



OCOVA 2007

Authentication / Identification Innovations in Chip Security and Design

Michel Bartosik

Product Line Manager

Banking & ID

ATMEL Rousset





What to Secure ?

- **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**

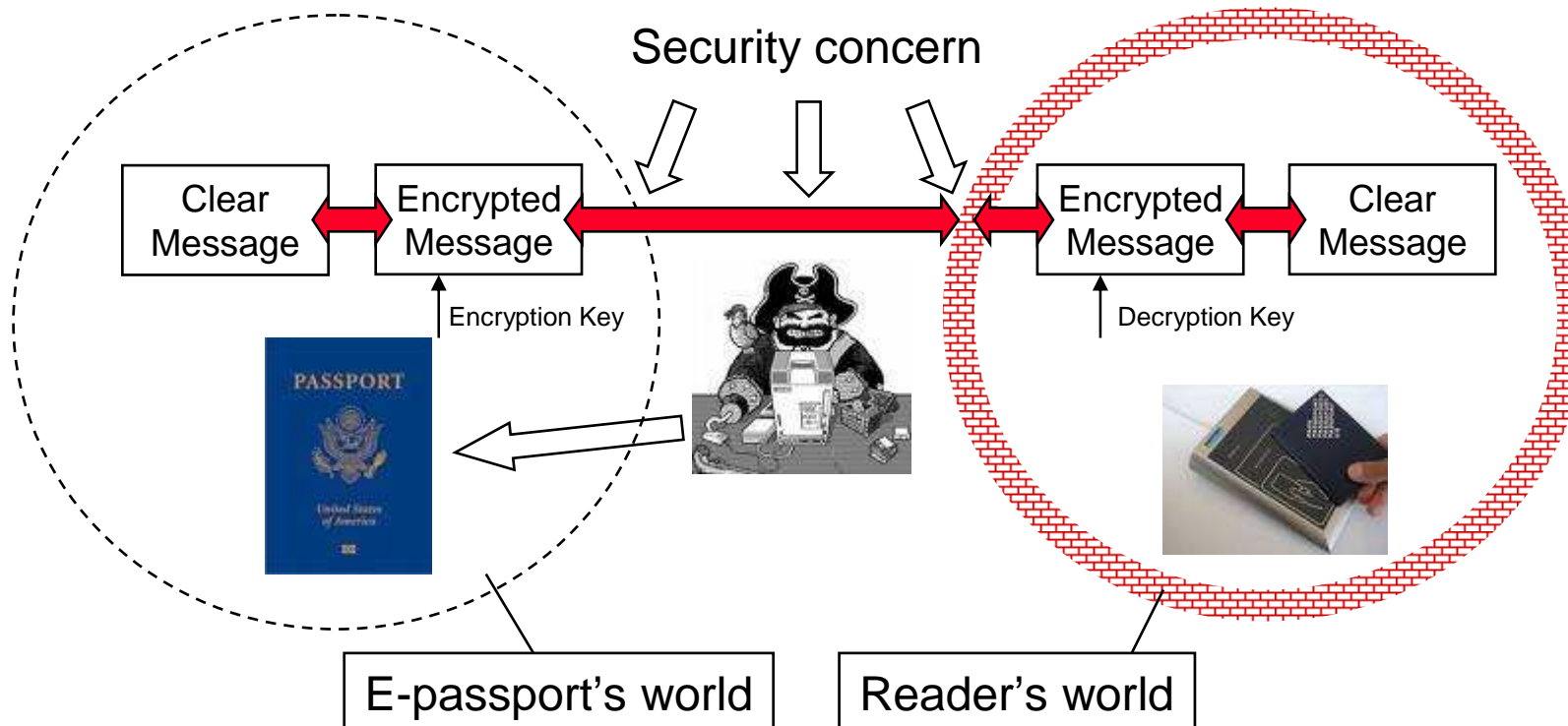
- Generate crypto Key
 - Encrypt/decrypt data (stored in EEPROM or transferred through I/O)
 - Secure the access to the EEPROM (verification right access)
 - Secure transaction with external reader (contact and/or contactless)
 - Execute Application (e.g. Java applets).

- **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,...

For Instance, to Secure the “e-Passport”

- Goal: securely transfer information between e-passport and reader
- Hacker has access to e-passport’s worlds
- Security relays on Encryption Algorithms, offer good security
- E-passport chip must be tamper resistant





Attack Protections (not exhaustive...by far)

■ Burt force attacks are protected thanks to

- **Trusted** Operating system and crypto algorithms, dynamic memory on chip encryption, Fire-wall / Memory Protection Unit, OTP zones, Chip ID,...

■ Side channel (analysis of electrical chip parameter: power, EMC,...) , Fault injections (Vcc, Frequency,.. spikes/glitches, Light attacks,..) attacks are protected thanks to

- Environment attacks counter-measures (V, t°, F, UV, Light,...), Filters, architecture (layout,, redundancy, memory encryption, clock management, Illegal code/address detection, CRC, code integrity check,...

■ Invasive attacks are protected thanks to

- secure/dense chip layout, active shield, memory encryption, Fast Memory wiping, secure test structures/protocols, fake circuitry,...

■ Moving from “patch” to “trap”

- Our mission: Be ahead of imagining new attacks an protections
- New attacks will come
- Difficult to find a patch now for future attacks
- Attacks may be unknown but effects of attack are known
- Solution: Focus on attack effect rather than attack source
- Requires stronger interactivity between chip Hardware and Operating System



To Protect the Electronics Industry

■ HIGH-TECH GOODS COUNTERFEITING

- Cell phones, computers, printer cartridges, ...
- \$100 B lost each year



■ MULTIMEDIA CONTENT COPYING

- Music, movies, software, ...
- Hackers regularly crack Digital Rights Management (DRM) systems, see the famous CSS (Content Scrambling System) algorithm used for DVD copy protection



■ IDENTITY THEFT OF WEB APPLICATIONS

- Banking, shopping, ...
- \$55 B lost in 2005 on the US alone
- Online attacks rare, phishing exponentially growing

Multi-Factor Secure Solutions to Use

■ SECURE YOUR HARDWARE – ANTI-CLONING SOLUTIONS

For instance, cell-phone battery anti-cloning system

■ SECURE YOUR DIGITAL CONTENTS – DRM AND SOFTWARE COPY PROTECTION

For instance, media player
... or software protection

■ SECURE YOUR PRIVACY – MULTI-FACTOR USER AUTHENTICATION SOLUTION

USB tokens common features to perform

- One-time password generation
- Challenge response authentication
- Token holder authentication

