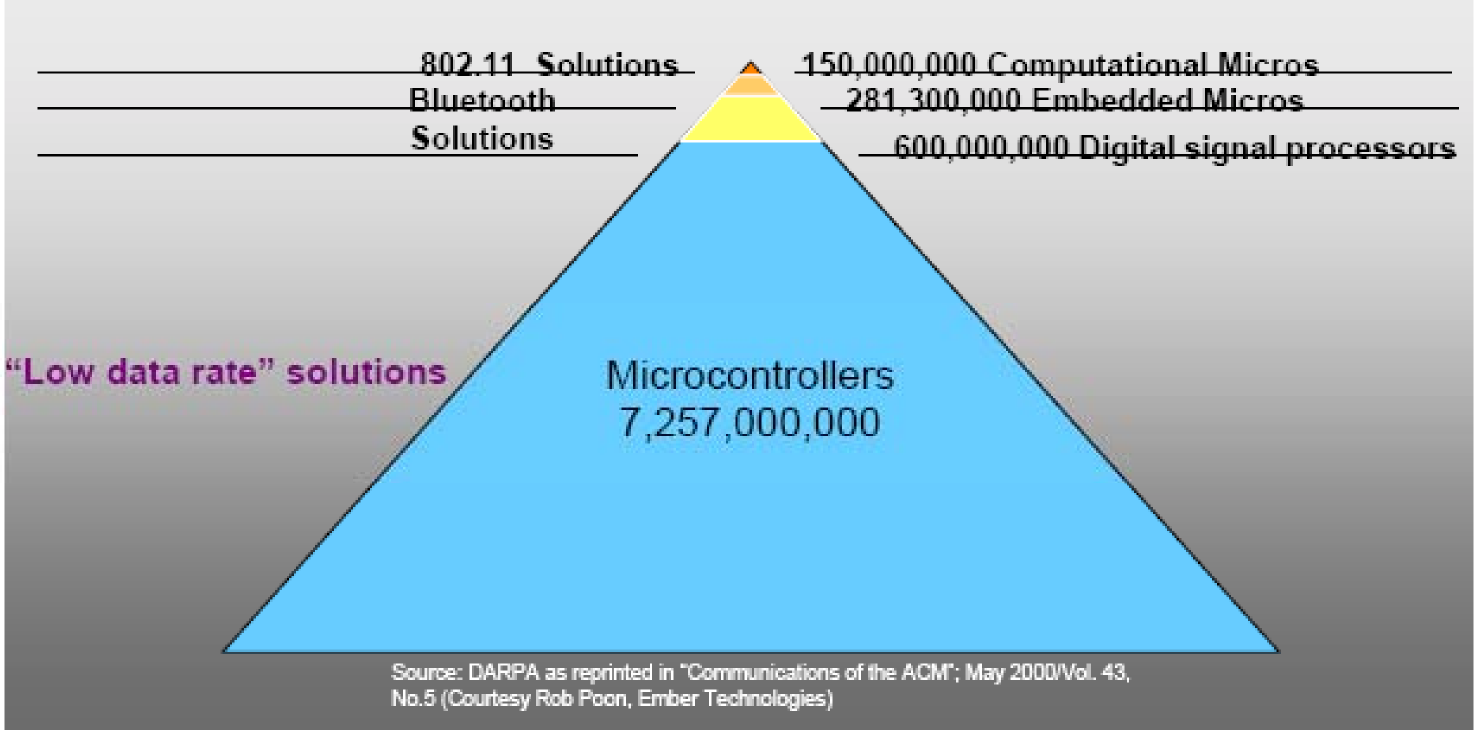
Security in Embedded Systems – Challenges and Oportunities

Octavio Nieto-Taladriz García - nieto@die.upm.es
Laboratorio de Sistemas Integrados
ETSI Telecomunicación - Universidad Politécnica de Madrid

