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

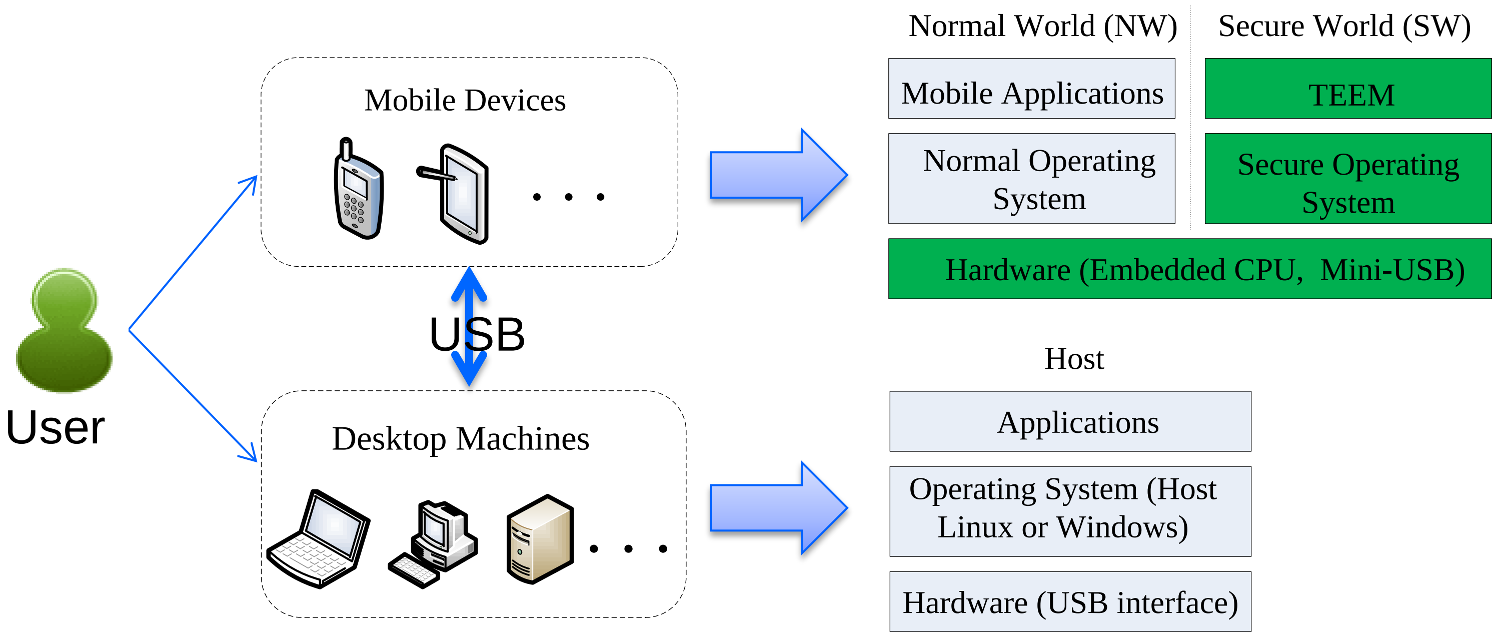
- **Mobile Trusted Module**
  - MTM provides TC APIs by software, and has been proven to be faster than TPM/TCM
  - Lack of isolated execution environment, its implementation relies on some secure elements: ARM TrustZone, Smart Cards, ...
- **Inspiration**
  - To achieve flexibility, software design of PTM's protected capabilities is a good choice
  - Using ARM TrustZone to provide Trusted Execution Environment for mobile-based PTM solution

