Tamper resistance and physical attacks

Part I: Introduction

Dr Sergei Skorobogatov

http://www.cl.cam.ac.uk/~sps32 *email: sps32@cam.ac.uk*

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Security Group, TAMPER Lab

Structure of the talk

- Introduction
  - Physical security
  - Attack technologies
  - Security protection levels
- Attack technologies
  - Non-invasive attacks
  - Invasive attacks
  - Semi-invasive attacks
- Security evaluation and defence technologies
- Ongoing research

Introduction

- Protection from physical attacks
  - Protecting objects from being stolen
  - Psychological and historical background
- Physical protection in pre-computer era
  - Burglary (doors, locks, fences, safes)
  - Theft (guards, chains, locks)
  - Military enemy (fortification, armed guards, tanks, missiles)
- Physical protection in computer era
  - Military enemy (control and spying)
  - Bank fraud (PINs, plastic cards, on-line cryptography, holograms)
  - Theft (CCTV, RF tags, electronic keys)
  - Services (prepayment meters and cards)
  - Pay-TV piracy (access using smartcards)
  - GSM service (access using SIMs)
  - Software piracy (hardware dongles, crypto-coprocessors)

Introduction

- Technical progress pushed low-cost cryptoprocessors towards ubiquity
  - Car industry
    - anti-theft protection
    - spare parts
  - Accessory control
    - mobile phone batteries
    - printer toner cartridges
    - memory modules
  - Access control (tokens and dongles)
  - Home appliances (door control, entertainment)
  - Intellectual property (IP) protection (in products)
    - Software copy protection
    - Protection of algorithms
    - Protection from cloning

Levels of physical protection

- Access control
- Obstruction
- Active protection
- Sensors
  - Lid switch
  - Environment
  - Tamper detection and tamper evidence
- Software level
  - Password protection
  - Encryption
  - Protocols
- Hardware level
  - Electronics – PCB, sensors
  - Microelectronics – Silicon implementation

Area of interest

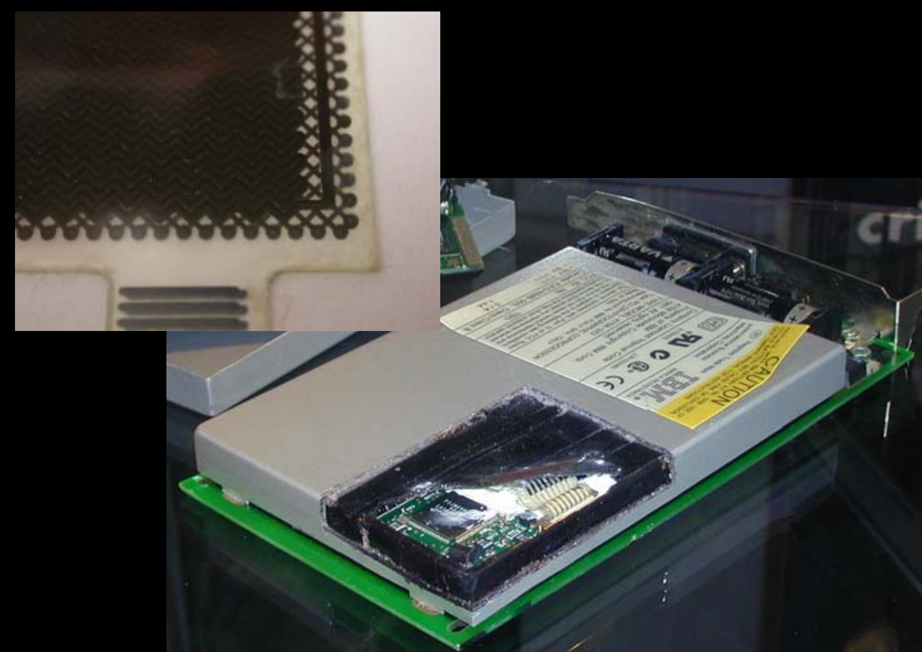
- Hardware security of semiconductor chips
  - Security modules
  - Smartcards
  - Microcontrollers
  - ASICs and custom ICs
  - Other single-chip solutions
- Do we have the same level of protection as in high-end applications?
- Do we have an adequate level of protection?

Tamper protection levels

- Level HIGH

D.G.Abraham et al. (IBM), 1991

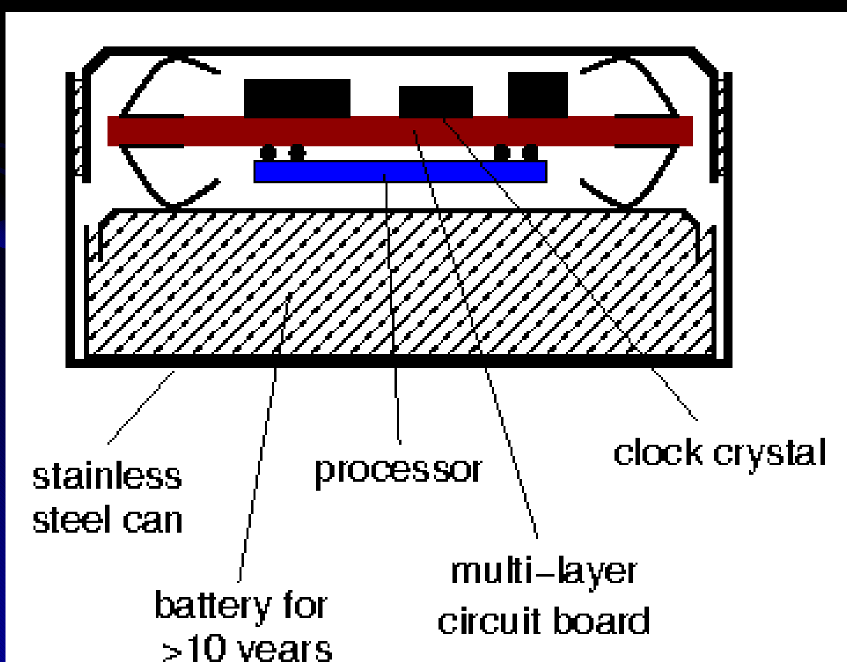
  - Military and bank equipment
  - All known attacks are defeated. Some research by a team of specialists is necessary to find a new attack. Total cost: over a million euros. Time to attack: months to years



Picture courtesy of Dr Markus Kuhn

Tamper protection levels

- Level MODH
  - Secure i-Buttons, secure FPGAs, high-end smartcards and ASICs
  - Special attention is paid to design of the security protection. Equipment is available but is expensive to buy and operate. Total cost: hundreds of thousand euros. Time to attack: weeks to months



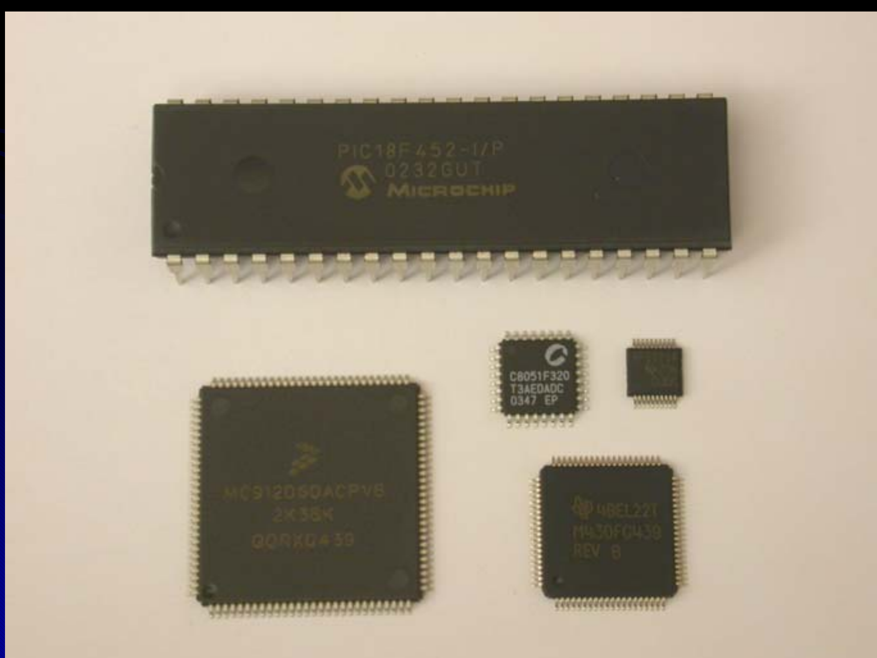
Picture courtesy of Dr Markus Kuhn

Tamper protection levels

- Level MOD
  - Smartcards, high-security microcontrollers, ASICs, CPLDs, hardware dongles, i-Buttons
  - Special tools and equipment are required for successful attack as well as some special skills and knowledge. Total cost: tens of thousand euros. Time to attack: weeks to months