Index

- Justification
- Attack – Countermeasure Race
- Conclusions

The market of embedded systems



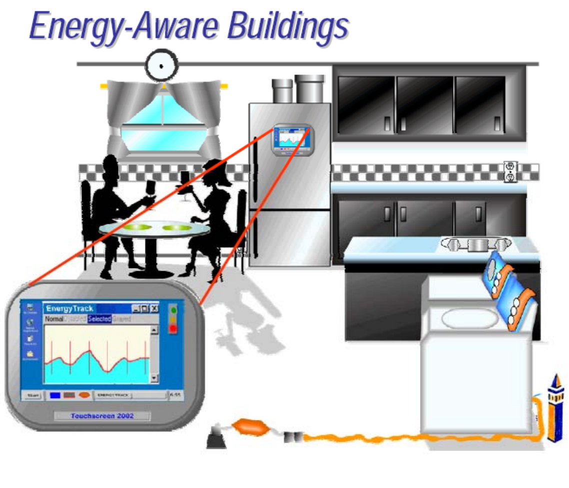
Key Metrics:

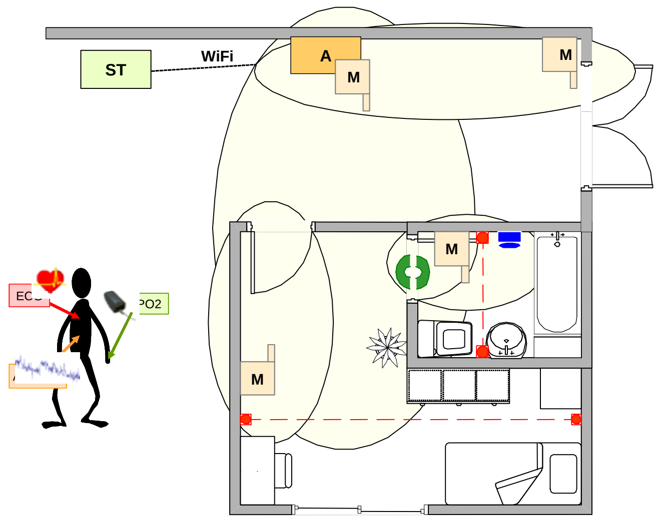
Cost, Size, Power, Reliability, and Ease of Use

Berkeley Wireless Research Center

Embedded systems everywhere

- **Ambient intelligence concept:**
  - o Security
  - o Medical
  - o Energy
  - o Comfort
  - o Etc.





Justification

- In embedded systems the security problems arise earlier:
  - o Reduced processing capability
  - o Strong limitation in available resources (batteries, small memories, etc.)
  - o Usually working in non secure environments
  - o Strong activity in security breaking technologies
- LSI background
  - o Wireless sensor networks
  - o Adaptable distributed systems

Security requirements

- Common requirements:
  - User identification
  - Network secure access
  - Secure communications
  - Secure information storage
  - Availability
- Specific system requirements

Embedded Systems Requirements

- High demand of the actual cipher algorithms
  - Security processing gap
- Flexibility and interoperability
  - Adaptability against attacks
- Power consumption
  - New cipher algorithms
    - AES or IDEA better in key establishment
    - Blowfish better in cipher
  - Battery life increase 5-8% per year

StronARM SA-1110 @206Mhz applying a 10% resources to SSL session would get 189 kbps

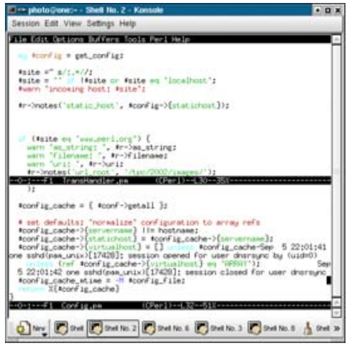
Pocket PC wit 3DES and SHA uses 21% of power resources to security

Taxonomy of security attacks

- Functional objectives:
  - Privacy attacks
  - Integrity attacks
  - Availability attacks
- Agents (Actives and passives):
  - Software attacks
  - Physical attacks
  - Lateral attacks – Execution time, power consumption and failure behavior

