Smart Cards & Digital Security

ReTrust Technical Workshop, Trento, September 25-26, 2007

Jean-Daniel Aussel, Technology & Innovation, gemalto
jean-daniel.aussel@gemalto.com

Smart Cards

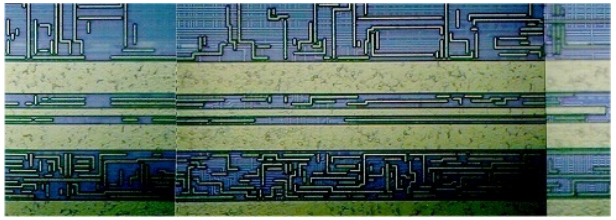
- Tamper resistant cryptographic devices
  - Securely store keys and private attributes
  - Perform cryptographic computations
  - Perform non-cryptographic computations
  - Portable (Nomadicity)

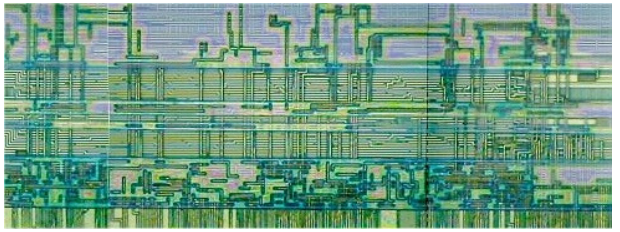
Why are smart card tamper resistant?

Physical Attacks

Invasive Attacks

- Deposit probe pads on a bus
- … or through conductive grid
- Expose hardwired ROM links
- Disconnect sensors, RNG…
- Connect tracks
- Cut tracks

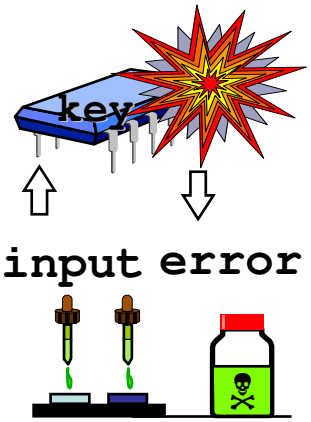




Fault Generation

Apply combinations of environmental conditions

- Vcc, Clock,
- Temperature, UV
- Light, Laser, …

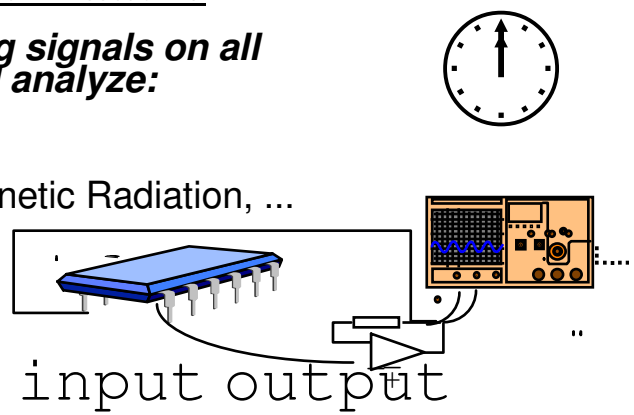


… and bypass protections or infer secrets

Side Channel Attacks

Monitor analog signals on all interfaces and analyze:

