Embedded System Security

Mobile Hardware Platform Security

Prof. Dr.-Ing. Ahmad-Reza Sadeghi
System Security Lab
Technische Universität Darmstadt
Germany
Summer Term 2016
Acknowledgement

This slide set is based on slides provided by Prof. N. Asokan, Aalto University, Finland
Overview

- General model for mobile platform security
  - Key hardware security techniques and general architecture
- Example(s)
  - ARM TrustZone
  - Trusted Platform Module
Platform Security Architecture

Legend

Role
- Platform Security Component
- Third-Party Software Component
- Hardware-Security Functionality
Hardware Platform Security

Trusted Execution Environment

- Boot Integrity
- Secure Storage
- Device Identification
- Isolated Execution
- Device Authentication

HW Security API
What is a TEE?

Trusted Execution Environment

Chances are that:
You have devices with hardware-based TEEs in them!
But you don’t have (m)any apps using them

Isolated and integrity-protected

Processor, memory, storage, peripherals

From the “normal” execution environment (Rich Execution Environment)
1. Platform integrity ("boot integrity")
2. Secure storage
3. Isolated execution
4. Device identification
5. Device authentication
Platform Integrity

Boot code certificate
- Boot code hash

Certified by device manufacturer:
\[ \text{Sig}_{SK_M}(H(\text{boot code})) \]

Mobile device hardware TCB

Verification root

Cryptographic mechanisms

Volatile memory
- Device key \( K_D \)
- Base identity
- Non-volatile memory
- Trusted Application (TA)
- TEE management
- Secure storage and isolated execution
- Device identification

Legend
- Trust anchor (Hardware)
- Trust anchor (Code)
- TEE code
- External certificate

Platform integrity

Launch boot code
Platform Integrity

**Legend**

- **Trust anchor (Hardware)**
- **Trust anchor (Code)**
- **TEE code**
- **External certificate**

**Platform integrity**

1. **Launch boot code**
2. **Boot sequence**
3. **Volatile memory**
   - **Verification root**
     - **Certified by device manufacturer:** $\text{Sig}_{\text{SK}_M}(\text{H}(\text{boot code}))$
   - **Device manufacturer public key:** $\text{PK}_M$
   - **External certificate**
   - **Volatile memory**
     - **Boot code certificate**
       - **Boot code hash**
   - **Secure storage and isolated execution**
     - **Device identification**
   - **Secure storage and isolated execution**
     - **Device key $K_D$**
   - **Signature verification algorithm**
     - **Stores measurements for authenticated boot**
   - **Device key $K_D$**
   - **Device identification**
   - **TEE management**
Secure Storage

Sealed-data = AuthEnc_{K_D}(data | ...)

Legend
- Trust anchor (Hardware)
- Trust anchor (Code)
- TEE code
- External certificate

Mobile device hardware TCB

Cryptographic mechanisms

Device key $K_D$
Non-volatile memory

Secure storage

Insecure Storage

Encryption algorithm
Protected memory
Rollback protection

Platform integrity
Device identification

Volatile memory

Base
Boot sequence
Trusted Application (TA)
TEE management

Trust anchor (Hardware)
Isolated Execution

Mobile device hardware TCB

Trust anchor (Hardware)

Trust anchor (Code)

TEE code

External certificate

Legend

Certified by device manufacturer

TA code certificate

TA code hash

Verification root

Cryptographic mechanisms

Volatile memory

Device key $K_D$

Non-volatile memory

Base identity

Controls TA execution

Platform integrity

Boot sequence

Trusted Application (TA)

Secure storage and isolated execution

TEE management

TEE Entry from Rich Execution Environment

Device Identification

Multiple assigned identities (Certified by device manufacturer)

Identity certificate
- Base identity
- Assigned identity

Mobile device hardware TCB

Legend
- Trust anchor (Hardware)
- Trust anchor (Code)
- TEE code
- External certificate

Verification root

Cryptographic mechanisms

Base identity
- One fixed device identity

Platform integrity

Secure storage and isolated execution

Volatile memory
- Boot sequence

Non-volatile memory

Device key $K_D$

Trusted Application (TA)

TEE management

Assigned identity

Device identification

Trust anchor

Device key $K_D$

Secure storage and isolated execution

One fixed device identity
Device Authentication (and Remote Attestation)

Mobile device hardware TCB

- Verification root
- Cryptographic mechanisms
- Volatile memory
  - Boot sequence
  - Trusted Application (TA)
  - TEE management
- Non-volatile memory
- Secure storage and isolated execution

Legend
- Trust anchor (Hardware)
- Trust anchor (Code)
- TEE code
- External certificate

Device authentication

- Device certificate
  - Identity
- Device public key $PK_D$

External trust root

Secure storage and isolated execution
Device Authentication (and Remote Attestation)

Legend:
- Trust anchor (Hardware)
- Trust anchor (Code)
- TEE code
- External certificate

Mobile device hardware TCB

- Cryptographic mechanisms
- Volatile memory
- Device key $K_D$
- External trust root

