Mobile Cloud Computing

Dr Samia Bouzefrane
Laboratoire CEDRIC
CNAM, 292 rue Saint Martin
http://cedric.cnam.fr/~bouzefra
Agenda

• Mobile Cloud computing
  – Mobile trusted computing
  – Cloud computing
  – Security Issues

• Mobile Cloud Computing & Internet of Things Convergence
Context/Involvement

- CNRS Action on Secure Smart Objects & Internet of Things du GDR ASR
  
  
  
Mobile Cloud Computing
Mobile Cloud Computing

• Mobile Computing
  – Untrusted mobile devices with limited resources
  – Trusted Platforms for trusted computing
    • Smart cards (contact, contactless), Secure Elements/NFC, Trusted Execution Environment
    • Etc.

• Cloud Computing
  – Elastic on-demand resource provisioning with minimum management effort
Trusted platforms for mobile devices
Smart cards as secure devices
According to Eurosmart

**Smart Secure Device (Mu)**

<table>
<thead>
<tr>
<th>WW shipments forecast</th>
<th>2013f</th>
<th>2014f</th>
<th>2014 vs. 2013 % growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecom</td>
<td>5,000</td>
<td>5,200</td>
<td>4%</td>
</tr>
<tr>
<td>Banking</td>
<td>1,480</td>
<td>1,730</td>
<td>17%</td>
</tr>
<tr>
<td>Government</td>
<td>360</td>
<td>410</td>
<td>14%</td>
</tr>
<tr>
<td>Others*</td>
<td>390</td>
<td>415</td>
<td>6%</td>
</tr>
<tr>
<td>Total</td>
<td>7,230</td>
<td>7,755</td>
<td>7%</td>
</tr>
</tbody>
</table>

**Smart Secure Contactless (Mu)**

<table>
<thead>
<tr>
<th>of which contactless</th>
<th>2013f</th>
<th>2014f</th>
<th>2014 vs 2013 % growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>500</td>
<td>650</td>
<td>30%</td>
</tr>
<tr>
<td>Government</td>
<td>200</td>
<td>240</td>
<td>20%</td>
</tr>
<tr>
<td>Transport</td>
<td>160</td>
<td>180</td>
<td>13%</td>
</tr>
<tr>
<td>Others</td>
<td>70</td>
<td>70</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>930</td>
<td>1,140</td>
<td>23%</td>
</tr>
</tbody>
</table>

**NFC Secure Elements (Mu)**

<table>
<thead>
<tr>
<th>WW shipment forecast</th>
<th>2013f</th>
<th>2014f</th>
<th>2014 vs 2013 % growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFC Secure Elements</td>
<td>265</td>
<td>435</td>
<td>64%</td>
</tr>
</tbody>
</table>

ISO7816 Standard

- The standard ISO 7816-1 defines the physical characteristics of the card
- The standard ISO 7816-2 defines the position of the contacts within the card
- The standard ISO 7816-3 defines the electric signals used to communicate with the card
- The standard ISO 7816-4 defines the basic commands to interact with the smart cards
Card Contacts in ISO7816-2

APDU protocol for communication
APDU communication

Mobile

SIM

samia.bouzefrane@cnam.fr
Physical characteristics

• Monolithic component:
  – CPU (8, 16, 32 bits)
  – PROM (32 to 64 KB) contains OS (JVM)
  – RAM (1 to 4 KB)
  – EEPROM/Flash 1KB to 128 KB (256 KB for Java Card) contains data and applications
  – I/O interface
  – crypto processor
A safety box

• Stores security keys and sensitive data
• Implements cryptographic algorithms
• Crypto-processor
• Physical sensors (light, power)
• Used for authentication and encryption
  – SIM card authentication with the cell networks
  – Banking card authentication with payment terminals
Java Card platforms