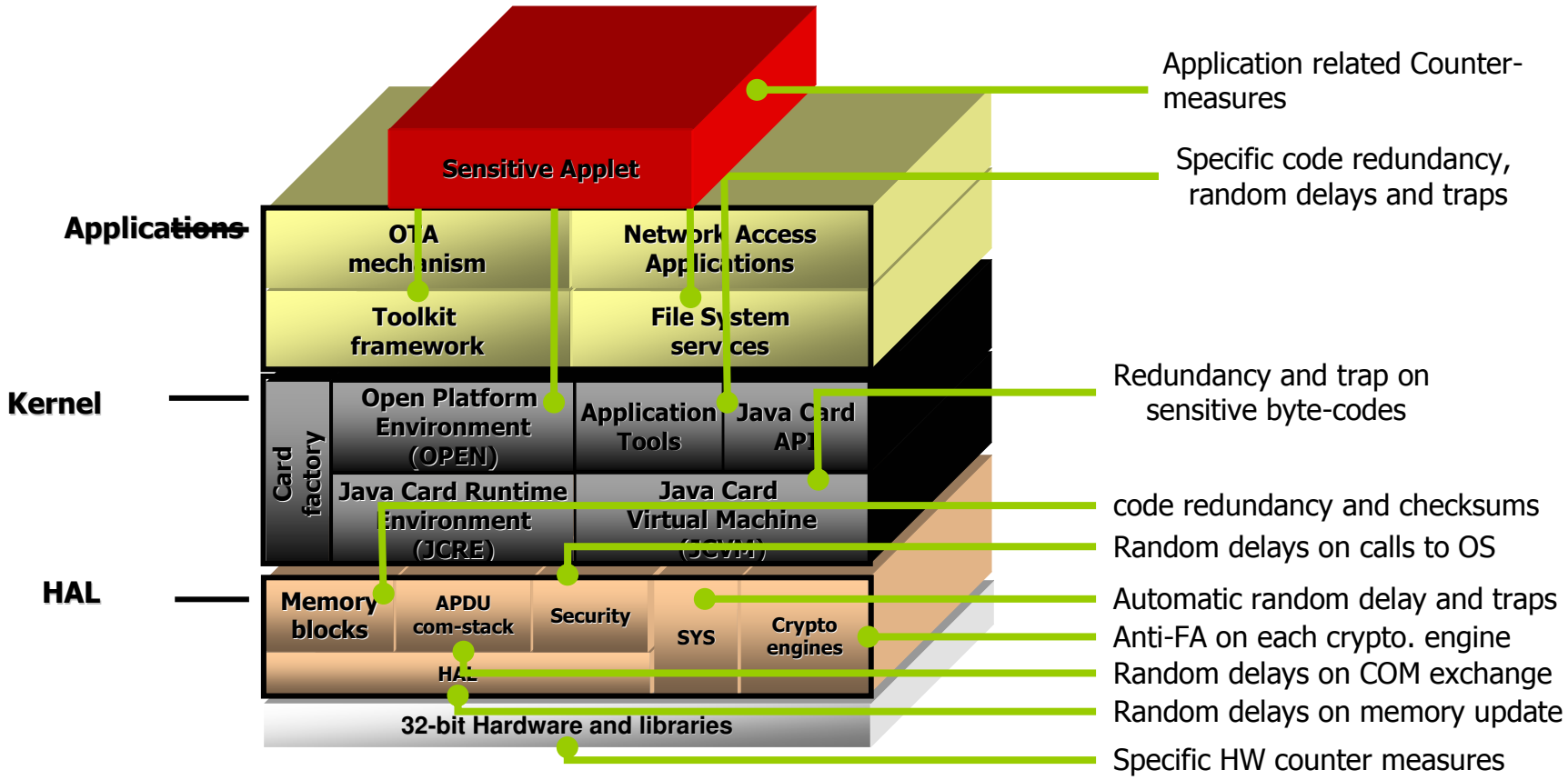
- Time
- Power
- Electromagnetic Radiation, ...



Countermeasures (hardware)