Device certificate
- Identity
- Device public key $PK_D$
- Issued by device manufacturer

Platform integrity
- Secure storage and isolated execution
- Boot sequence
- Trusted Application (TA)
- TEE management
- Trusted Storage

Sign system state in remote attestation
- Used to protect/derive signature key
1. Platform integrity
   - Secure boot
   - Authenticated boot

2. Secure storage

3. Isolated execution
   - Trusted Execution Environment (TEE)

4. Device identification

5. Device authentication
   - Remote attestation

Legend

- **Trust anchor (Hardware)**
- **Trust anchor (Code)**
- **TEE code**
- **External certificate**

Mobile device hardware TCB

- **Identity certificate**
  - Base identity
  - Assigned identity
- **Boot code certificate**
  - Boot code hash
- **TA code certificate**
  - TA code hash

- **Verification root**
- **Cryptographic mechanisms**
- **Volatile memory**
- **Device key $K_D$**
- **Non-volatile memory**
- **Base identity**
- **Device pub key $PK_D$**

- **Eviction**
- **Launch boot code**
- **TEE Entry from Rich Execution Environment**

**Device certificate**

- **Identity**
- **Device pub key $PK_D$**

**Legend**

- **Device authentication**
- **Trust anchor (Hardware)**
- **Trust anchor (Code)**
- **TEE code**
- **External certificate**

**Platform integrity**
TEE System Architecture

Architectures with single TEE
- ARM TrustZone
- TI M-Shield
- Smart card
- Crypto co-processor
- Trusted Platform Module (TPM)

Architectures with multiple TEEs
- Intel SGX
- TPM (and “Late Launch”)
- Hypervisor

Device

Rich execution environment (REE)

Device OS

TEE API

App

Trusted execution environment (TEE)

Trusted app

Trusted app

TEE management layer

TEE entry

Device hardware and firmware with TEE support

TEE Hardware Realization Alternatives

External Secure Element (TPM, smart card)

Embedded Secure Element (smart card)

Processor Secure Environment (TrustZone, M-Shield)

Legend:
SoC: system-on-chip
OTP: one-time programmable
ARM TrustZone Architecture

System on chip (SoC)

- On-chip memory
- Boot ROM
- Main CPU
- SoC internal bus (carries status flag)

- Modem
- Memory controller
- Off-chip/main memory (DDR)
- Peripherals (touchscreen, USB, NFC...)

- Secure World and Normal World

TrustZone hardware architecture
ARM TrustZone Architecture

System on chip (SoC)

- On-chip memory
- Boot ROM
- Main CPU
  - Access control hardware
  - Memory controller
  - Off-chip/main memory (DDR)
  - Peripherals (touchscreen, USB, NFC...)

Secure World and Normal World

- Modem
- Access control hardware
- Security World
- Trusted OS
- Trusted app
- Normal World
- REE
- App
- Trusted OS
- TEE entry
- SoC internal bus (carries status flag)
- Interrupt controller

TrustZone system architecture

TrustZone hardware architecture
TrustZone Overview

Normal World (NW) | Secure World (SW)
---|---
User mode | User mode
Secure Monitor Call (SMC) | Secure Monitor Call (SMC)
Privileged mode | Privileged mode
SCR.NS = 1 | SCR.NS = 0
User | User
Supervisor | Supervisor
SCR.NS := 1 | SCR.NS := 0
Monitor

Address space controllers
TZ-aware MMU

Legend:
MMU: memory management unit

On-chip ROM | On-chip RAM | Main memory
---|---|---
SW RW | SW RO | SW RW
NW NA | NW WO | NW RW

Physical address range

Boot sequence
1. Boot begins in Secure World Supervisor mode (set access control)

Boot sequence → Secure World Supervisor

- On-chip ROM:
  - Secure World (SW)
  - Read (RW)
  - Not Write (NW)
  - Not Accessible (NA)

- On-chip RAM:
  - Secure World (SW)
  - Read (RW)
  - Not Write (NW)
  - Not Accessible (NA)

- Main memory (off-chip):
  - Secure World (SW)
  - Read (RW)
  - Not Write (NW)
  - Not Accessible (NA)
TrustZone Example (1/2)

1. Boot begins in Secure World Supervisor mode (set access control)

   **Boot sequence**
   - Secure World Supervisor
   - code (trusted OS)
   - device key

2. Copy code and keys from on-chip ROM to on-chip RAM

   - On-chip ROM
   - On-chip RAM
   - Main memory (off-chip)
TrustZone Example (1/2)

1. Boot begins in Secure World Supervisor mode (set access control)

   Boot sequence

   Secure World Supervisor

   code (trusted OS)

   device key

2. Copy code and keys from on-chip ROM to on-chip RAM

   Secure World Supervisor

   On-chip ROM

   SW NA
   NW NA

   On-chip RAM

   SW RW
   NW NA

3. Configure address controller (protect on-chip memory)

   Secure World Supervisor

   Main memory (off-chip)

   SW RW
   NW NA
TrustZone Example (1/2)