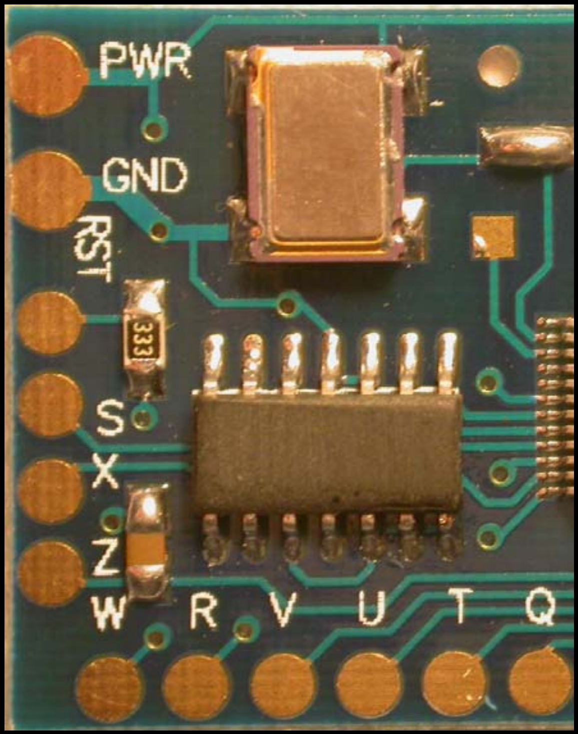
Tamper protection levels

- Level MODL
  - Microcontrollers with security protection, low-cost hardware dongles
  - Protection against most low-cost attacks. Relatively inexpensive tools are required, but some knowledge is necessary. Total cost: thousands of euros. Time to attack: days to weeks



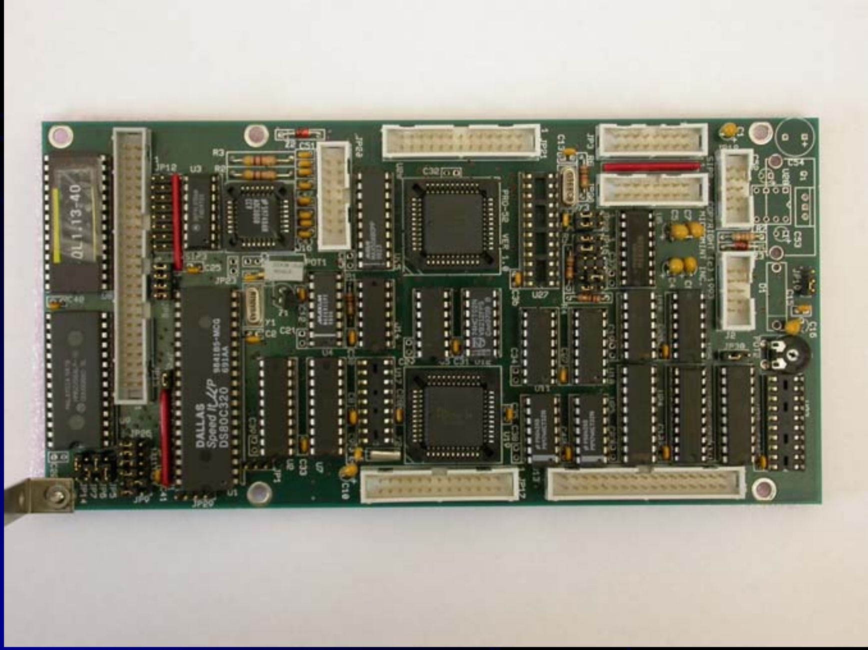
Tamper protection levels

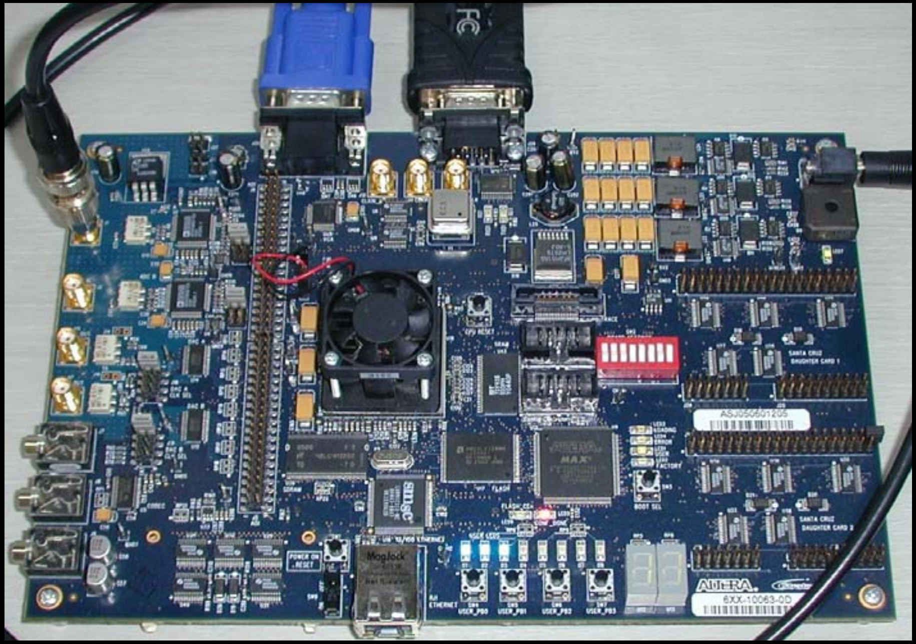
- Level LOW
  - Microcontrollers with proprietary read algorithm, remarked ICs
  - Some security features are used but they can be relatively easy defeated with minimum tools required. Total cost: hundreds of euros. Time to attack: hours to days



Tamper protection levels

- Level ZERO (no special protection)
  - Microcontroller or FPGA with external ROM
  - No special security features are used. All parts have free access and can be easily investigated. Total cost: less than a hundred euros. Time to attack: less than an hour





Tamper protection levels

- Division of levels from HIGH to ZERO is relative
  - Some products designed to be very secure might have flaws
  - Some products not designed to be secure might still end up being very difficult to attack
  - Technological progress opens doors to less expensive attacks, thus reducing the protection level of some products
- Proper security evaluation must be carried out to estimate whether products comply with all the requirements
  - Design overview
  - Test against known attacks

Attacks and attackers

- Who is going to attacks our system?
  - Classes of the attackers
- What tools will they use?
  - Attack categories
  - Attack methods
- What is the reason to attack?
  - Attack scenarios
- How to protect?
  - Security engineering

Classes of the attackers

- Class I (clever outsiders):
  - very intelligent but may have insufficient knowledge of the system
  - have access to only moderately sophisticated equipment
  - often try to take advantage of an existing weakness in the system, rather than try to create one
- Class II (knowledgeable insiders):
  - have substantial specialised technical education and experience
  - have varying degrees of understanding of parts of the system but potential access to most of it
  - often have access to highly sophisticated tools and instruments for analysis
- Class III (funded organisations):
  - able to assemble teams of specialists with related and complementary skills backed by great funding resources
  - capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools
  - may use Class II adversaries as part of the attack team

Attack methods

- Non-invasive attacks
  - Observe or manipulate with the device without physical harm to it
  - Require only moderately sophisticated equipment and knowledge to implement
- Invasive attacks
  - Almost unlimited capabilities to extract information from chips
  - Normally require expensive equipment, knowledgeable attackers and time
- Semi-invasive attacks
  - Chip is depackaged but the passivation layer remains intact
  - Fill the gap between non-invasive and invasive types, being both inexpensive and easily repeatable

