Developing Trusted Services for Mobile using GlobalPlatform Standards

Christophe Colas
GlobalPlatform Device Committee Chairman
GlobalPlatform is the standard for managing applications on secure chip technology.

Across several market sectors and in converging sectors:
Device Committee Activities

Device Committee
Christophe Colas, Trusted Logic

Trusted Execution Environment (TEE)

- TEE Roadmap WG
  Christophe Colas, Trusted Logic
- TEE Spec WG
  Don Felton, ARM
- TEE Compliance WG
  Hervé Sibert, ST-Ericsson
- TEE Security WG
  Hervé Sibert, ST-Ericsson

Device Services

- SE Remote Administration WG
  Christophe Colas, Trusted Logic (acting)
- SE Access Control WG
  Erwan Louët, Orange Labs
Google Pulls 21 Apps In Android Malware Scare

Google has just pulled 21 popular free apps from the Android Market. According to the company, the apps are malware aimed at getting root access to the user's device, gathering a wide range of available data, and downloading more code to it without the user's knowledge.

Although Google has swiftly removed the apps after being notified (by the ever-vigilant Android Police bloggers), the apps in question have been downloaded by at least 50,000 Android users.

Netflix Only Coming to 'Select' Android Phones Next Year

Netflix has not yet extended its streaming service to the entire Android platform due to security and content protection concerns, but the company will roll it out to select Android handsets next year, Netflix said in a Friday blog post.

“The hurdle has been the lack of a generic and complete platform security and content protection mechanism available for Android,” wrote Greg Peters with Android product development. The same security issues that have led to piracy concerns on the Android platform have made it difficult for us to ensure a common Digital Rights Management (DRM) system on these devices.”

Without these protections, major studios will not provide their content to Netflix, Peters wrote. But while Netflix does not have a "common platform security mechanism and DRM" for Android, the company has been able to work with individual handset manufacturers to add content protection to their devices, he said.
OMTP Security Requirements

Reference for mobile platform security and TEE

• Trusted Environment TR0 *(V1.2 – May 2009)*
  – Hardware unique key
  – Debug port protection
  – Secure boot and secure flash update
  – IMEI & SIM lock protection

• Advanced Trusted Environment TR1 *(V1.1 – May 2009)*
  – Isolated environment from main mobile operating system (OS)
    → TEE
  – Secure storage
  – Flexible secure boot
  – Secure communication with USIM and key exchanges
  – Runtime integrity check
  – Secure user interface

What is a TEE?

• TEE provides **hardware-based isolation** from rich OS such as Android, Windows Phone and Symbian

• TEE runs on the **main device chipset**

• TEE has **privileged access** to device resources (**user interface, crypto accelerators, secure elements**...).
Why a TEE?

Some use case examples

**Mobile Financial Services:**
- mBanking
- Online payment
- User authentication
- Transaction validation

**Content Protection:**
- IP streaming
- DRM
- Key protection
- Content protection

**Corporate:**
- Secure networking
- Secure email
- User authentication
- Data encryption
TEE Positioning

- Trusted Execution Environment (TEE)
- Physically Removable
- Access Control
- Attack Resistance

Rich OS

User Interface
Ease of Development
Processing Speed
TEE Standardization Principles

- Overall objective: promote the TEE ecosystem
  - Have interoperable TEEs across silicon vendors and devices
  - Have one single set of APIs for service providers whatever the silicon vendors and devices
  - Have a standardized way to administrate the TEE

- Technology agnostic

- Resistant to:
  - any software attack (remote and local)
  - basic hardware attacks (local)
    - debug interface, firmware tampering…

- TEE programming environment
  - Native-based (C-based)
  - Isolation between trusted applications
APIs for TEE

Rich OS Application Environment
- Client Applications

Trusted Execution Environment
- Trusted Application DRM
- Trusted Application Payment
- Trusted Application Corporate

GlobalPlatform TEE Internal APIs
- Trusted Core Environment
- Trusted Functions

GlobalPlatform TEE Client API
- Rich OS

Hardware Platform
- HW Secure Resources
  - HW Keys, Secure Storage,
  - Trusted UI (Keypad, Screen),
  - Crypto accelerators,
  - NFC controller,
  - Secure Element, etc.

GlobalPlatform TEE Functional API

July 2010 → V1.0 Dec 2011
Trusted User Interface: A Trusted Function Example

- Critical for mobile financial services
- Necessary for secure element-based transactions
- Enables:
  - The secure entry of a password / PIN
    - A malware is unable to access password / PIN info
  - The validation of transaction information
    - A malware is unable to forge transaction information

- TEE has direct access to display / touch-screen / keypad without interacting with the rich OS.
Compliance Program

- Managed by the GlobalPlatform Compliance Secretariat
- UML-based Test Suite and Test Applications generation
GlobalPlatform TEE Certification

- Full TEE
- GP TEE
- HW

Based on Common Criteria Protection Profile (not certified to start with)
TEE Roadmap

TEE APIs

- Basic Core APIs
- Secure Storage
- Cryptography
- Secure Date

v1.0

v1.1

+ Trusted User Interface
+ SE interface

v1.2

+ NFC
+ Network API

v2.x

+ Higher services (e.g. certificate, ...)

Trusted Applications Management

Implementation dependent

Multiple Security Domains

4Q2011

2Q2012

3Q2012

4Q2012

2013

TEE Compliance

TEE Certification
Liaisons

- GSMA Pay-Buy Mobile
- Mobey Forum
- OMA
- Payez Mobile
- European Payments Council (EPC)
- StolPan
- SIMalliance

- National Institute of Standards and Technology (NIST)
- European Committee for Standardization (CEN)
- Next generation IC Card System Study group (NICSS)
• The need for security in mobile handsets
• Introducing the TEE
• Positioning of the TEE
• Use Cases
  – Corporate
  – Content management
  – Mobile payment
  – Service deployment in a TEE
• Why standardizing a TEE?
• TEE Roadmap

http://www.globalplatform.org
GlobalPlatform Members