Tamper resistant devices

Levente Buttyán, László Csik
Laboratory of Cryptography and System Security (CrySyS)
Budapest University of Technology and Economics
{levente.buttyan,laszlo.csik}@crysys.hu

Tamper Proof Modules - Overview

- Reminder of the previous presentation
  - Why are they required
  - How to measure them (FIPS-140)
- Classification of attackers
- Classification of attacks
  - Invasive attack
  - Local non-invasive attack
  - Semi-invasive attack
  - Remote attack
- Example tamper proof devices
  - Smart Cards
  - IBM Cryptoprocessor
- Conclusions

Necessity of a Tamper Proof Module

- Implementing security services in vehicular networks requires cars to store sensitive data [RayaH05sasn]
  – Cryptographic keys (secret keys, private keys), event logs, …
- Sensitive data needs to be protected from unauthorized access
- Cars operate in a *hostile environment*
  – Unsupervised access to all parts of a car by potentially malicious parties (car owners and maintenance service providers) is possible
  – There may be incentives to compromise the data (e.g., to modify event logs by the car owner, extract private keys)
- Logical AND Physical attacks should be *prevented*
  – If physical attack is easy, there is no use of logical security

→ Tamper resistant hardware in cars is required!

Measuring a Tamper Proof Device – FIPS-140

- Benchmark standard that specifies the security requirements for cryptographic modules
- level 1
  - Basic requirements on cryptographic algorithms
  - No physical security mechanisms are required in the module
- level 2
  - Needs tamper evident coating or seals and role based access control
  - OS evaluated at CC level EAL2 (or higher)
- level 3
  - Physical security preventing unauthorized access to sensitive data
  - Requires identity based access control
  - Data ports used for critical security parameters must be separated
  - OS evaluated at CC level EAL3 (or higher)
- level 4
  - Highly reliable tamper detection and response (erasing all secret data)
  - Protection against a compromise due to environmental conditions
  - OS evaluated at CC level EAL4 (or higher)

→These are only *required* properties

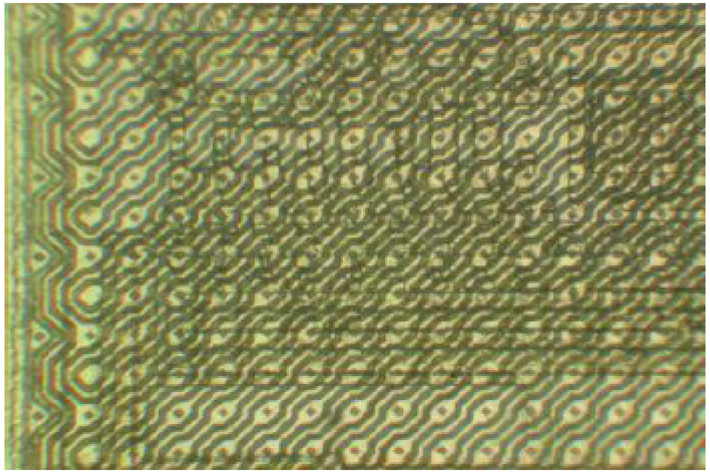
Classification of attackers

- Clever outsider
  - Intelligent but may have limited knowledge about the system
  - Access to moderately sophisticated equipment
  - Takes advantage of known weaknesses rather than create new ones
- Knowledgeable insider
  - Specialized technical education and experience
  - Varying degrees of understanding of parts of the system
  - Highly sophisticated tools and instruments for analysis
- Funded organization
  - Able to assemble teams of specialists with complementary skills
  - Advanced analysis tools
  - Backed by great funding resources

Invasive attacks

- This is a purely Physical attack against the chip
- It destroys the chip or at least leaves detectible signs
- Goals
  - Access on-chip signals
  - Extract data from the chip
- Used attacking techniques
  - Reverse Engineering
  - Microscope + Laser Cutter & Drill
  - Microprobing needles or electron beam testers

- Possible prevention:
  Tamper sensing membrane
  (Can trigger self-destruction)

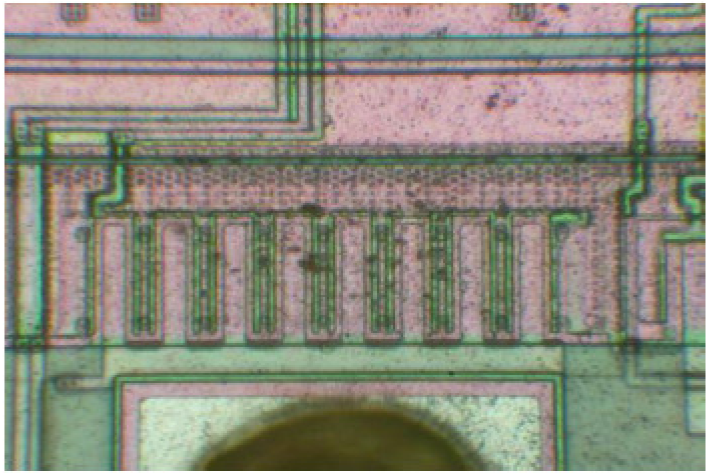


Invasive attacks II.