Outline

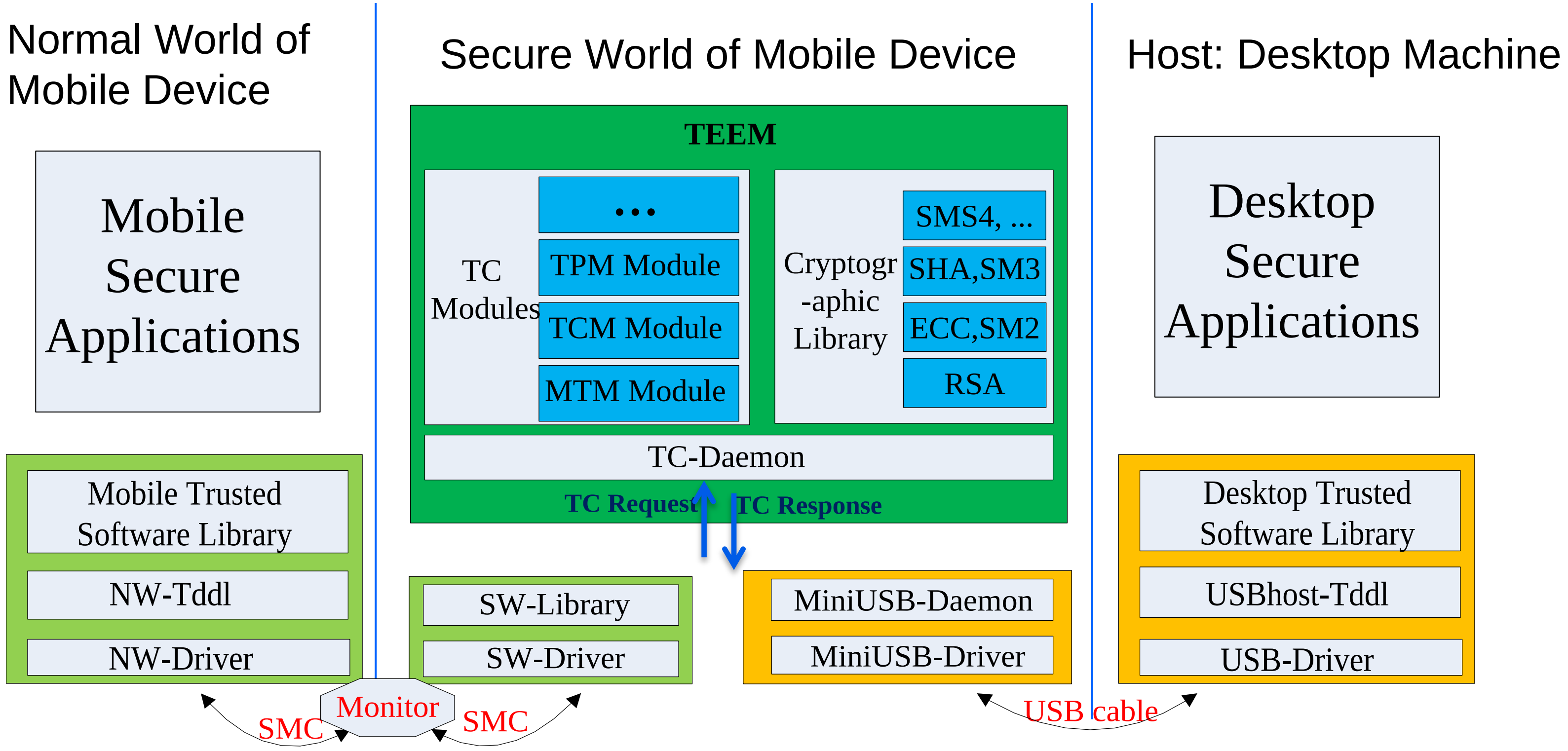
- Introduction & Motivation
- **TEEM Architecture**
- Implementation & Evaluation
- Conclusion and Future Work

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



✓**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

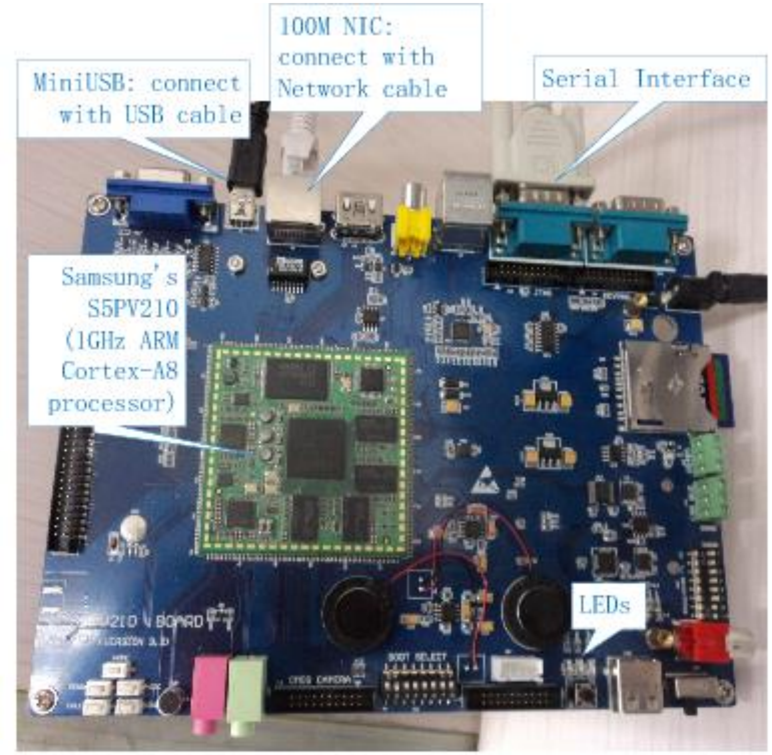
✓**Communication components between TEEM and host application**:
USB cable and related software modules