99% of SIM Cards are Java Card platforms
Java Card Specification

- Java Card 3 Specification by Oracle
  - Classic edition (extension of Java Card 2.2)
    - Java Card API Specification
    - Java Card Runtime Environment Specification
    - Java Card Virtual Machine Specification
  - Connected edition (Web oriented, not deployed)
- Global Platform defines a trust environment in multi-application cards (used in Java Card platforms)
Global Platform Card Specification

v2.2.1
Security domains in Java Card

- In Java Card platforms
  - Each application (package) in a Security Domain
  - Many applications from distinct providers may co-exist in the same card
  - A firewall applet checks the isolation
  - Each application has its own trusted execution environment
  - The applications may share objects
Secure Elements
Secure Elements

- are Java Card platforms
  - SIM cards (SIM centric)
  - Embedded secure elements (Phone centric)
  - External secure SD Card (SD centric)

- Use NFC capabilities
  - distance: 0 - 20 cm, frequency: 13.56MHz (HF), rate: 424 kbits/s

- Use the security domains of GlobalPlatform
Secure Elements
NFC Forum specifications

Applications

Peer to peer mode

Read/Write mode

Card emulation mode

LLCP
(Logical Link Control Protocol)

RTD
(Record Type Definition)
&
NDEF
(Data Exchange Format)

Card Emulation
(Smart Card Capability for Mobile Devices)

RF Layer ISO 18092 + ISO 14443 Type A, Type B + FeliCa

samia.bouzefrane@cnam.fr
Mobile Payment

- Single Wire Protocol (SWP): the SIM card (SE) is linked to the NFC chip.
- GlobalPlatform is used for isolation & security.
Standards for mobile payment

- ETSI SCP (Smart Card Platform) to specify the interface between the SIM card and the chip NFC.

- Global Platform to specify the multi-application architecture of the secure element.

- EMVCo for the impact on the EMV payment applications.
Host Card Emulation
HCE (Host Card Emulation)

- Google Solution
- Alternative solution for SE
- Software platform
- Implements a stack protocol to support APDU and NFC standards from Android 4.4
- Motivation: to be independent from the SE providers (ex., telecom operators for SIM cards)
HCE


NFC card emulation with a secure element
HCE supports APDU stack protocol

NFC card emulation without a secure element
Pros & Cons

- As a software, HCE is less secure than a secure hardware device
- HCE concept does not target applications with high level of security
- Has larger resources (memory & processor)
- Independent from SE providers
Trusted Execution Environment
According to GP

- Target mobile devices
- Rich OS is vulnerable to attacks
- SE is resilient to attacks but limited
- TEE can serve as a compromise between Rich OS performance and SE security

Architecture of TEE

Benefits of TEE

• Created for security and speed

• Has larger resources than SE
  – RAM size (up to 1 MB), RAM speed (64bits/200 to 800MHz, Flash size (shared with Rich OS)
  – Secure storage per application

• TEE may cooperate with SE

• Offer security mechanisms (*Generation and storage of cryptographic keys, Attestation mechanism, Secure boot, etc.*)

• Examples of implementations: *SierraVisor and SierraTEE (ARM), ARM TrustZone, Trustonic TEE*
Trusted Platform Module
Trusted Platform Module

- Manufacturers: HP, Infineon, Intel Dell, FUJITSU, etc.
- Convert non secure PCs, printers, mobile devices, etc. to trusted environment
- More than 500 millions of PCs with TPMs

http://trusted-computing.wikispaces.com/M+-+TPM+Chip+can+be+turned+off+Entirely
"TPM chip" or "TPM Security Device"

TPM Specifications by Trusted Computing Group (consortium of companies)


samia.bouzefrane@cnam.fr
First trusted platforms: PCs

- to store secret keys, to encrypt data files/messages, to sign data, etc.

- implement mechanisms and protocols to ensure that a platform has loaded its software properly.

- Have their own hardware and are independent from the operating system of the PC.
Cloud Computing
Motivations

- Mobile devices (e.g., smartphone and tablet PC) are becoming an essential part of human life.

- Explosion of mobile applications that provide services/data (e.g., iPhone apps and Google apps).

- As a consequence, Mobile devices deal with heavy computation tasks/data (Image/video-multimedia processing, Natural language processing, Social networking, Sensor data applications, Cloud gaming, etc.).
Challenges

• Mobile devices face challenges in terms of
  – Resources (e.g., battery life, storage, and bandwidth)
  – Communications (e.g., mobility and security)

• The limited resources significantly impact the service quality
Cloud computing

• Cloud computing is viewed as a solution for mobile applications to:
  – prolong the resources of mobile devices
  – in elastic on-demand fashion.