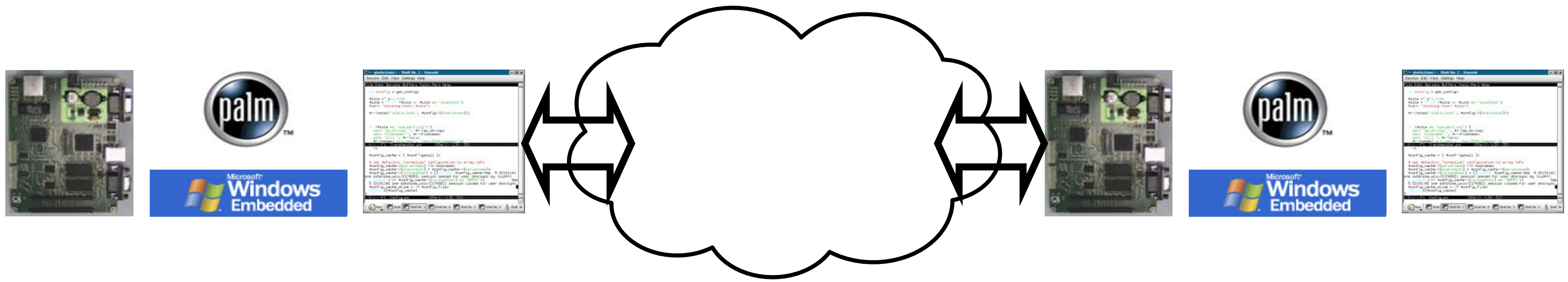
Initial Scenario

- **Embedded system with communication capabilities**



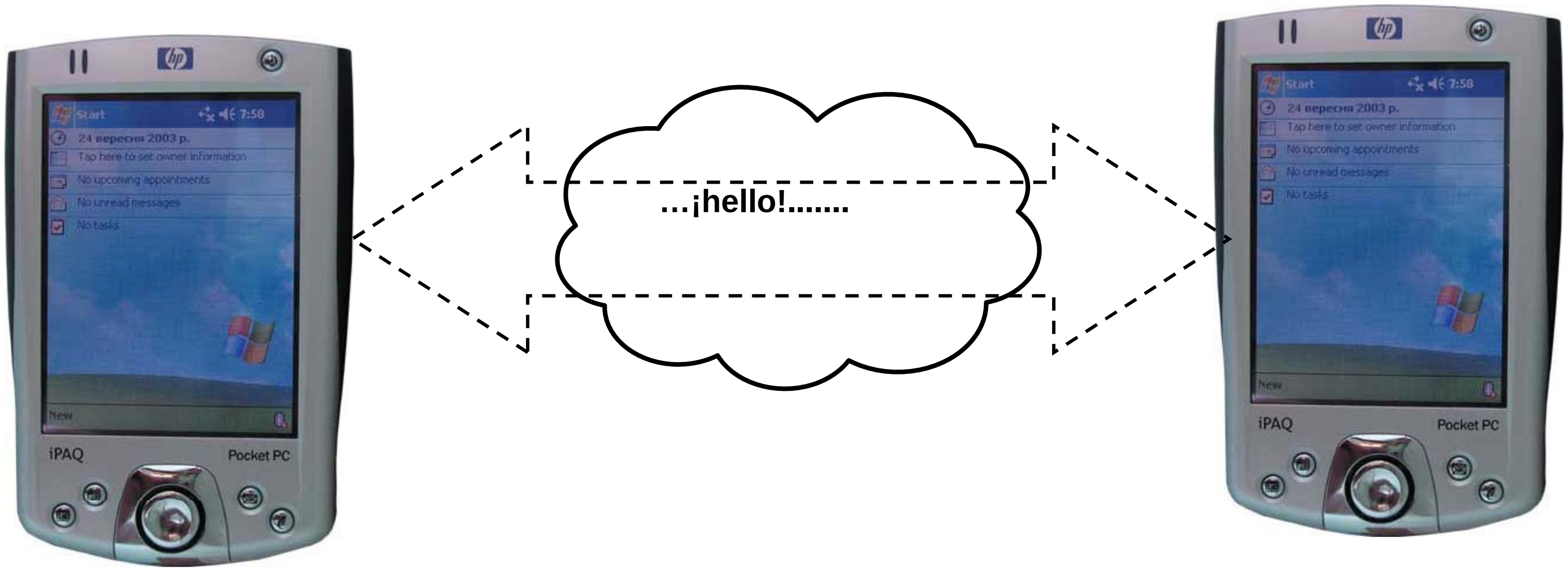
Initial Scenario

- **Embedded system with communication capabilities**



Initial Scenario

- **Embedded system with communication capabilities**



