

Survey of Cryptographic Smart Card Capabilities and Vulnerabilities

by Ronald Ward

May 3, 2001

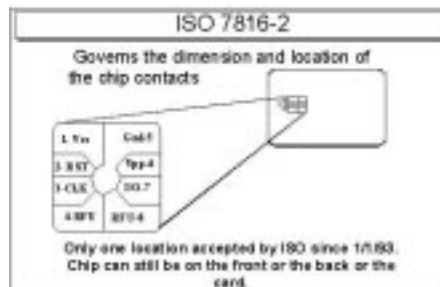
Outline of Presentation

- Introduction to Smart Cards
- Cryptographic Smart Cards
- Security Attacks
- Conclusions

Introduction to Smart Cards

Smart Card Interfaces and Sizes

- ISO 7816 is the standard interface for virtually all smart cards
- Smart cards come in three sizes
 - the largest is credit card sized
 - the smallest is a little bigger than the ISO 7816 interface



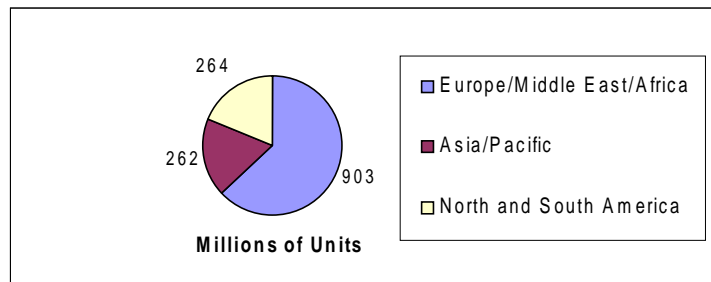
- Smart Tokens with USB ports are becoming widespread, also.

Applications of Smart Cards

- Authentication Card
 - for network access, digital signatures
- Stored Value Card
 - for loyalty programs, prepaid TV, telephone services
- Multiple Application Card
 - JavaCard
 - Smart Card for Windows

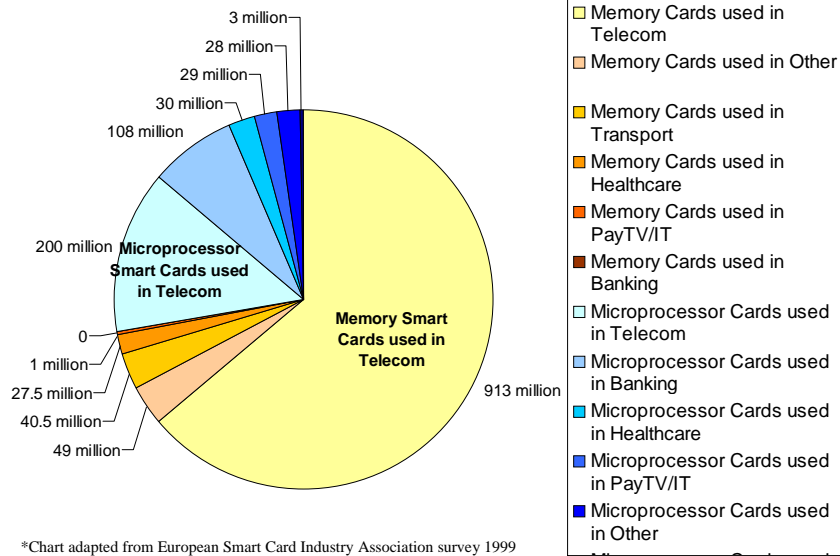
Markets for Smart Cards

- The main market for Smart Cards is currently in European Telecommunications (GSM)



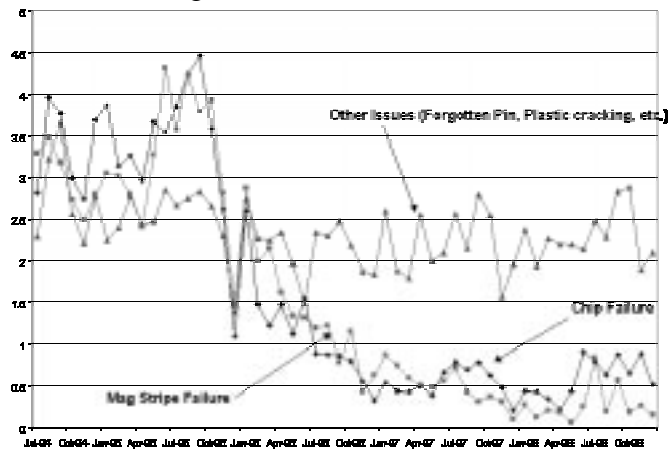
*Chart adapted from European Smart Card Industry Association survey 1999