• Cloud computing infrastructure models: public, private, hybrid

• Cloud computing service models:
  – Infrastructure as a service (IaaS)
  – Platform as a service (PaaS)
  – Software as service (SaaS)
MCC definition

• According to:
  http://www.mobilecloudcomputingforum.com/

‘Mobile cloud computing at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and MC to not just smartphone users but a much broader range of mobile subscribers.’
Architecture of MCC
Advantages of MCC/1

- **Extending battery life:** computation offloading techniques have been proposed to migrate the large computations from resource-limited resources (mobile devices) to resourceful machines (Cloud servers).

- **Improving data storage and processing power and save energy:**
  - mobile users store/access through wireless networks to data on the Cloud (ex.; sharing photos)
  - intensive computation may be performed on the Cloud (ex. Mobile healthcare, Mobile commerce, Mobile learning, Mobile gaming, etc.)
Advantages of MCC/2

- **Improve reliability**: storing data or running computation on the Cloud improve the data and computation reliability because they are replicated in different Cloud nodes.

- **Dynamic provisioning**: is a flexible way to access data/services when desired.

- **Scalability**: the deployment of mobile applications is scaled thanks to the scalability feature offered by the Cloud.

A remote cloud server acting as service provider to mobile devices
Important issues in Cloud Server model

- **Low bandwidth:** Unlike wired networks, the radio resource for wireless networks is scarce

- **Service availability:** unable to connect to the Cloud because of congestion, network failures, etc.
Alternative solutions

• **Cloudlet** (introduced by [1])
  - is a trusted, resource-rich computer (multi-core or a cluster of computers) that may access to the Internet, and accessible by nearby mobile devices.
  - A concept supported by the NIST due to WIFI hotspots that are becoming powerful computers.

• **Virtual Cloud:**
  - Built up with peer-to-peer connected mobile devices so that mobile devices are resource providers of a virtual cloud.

Cloudlet Elements

Cloudlet architecture

The Cloudlet is the service provider

N. Fernando et al. / Future Generation Computer Systems 29 (2013) 84–106

samia.bouzefrane@cnam.fr
Virtual Cloud

The mobile devices are service providers

N. Fernando et al. / Future Generation Computer Systems 29 (2013) 84–106

samia.bouzefrane@cnam.fr
Security issues for MCC
What we need to secure?

- **Security for mobile users**
  - Mobile devices are exposed to numerous security threats like malicious codes (e.g., virus)

- **Securing data on Clouds**
  - Both mobile users and application developers must be careful regarding data/applications integrity and authentication.
Security for mobile users

• Security for mobile applications.
  – A simple solution: installing security software such as antivirus programs on mobile devices
  – Cons: mobile devices are not resourceful like PCs.
  – Trusted platforms can be the solution
    • SE
    • TEE and SE
    • TPM and SE
Cloud as a Server

- The use of a TSM (Trusted Service Management) within the Cloud.
- Externalize the secure processing on the Cloud (ex. Mobile payment on the Cloud)
- Security on Demand: allocate a SE from a Cloud of SE (CoSE)
Cloudlet

- The Cloudlet is an offloading element
- A TPM can be used on a Cloudlet with a TEE/SE on a mobile device
MCC and IoT convergence
Some scenarios

• The IoT involves objects such as sensors/actuators
  – Healthcare (bio sensors)
  – Home access (RFID tags)
  – The mobile devices have also sensors
  – Etc.

• In these applications, the mobile device can be used to process data collected from sensors or transfer data to a Cloud for processing
Trends

• Smart devices (like mobile devices)
  – Can be partly or completely virtualized on the Cloud

• The objects (like sensors)
  – interact with resourceful platforms like mobile devices
  – can be virtualized on a Cloud or a Cloudlet
A developed scenario

- Implemented by two Master students (Amir Attar and Brian Kennedy) from Master of Secure Embedded and Mobile Systems of CNAM
Thanks