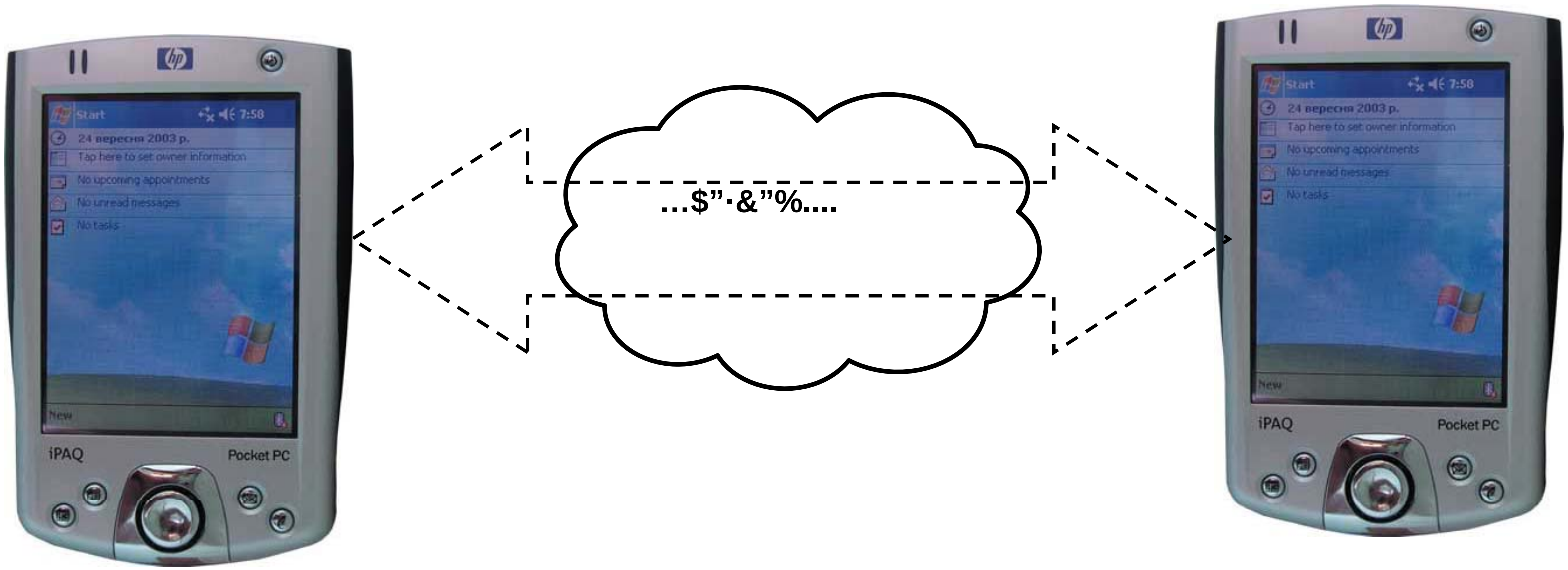
Threats

- **System**
  - o **Intrusion**

- **Communication channel**
  - o **Listenings**

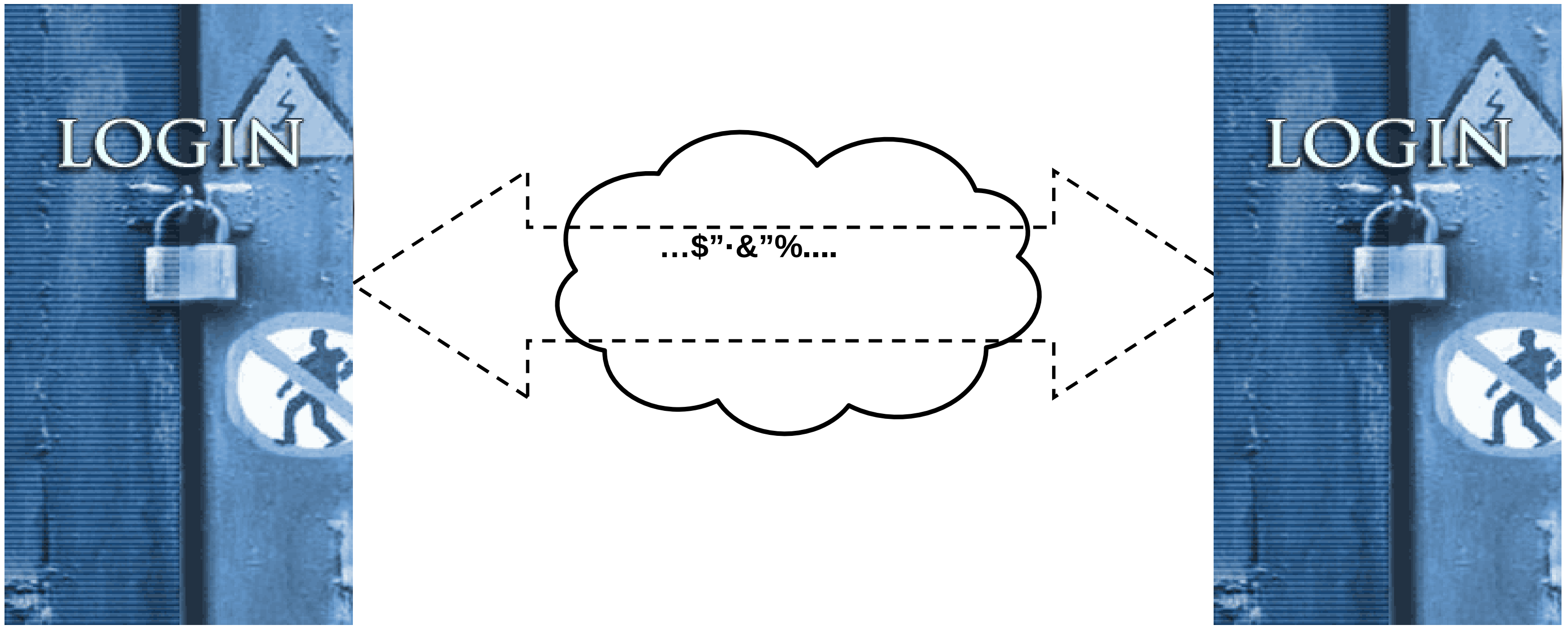
Security – First attempt

- **Cipher algorithm**



Security – First attempt

- **Authentication**



Security – First attempt

Is the System SECURE?

