TEEM: A User-Oriented Trusted Mobile Device for Multi-platform Security Applications

Wei Feng
Institute of Software Chinese Academy of Sciences
vonwaist@gmail.com
2013-06-18
Outline

• Introduction & Motivation
• TEEM Architecture
• Implementation & Evaluation
• Conclusion and Future Work
Introduction

• Today, a user often has multiple computing devices
  – Desktop, laptop, smart phone, tablet, ...
  – Security applications may run on these devices
  – The untrusted state of any device may compromise the security and privacy of the user

• Trusted Computing can enhance the security of these devices

  Trusted Platform Module, Trusted Cryptography Module, AMD’s SVM, Intel’s TXT…

  Mobile Trusted Module, ARM TrustZone, other secure elements
Introduction

• However, to our knowledge, no method can provide trusted computing support for both kinds of the devices (multi-platform property)
  – Desktop machines and mobile devices have different CPU architectures (x86 vs ARM)
  – Limited in resources and spaces, secure chips are not suitable for mobile devices

• Users have to learn different security mechanisms when using different devices
  – troublesome for user
Introduction

• Flexibility of Trusted computing: using security chips, we cannot customize our own security features to meet some experimental demands
  – Adding new commands to support new applications (LBS)
  – Replacing cryptography algorithms (RSA to ECC, SHA1 to SHA256)
  – Updating authorization protocols (OIAP and OSAP to SKAP)
  – Upgrading modules (TPM 1.2 to TPM 2.0)

• Every updating leads to purchasing a new chip
  – unacceptable for user
Motivation

• Portable Trusted Module
  – PTM is attached to the platforms via USB rather than LPC
  – Unlike TPM/TCM, PTM is bound to one user and several devices can use one PTM, it is user-oriented

• Inspiration
  – To achieve multi-platform property, PTM is a good choice
  – Building PTM solution based on mobile devices rather than USB devices, so the mobile devices can also use the TC functions
Motivation

• Mobile Trusted Module
  – MTM provides TC APIs by software, and has been proven to be faster than TPM/TCM
  – Lack of isolated execution environment, its implementation relies on some secure elements: ARM TrustZone, Smart Cards, ...

• Inspiration
  – To achieve flexibility, software design of PTM’s protected capabilities is a good choice
  – Using ARM TrustZone to provide Trusted Execution Environment for mobile-based PTM solution
Outline

• Introduction & Motivation
• TEEM Architecture
• Implementation & Evaluation
• Conclusion and Future Work
TEEM Design

- **Our mobile-based PTM solution**
  - a Trusted Execution Environment Module (TEEM) in a mobile device with TrustZone
  - Provide flexible trusted computing support for both the desktop machines and mobile devices
**TEEM Components**

**Normal World of Mobile Device**
- Mobile Secure Applications
  - Mobile Trusted Software Library
  - NW-Tddl
  - NW-Driver

**Secure World of Mobile Device**
- TC Modules
  - TPM Module
  - TCM Module
  - MTM Module
- Cryptographic Library
  - RSA
  - ECC, SM2
  - SHA, SM3
  - SMS4, ...

**TEEM**
- TC-Daemon
- TC Request
- TC Response

**Host: Desktop Machine**
- Desktop Secure Applications
  - Desktop Trusted Software Library
  - USBhost-Tddl
  - USB-Driver

**Mobile Secure Applications**
- USB cable

**Desktop Secure Applications**
- USB cable

**Host: Desktop Machine**
- Monitor

**Communication components between TEEM and mobile application:**
- ARM SMC instruction and related software modules

**Communication components between TEEM and host application:**
- USB cable and related software modules

**✓ TEEM:** provide multiple TC modules in the SW of mobile device

**✓ Communication components between TEEM and mobile application:**
- ARM SMC instruction and related software modules

**✓ Communication components between TEEM and host application:**
- USB cable and related software modules
Outline

• Introduction & Motivation
• TEEM Architecture
• Implementation & Evaluation
• Conclusion and Future Work
Implementation

• Using an ARM development board Real210 as the mobile device for TEEM
  – a Samsung S5PV210 SoC, include TrustZone support
  – TrustZone not used at present, we are testing TrustZone on other board (Xilinx Zynq-7000 SoC ZC702)

• TEEM implementation
  – Modify the socket TPM/MTM emulator to support more TC modules (TCM in China) and cryptography algorithms (SM2,SM3 and SMS4), 4000 lines of C

• USB Communication
  – Use gadget serial driver, 924 lines of C

• Trusted Software Library
  – Use IBM’s libtpm, modify the library to support TCM, 1000 lines of C
Evaluation

• **Experiment Environment**

  - **Windows Host**: XP, 2.4GHz Intel CPU
  - **Linux Host**: Vmware Virtual Machine running Ubuntu, 512M memory

  ![Experiment Environment Diagram](image)

  Our Portable Trusted Device based on Real210

  - **Windows Host**: XP, 2.4GHz Intel CPU
  - **Linux Host**: Vmware Virtual Machine running Ubuntu, 512M memory

• **USB Communication Overhead**

  ![USB Communication Overhead Graph](image)

  Most TEEM commands transfer no more than 800-bytes data, and 10 bytes at least.

  From the table, the time increases linearly with the increase of the transferred data.
Evaluation

• TEEM’s Execution Time

• Performance Comparison with actual TPM/TCM chip

<table>
<thead>
<tr>
<th>TEEM Commands</th>
<th>TPM</th>
<th>TCM</th>
<th>TEEM-RSA</th>
<th>TEEM-SM2</th>
<th>TEEM-SM3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Takec CreateKey</td>
<td>407ms</td>
<td>704ms</td>
<td>4432ms</td>
<td>174ms</td>
<td>12ms</td>
</tr>
<tr>
<td>ReadL LoadKey</td>
<td>781ms</td>
<td>438ms</td>
<td>611ms</td>
<td>170ms</td>
<td>10.7ms</td>
</tr>
<tr>
<td>Creat Sign</td>
<td>609ms</td>
<td>625ms</td>
<td>83ms</td>
<td>176ms</td>
<td>n/a</td>
</tr>
<tr>
<td>LoadL Bind or Encrypt</td>
<td>63ms</td>
<td>15ms</td>
<td>3.5ms</td>
<td>315ms</td>
<td>7.0ms</td>
</tr>
<tr>
<td>Evict UnBind or Decrypt</td>
<td>625ms</td>
<td>891ms</td>
<td>84ms</td>
<td>302ms</td>
<td>7.1ms</td>
</tr>
</tbody>
</table>

- **Req**: data size of Command Request
- **Resp**: data size of Command Response

TEEM running on Real210 is faster than the actual TPM/TCM chip, because the computing power of Real210 is stronger than TPM/TCM chip. The implementation for SM2 is non-optimized at present.

TPM Host: IBM ThinkCentre M52 81114

TCM Host: Lenovo ThinkCentre M4000t

vonwaist@gmail.com
Conclusion and Future Work

• We design a mobile-based portable TC module TEEM, which can provide trusted computing functions for various devices of users, including both desktop machines and mobile devices.

• We implement a prototype of TEEM using a general ARM SoC development board Real210.

• For future work, we will experiment with ARM TrustZone on the Real210 development board and other TrustZone-enabled boards and further improve the TEEM prototype. We will also develop and implement some specific desktop or mobile security applications using TEEM.
Thanks!

For Questions:
vonwaist@gmail.com