- For the invasive attack, the attacker should know the internal structure
  - He should navigate on the chip surface visually
- Old chips can be reverse engineered with a microscope

  →Reverse engineering should be hardened

- This can be achieved with Chemical-Mechanical Polishing



Local non-invasive attacks

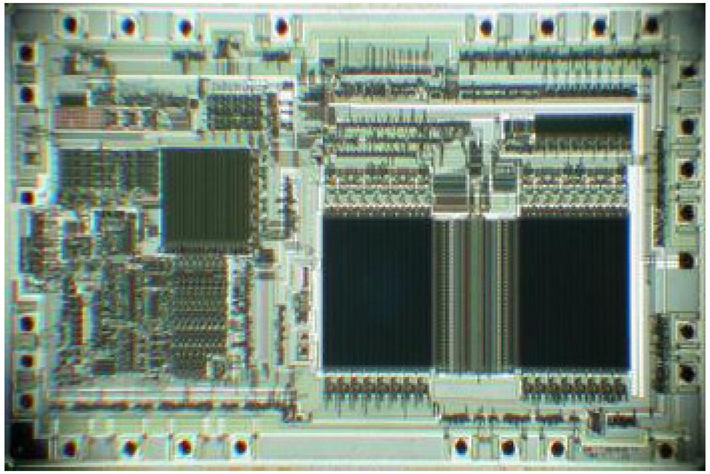
- Non-invasive attacks do not destroy the card
- Side-channel attacks
  - Careful observation of the interaction of the card with its environment during critical operations may reveal some amount of information about the sensitive data stored in the card
  - Examples: RSA timing attacks and power analysis

  → Randomized implementations
- Unusual operating conditions may have undocumented effects
  - Unusual temperatures or voltages can affect EEPROM write operations
  - Power and clock glitches may affect the execution of individual instructions

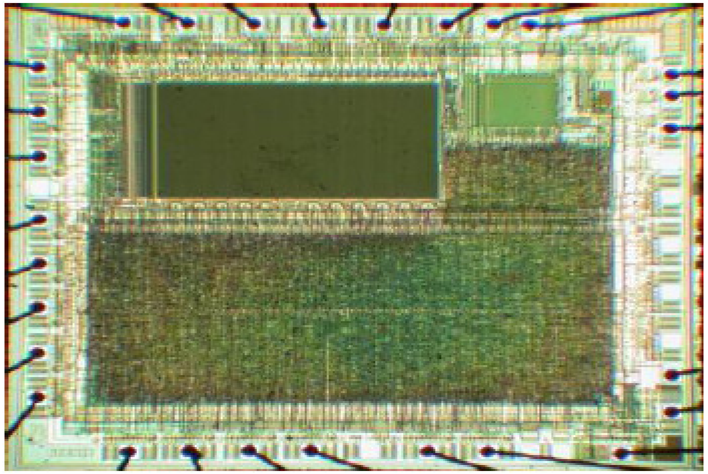
Semi-invasive attack

- These attacks require access to chip surface, but do not require penetration of the passivation layer or direct electric contact
- Goal is to inject security fault into the system
  - UV light to reset protection bit
  - Flashlight to set/reset individuals bit of an SRAM microcontroller

→Can also be prevented with special layers and with new designing considerations: Randomize internal logic



Distinguishable design



Glue logic design

Remote attacks

- These attacks are independent of the distance between the attacker and the cryptoprocessor
  - They are purely logical attacks without physical access
- Attack can be passive or active
  - Passive: Only observe the transactions
  - Active: Modifies the transaction streams

- Two well known example
  - Cryptanalysis: Exploits design flaws in crypto primitives
  - Protocol analysis: Looks for protocol flaws

- *API analysis*
  - This was developed only in the last few years
  - Most cryptographic processor have turned out to have at least one API vulnerability

API analysis

- All internal sensitive data can only be accessed through the Application Programming Interface (API)
  - Top-level software component of the cryptoprocessor

- This *security* API
  - Provides cryptographic services
  - Also enforces *policy* on the interaction

