

ID TECHNOLOGY
PARTNERS

"we make ID work"

Smart Card Security Past, Present and Future

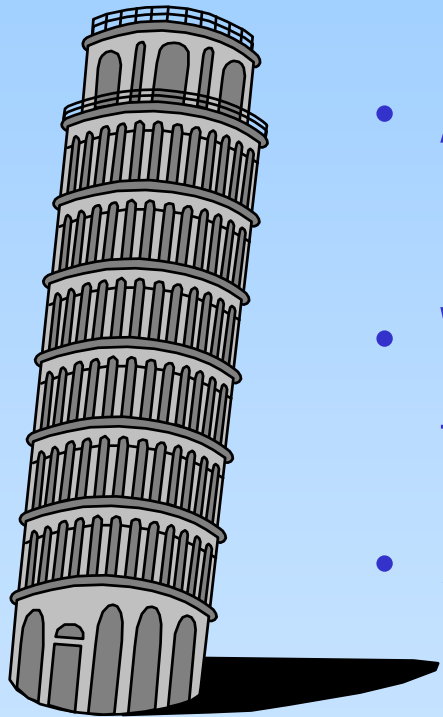


Gilles Lisimaque

Partner

GLisimaque@idtp.com

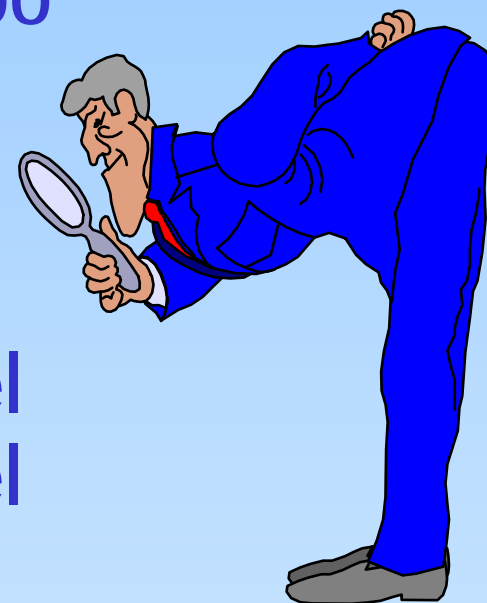
Absolute Security is a myth



- A system is only as secure as its weakest point
- What is secure today may be broken tomorrow
- Security has a cost and it is up to each business to decide the level of risk (as well as level of fraud) it can cope with

Security is an Attitude, not a Position

- A perfectly secure system is always too *expensive* (when it can be defined)
- The ideal system should be able to *detect* fraud and move to the next level of security when an unacceptable level of risk is detected



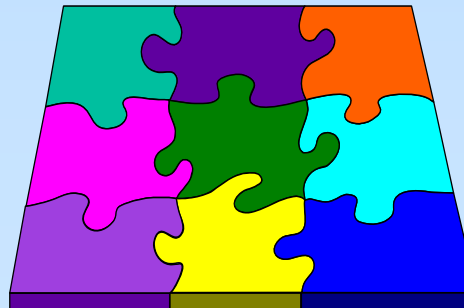
Smart Cards allow various level of security to exist in an existing application without changing the whole system

Some Attacks Announcements in the press

- March 1994 - Phrack Magazine (Volume Seven, Issue Forty-Eight, File 10 of 18)
Electronic Telephone Cards: How to make your own!
- Dec. 1995 - "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems", Paul C. Kocher,
- Sept. 96 - "Fault Analysis" attack on public key systems - Bellcore
- Oct. 96 - "Differential Fault Analysis" on DES - Weizmann Institute
- June 98 - Differential Power Analysis on Smart Cards by Paul Kocher
- March 2000 - RSA private signature key of the French Banking cards published on the Internet
- May 2002 - Optical Fault Induction Attacks in Smart Cards by Sergei Skorobogatov and Ross Anderson
- August 2000 - FBI dismantles a ring of illegal smart cards resellers for Direct-TV decoder boxes
- May 2002 - IBM attack of GSM SIM cards using side channels (optical fault attack)
- RSA 2004 - Demonstration of JavaCard memory dump by Marc Witteman (Riscure)
- Feb 2007 - "PIN & CHIP" Attack in UK using fake bank terminals
- March 2008 - Mifare Classic is found using a weak key (48 bits) by Karsten Nohl
- August 2008 - EMV terminals found with an "extra chip" used to capture PINs

The Smart Card is part of a bigger system

- A smart card application consists of
 - Cards
 - Security application modules
 - Terminals
 - Collection devices
 - Network(s)
 - Node computers
 - Back end system
- But also of
 - Software
 - In cards
 - In terminals
 - In back end systems
 - Policies
 - Security surveillance
 - Administration activities
 - Key management
 - Personalization



