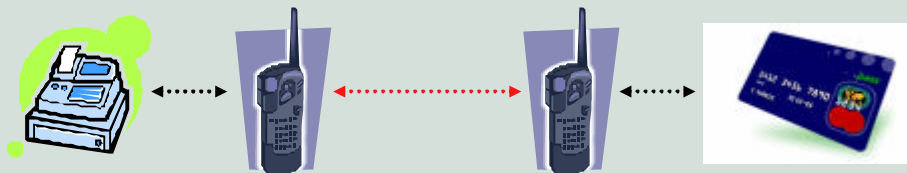
Security Testing

## Protocol attack



### Relay-attack:

- Attackers use radio-connected contactless devices to increase distance artificially
- Crypto protocol does not detect relay
- Charge remote card without owner consent!



Security Testing

## Vulnerability attacks



- Abuse weaknesses in implementation
- Design may be open or closed, bugs may be known or guessed
- Exploit obtains access rights, retrieves secrets or performs illegal modifications

Security Testing

## Example vulnerabilities in PIN verification



```
public boolean check( byte[] pin, short offset, short length )
{
    if (try_cntr > 0 && length == pin_size)
    {
        if (Util.arrayCompare(pin, offset, card_pin, (short)0, length ) == (byte)0)
        {
            try_cntr = try_limit;
            validated_pin = true;
            return true;
        }
    }
    validated_pin = false;
    try_cntr--;
    return false;
}
```

Security Testing

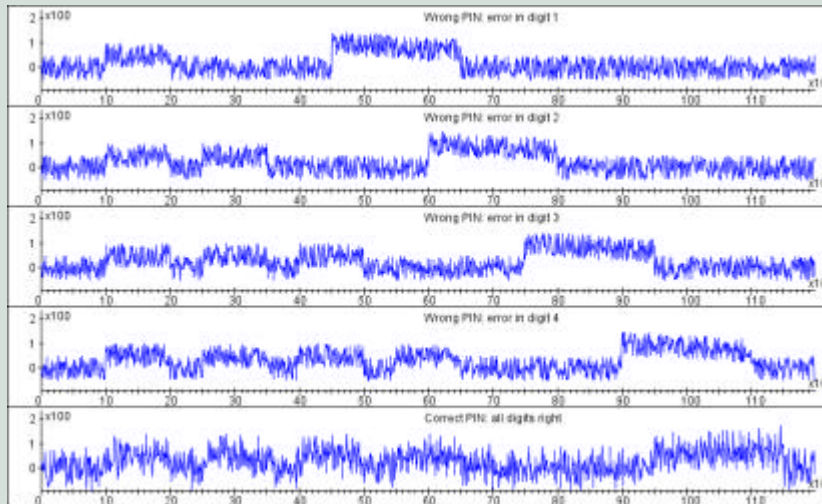
## Side-channel Attacks



- Systems are designed to communicate over defined interfaces
- Practical implementations have unintended side channels that can be abused to obtain information or manipulate behaviour
- Example side channels:
  - time
  - power consumption
  - radiation

Security Testing

## Timing attack on PIN

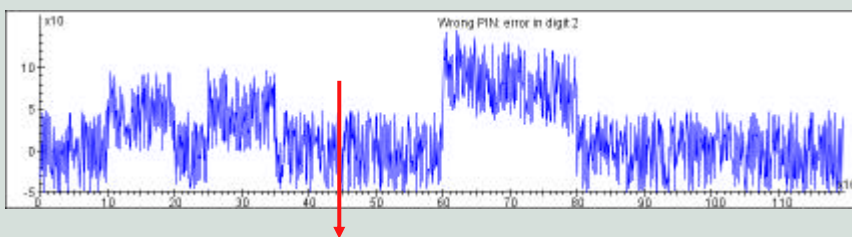


Need only 20 tries instead of 5000 to find PIN

## Power manipulation attack



Switch off power before decreasing counter



Switch off now!

... and find PIN without any failures

Security Testing

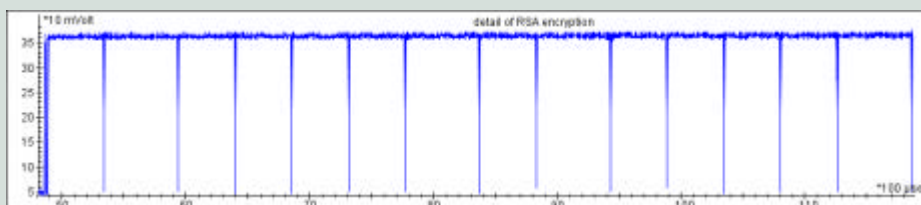
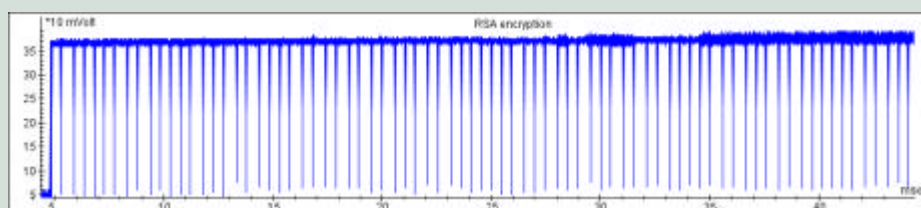
## Time-Power attack on RSA (1)



- RSA is based on exponentiation ( $C = M^k$ )
- Binary exponentiation:
  - $C := 1$
  - For each key bit  $k_i$  do:
    - $C := C * C$
    - If  $k_i = 1$ , then  $C := M * C$
- Multiplications performed by numerical co-processor

Security Testing

## Side Channel Attacks Time-Power attack on RSA (2)



1 0 0 0 1 1 0 0 0 1

Security Testing

## Conclusion



(Smart card) security testing:

- is risk based, not function based
- is very diverse and involves a lot of expertise: software engineering, electronics, cryptology, physics & mathematics
- is still developing and facing significant challenges with respect to: systematics, automation, quality and coverage.

Security Testing

## Thanks!



Want to know more?

Email [witteman@riscure.com](mailto:witteman@riscure.com)

or visit [www.riscure.com](http://www.riscure.com)

Several smart card and security related articles can be downloaded

Security Testing