Attack categories

- Eavesdropping (non-invasive)
  - techniques that allows the attacker to monitor the analog characteristics of supply and interface connections and any electromagnetic radiation
- Software attacks (non-invasive)
  - use the normal communication interface and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation
- Fault generation (non-invasive and invasive)
  - use abnormal environmental conditions to generate malfunctions in the system that provide additional access
- Microprobing (invasive)
  - can be used to access the chip surface directly, so we can observe, manipulate, and interfere with the device
- Reverse engineering (invasive)
  - used to understand the inner structure of the chip and learn or emulate its functionality; requires the use of the same technology available to semiconductor manufacturers and gives similar capabilities to the attacker

Tamper evidence

- Non-invasive attacks
  - Normally do not leave evidence of the attack
  - Many are reversible
- Invasive attacks
  - Destructive, hence, leave evidence of the attack
  - Most are irreversible
- Semi-invasive attacks
  - Destructive to the packaging of the chip
  - Many are reversible

Attack scenarios

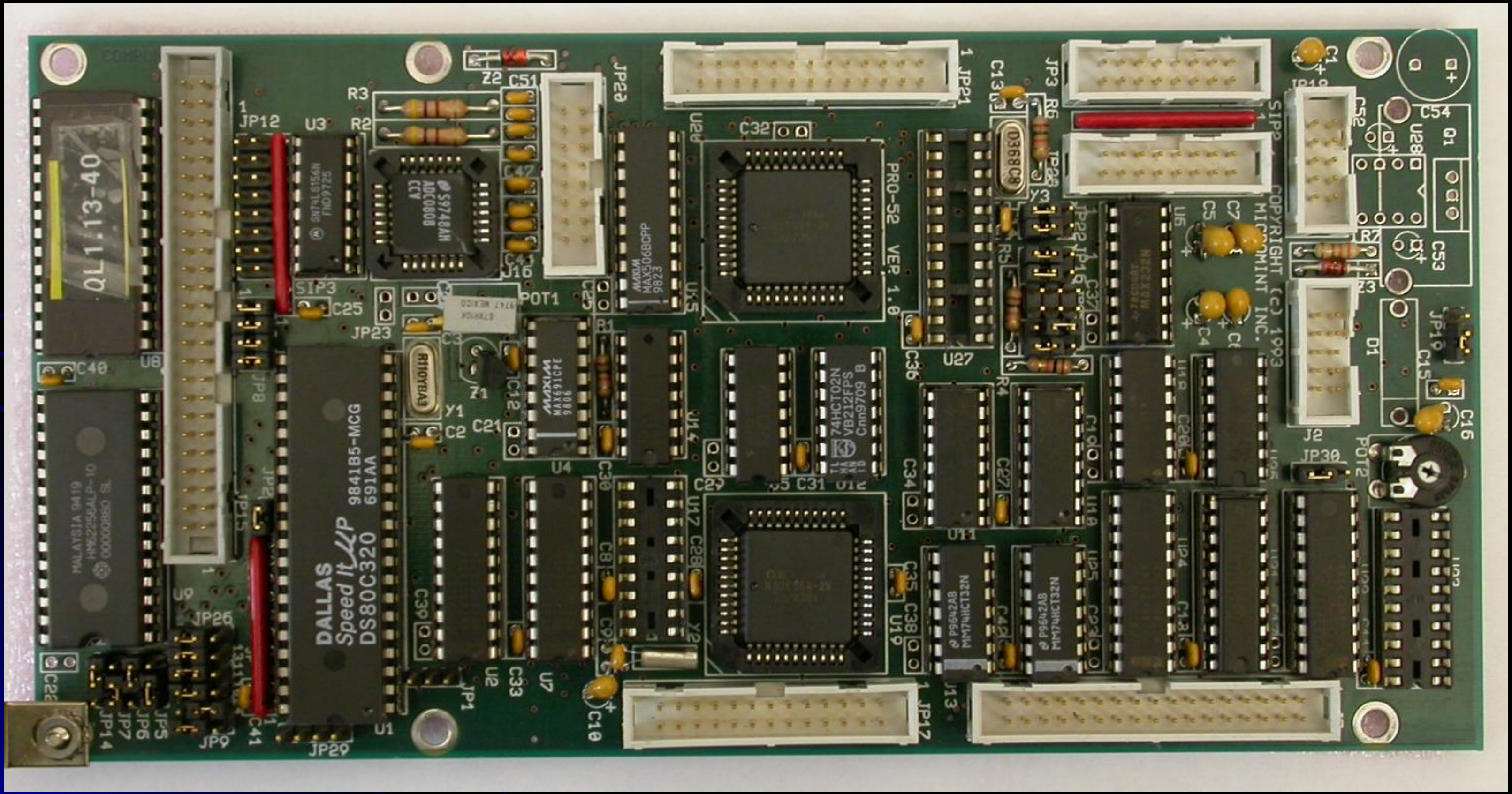
- Cloning
  - Most widely used attack scenarios (from individuals to companies)
  - Increasing sales without investment in design
- Overbuilding
  - Mass production
- Theft of service
  - Attacks on service providers (satellite TV, electronic meters, phones)
- Denial of service
  - Dishonest competition
- Decryption
  - Information recovery
  - Read cryptographic keys in plaintext
  - Force crypto keys to a known value
  - Force cryptosystem to insecure mode
- Extraction of information
  - Trade secrets and IP piracy

Security engineering

- Understanding motivations of the attackers
  - Attack scenarios
- Figuring out what to protect
  - Locating the most sensitive points (fuses, keys)
- Estimating capabilities of the attackers
  - Equipment
  - Knowledge
- Developing adequate protection
  - Hardware level (Silicon design, PCB, sensors)
  - Software level (encryption, protocols)

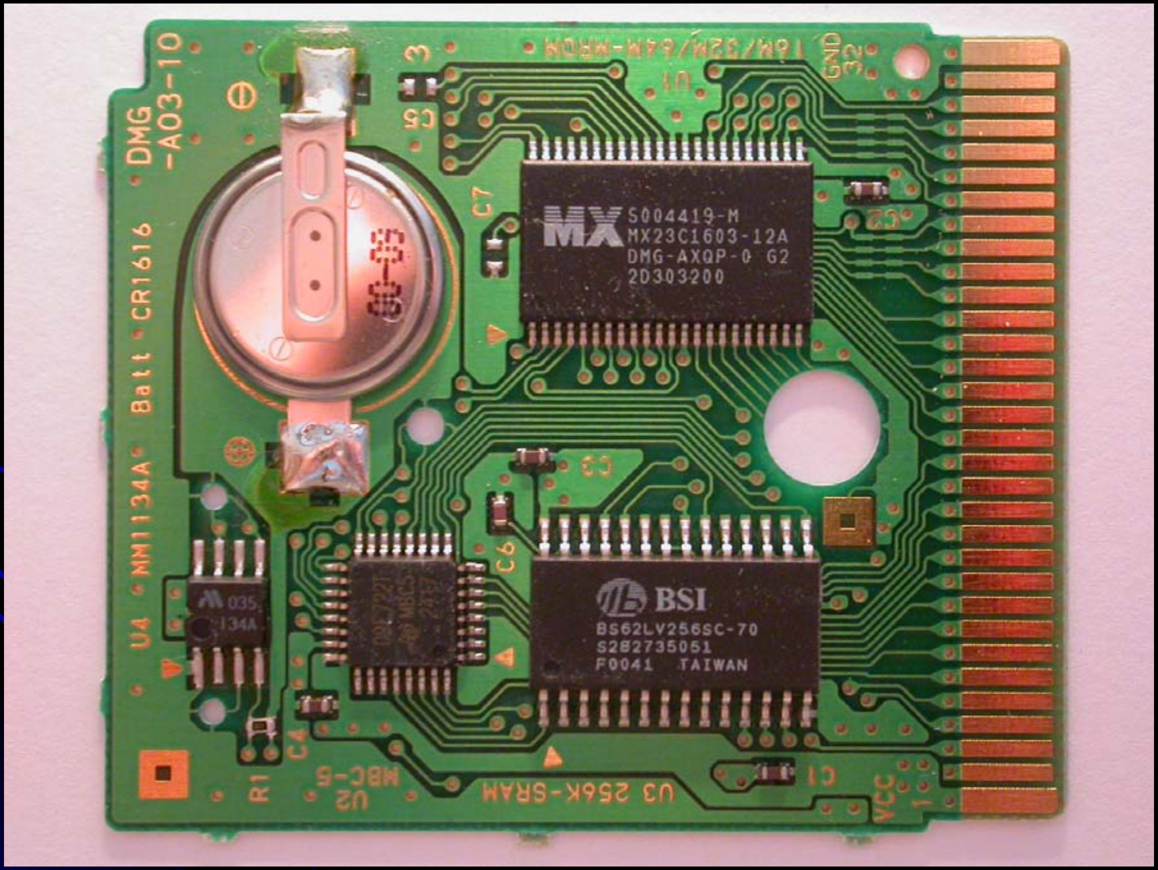
Security evolution in semiconductors

- Years 1970 – 1985
  - Tamper protection level ZERO or LOW
  - All components are easy to access and test