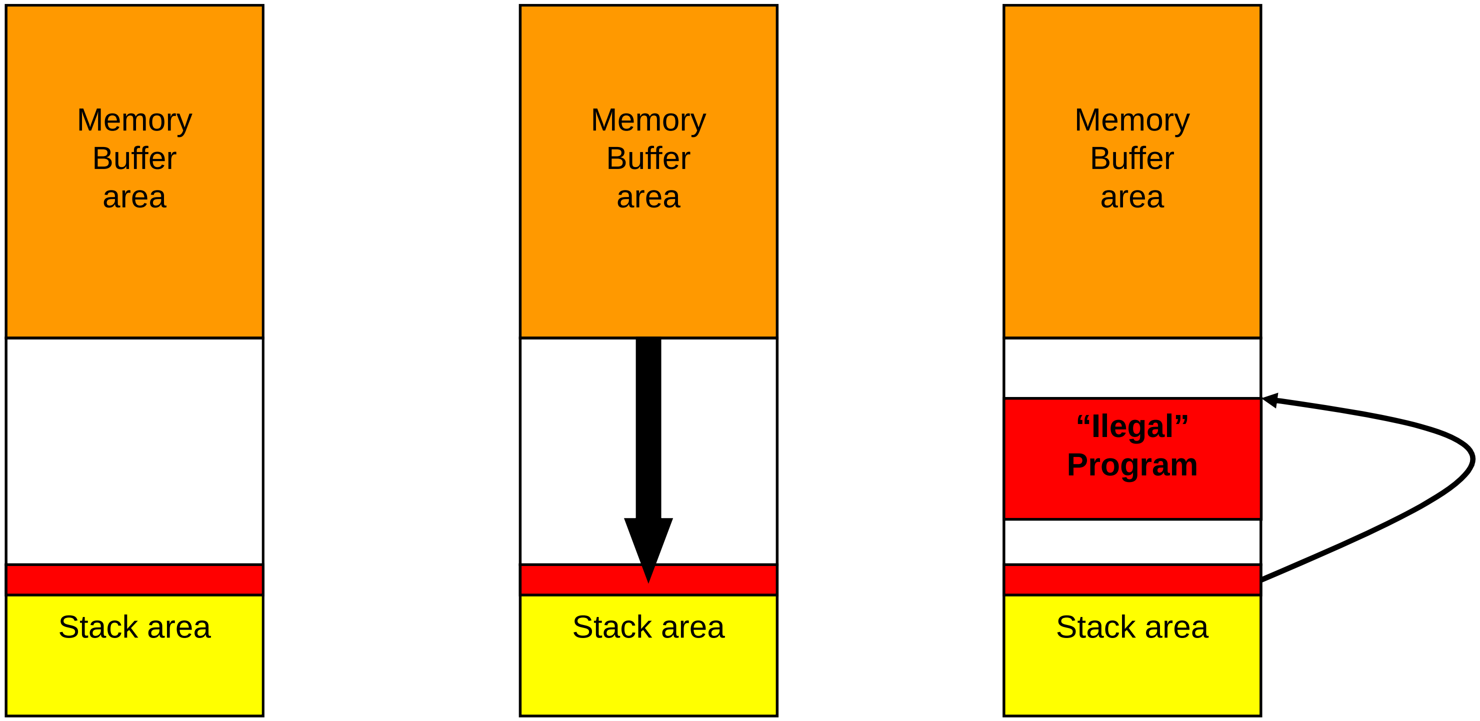
Logic attacks

- **Objective:**
  - o Execute a program in the system
- **Way:**
  - o Exploit the system weaknesses
- **Example:**
  - o Buffer overflow

Buffer overflows

- Search variable size data storage areas in the system memory
- Limits of the storage block can be override and it is possible to write in other memory areas
- If the stack, the dynamic memory area or the pointer to functions are overwritten, it is possible to execute arbitrary code

Buffer overflows



Countermeasures - logical attack

- Solution: Make the programs in the correct way:
