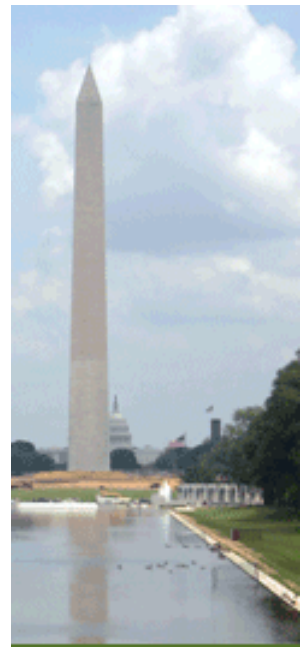
Chip Security and Design

Benoit Makowka

Agenda

- Security Basics (reminder)
- Attacks
  - Actual, New
- Countermeasures
- Security Certifications
- Flash vs ROM
- Conclusion



Secure What ?

- **Secure information stored inside the EEPROM**

  Direct Value

  e.g. Personal records (biometry), Money (e-purse),...

  Indirect Value

  e.g. Encryption key (crypto cards),..

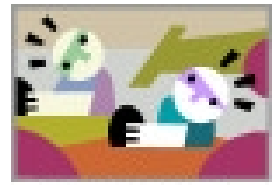
Microcontroller + Operating System (vs Memory) used to

- Generate crypto Key
- Encrypt/decrypt data (stored in EEPROM or transferred through I/O)
- Secure the access to the EEPROM (verification right access)
- Secure transaction with external reader (contact and/or contactless)
- Execute Application (e.g. Java applets).

Hacker will either try to:

- Get (corrupt, change, dump) data directly from the EEPROM
- Understand Chip and/or O.S. functionality to retrieve indirectly information

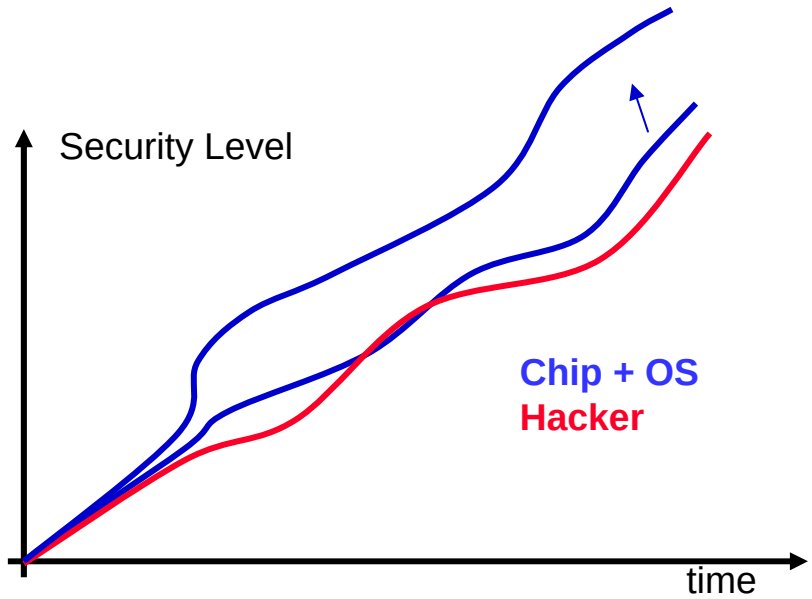
  e.g. bypass keys, checks,…



Racing

- **Hacker considerations**
  - Time spent to perform the attack
  - Cost of equipment to perform the attack
  - Expertise required to perform the attack
  - Collusion (level of information of product chip+OS)
    - **Security by obscurity**

- **Chip + OS solution**
  - To be ahead of hacker
  - Anticipate new attacks
  - React quickly to new attacks



Attacks

- **Non invasive attacks**

  Try to find a mode where chip security is not strong enough

  – **Software attacks** (OS Protection),

  Exploit vulnerabilities in protocols, crypto algorithm

  Low IC expertise
  No sophisticated equipment

  – **Side channel attacks**

  Use information leakage to retrieve sensitive data

  Monitoring and analysis Power consumption, Timi

  SPA, DPA, SEMA, DEMA, CEMA…

  Medium IC expertise
  Medium sophisticated equipment

  – **Fault injection attacks**

  Use abnormal environmental conditions to cre

  Voltage, Clock Glitches, Laser, Light pulses, Elec

  Glitch attacks, ...

  DFA on crypto operations,...

  Medium IC expertise
  Medium sophisticated equipment

- **Invasive attacks**

  Break into the chip to modify or clone it

  Reverse engineering, Microprobing, FIB, e-beam ...

  High IC expertise
  Very sophisticated equipment

New Path of Attacks

- **New attacks**
  - Chips (from “trusted” silicon vendor) now well secured against invasive attacks
    - Attack too expensive
  - Software (from ‘trusted” software developers) well secured against software attacks

  Hacker using mainly side channel or fault injection attacks

  - Mainly evolution not revolution of attacks
    - More sophisticated tools efficient with lower leakages

- **New attack paths**

  New technologies may present new/unknown weaknesses

  Lack of history in the field, less time spend by hackers

  - **Contactless**
    - Limited power budget (some application) => reduce possibility of countermeasures (less computing power e.g. key length reduction…)
    - Chip Power generated by RF
  - **New crypto Algorithms**
    - E.g. Elliptic Curves,…

Attacks Countermeasures (non exhaustive)