The card is a soldier in the field



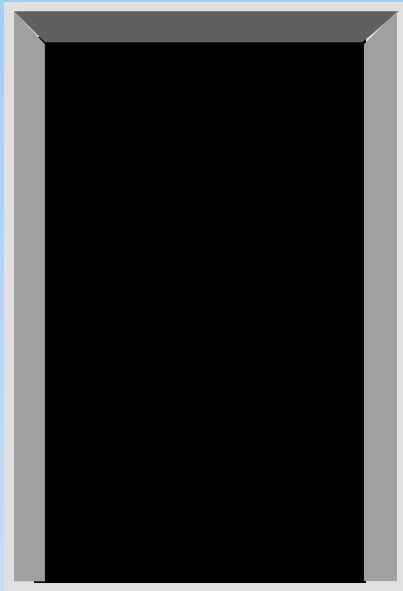
- As for any war, a soldier alone can be easily defeated. The smart card is part of a system which will hold even when one soldier is down.
- The smart card is the first line of defense in any application and the system as a whole is involved in the security.
- When one card is defeated, the system should be designed to detect the breach and contain the damage to a minimum.

Security is team work



- ***Smart card security*** relies on:
 - The hardware security of the component used
 - The software design used in the card for its OS
 - The secure procedures used during development, Initialization and issuance
 - Execution of algorithms using keys protected by the card
 - Self locking mechanisms in the card when under attack
- ***System security relies*** on:
 - The security of each individual smart card
 - The low cost of the card allowing replacement when one card has been broken
 - The fraud detection mechanisms built in the back-end
 - Traceability and accountability of smart cards