Markets for Smart Cards



Reliability of Smart Cards

Percentage of Cards Returned Over Time



*Graphic courtesy Schlumberger and GE Carte Bancaire

Cryptographic Smart Cards

Cryptographic Smart Card Vendors

Europe	US
Gemplus	Invincible Data Systems
ORGA	Litronics, Inc.
Schlumberger ET	Racal Security & Payments
Bull - CP8	VASCO Data Security, Inc.
Gieseche & Devrient	ActivCard, Inc.
BasicCard	Certicom
SCM Microsystems	HID Corporation
Omnikey	IBM Corporation
Advanced Card Systems	Information Resource Engineering, Inc.
Athena SmartCard Solutions	Ankari
Intertex IX	Okiok Data

Major Manufacturers of Crypto Co-Processors (CCP)

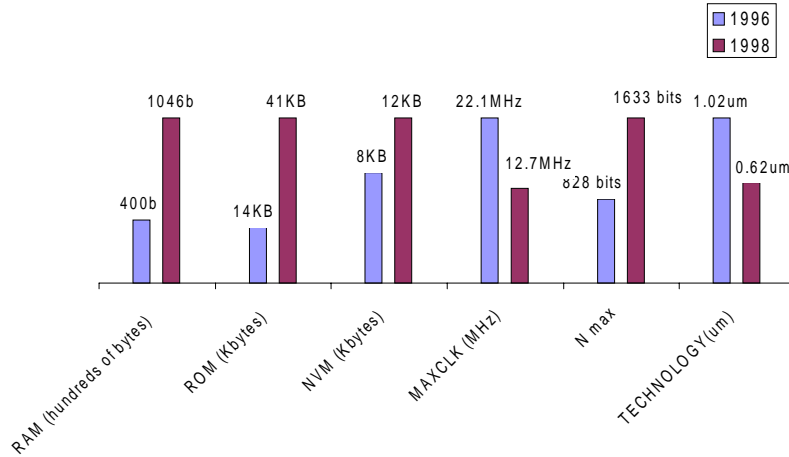
- SGS Thomson
- Siemens
- Philips
- Motorola
- SEPT
- Cylink Corporation
- Atmel
- Fondazione Ugo Bordoni/Amtec
- Pijnenburg
- Hitachi
- Oki

Key Sizes on CCP's

- DES and SHA
 - Available on most ccp's with standard key sizes (64 bits and 512 bits, respectively)
- MD5
 - Available on a few ccp's with key size of 512 bits.
- Elliptic Curve Digital Signature Algorithm
 - Available on only a few ccp's with key size up to 255 bits
- RSA Signature
 - Available on virtually all ccp's with key size of 512 bits on most, and up to 2048 bits on a few
- Digital Signature Algorithm
 - Available on many ccp's with key size up to 1024 bits

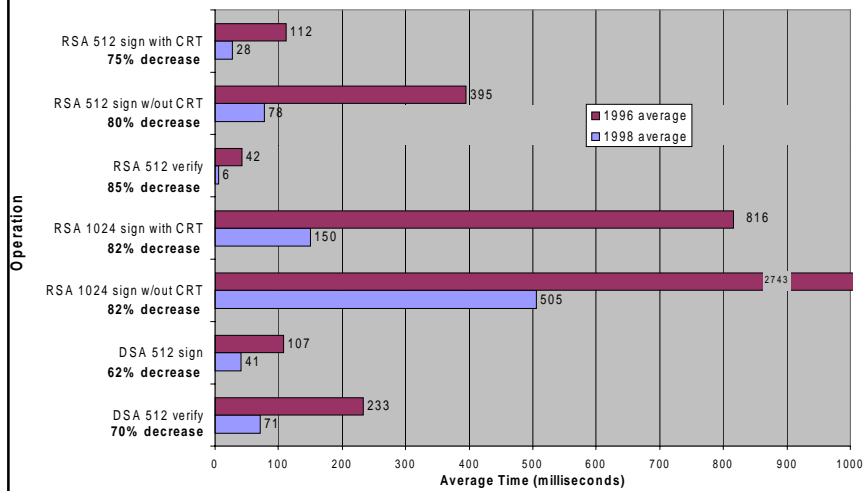
Improvement of CCP's

Comparison of Common Characteristics of Crypto Co-Processors
1996 vs 1998



Improvement of CCP's ... (continued)