1. Boot begins in Secure World Supervisor mode (set access control)

   Boot sequence
   
   Secure World Supervisor

   code (trusted OS)
   device key

   On-chip ROM
   
   SW NA
   NW NA

2. Copy code and keys from on-chip ROM to on-chip RAM

   Secure World Supervisor

   On-chip RAM
   
   SW RW
   NW NA

3. Configure address controller (protect on-chip memory)

   Secure World Supervisor

   Main memory (off-chip)
   
   SW RW
   NW RW

4. Prepare for Normal World boot

   Secure World Supervisor

   SW RW
   NW RW
TrustZone Example (1/2)

1. Boot begins in Secure World Supervisor mode (set access control)

Boot sequence

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World Supervisor

Secure World S
5. Jump to Normal World Supervisor for traditional boot

Secure World Supervisor

Normal World Supervisor

SCR.NS → 1

An ordinary boot follows: Set up MMU, load OS, drivers...

On-chip ROM

On-chip RAM

Main memory (off-chip)
TrustZone Example (2/2)

5. Jump to Normal World Supervisor for traditional boot

Secure World Supervisor

Normal World Supervisor

SCR.NS → 1

On-chip ROM

On-chip RAM

Main memory (off-chip)

6. Set up trusted application execution

An ordinary boot follows: Set up MMU, load OS, drivers...

Normal World User

Normal World Supervisor

On-chip ROM

On-chip RAM

Main memory (off-chip)

Secure World

Normal World

On-chip RAM

Main memory (off-chip)
TrustZone Example (2/2)

5. Jump to Normal World Supervisor for traditional boot

Secure World Supervisor → Normal World Supervisor
SCR.NS → 1

An ordinary boot follows: Set up MMU, load OS, drivers...

6. Set up trusted application execution

Normal World User → Supervisor

trusted app and parameters

On-chip ROM

SW NA
NW NA

On-chip RAM

SW RW
NW NA

Main memory (off-chip)

SW RW
NW RW
5. Jump to Normal World Supervisor for traditional boot

6. Set up trusted application execution

7. Execute trusted application

An ordinary boot follows: Set up MMU, load OS, drivers...
TrustZone Example (2/2)

5. Jump to Normal World Supervisor for traditional boot

Secure World Supervisor → Normal World Supervisor

An ordinary boot follows: Set up MMU, load OS, drivers...

6. Set up trusted application execution

Normal World User

Supervisor

7. Execute trusted application

Normal World Supervisor

Secure World Monitor

trusted app and parameters

SMC, SCR.NS → 0

On-chip ROM

SW NA

NW NA

On-chip RAM

SW RW

NW NA

Main memory (off-chip)

SW RW

NW RW
Secure Boot vs. Authenticated Boot

Secure Boot

- Firmware
  - Boot block
    - OS Kernel
      - checker
        - pass/fail
  - checker
    - pass/fail

Authenticated Boot

- Firmware
  - Boot block
    - OS Kernel
      - measurer
  - measurer
    - state
Secure Boot vs. Authenticated Boot

Why?

How will you implement a checker?
- hardcode $H(\text{boot code})$ as reference value in checker (in Firmware)?

Why?

State can be:
- bound to stored secrets (sealing)
- reported to external verifier (remote attestation)
Mobile TEE Deployment

- TrustZone support available in majority of current smartphones
- Mainly used for manufacturer internal purposes
  - Digital rights management, Subsidy lock...

- APIs for developers?
// create RSA key pair
Context ctx;
KeyPairGeneratorSpec spec = new KeyPairGeneratorSpec.Builder(ctx);
spec.setAlias("key1")
...
spec.build();

KeyPairGenerator gen = KeyPairGenerator.getInstance("RSA", "AndroidKeyStore");
gen.initialize(spec);
KeyPair kp = gen.generateKeyPair();

// use private key for signing
AndroidRsaEngine rsa = new AndroidRsaEngine("key1", true);
PSSSinger signer = new PSSSinger(rsa, ...);
signer.init(true, ...);
signer.update(signedData, 0, signedData.length);
byte[] signature = signer.generateSignature();

Mobile Hardware Platform Security

Android Key Store Store Implementation

Selected devices
- Android 4.3
- Nexus 4, Nexus 7

Keymaster operations
- GENERATE_KEYPAIR
- IMPORT_KEYPAIR
- SIGN_DATA
- VERIFY_DATA

Persistent storage on Normal World

What Protects Hardware Platform Security?

A well-known scientist (some say it was Bertrand Russell) once gave a public lecture on astronomy. He described how the earth orbits around the sun and how the sun, in turn, orbits around the center of a vast collection of stars called our galaxy. At the end of the lecture, a little old lady at the back of the room got up and said: "What you have told us is rubbish. The world is really a flat plate supported on the back of a giant tortoise." The scientist gave a superior smile before replying, "What is the tortoise standing on?" "You're very clever, young man, very clever," said the old lady. "But it's tortoises all the way down!"

- Stephen Hawking, in A Brief History of Time