Security is not a chopper's list

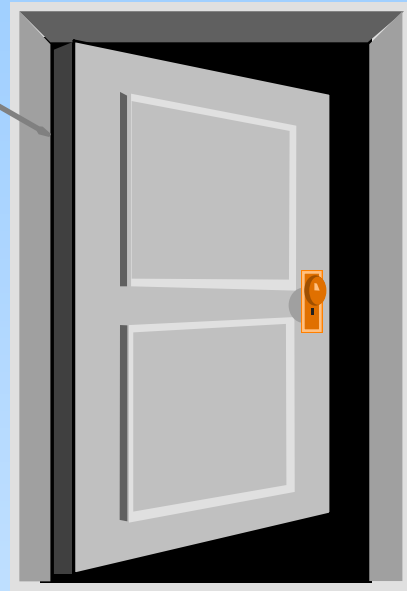


secure

+



secure



may be flawed

Combinations of individually secure building blocks are not necessarily secure

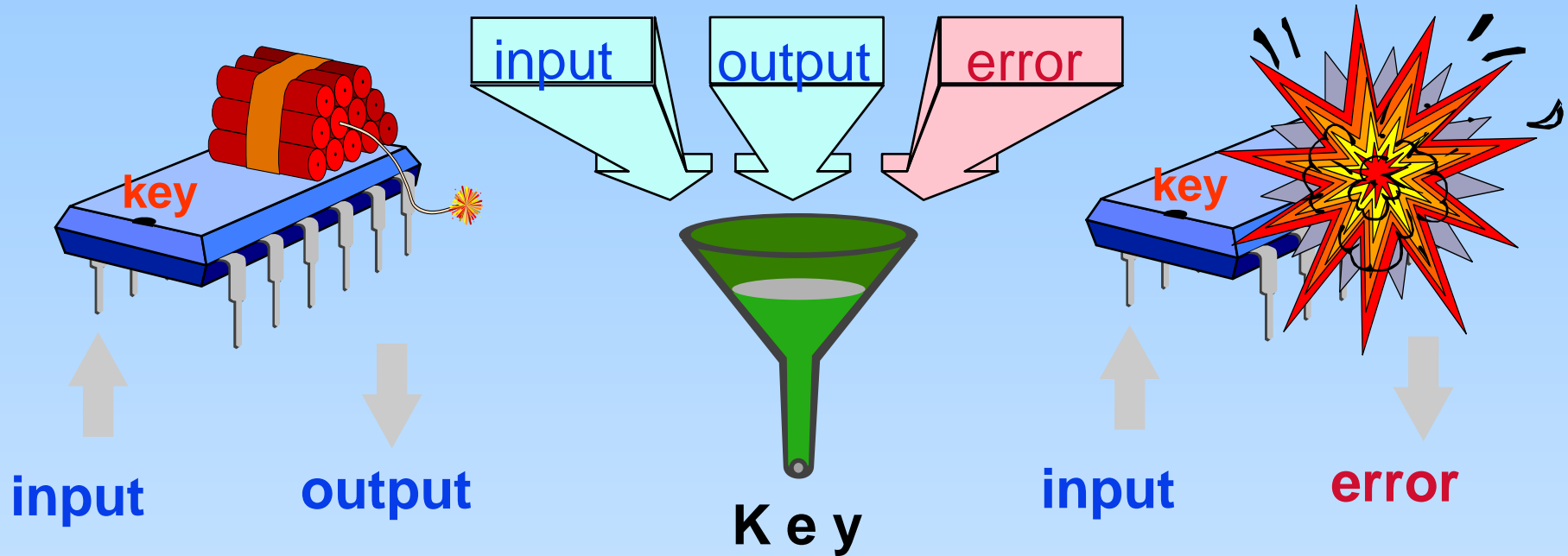
Attacks on Smart Cards

- External attacks
 - Modifying operational conditions
 - Monitoring signals of the chip
- Internal attacks
 - Monitoring signals inside the chip
 - Forcing internal signals
 - Reading memory locations



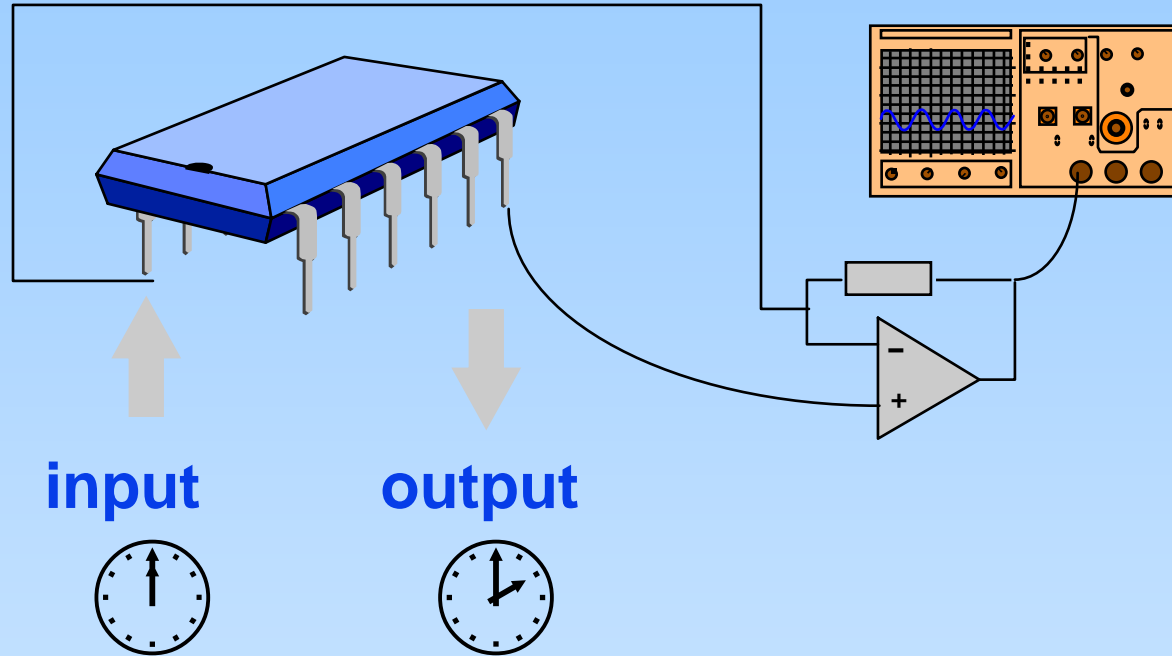
An attack on the chip requires an important investment in time and resources and gives access to only one card, not the whole system