Security evolution in semiconductors

- Years 1980 – 1990
  - Tamper protection level LOW
  - Obscurity vs security

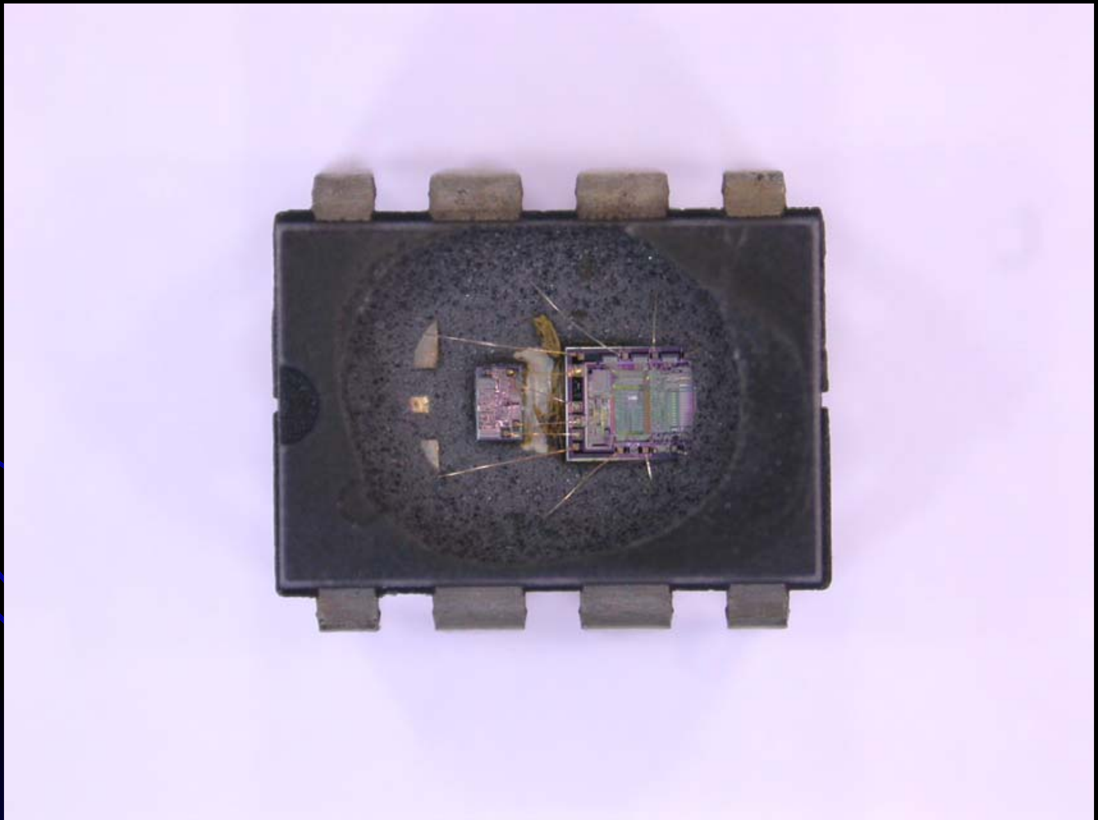


Security evolution in semiconductors

- Years 1985 – 1995
  - Tamper protection level LOW or MODL
  - No special protection used

Security evolution in semiconductors

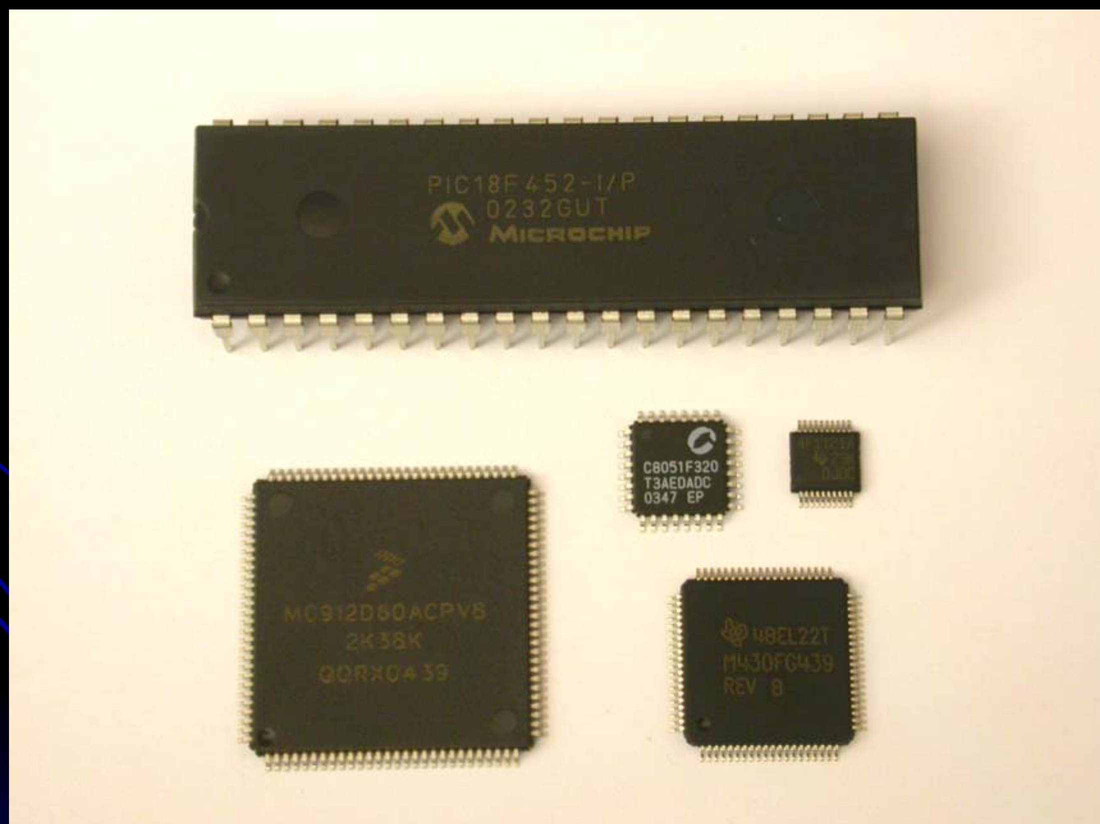
- Years 1990 – 2000
  - Tamper protection level MODL
  - Restricted access



