Smart Cards & Remote Entrusting

Jean-Daniel Aussel & Jerome d’Annoville

RE-TRUST workshop, Trento

October 15, 2008
Voice Over IP Softphone

- The softphone needs access to the card (UICC) for retrieving phonebook entries or authenticate to the network.
- The card must be sure that it is used by the genuine softphone, and that the softphone has not been tampered with before releasing data or performing authentication.
Overview of Remote Entrusting with Smart Cards

Smart Card
- Service: Data Access
  - Cryptography
- Properties Analyzer

Untrusted Computer
- Monitor
  - Keys
  - Memory thumbprints
- Report Properties
  - Update Properties

Provide or shutdown service

Trusted Application

Service:
- Data Access
- Cryptography
Smart Card for Remote Entrusting

• Dongle with USB 2.0 interface for high speed communication
• Flash memory to store trusted application that will be provisioned to the un-trusted terminal
• Monitor, keys and thumbprints are embedded in the trusted application
• Zero install: does not required any driver, and uses the mass-storage interface (USB memory stick and CDROM operating system drivers)
• Provide secure channel access to standard smart cards (e.g. SIM card)
Secure Channel Establishment: Card Insertion

- **CTRL**
- **CDRom (wireless)**
- **Private**
- **Public**
- **TrustedApplication.exe**
- **BUS flash**
- **ISO 7816**
- **Opaque**
- **Obfuscation Algorithm**
- **[Security Level, Km, Ks, Kt]**
- **Diversified area**
- **Km**
- **Ks**
- **Random**
Secure Channel: Messaging

Host PC
get and execute
TrustedApplication.exe

Message To Send

Masked Keys (Km, Ks)

Obfuscation Algorithm
Extract Ks

Ks

Ciphered Message

Cipher

Message

TrustedApplication.exe

ctrl

CDRom (wireless)

TrustedApplication.exe

ISO 7816

Private

Public

UICC

Ks

Ciphered Message

Decipher

Message
Thumbprints

- A thumbprint is a section of code segment which is hashed
- A set of thumbprints is stored in the smart card at personalization time (code segment hash, offset and length)
- Thumbprints are used for secure channel session key renewal regularly
Thank You

Questions?