Fault Inoculation



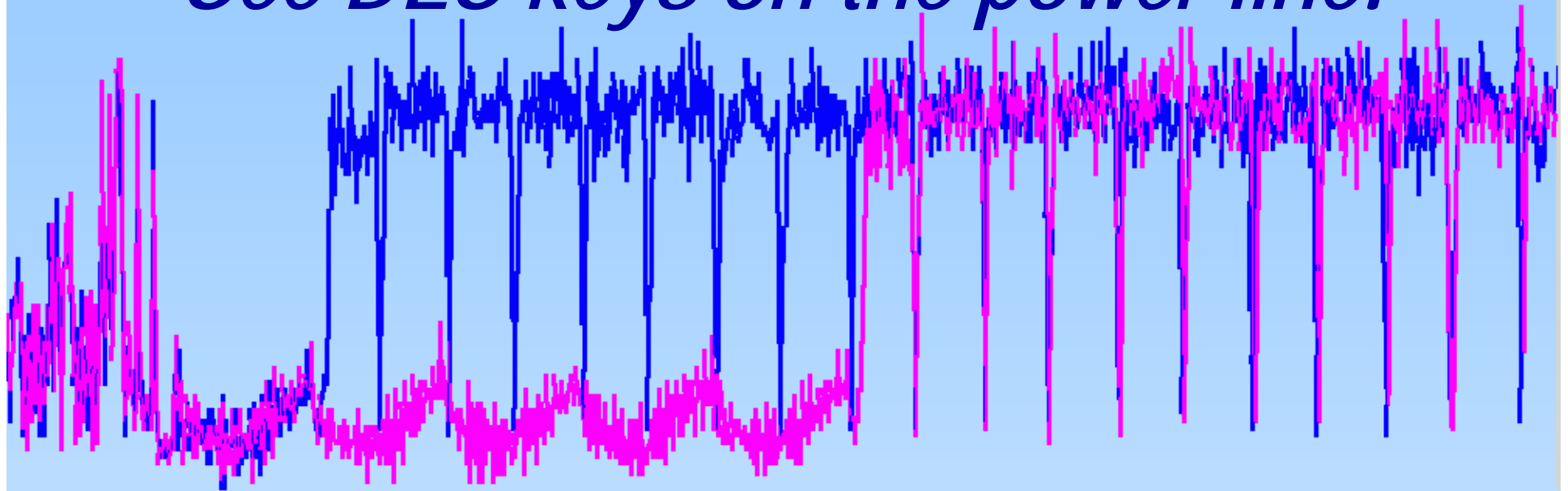
***Provoke a hardware failure,
analyze the error and infer secret data***

Behavior Patterns



Measure the circuit's processing time and current consumption to infer what is going on inside it

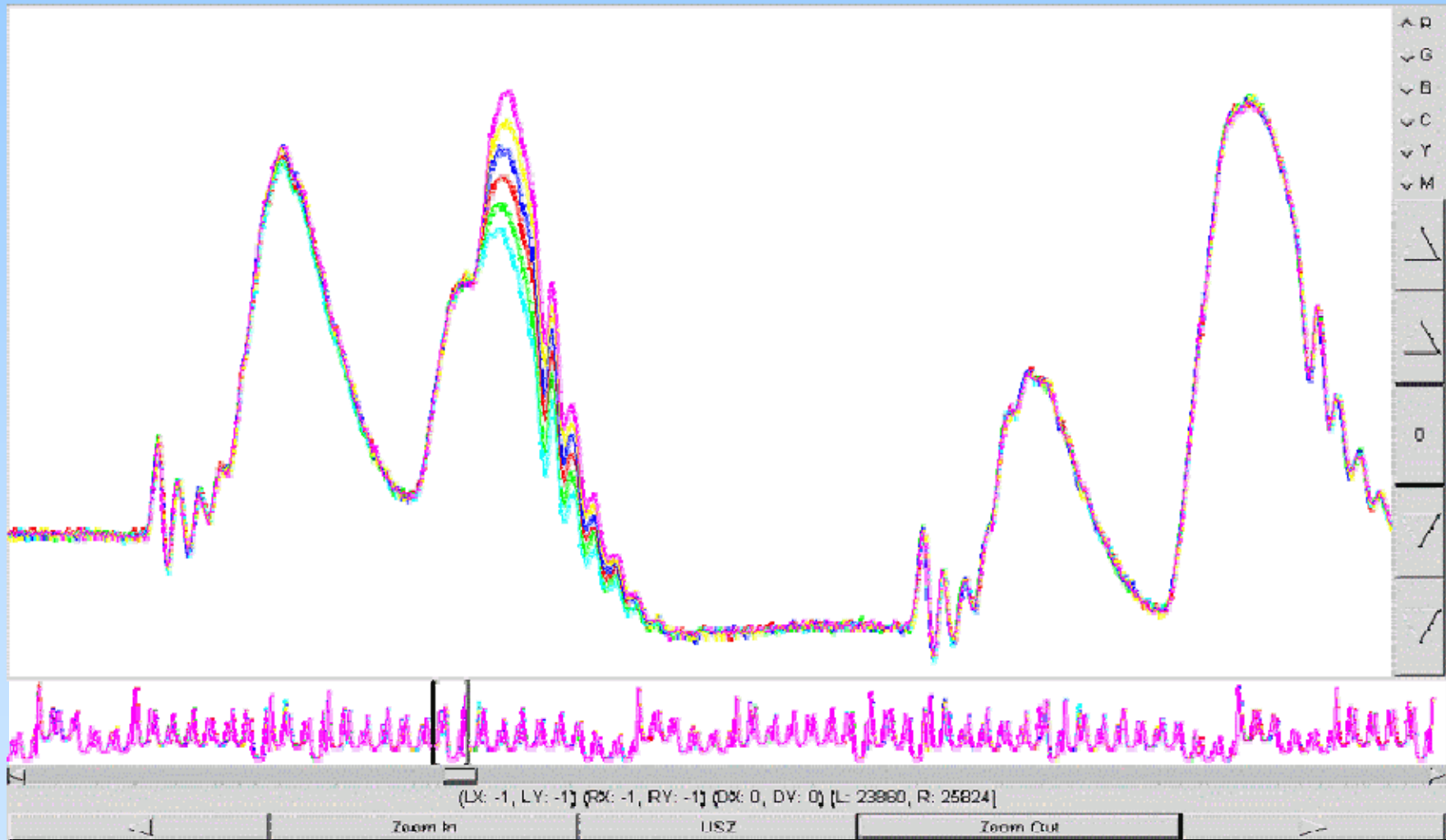
See DES keys on the power line!