  → It differs from a cryptographic API

- Security API designer must assume, that the host with which the cryptoprocessor interacts is under the control of the opponent

  → Information leakage must be prevented

Serious API error - Example

- VISA Security Module
- The terminal master key was derived from to encrypted components by XOR-ing them

  $\{Tmk_1\}_{km}$

  $\{Tmk_2\}_{km}$

  $TMK=Tmk_1 \text{ XOR } Tmk_2$

  → The terminal Master key could be resetted:

  $\{Tmk_1\}_{km}$

  $\{Tmk_1\}_{km}$

  $TMK = Tmk_1 \text{ XOR } Tmk_1 = 0$

→ PIN derivation keys could be extracted

Smart cards – Overview

- Smart cards are used in a wide range of applications

- They store sensitive data
  - Crypto keys (even system master keys), access codes, account balance, …

- Many smart cards support cryptographic operations
  - Custom hardware for DES and modular arithmetics

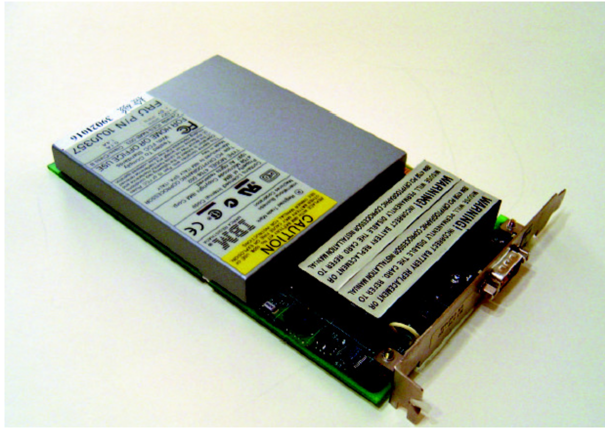
- Smart cards are intended to protect sensitive data in hostile environments, but …
  - Their use is usually extended with other security measures
  - When such additional measures are not applied, smart cards become less efficient and fraud pervades (see e.g., payTV systems)

Smart cards – Overview II.

- The main advantage of smart cards is their *low cost*
  - Access to sensitive data through the interface is controlled by the smart card (OS)
  - Authorization of access is based on PIN codes
  - After a certain number of unsuccessful attempts, the card blocks itself

- However, physical security is not very strong
  - Smart cards do not resist tampering by a determined attacker with slightly above-average knowledge
  - No tamper resistance against a determined attacker
    - although there exist smart cards already with FIPS 140 level 3 evaluation
  - Additional security measures (surveillance, blacklisting) are not feasible in the SeVeCom scenario

The IBM 4758 cryptographic coprocessor



- Programmable PCI board with custom hardware to support cryptography and tamper resistant packaging
- Main features:
  - Pipelined DES encryption engine
  - Pipelined SHA-1 hash engine
  - 1024-bit and 2048-bit modular math Hardware to support RSA and DSA
  - Hardware noise source to seed random number generation
  - Pseudo-random number generator
  - Support for RSA key pair generation, encryption, and decryption
  - Support for key management
    - DES based, RSA based, key diversification, PIN generation
  - Secure clock-calendar
  - Support for PKCS#11 and IBM Common Cryptographic Architecture (CCA)
  - Battery backed RAM (BBRAM) to store secrets persistently
  - Steel house with tamper detecting sensors and circuitry to erase the sensitive memory

High-end secure coprocessors - Overview

- Advantages:
  - Very high level of security
  - High performance
  - Flexibility (loading and updating the OS and the applications)

- Disadvantages:
  - Even the 4758 had API vulnerabilities
    - Firmware upgrades
  - Price
    - the 4758 costs around 4000 dollars
  - Battery lifetime
    - batteries need to be changed after 3 years
  - Robustness
    - e.g., operating temperature: 10 – 40 C

Final realization

- We presented two extremes of the spectrum of tamper resistant devices
- The solution for SeVeCom may lie between this two extremes
- In order to find the suitable solutions
  - We must better understand the threats and the security requirements
  - We must determine the decision criteria
    - level of security provided
    - cost

- But it can be said that the module should be protected against clever outsiders and keys against not invasive attacks

Conclusions

- The threats and security requirements should be clarified
- The realization will depend upon it

  → But the hardware does not depends on us
- However we should specify the types of physical attacks it should resist
  – Mainly Non and Semi-invasive attacks

- OUR goal is to define the API
  – It should provide sufficient cryptographic background
  – Although it should not leak information
  – Should be logically correct and resist Remote attacks