Trusted Input Devices
Distributed Strong Authentication

States Security Research Workshop
Carnegie Mellon University
March 28, 2002
Lark M. Allen / Wave Systems
Lallen@wavesys.com

Authentication Challenges

- Personal computers are *untrusted* devices
  - Input, processing, and output cannot be protected or hidden from interception, observation, and hacking
- Centralized authentication approaches have major issues
  - Broadly available national biometric databases for fingerprints, facial prints, iris scans, and other personally identifiable information are unlikely due to privacy issues
  - Inadequate scalability and long response times for most applications
- Identity is context related (businesses, organizations, states) with little or no interoperability
- No indemnification for authentication 'mistakes'
Authentication and Privacy

- Privacy is growing social issue, even post 9/11
- EU, Canada and others with tough Data Protection laws
- Authentication and Privacy must find acceptable ‘balance’
- Where authentication is done will affect privacy concerns
- Users will ‘opt-in’ for benefits, i.e. faster airport security

Authentication –Trusted?

Identity

- HAVE
- KNOW
- ARE
  - Password
  - User ID
  - PIN

Authentication

- Trusted
- Untrusted

Access
**Trusted Input Device - Architecture**

- **Authentication** must be done in a trusted location.
- Trusted devices can communicate securely over untrusted networks.

**Extending Trust to the Edge**

- End-end security
- Multi-layer protections
- Workgroups and peer-peer enabled
- Data / user level trust boundaries
Infrastructure Security Requirements

- Dynamic and broad range of security needs
  - Platform, File, and Application Security
  - Strong Authentication
  - Content and Services Protection
  - Privacy Solutions
  - E-Commerce
  - VPNs, Communications
  - Digital Signatures
- Security of hardware, flexibility of software, future-proof
- Internet must deploy new trusted layer – every component and device must have ‘trusted’ mode

Challenge - Interoperable Trusted Entities
Trusted Input Device - Components

- EMBASSY
- Trusted Client Platform
- Strong Cryptography
- Secure Display
- Secure Input
- Secure Processing
- Secure Storage
- Secure Time

Trusted Input Devices - Applications

- Finance Industry
  - FinRead – European Union Spec for Trusted Financial Readers
    - ‘Card Holder Present’
    - E-Commerce Transactions
- Strong Authentication
  - Network and System Access
  - Digital Signature
  - Physical Access
- On-Line Gaming
  - Financial, GPS, Biometric, Smart Card, Password Authentication
- Entertainment
  - Age-Based Access
EMBASSY Trusted Client Platform

‘Sovereign and Protected Place in a Hostile Territory’

Trust Assurance Network
- Digital Signature
- Music DRM
- Video PPV

Device Trust Services, Secure Applet Management

Video PPV
- Processor
- Interfaces /Storage
- Clock
- Crypto

Application
- EMBASSY CHIP/Trusted OS
- Hard Disk
- Music DRM

Pyramid of Protection

EMBASSY Trust System
- Trusted Unshared Hardware
- Trusted Shared Hardware
- DRM
- TCPA
- BIOS

Security Strength

Secure Software
EMBASSY Trusted Client Applications

- Strong Authentication
- Privacy Protection
- Platform Security (TCPA)
- Content Protection
- Secure Delivery
- E-Commerce
- Distributed Transactions
- Conditional Access
- Secure Peer-Peer

Strategic: Independent Trust Domains

- SERVICE A Trust Domain
- Applet A
- SERVICE B Trust Domain
- Applet B
- SERVICE C Trust Domain
- Applet C
- Device Trust Domain

Shared, Multi-Party Trusted Devices
Trust Assurance Network - PKI

Benefits – Trusted Client Devices

- **Authentication at the network edge**
  - Strong, multi-factor authentication
  - Addresses major security exposure – The PC
  - Scalability and responsiveness
  - Key building block for end-to-end security
  - Extends existing network and server security solutions

- **Balances authentication and privacy**
  - Minimizes need for centralized databases and monitoring of entire population
  - More easily addresses issues of small high risk security exposure groups

- **Flexibility and future-proofed infrastructure**
  - Programmable security
  - Multi-party trust – supports multiple identity systems and trust domains in single devices