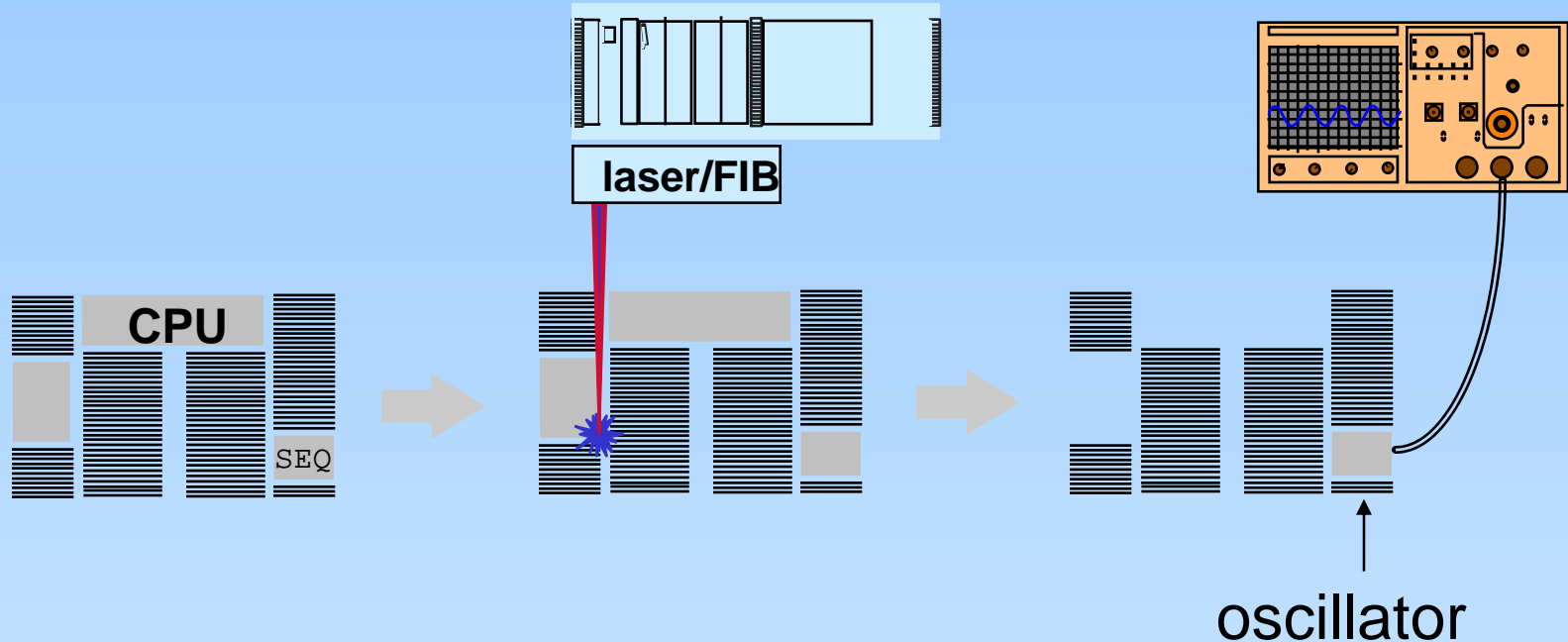
Current measured on an old microcontroller executing single DES with two different keys

- Red: decryption with key = 0000 1111 ...
- Blue: decryption with key = 1111 1111 ...