Microchip PIC12CE518

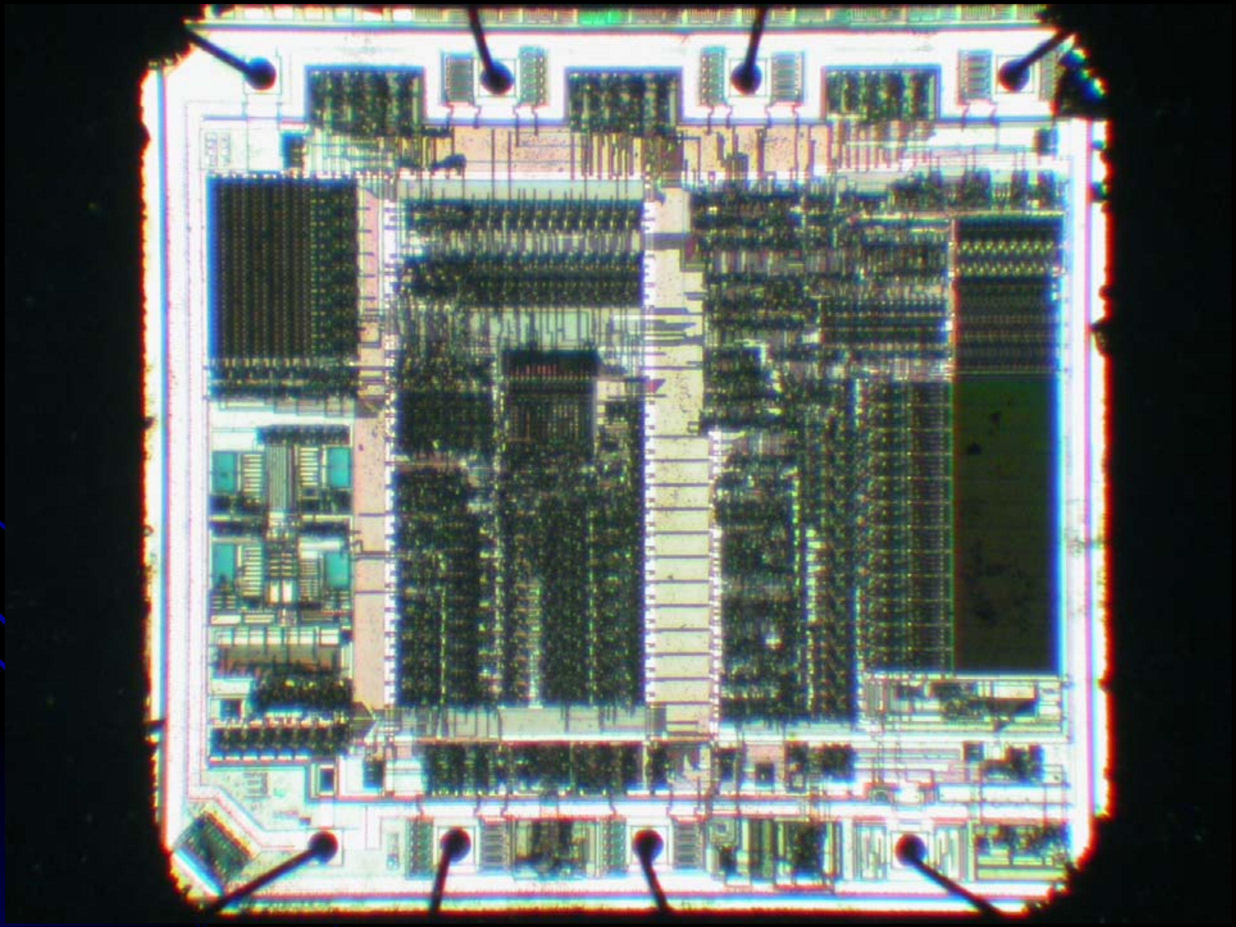
Security evolution in semiconductors

- Years 1990 – 2000
  - Tamper protection level MODL or MOD
  - Microcontrollers with security protection



Security protection in microcontrollers

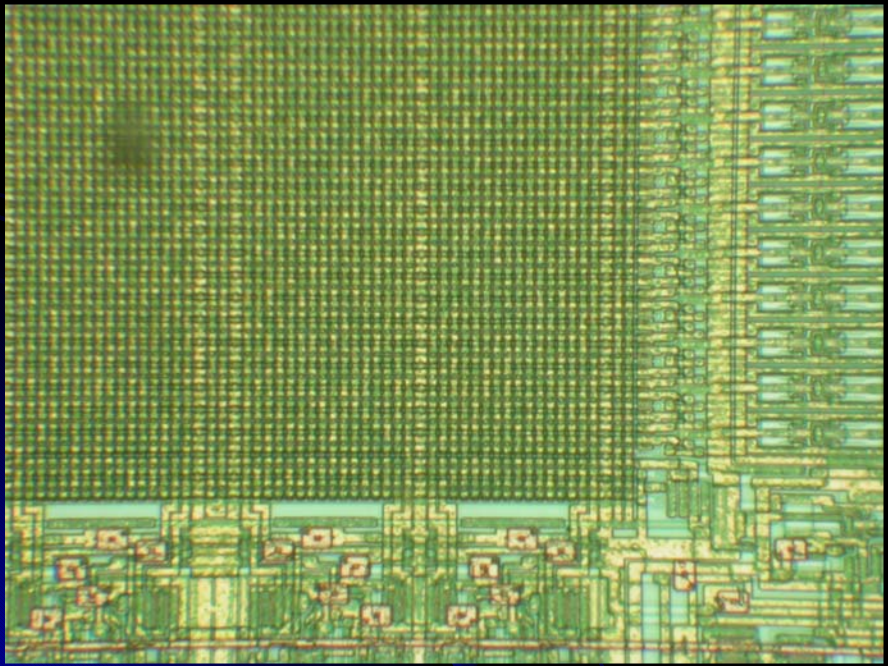
- Security fuse is placed separately from the memory array
  - Easy to locate and defeat



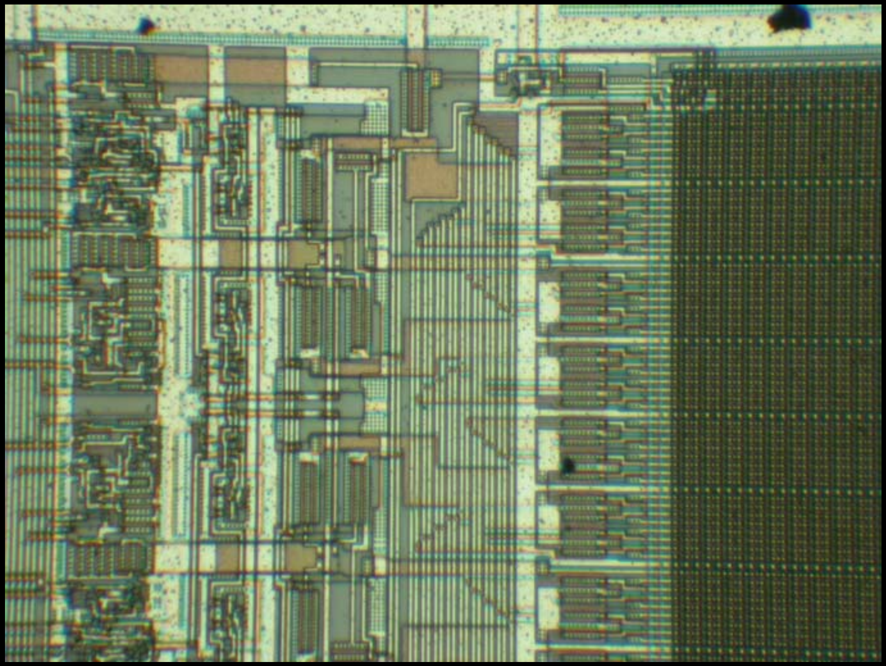
Microchip PIC12C508 microcontroller

Security protection in microcontrollers

- Security fuse is placed inside the program memory array
  - Hard to locate and defeat



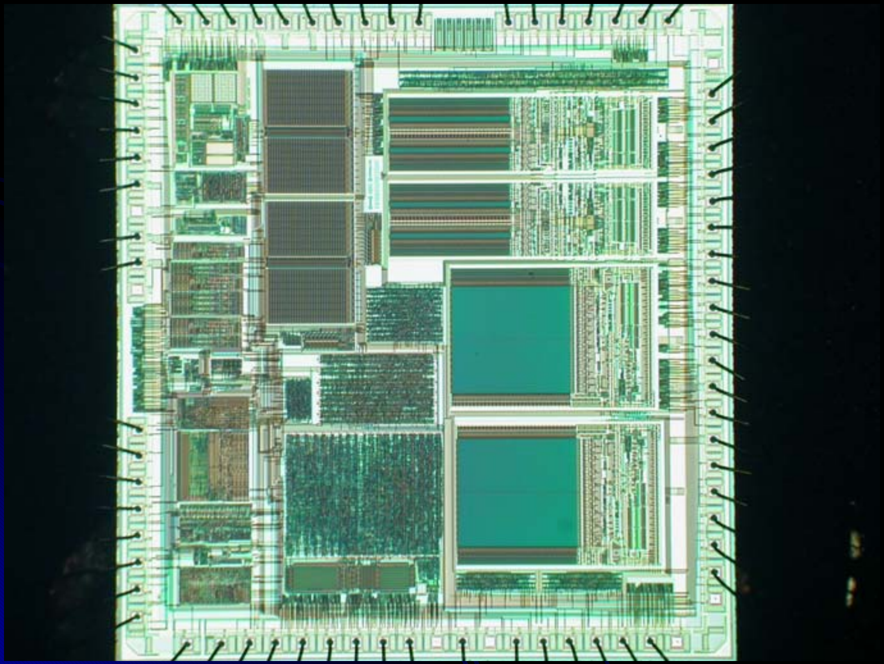
STMicroelectronics ST62T60 microcontroller