- **Non invasive attacks**
  - Software attacks counter-measures
    - Operating system, crypto algorithms: controls most of the non invasive attacks in software (no residual ISO test commands, brute force attacks resistance, …)
    - FireWall/Memory Protection Unit, OTP, Chip ID,..: controls access to memories
    - Environment attacks counter-measures: (V, t°, F, UV, Light,…)
  - Side channel attacks counter measures
    - Filters, clock management, random processes, bus and memory encryption: minimize exploitable leakage, desynchronizes the traces (no ref)
    - Timing analysis resistance, hamming weight
  - Fault injection counter measures
    - Filters, clock management, specific layout: reduce attack entry point
    - Illegal code/address detection, CRC,…: treat residual attack effect
- **Invasive attacks**

  Secure/dense chip layout, active shield, physical encryption of memories ,Fast Memory wiping, secure test structures/protocols, fake circuitry,…

Attacks Countermeasures (trends)

- **Strategy**
  - **Up to recently**
    - Focus on countermeasure for specific attack, reduce attack “power”
      - E.g. laser attack => shield
      - Difficult to find a “patch” for each attack, specifically new attacks
      - “Costly” strategy, does not prevent new attacks
  - **Now**
    - Focus on effect of a set of attacks
      - E.g. Fault injection => memory corrupted => check memory integrity
      - Provide more “checkers” to software developer
      - Better trade off cost-security
- **Conclusion**
  - Secured smart card (or e-passport) = Secured Hardware + Secured Software
    - Good adaptation of software with hardware
    - For given security target / price => best distribution of security tasks between soft and hardware

Security Certification Schemes

- **Common Criteria (ISO 15408) Rev 2.4 => Rev 3.0 (2007)**
  - Flow: Hardware security Test -> Software development -> Hardware + Software test
  - Complete evaluation, but long process
  - Wildly recognized (C.C. Mutual arrangement www.common-criteria.org)
  - Protection Profile PP9806 (Eurosmart) and PPSSVG (BSI-PP0002)
  - AIS 20 (Deterministic RNG), AIS 31 (TRNG)
  - EAL4+ vs EAL5+
    - Same security features and physical security level for both4+ and 5+
      - AVA_VLA.4, AVA_VAN.5
    - EAL5+ adds semi-formal or formal modeling of the chip to ensure design and test is done more systematically (quality assurance, not security assurance !).
- **FIPS**
  - **FIPS140-2 Level 4**
    - Hardware + Software Only
    - Strong on crypto (compliance w/ NIST standards), tamper resistant hardware
      - FIPS 140-3 should better cover mitigation of other attacks (side channel, fault injection)
      - Verification of algorithm implementation
  - **FIPS 201**
    - Functional specification for HSPD12 (NIST SP800-xxx/X.509)

Security Certification Schemes

- **Visa / Master Card**
  - EMV, SDA/DDA,..
  - Penetration test on hardware (approved labs), penetration test on software
  - Evolution to C.C. scheme (EMVco)

- **ZKA (German banks)**
  - Penetration test on hardware (approved labs), software audit
  - Evolution to C.C.

- **JCB**
  - Penetration test on hardware (approved labs), penetration test on software

- **Conlcusion**
  - **Many different schemes: still low mutual recognition => costly, time consuming**
  - **Time to market can be critical**
  - **Security has a cost, security level to be in line with value to protect**

Examples: Third Parties Security Evaluations

	Common Criteria				Other Approvals
Product Name	**Cert Date**	**PP**	**Cert #**	**Level**	
AT05SC1604R	06-Dec-04	PP-9806	2004/22	EAL4+	
AT90SC6464C	24-Aug-01	PP-9806	2001/14	EAL1+	
AT90SC19264RC	4-Nov-02	PP-9806	2002/24	EAL4+	
AT90SC9616RC	22-Sep-03	PP-9806	2003/16	EAL4+	
AT90SC9608RC	2-Apr-04	PP-9806	2004/05	EAL4+	
AT90SC6404R	19-Feb-04	PP-9806	2004/02	EAL4+	
AT90SC3232CS	13-Nov-03	PP-9806	2003/20	EAL4+	
AT90SC6404RT	14-Feb-05	PP-9806	2005/03	EAL4+	
AT90SC7272C	11-Mar-05	PP-9806	2005/05	EAL4+	
AT90SC12836RCT	28-Jul-05	PP-9806	2005/20	EAL4+	
AT90SC9618RT	02-Dec-05	PP-9806	2005/43	EAL4+	
AT90SC6404RFT	N/A				
AT90SC12872RCFT	22-Dec-05	PP 9806	2005/49	EAL4+	

Flash-based vs ROM-based Products

- **Flash-based products vs ROM-based products**
  - **Time to market**
  - **Easy deployment of new cards in the field**
    - Algorithm changes
- **Security**
  - **NVM Memory point is made of charges, ROM of physical patterns**
  - **Customer needs to submit ROM code to silicon manufacturer**
    - Tracibility
  - **Atmel has EAL4+ security certification for Flash based products**
- **Specific security for Flash based products**
  - **Secure bootloader (download code to Flash with authentication)**
  - **Flash locked at factory, cannot be updated in the field**
    - Flexibility for card manufacturing
  - **Controlled distribution**
    - Only samples or
    - Factory programming with lock Flash option

Conclusions

- **Non invasive attacks are deploying very fast**
  - **System security is more and more dependant on the close link between Hardware and Software**
- **Amel has products for every applications**
  - **With the right level of security**
  - **With appropriated security certification**

A reference in the security market

✉ benoit.makowka@rfo.atmel.com

www.atmel.com

During breaks, please come and see our demos:

- e-passport
- HSPD12