Power as a Function of the Hamming Weight

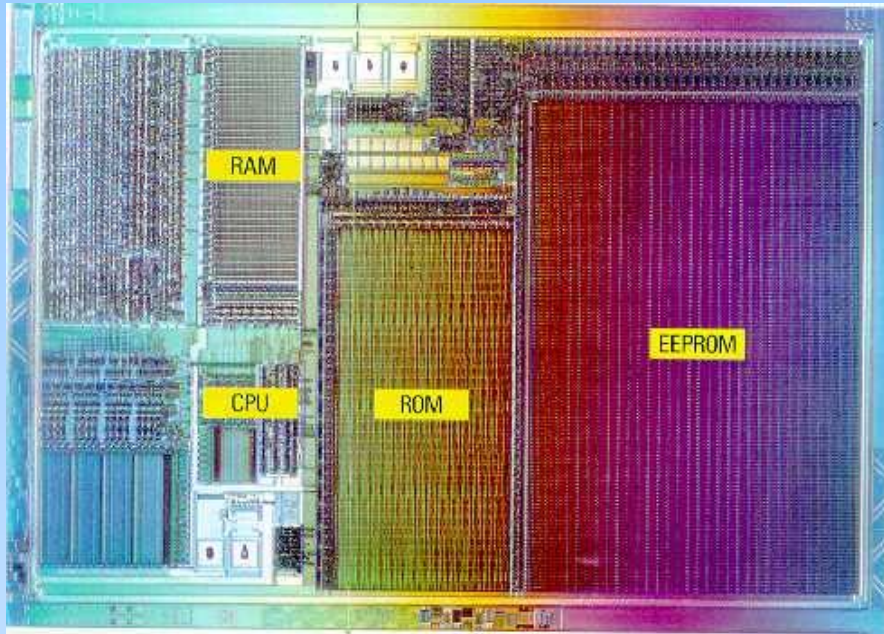


Microprocessor Mutilation

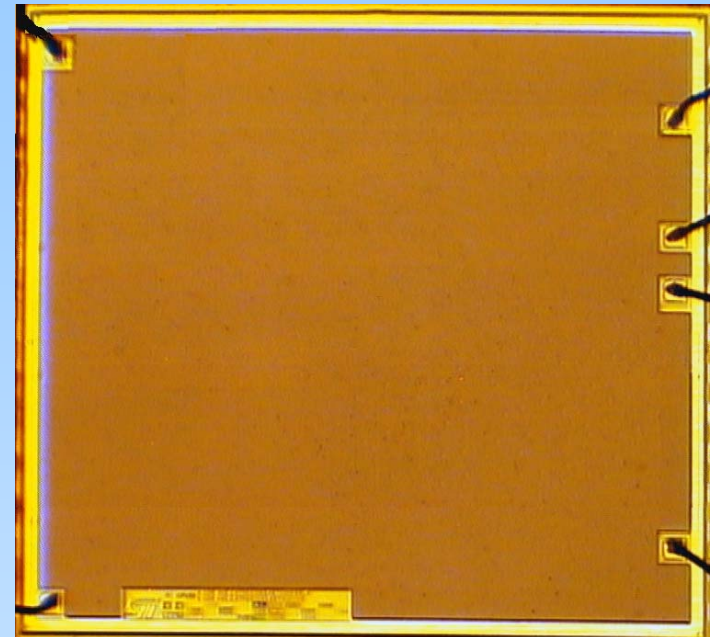


Cut the card's microprocessor free from the address sequencer and wait for it to dump the entire address-space

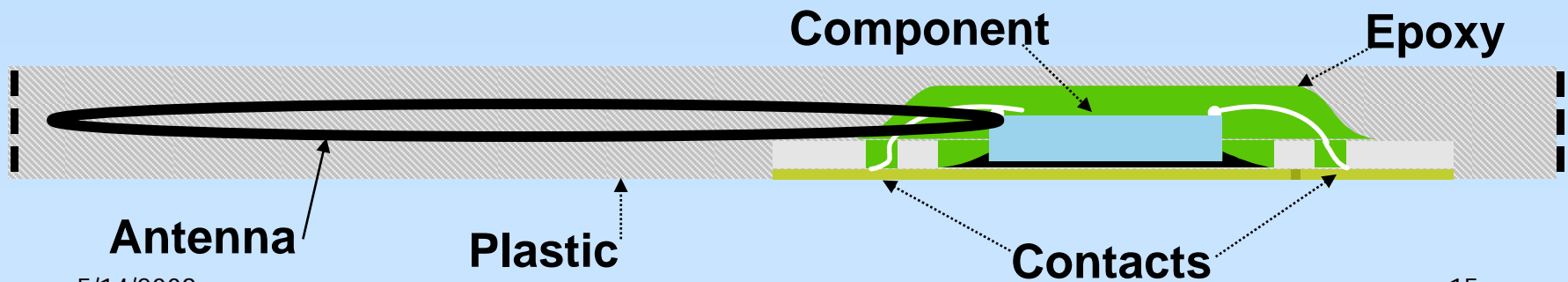
A chip build to serve & protect



DESIGN IN 1996



DESIGN IN 2000



Security Certification of Smart Cards

- In Europe Common Criteria are widely used
 - A ***Protection Profile*** defines the type of protection a group of applications has to consider
 - A ***Security Target*** is defined by the vendors on the ***Target Of Evaluation*** (TOE) proposing products addressing the Protection Profile
- In the United States, Government smart cards have to be FIPS 140 certified which takes a different approach

