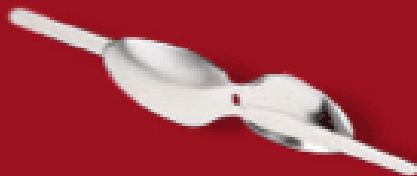




**IMPROVE YOUR
PATTERNS AT
JAVAPOLIS 2005.**

**METROPOLIS ANTWERP,
DECEMBER 12 UNTIL 16.**





JavaCard vs. Secure Smartcard-using Applications

Danny De Cock

Researcher Applied Cryptography

K.U.Leuven ESAT/COSIC





Overall Presentation Goal

Risks and False Assumptions Using JavaCard





Speaker's Qualifications

- Danny De Cock is well known in the Belgian eID card environment
- Danny De Cock cooperates with governments and large/huge companies to integrate and support smart card technology
- Danny De Cock manages several identity management projects relying on javacard prototypes
- Danny De Cock speaks frequently on security issues at conferences and workshops





This Slide Gains Your Audience's Attention

JavaCard

Opens the Gates to Heaven

AND

The Gates to Hell





Outline

- Clear advantages of JavaCard
- Wide variety of applications
- Risks & Tendencies
- Consequences
- Summary



Advantages of JavaCard

- Wide availability
- Vendor-independence
 - No ROM masking
- Easy and rapid prototyping
- Java-based
 - Easy to understand and learn
- Provides efficient means for
 - Strong authentication mechanisms
 - Tamper-evident hardware





Wide variety of applications

- Tendency to replace custom-designed smart cards
 - Loyalty & Membership (multi-application badges)
 - Money transactions (EMV, Proton,...)
 - Identity documents (eID, passport,...)



Risks

- Years of standardization effort risk to be lost
- False sense of security when using smart cards in security-critical applications
- Wide diversification of smart card standards and their APIs
- In the old days: smart card = top-shelf security
- Near future: very critical with respect to smartcard using applications!
- Rapid prototyping leads to trial-and-error deployment





Advantages of Custom-design

- Centralized know-how
 - Security-critical design criteria
 - Advanced attacks: SPA, DPA, EMA, timing
 - Longer time to market
 - Time = money
 - Each design or security problem results in significant losses
- Dedicated personalization centers





Advantages of Custom-design (ctd)

- Devices can be carefully audited
 - E.g., Common Criteria EAL4+, EAL5+,...
- Bottom line:
 - Smart card-using applications depend on a carefully build-up context of trust
 - But JavaCards provide a false sense of security!





JavaCard Business Models

- Vendors provide JavaCards
 - With personalized applets
 - But: push model for PC middleware licenses
 - With non-personalized cards
 - Default personalization keys
 - No applets
 - With EAL5+ certificate for chip
 - With EAL4+ certificate for JavaCard OS

- Customer is stimulated to write **proprietary** applications

Expensive!

Undermines
certificate
reputation!



Proprietary JavaCard

- Customized APDU commands
- Insecure PIN management
- Insecure private key usage
- Non-standard behavior
- Trojan horse implementations





What to do about it?

- Very little
- Doing it properly costs much money
 - Hire experienced implementers
 - Order personalized JavaCards
 - Personalize the cards with audited applets
- Applications must carefully verify
 - What smart card is being used
 - Huge responsibility for application developers!





Summary

- JavaCard is ideal enabler for widespread integration of smart card functionality
- Significant risks that smart cards become untrustworthy
 - Lack of standardization
 - Lack of control mechanisms
 - Everybody re-implements the wheel
- Smart card-using applications must carefully validate
 - Smart card type
 - Smart card crypto content





If You Only Remember One Thing...

Do not do program JavaCards at home 😊





Q&A

My email: godot@godot.be

Slides available at:

<http://www.godot.be/slides>





**IMPROVE YOUR
PATTERNS AT
JAVAPOLIS 2005.**

**METROPOLIS ANTWERP,
DECEMBER 12 UNTIL 16.**