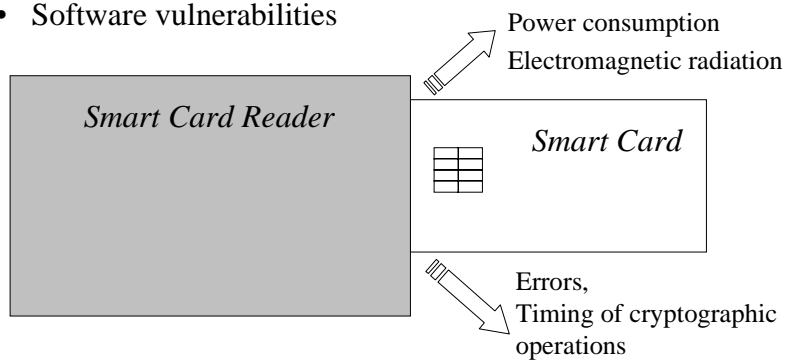
Average Time of Cryptographic Operations 1996 vs 1998



Security Attacks

Non-Invasive Attacks

- Simple and Differential Power Analysis
- Timing Analysis
- Glitch attacks, or fault generation attacks
- Software vulnerabilities



Invasive Attacks

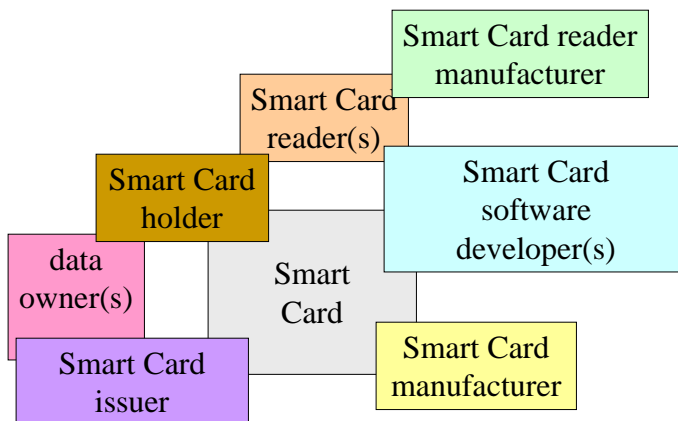
- Test pad repairing
- Microprobing
- Layout reconstruction
- Focused Ion Beam editing



Blown polysilicon fuse near test pad (Motorola)

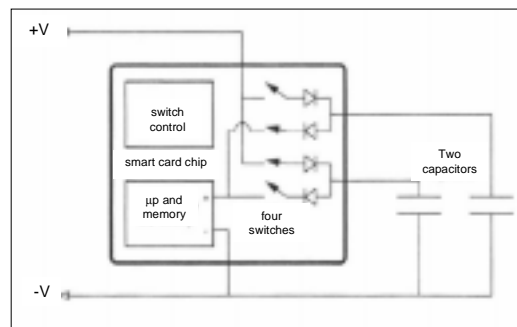


Attacks Because of Trust Splits



Countermeasures

- Non-Invasive Attacks
 - SPA/DPA can be prevented with capacitor network at the power supply input, proposed by Shamir at CHES 2000.



Countermeasures ...(continued)

- Non-Invasive attacks ...(continued)
 - Timing Analysis can be prevented using non-linear key updating.
 - Glitch attacks and fault generation attacks can be prevented using 1) randomized clock signals/multithreading or 2) sensors to detect out of range clock speeds, voltages and temperatures.
- Invasive attacks
 - glue logic, a random layout of chip logic; implemented in some Philips chips
- Trust Splits
 - Promote widespread public examination of smart card based systems before deployment
 - Authenticate all parties involved in transaction
 - Use open source implementations

Conclusions

Conclusions

- Smart Cards are
 - continually improving
 - Inexpensive
 - ultra-convenient
- Yet, there are many security risks to be overcome
 - Tamper resistance
 - Differential Power Analysis

Conclusions

- Proponents of JavaCard claim that it is eventually going to be the largest deployed computing platform in the world.
- Smart Cards have great potential and will likely be applied to new markets not yet conceived of.