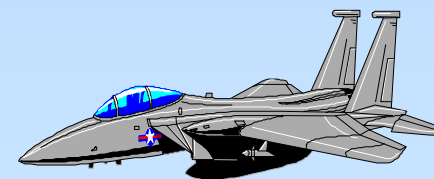
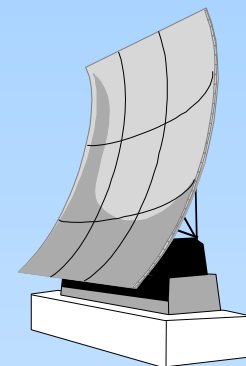
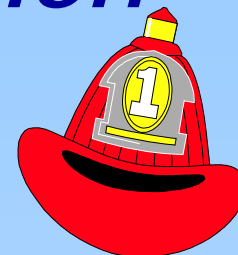
http://www.ssi.gouv.fr/site_documents/pp/pp0103.pdf

http://en.wikipedia.org/wiki/Common_Criteria

<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

Protection, Detection, Reaction

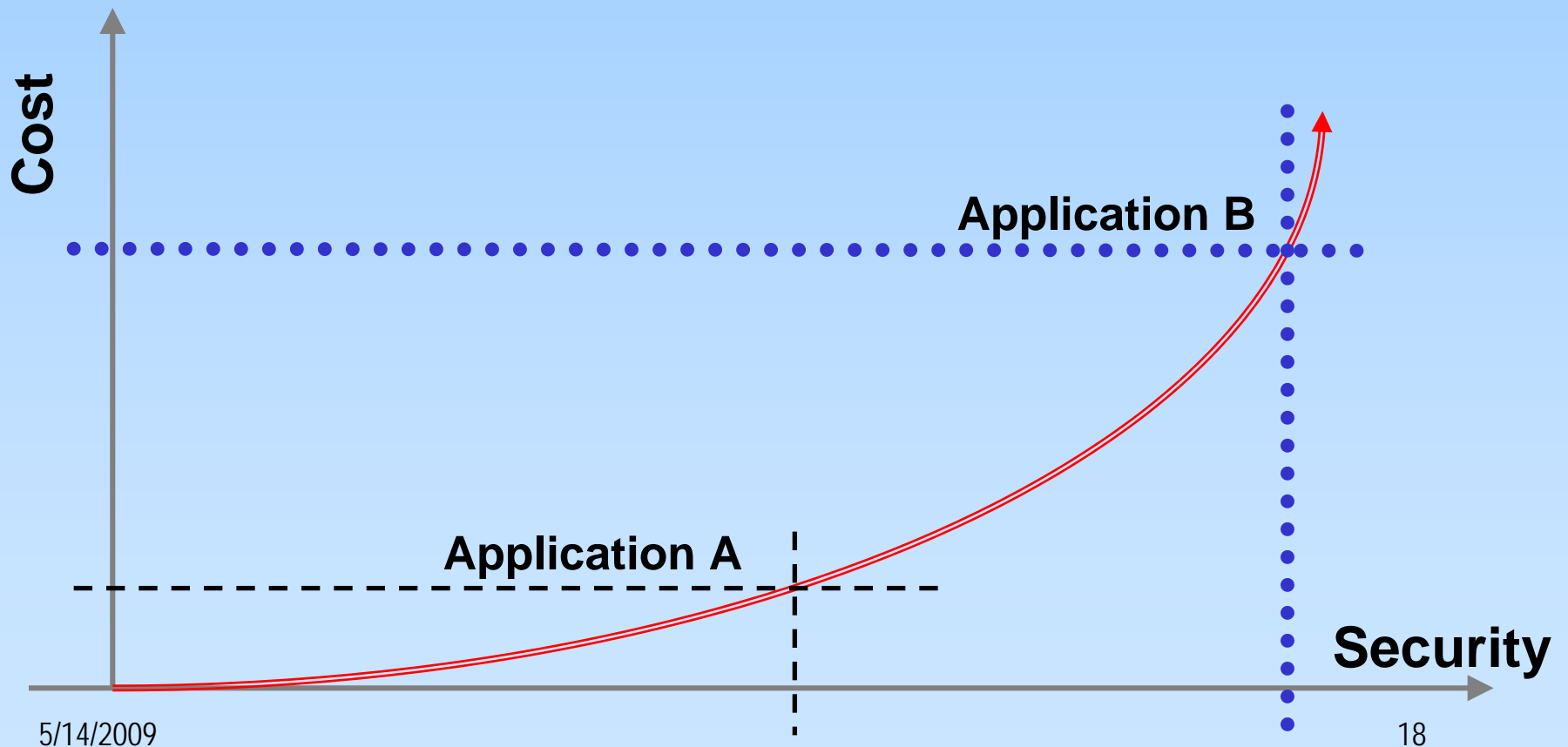
- *Smart cards*, along with cryptography, provide a very high level of ***protection*** against fraud
- The ***back-end system*** must provide an appropriate level of fraud ***detection*** as well as traceability when required
- The whole ***application***, including procedures, should provide a possibility of ***reaction*** when fraud is detected