Outline

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

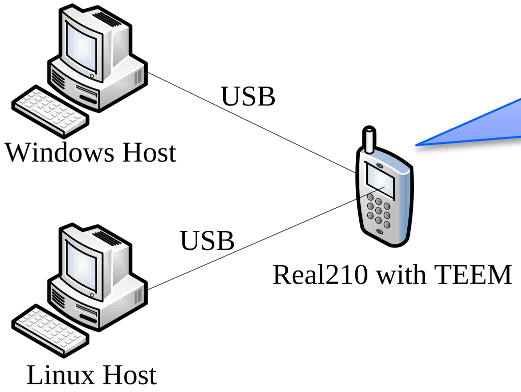
Implementation

- **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 imp**
  - Modify t ulator to support more TC moc tography algorithms (SM2,S C
- **USB Com**
  - Use gad C
- **Trusted S**
  - Use IBM support TCM, 1000 lines of


100M NIC: connect with Network cable
MiniUSB: connect with USB cable
Serial Interface
Samsung's S5PV210 (1GHz ARM Cortex-A8 processor)
LEDs

Evaluation

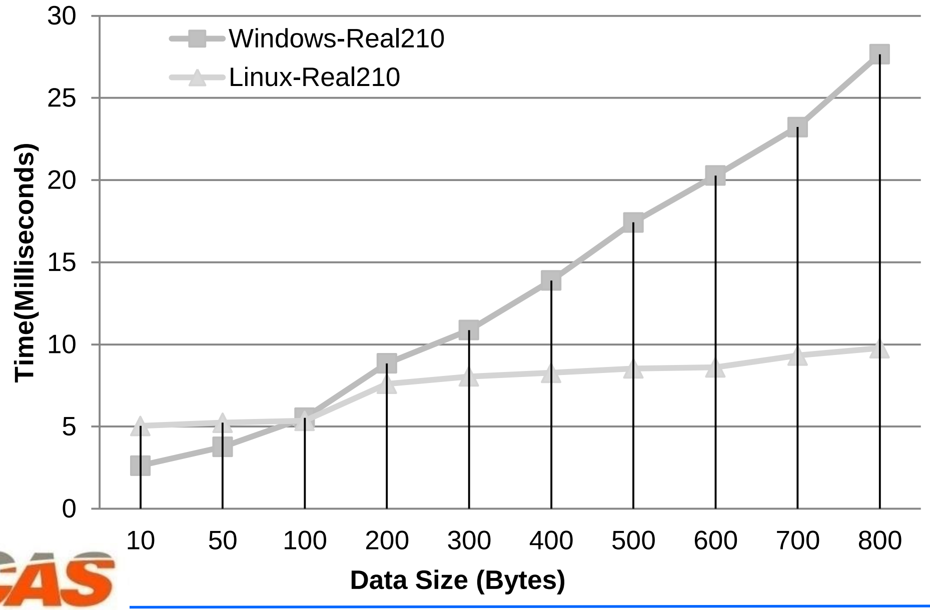
- Experiment Environment



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

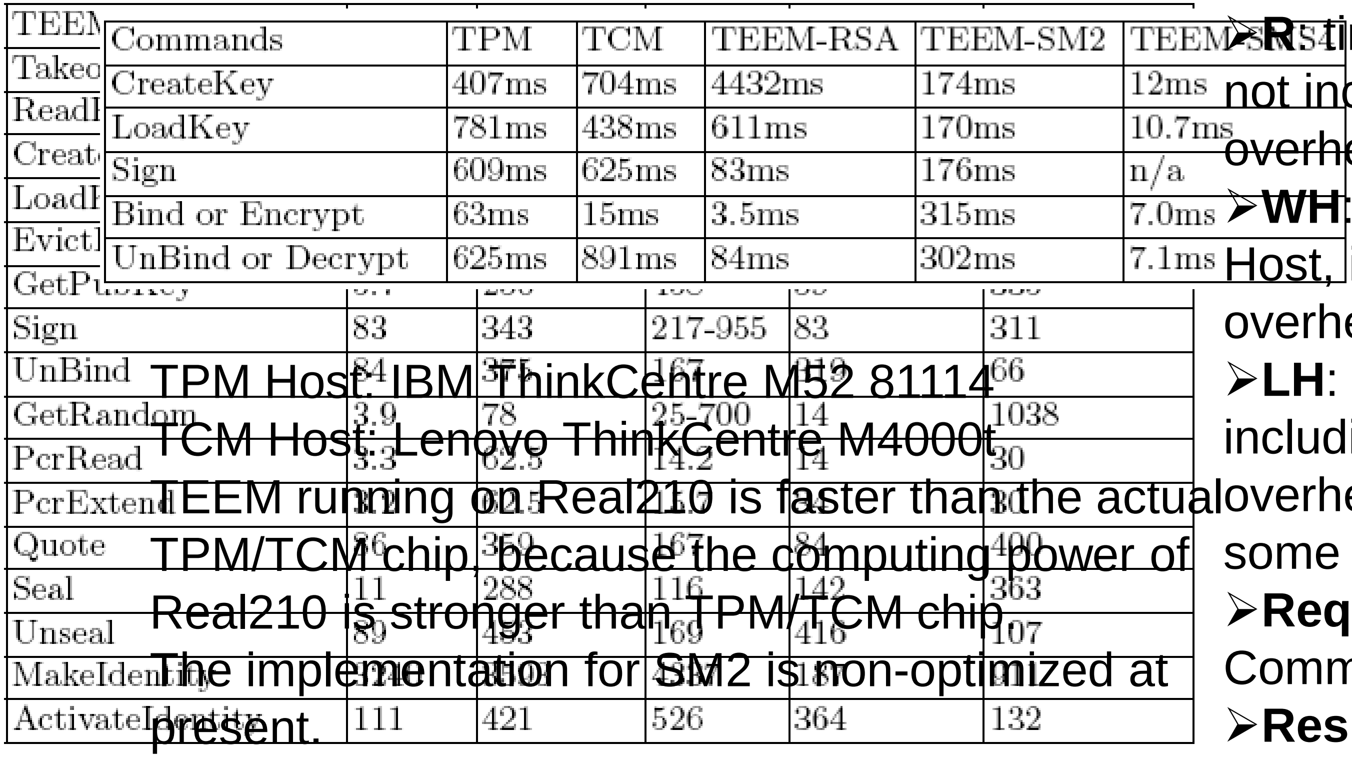


Most TEEM commands transfer no more than 800-bytes data, and 10 bytes at least.

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**



Commands	TPM	TCM	TEEM-RSA	TEEM-SM2	TEEM-SMS4
CreateKey	407ms	704ms	4432ms	174ms	12ms
LoadKey	781ms	438ms	611ms	170ms	10.7ms
Sign	609ms	625ms	83ms	176ms	n/a
Bind or Encrypt	63ms	15ms	3.5ms	315ms	7.0ms
UnBind or Decrypt	625ms	891ms	84ms	302ms	7.1ms

TEEM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Takeo	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
ReadP	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Creat	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
LoadK	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Evict	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
GetPubKey	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Sign	83	343	217-955	83	311
UnBind	84	[illegible]	167	[illegible]	66
GetRandom	3.9	78	25-700	14	1038
PcrRead	3.3	62.5	14.2	14	30
PcrExtend	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Quote	86	359	167	84	400
Seal	11	288	116	142	363
Unseal	89	453	169	416	107
MakeIdentity	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
ActivateIdentity	111	421	526	364	132

TPM Host: IBM ThinkCentre M52 81114

TCM Host: Lenovo ThinkCentre M4000t

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.

- ➢**R**: time for Real210, not including TrustZone overheads now
- ➢**WH**: time for Windows Host, including USB overheads
- ➢**LH**: time for Linux Host, including USB overheads, not stable for some commands
- ➢**Req**: data size of Command Request
- ➢**Resp**: data size of Command Response

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