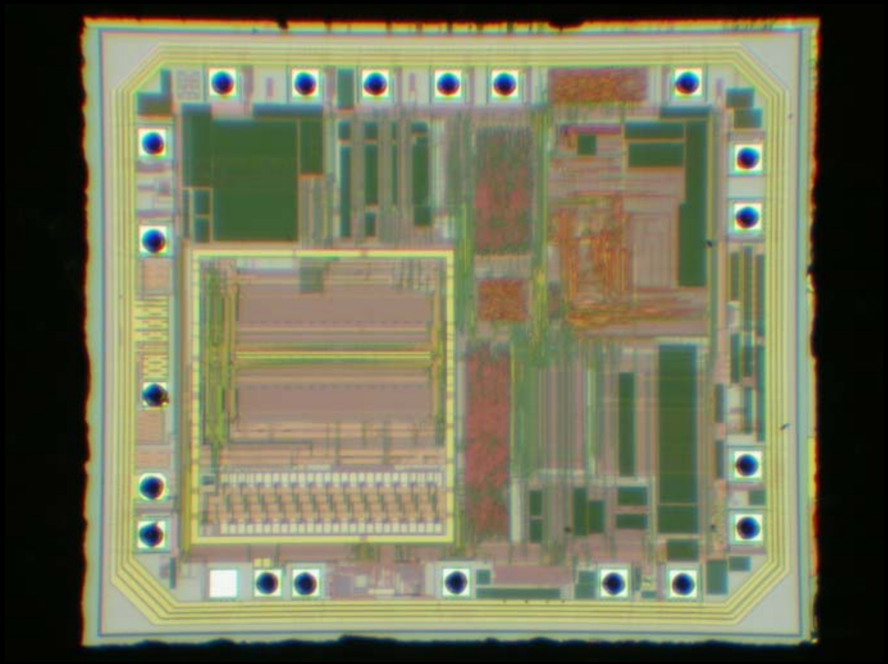
Motorola MC68HC705C9A microcontroller

Security protection in microcontrollers

- Security fuse is embedded into the program memory
  - Very hard to locate and defeat
  - Similar approach is used in many smartcards



Motorola MC68HC908AZ60A microcontroller



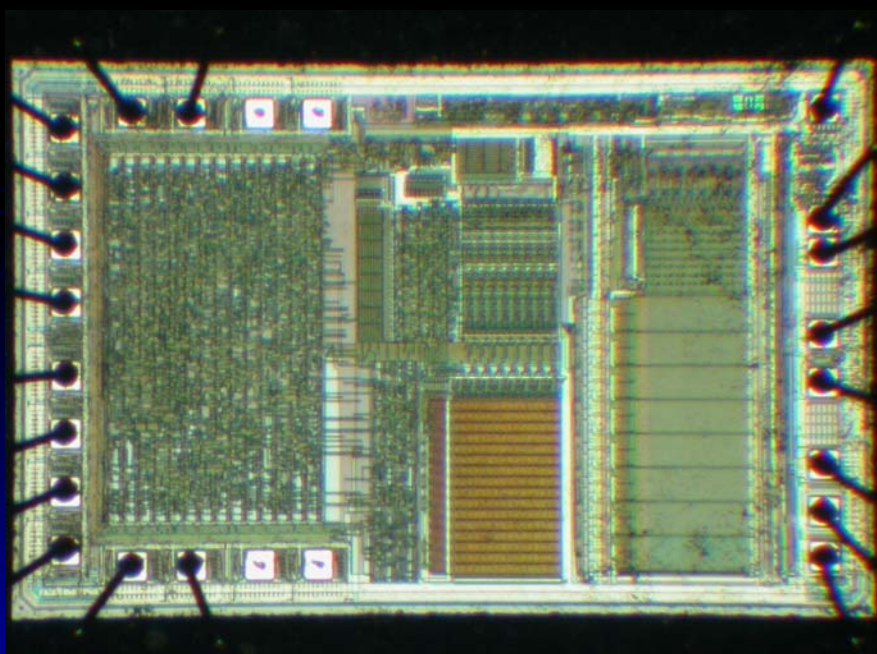
Texas Instruments MSP430F112 microcontroller

Security protection in microcontrollers

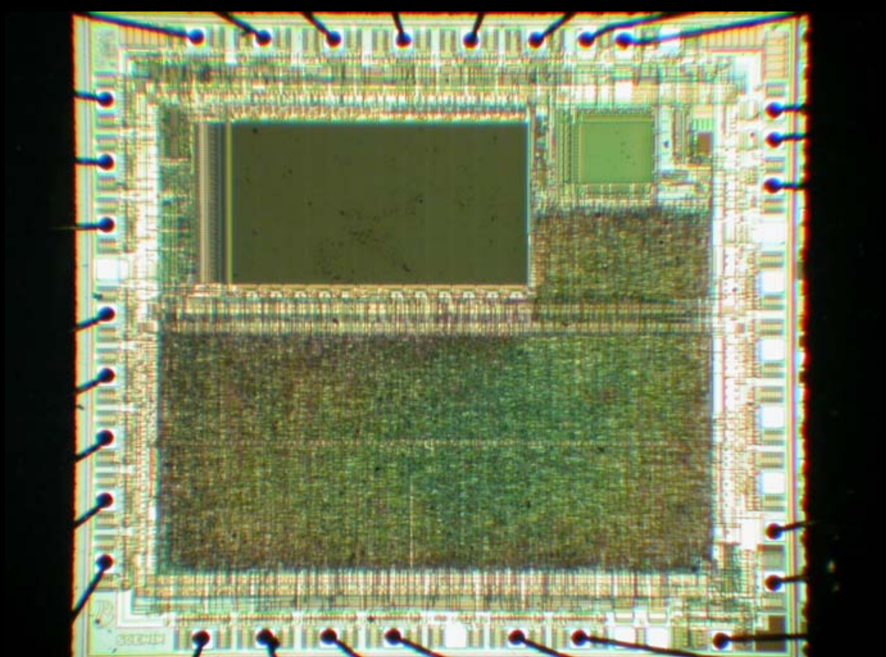
- Monitoring of the security protection
  - Single check on power-up or reset
    - Sensitive to glitching
  - Single check on power-up and store state in a register
    - Sensitive to glitching and fault injection
  - Check each time access is required
    - Harder to attack because of synchronization requirements
  - Permanent monitoring
    - Best choice for protection, however, not always convenient

Security evolution in semiconductors

- Years 2000 – 2005
  - Tamper protection level MOD or MODH
  - Glue logic design
    - used in modern microcontrollers and smartcards