  - Engineering instead of art
  - Formal techniques (verification and synthesis)
- Is it enough? NO

Timing analysis

- Objective:
  - o Discover the cipher key
- Way:
  - o Cipher algorithm execution time depends on the data
- Variation source:
  - o Algorithm
  - o Processor instruction set (ie. modular exponentiation uses processor multiplications and divisions that are in time data dependent)
  - o Compiler optimization (i.e. Chinese Rest Theorem)

Countermeasures – Timing attack

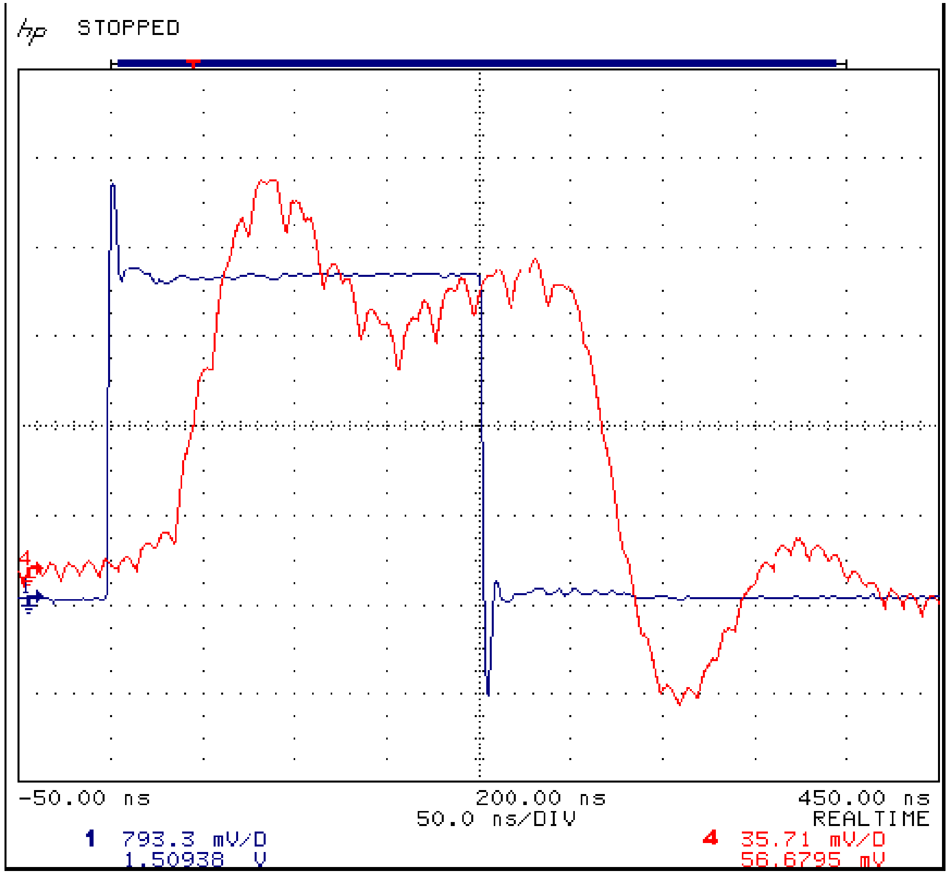
- **Solution:**
  - o Timing balance
  - o Introduction of random delays