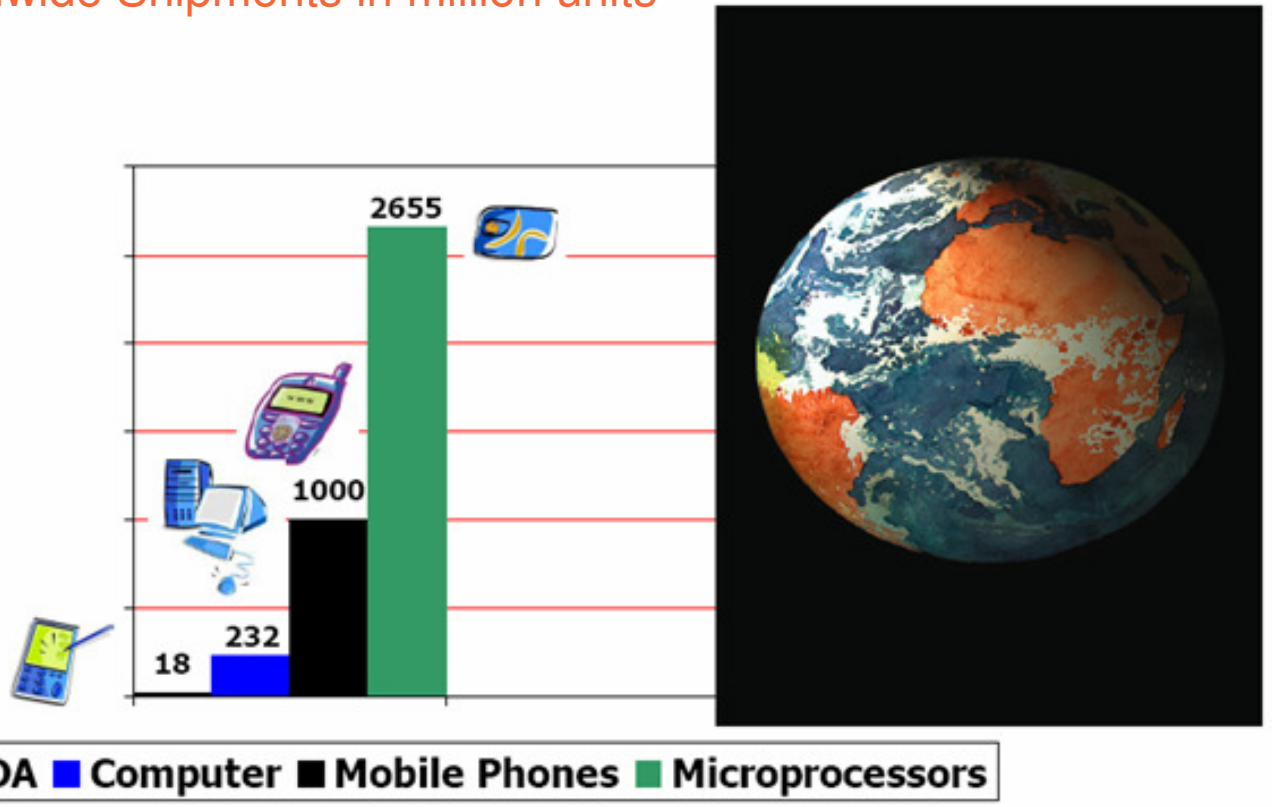
- Functional blocks are mixed into a glue logic design
  - Makes it more difficult for an attacker to analyze the structure of the logic and locate functional blocks such as the CPU or coprocessor
- Buses are scrambled and buried
  - Inaccessible from outside the chip, thus impossible to recover memory content
  - Latest chips implement strong cyphering of bus
- A current carrying protective layer is placed on top of the chip
  - The chip does not operate if the layer is removed
- Sensors are monitoring abnormal variations of voltage, temperature, clock frequency and light
- Power signals and electromagnetic radiations are reduced to a minimum
- Random interrupts are generated to change the clock speed

Countermeasures (software)