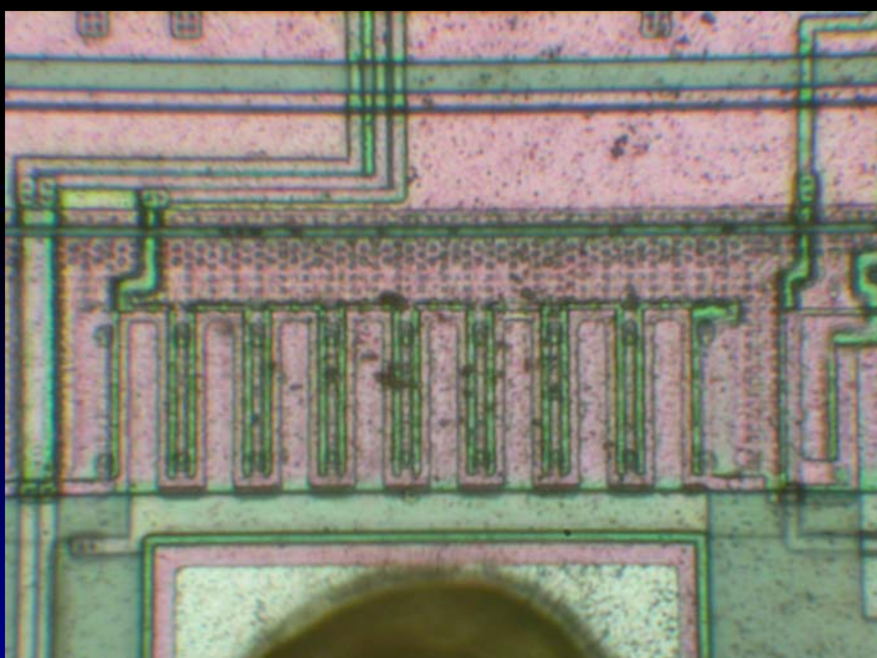
Cypress CY7C63001A microcontroller



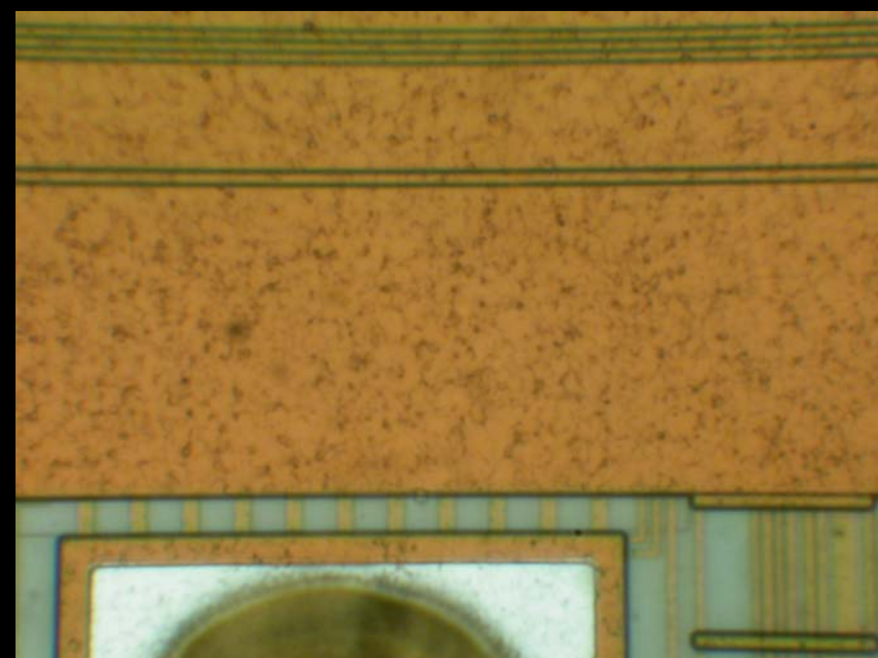
Scenix SX28 microcontroller

Security evolution in semiconductors

- Years 1995 – present
  - Tamper protection level MOD or MODH
  - Planarisation as a part of modern chip fabrication processes (0.5 μm or smaller feature size)



Microchip PIC16F877 microcontroller

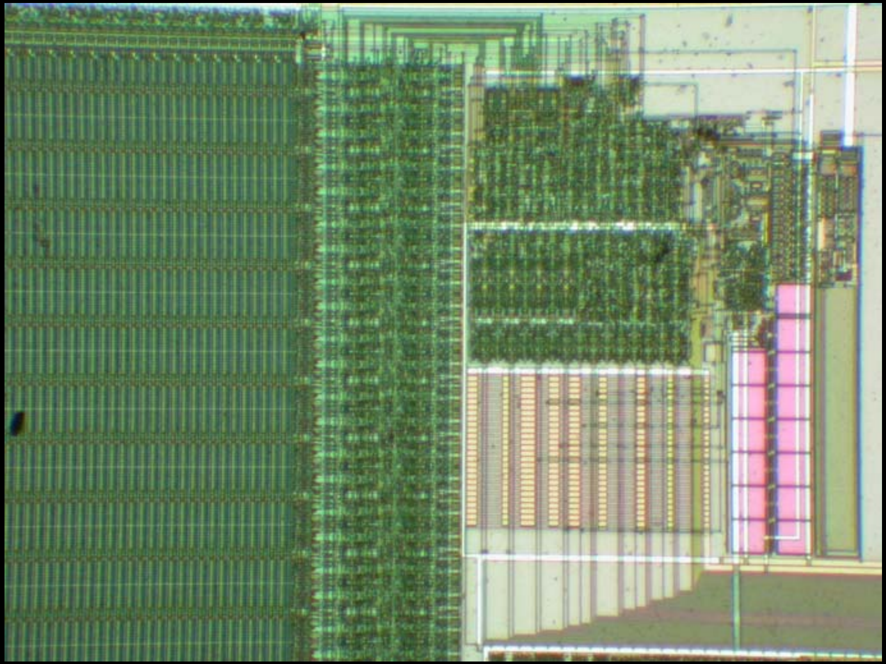


Microchip PIC16F877A microcontroller

Security evolution in semiconductors

- Years 1995 – present
  - Tamper protection level MOD or MODH
  - Bus encryption
    - Simple algorithms not to slow down the communication

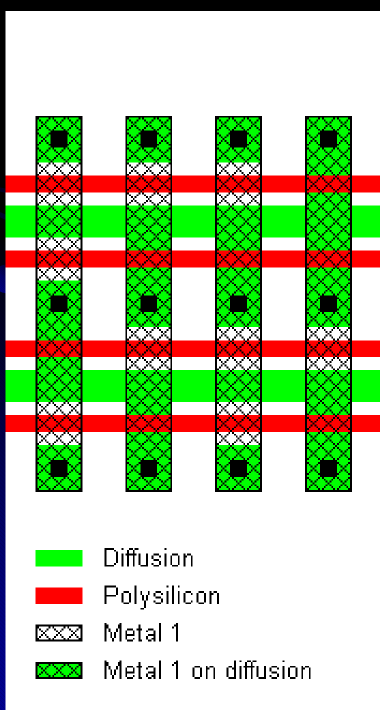
Dallas Semiconductor DS5002FP microcontroller

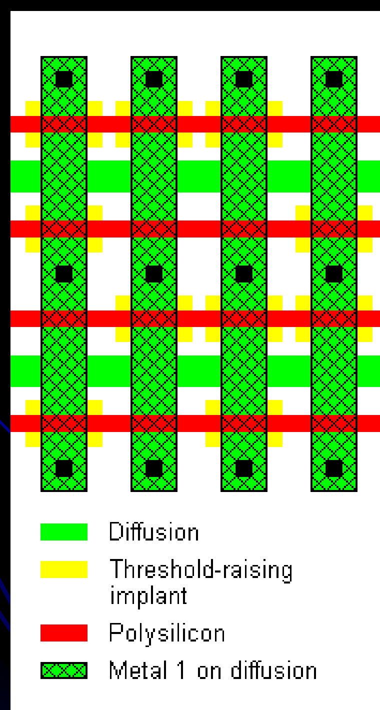


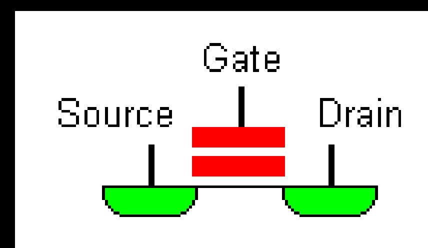
Infineon SLE66 smartcard

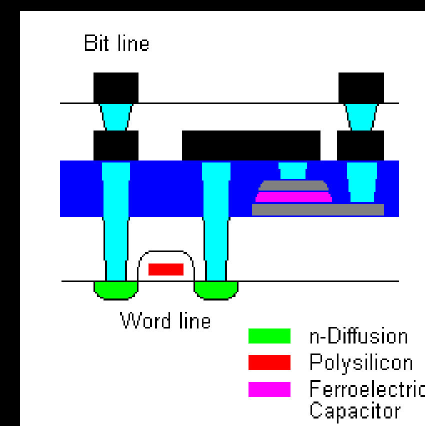
Security evolution in semiconductors

- Years 1995 – present
  - Tamper protection level MOD or MODH
  - Secure memory
    - VTROM for Mask ROM implementation
    - Flash and FRAM for non-volatile memory



