Toward Common Understanding of Smart Card Protection Profiles

EU- Japan Security Conference

Ken Ayer

Chair, SCSUG

Vice President, Visa International

Today's Presentation Agenda

- Why test at all
- Smart Card Security Working Group
- Smart Card Profile Status
- Lessons Learned
- Next steps

Why test?

- Visa has tested hundreds of smart cards since 1995.
- Most fail functional testing the first time around.
- About a third failed security testing after they passed functional.
- Situation is improving considerably.

Why Use the Common Criteria

- International Standard – ISO 15408
- Multi-Industry
- Permits competitors to cooperate on security
- Consistent evaluations permit comparison shopping by Users
- Has dispute resolution process

Smart Card Security Users Group

- Formed June 1999
- American Express, Europay, JCB, MasterCard, Mondex, Visa with NIAP & other Common Criteria Authorities
- Goal: Protection Profile(s) for financial applications & others with similar needs
- Smart Card Profile drafted, posted for comment, reviewed - 6th draft now

SCSUG Smart Card Protection Profile

- Covers basic platform, single or multiple application, fixed or the new reconfigurable technologies
- Evolved from earlier work by each payment system, others
- Draft was posted for comment for 3 months, after separate vendor reviews
- Has been evaluated by labs accredited in Canada, France, Germany, US

Lessons Learned

- **Some Common Criteria concepts are not clear when smart cards are involved**
  - **Technological questions**
    - **Can smart card achieve the highest security rating? What does AVA_VLA.4 mean?**
    - **Can smart cards have a Covert Channel (AVA_CCA)?**
    - **How does one say “disable test mode” in CC?**
  - **Composability, re-usability**
    - **How can evaluator do chip families?**
    - **How can card evaluator share chip evaluation, perhaps done in a different country?**

Answering Questions

- Must have authoritative clarification to achieve comparability
- Everyone needs comparability – all evaluations must be done to same standard
- CC Interpretations Management Board can provide that

Cooperation with Others

- Global Platform, Inc - Open Platform Profile

  see http://www.visa.com/nt/suppliers/open/protect_form
- Secure Silicon Vendors Group
- Eurosmart
- Japan – ECSEC, NMDA
- Other application providers

EMV Security Working Group

- Currently working on draft Protection Profile for EMV credit/debit application
- Will use SCSUG PP as platform
- Work in Progress
- Will be shared across EMV systems

Future Activities

- Certify & Register Profile
- Ask CC Interpretations Management Board to clarify several points
- Write application Profiles
- Vendors will build Security Targets
- Smart cards will be built & evaluated
- Will be revised as necessary as we gain experience with CC process

Future Activities

- Lab accreditation needs smart card specific capability
- Test methods need development
- Additional application specific profiles possible
- Revise in light of feedback from ST, product evaluations
- On-going monitoring & evolution of process

Information & Comments

www.scsug.org or http://csrc.nist.gov/cc/sc/sclist.htm

- **American Express**
  Mark Merkow
  mark.merkow@aexp.com
- **Europay**
  Fernando Lourenco
  fel@europay.com
- **JCB**
  Toshiaki Kuzuki
  kuzuki@jcb.japanglobe.net
- **MasterCard**
  Simon Pugh
  Simon_Pugh@mastercard. com
- **Mondex**
  Alan Mushing
  alan.mushing@mondex.com
- **NIAP**
  Gene Troy
  eugene.troy@nist.gov
- **Visa**
  Ken Ayer
  kayer@visa.com