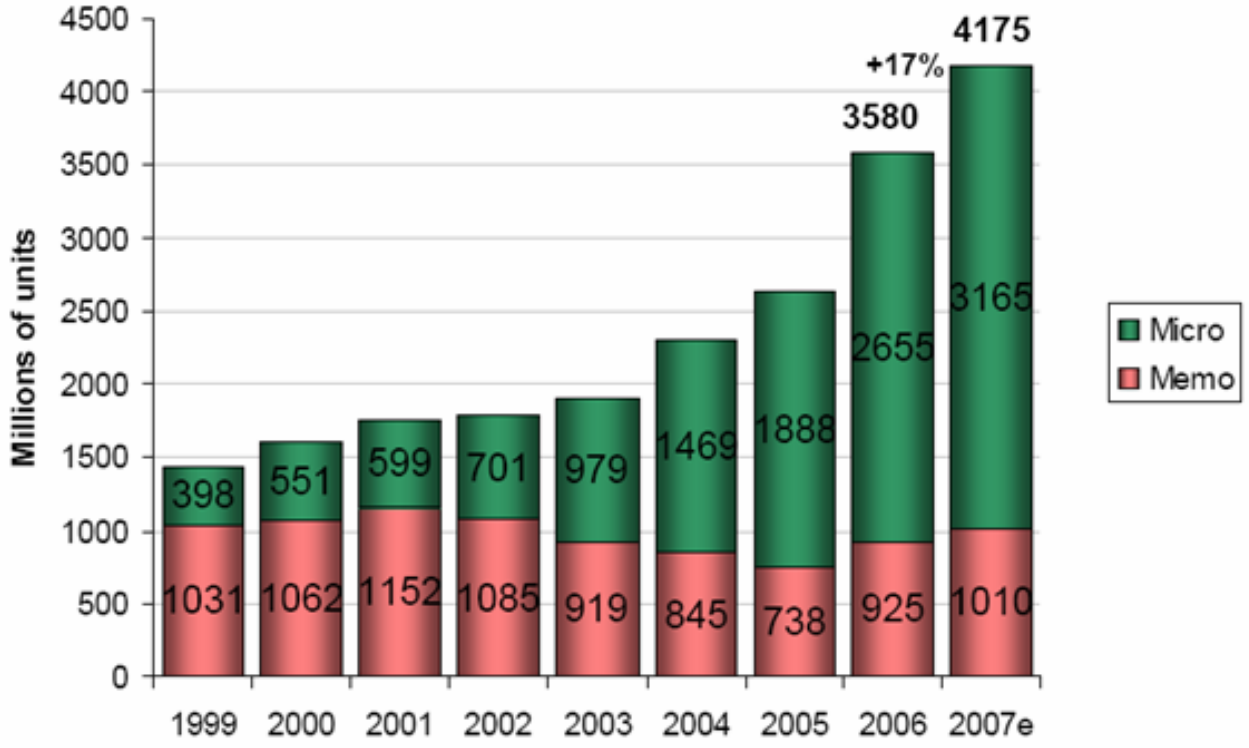
Smart Cards is by far the most sold personal computing device

2006 Worldwide Shipments in million units



Source: Gartner and Eurosmart for Microprocessor Cards

Smart card shipments to total over 4 billion in 2007



The recent growth in memory cards is due to China Identity cards shipments.
Source: Eurosmart 2007

Smart cards main usages

- Secure GSM or 3G networks

- Secure payment transactions

- Secure documents

- Secure personal computers

Logical Attacks

- Buffer overflow
- Trojan horses
  - In terminal (e.g. PC, handset) to retrieve PIN
- Bug exploitation

Smart Cards Current Ecosystem

- Connected thru readers
  - Point-of-Sale readers (payment cards)
  - Baseband modem (handsets)
  - Smart card reader (PC)
- Standardized
  - Serial interface ISO7816
  - Byte based Half-duplex protocol (APDU)
  - Industry standards with closed set of messages
    - Eurocard Mastercard Visa (EMV)
    - Subscriber Identity Module (SIM)
- Single application cards
  - EMV, SIM, passport, ID/Health card

Emerging Smart Card Applications

- Contactless Payment with Mobile phone
  - Dual contactless (single wire protocol) and SIM card
- Mobile-TV
  - DRM
  - OMA-BCAST
- PC Connectivity
  - WiFi, WiMax, 3G+
- Voice-over-IP authentication
- ID/Health online services
  - Tax return
  - Oncard/online medical record
- Consumer market identity management
  - Financial institution (Home banking), mobile network operator identity,

Emerging Smart Card Ecosystem Opens New Possibilities for Logical/Hardware Attacks

- New communication channels
  - Contactless
  - USB
  - Not buffered any more by smart card reader
- Multiple chip configuration
  - Contactless chip + smart card
  - Nand flash + smart card
- Uncontrolled terminals
  - PC, Open handsets (Windows Mobile, linux)
- New incentives
  - Mobile TV, Internet identity
- New on-card applications can be attack targets
  - Smart card web server

R&D Workload increase to secure smart cards