- **Price to pay: Performance degradation!**

Simple power analysis (SPA)

- **Objective:**
  - Get the cipher key
- **Way:**
  - Power consumption depends on the switching activity
  - Switching activity depends on the input data
  - Capture the power consumption temporal evolution

Simple power analysis (SPA)

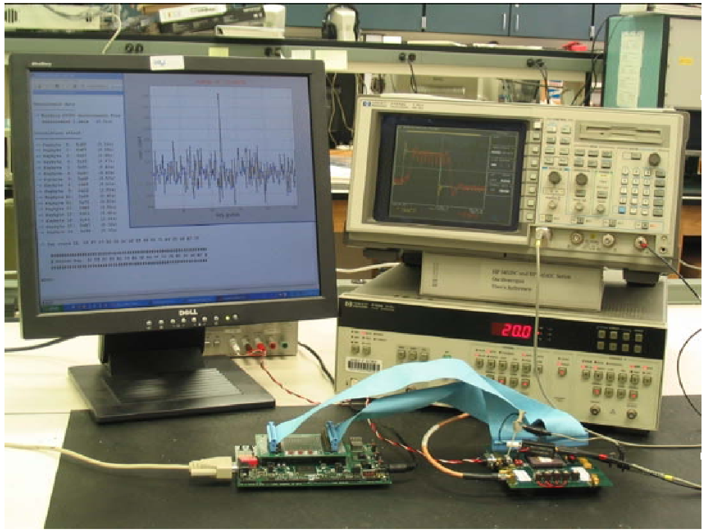


Countermeasures - SPA

- **Solution:**
  - Decrease the signal to noise ratio:
    - ❑Reduce the signal levels
    - ❑Execute additional programs
    - ❑Power management unit

Differential power analysis (DPA)

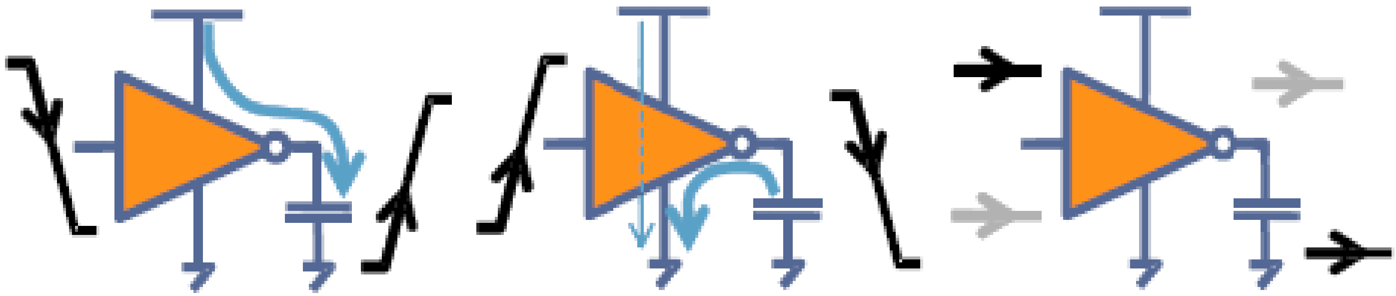
- Performs an statistical analysis
- Hypothesis are confirmed by statistical correlation
- Robust against measurement inaccuracy
- Good results with high noise



