Emerging Security Technologies:  
E-Cash, Passport, and TCPA

Facilitator: Jonathan Aldrich

Today: New Security Technologies

- Anonymous micropayments
  - E-Cash
- Universal authentication
  - Passport
- Remote verification of software
  - TCPA
Electronic Micropayments

Security application:
• Shift cost of denial of service attacks
  – Users pay for bandwidth, web usage
  – Encourage users to secure machines
• Sufficient incentive?
  – Cost diluted over all compromised users
  – Web site still down
• May be unrealistic
  – Market pressure towards simple cost models

Anonymous E-Cash

• An electronic bank note
  – Comes in 2 halves
    • Random number a
    • a XOR account #
  – Also signed by the bank
• Spending the note
  – Vendor gets to choose learning first or second half
  – If spent twice, 50% chance account # is revealed
    • Use an array of halves to increase chance
Anonymous E-Cash

- Do we really care about anonymity?
  - Micropayments can be provided other ways
- Who would want anonymity?
  - Criminals
  - Paranoid users
  - Anonymous donors
  - Others?

Passport Motivation

- Many online merchants
  - Each authenticates with username + password
- Single signon via Passport
  - Central authentication server
  - Access multiple sites with one password
- Future extensions?? (speculative)
  - Single notion of identity on network
  - Access control, rate limiting, logging, analysis
The Passport Protocol

1. Request page
2. Auto-redirect
3. Redirect with tokens in header
4. Request credentials
5. Login & password
6. Redirect w/username in header
7. Request page w/credentials
8. Set cookie

Is This a Good Idea?

- Single signon introduces risks
  - Centralization
  - Technological
- Alternatives
  - Use same username/password everywhere
  - Write down a list of passwords
  - Others?
Risks and/or Attacks

• User interface issues
  – Hotmail confusion: two ways to log out
  – Netscape: lack of sign-off confirmation
• Denial of Service on centralized system
• Build fake Passport site
  – Need to fool, break, or bribe a CA
  – DNS spoofing makes this more believable

Could Passport Be Done Better?

• My opinion: not without better technology
  – Secure redirects
  – Secure DNS
  – Defense against DoS
  – Smart card authentication
• Still issues
  – Bugs, UI, central server, impersonation
TPCA/Palladium Motivation

- Software agents
  - Run on machine owned by untrusted entity
  - Ensure that private data isn’t compromised
- Hardware provides trust
  - Software easily broken or simulated
  - Hardware expensive to break or reverse-engineer
- This is about trusting a remote system, not your own

The “Fritz” Chip
(in honor of Senator Fritz Hollings, Hollywood puppet)

- Takes control of OS loading
  - Ensures a “trusted” OS, signed by TPCA lab
  - OS then ensures select apps are trusted
- Verifies trusted platform to clients
  - Client challenges server to prove it’s trusted
  - Fritz chip holds the secret used for verification
  - Client proceeds if it trusts the app
Potential Applications

• Software agents
• Grid computing
• Digital rights management
• Anti-piracy
• Rented software
• Enforce classified rules
• Disable rogue software and data remotely
• Enforce monopoly on related products

Possible Social Consequences

• Draconian copyright enforcement
  – No way to support fair use
  – Can’t translate an e-book to Braille
• Forced incompatibility \rightarrow reduced competition
• Marginalizes or restricts free software
• Enabler for censorship
  – Documents can be made unreadable remotely
  – Whistle-blowers are handicapped