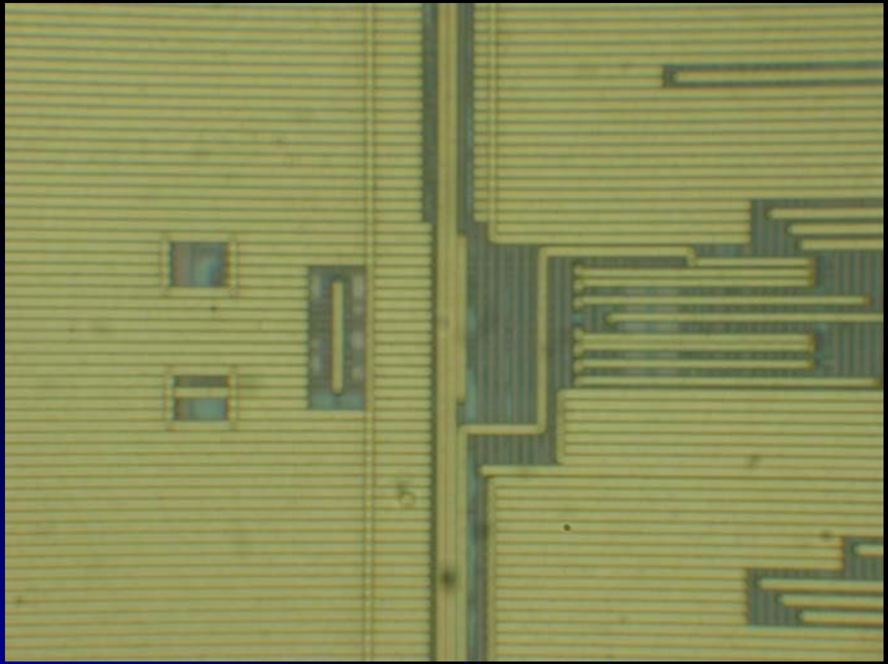


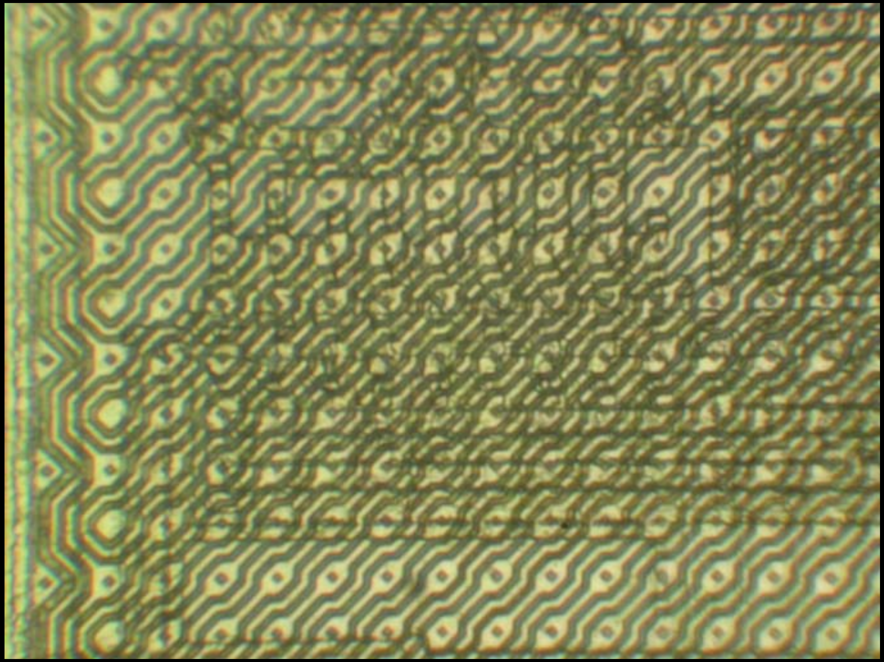




Security evolution in semiconductors

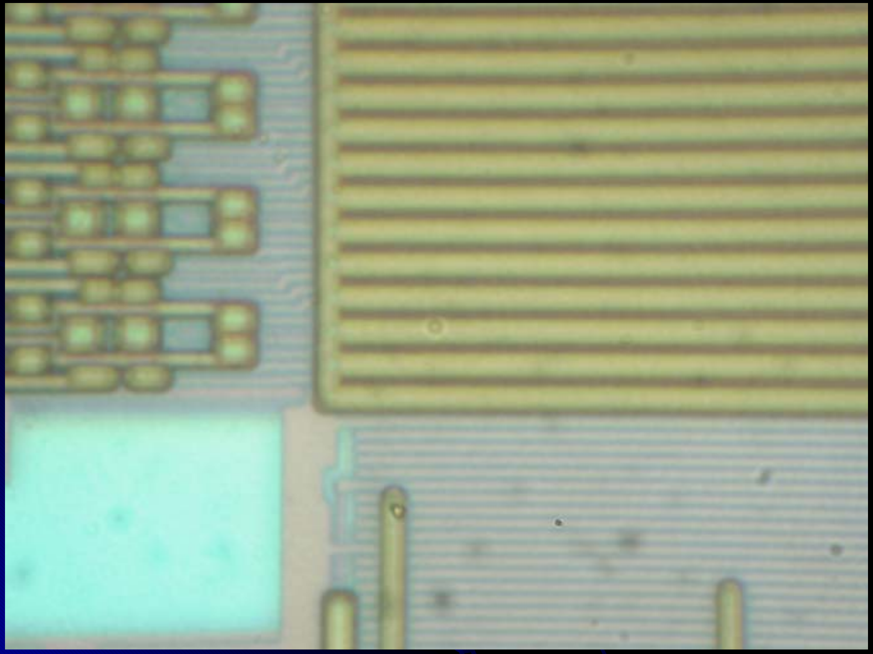
- Years 1995 – present
  - Tamper protection level MODH
  - Top metal layers with sensors
  - Voltage, frequency and temperature sensors
  - Memory access protection, crypto-coprocessors


Temic T89C51RD2 microcontroller

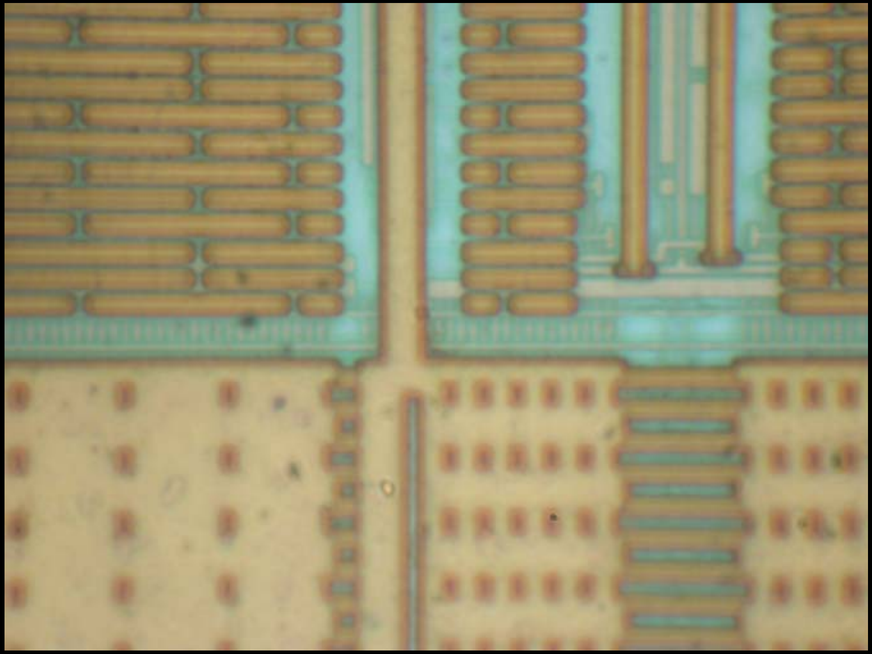

STMicroelectronics ST16 smartcard

Security evolution in semiconductors

- Impacts of technological progress
  - Size of transistors reduced to less than 0.3 µm
  - Multiple metal layers obstruct direct observation
  - Complexity of circuits significantly increased
  - More security features could be implemented



Motorola MC68HC908AP16 microcontroller



Atmel ATmega16 microcontroller

Conclusions

- There is no absolute protection – any device can be broken given enough time and resources
- Division of levels from HIGH to ZERO is relative
  - Some products designed to be very secure might have flaws
  - Some products not designed to be secure might still end up being very difficult to attack
- Proper security evaluation must be carried out to estimate whether products comply with all the requirements
- Main concern is the cost of an attack
- With technological progress it becomes more difficult to attack devices
- Attack motivations is the major driving factor in compromising security of a device
- Insiders could be potentially more dangerous as they could have more information about the devices