Security is a Business Decision

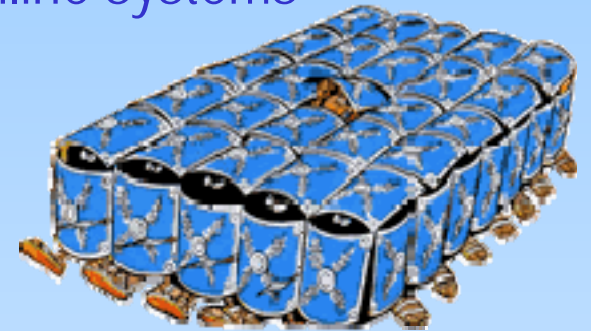
Maintaining Customer Confidence
Recovering from Security Breaches

Detecting Security Breaches
Securing Card Transactions



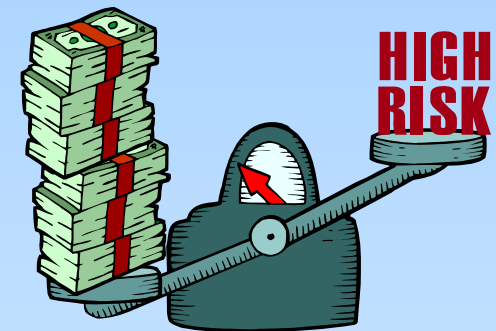
Each Application has its own Security Needs

- Payment
 - Limit the level of fraud to an acceptable level using either smart cards in offline systems or a strong back end transaction risk management software in online systems
- Pay-TV
 - Detect and track the fraud when its level is too high mainly by market monitoring
- Cellular Phones
 - Prevent as much as possible (with smart cards) and detect when it happens (in the back end) subscription clones
- Identification
 - Smart Cards protecting the personal information with strong device authentication combined with trusted user biometrics



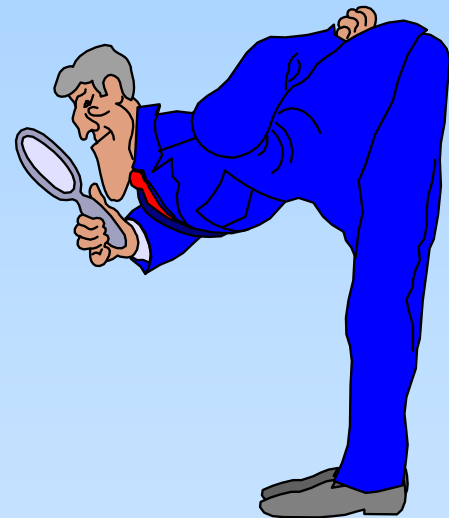
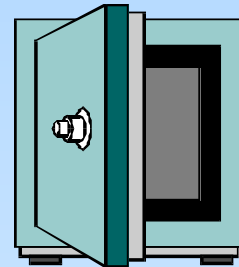
Risk Assessment

- Threats
 - Who is the adversary ?
 - What capabilities does he have?
 - What are the overall risks?
- Vulnerabilities
 - What could be a target in the system ?
 - What would be helpful for an attacker ?
 - What is the system more sensitive to ?
- Countermeasures
 - What could be done to eliminate or minimize a vulnerability?
 - What could be designed to contain/limit the risks?
 - What are the costs and the business risks?



Other Areas to Watch out For

- Security of Card Manufacturer
- Security of Card Personalization
- Loading software into Chips
- Card Life Cycles
- Hackers and PR
- Multiple Applications on Single Card



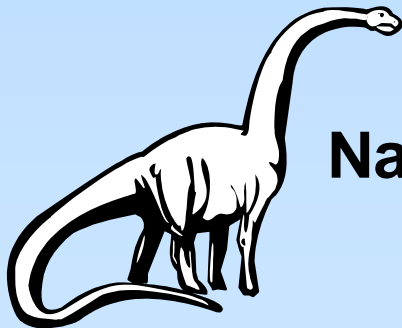
The Next Security Level

- Smart Cards with a source of power on board allow to increase the level security as:
 - It provides a *trusted time* reference to the card
 - It allows the card to commit suicide when an attack is detected
 - It allows the card to display information on a *trusted interface*
 - It allows the card to always be “on the watch”



The Advantages of Smart Cards

- Secure and active intelligent component
- Enforces the business rules of the application even when used offline
- Very expensive to attack for a low cost device
- Allow system security to adapt and evolve



Nature has proved to us that the only way to survive is to adapt and evolve