i.e. 8.000 ciphers to discover a 128 bit AES key

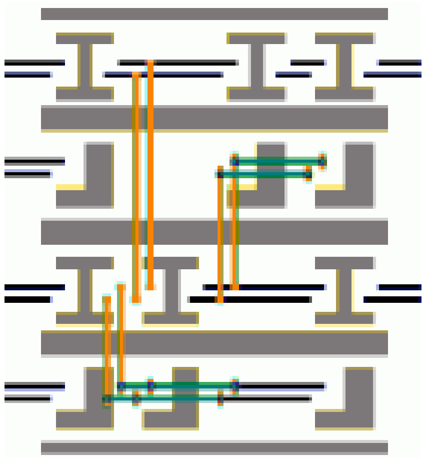
Countermeasures - DPA

- **Problem: Asymmetrical CMOS power consumption**



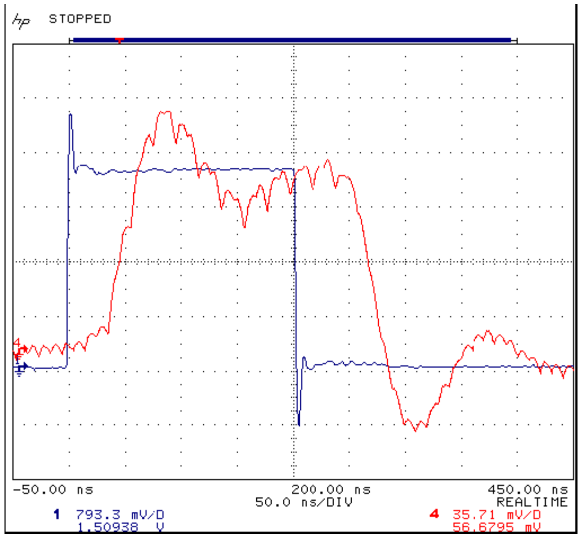
Countermeasures - DPA

- **Solution:**
  - o Dynamic differential logic
    - ❑Switching activity
  - o Differential routing
    - ❑Constant capacity

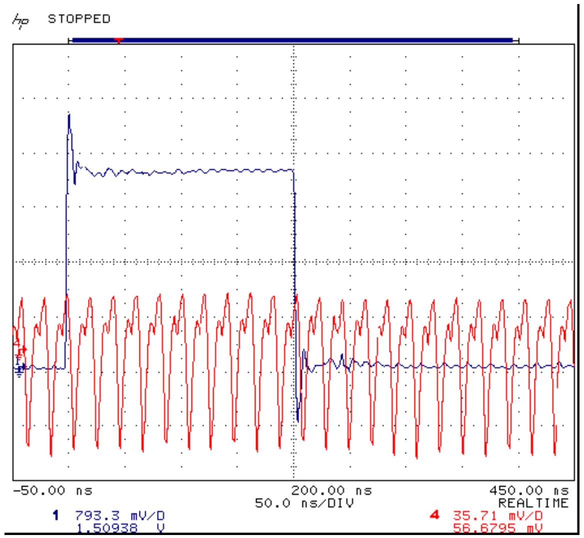


Countermeasures - DPA

AES without protection

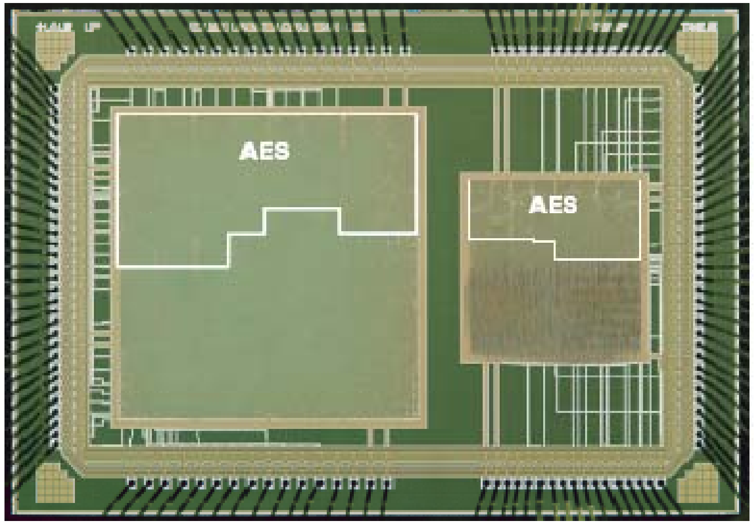


AES with protection



Countermeasures - DPA

- **Heavy increase in area and power consumption**



But….

Is the System SECURE?

Other attacks…

- Physical attacks (Special packages)
- Electrical attacks (Power supply voltages)
- ASIC reverse engineering
- Fault injection
- Electromagnetic emission analysis (Tempest)
- Safe power on?
- …

Summary

- The attacks look for asymmetries:
  - o SW architecture, algorithm, compiler, HW architecture, logical design , chip routing, behavior in abnormal conditions.
- Remove asymmetries implies the mixture of different knowledge domains

Conclusions

- Security: A new dimension in the design process
  - Cost, features (performances), power consumption, security
- Need to define a design flow tolerant to security attacks