Smart Cards: Issues and Answers

1

Convenience and Security

- For a system to be *secure* and *convenient* it must transparently incorporate authentication, access control, and encryption
  - Wallet portability is a ***must-have***
- Systems that are not *convenient* are never *secure* because users bypass the security

2

Over-Security

- If the security of the system is stronger than the security of the user then you've achieved about as much as you can with technology
  - A .44 magnum and a kind word will compromise ***all*** known security systems
- Smart cards are a great technology for high grade convenient security

3

Why Smart Cards?

- Smart cards:
  - Carry stored values
  - Carry encryption/authentication keys
  - Carry storage for multiple purposes at once
  - Perform secure computation on the card
  - Fit in your wallet
  - Cost less than other authentication tokens

4

Why not Smart Cards?

- Factors inhibiting uptake of smart cards
  - Lack of ubiquitous card readers
  - Lack of standards
    - Cards are standard but applications are not
  - Lack of software
    - Card vendors using incompatible APIs
  - Lack of industry focus
    - End users are not ready - yet
    - Incompatible base of automatic teller machines

5

What about X.509 IDs?

- X.509 certificates are a software public key-based identity
  - Require a host processor and application in order to use them
  - Require more data than can be memorized and carried in user's head (~2-3Kb)
  - Host-processor applications vulnerable to certificate stealing applications

6

Smart Cards and X.509

- Within 1 year X.509 certificates will be widely used for Ecommerce
- Within 2 years X.509 certificates will be widely stolen by hacker software
- Within 5 years smart cards will be the preferred carrying place for X.509 certificates

7

Evolution of Online Banking

- Phase 1: Early Dialup Phase
  - Access to banking online via dedicated dial system
  - Minimal security: nobody can hack a ***telephone***, right?
  - Minimal functionality: check balances, authorize checks

8

Evolution of Online Banking

- Phase 2: Early Web Phase
  - Access to banking via web
  - Minimal security: passwords + SSL or worse
  - Minimal functionality: check balances, authorize checks
  - Some micropayment prototypes

9

Evolution of Online Banking

- Phase 3: Current State of Art
  - Access to banking via secure web transaction
  - Moderate security: X.509 certificates + SSL
  - Moderate functionality: move cash around, perform simple transactions
  - Interface to micropayment / some web payment systems

10

Evolution of Online Banking

- Phase 4: Completely Integrated Networked Cash Environment:
  - Web based access with smart card based security
  - Portable cash storage on card
  - Card downloadable via web
  - Card accepted at point-of-sale terminals
  - Card uploadable to other businesses

11

1996: The State of the Art

- Wells Fargo Bank current strategies:
  - Internet-based banking using Netscape and SSL
  - Smart-card-based banking using automatic teller machines that update stored value
  - Smart-card-based point of sale terminals with selected merchants in San Francisco area

12

1999: The State of the Art

- Completely integrated network cash
  - User accesses bank
  - User downloads $50 to card
  - User puts card in wallet and walks to ***7-11***
  - User purchases coffee
- Cash-and-carry solutions cannot be implemented via browser/host system
  - Imagine hauling your PC to ***7-11***!!

13

Other Smart Card Applications

- Medical records:
  - Health care service gives user a smart card
  - Card contains
    - Public data area with emergency information (blood type, allergies, etc.)
    - Private data area with access keys to full medical records
  - User may choose to authorize access to full records via Internet as appropriate

14

Other Smart Card Applications

- User file protection:
  - Data in database is stored encrypted under user's key
  - Key is stored in card protected by a PIN
  - User can now access data ***independent of location*** with complete security
  - Encryption/decryption may be performed at user's desktop for maximum security/performance

15

Location Independence

- Perhaps the greatest value of smart cards is they may offer location independent computing
- Wherever you go, there you are
- Location Independence is why almost everyone carries credit cards
  - Market penetration is best when portability is best!

16

Current Technologies

- Visa cash
  - Stored value cards for Atlanta Olympics
  - No network connectivity
- Java Smartcard Spec
  - Cooperative effort to design a smart card interface callable from Java
  - Will enable (hopefully) card-independent and machine-independent smart cards

17

The Future of Authentication

- Future authentication technologies will split into 2 forms:
  - Software based solutions
  - Smart card based solutions
- Current authentication tokens (time cards, authentication calculators, etc.) will fall by wayside
  - They cannot ***participate*** in transactions

18

Summary

- Smart cards are here
- Smart cards are very cool
- Smart cards are the future

19