GlobalPlatform TEE* & ARM® TrustZone® technology: Building security into your platform

Rob Coombs Security Marketing Director
Simon Moore Security Technical Marketing Director
Agenda

- Introduction
- The Four Compartment Security Model
- Comparing the Hypervisor and the TrustZone® based Trusted Execution Environment
- TrustZone Media Protection
- Achieving “Secure by default” using TrustZone based TEE & TrustZone Ready
- Summary
The Vision

- System wide security delivering trusted services and applications
  - Any content on any screen
  - Enterprise strength security for business apps
  - Protecting payment transactions from fraud

- Based on a range of ARM technology that can match the use case
  - Protected
  - Trusted
  - Secure
The Threat Environment

- Malware
- Social engineering, trojans, phishing, APT
- Theft and loss of devices
- Weak security controls – no PIN lock
- User intervention – jail breaking, unlocking, etc.
Security Profiles

Invasive HW Attacks
- Well resourced and funded
- Unlimited time, money & equipment.

Non-invasive HW Attacks
- Side channels (DEMA, DPA)
- Physical access to device – JTAG, Bus Probing, IO Pins, etc.

Software Attacks
- Malware & Viruses
- Social engineering

GlobalPlatform TEE

Cost/Effort To Attack

Cost/Effort to Secure

SmartCards / HSMs

Value to attacker
Security Inside a Modern Mobile Device

- Secure Element for tamper proof security e.g. card data, wallet
- Small, certifiable Trusted Execution Environment inside Application processor isolated using TrustZone® technology
- Hypervisor & system MMUs
4 Compartment Model – Hierarchy of Trust

**Secure Domain**
- Secure Element
  - Smartcard
  - SIM & TPM
- Tamper Proof, Physically Isolated, EAL Certified
- SecurCore™ SEE

**Trusted Domain**
- Secure Firmware
  - Device Management
  - Key Management
- Trusted Applications executing from a Trusted Execution Environment
- TrustZone® TEE

**Protected Domain**
- Protected Video Path
  - BYOD
  - System Management
- Virtual Machines and bus masters isolated by a Hypervisor
- Hypervisor HYP

**Rich Domain**
- User Apps
  - Rich OS
- Android or other OS
- Privileged Supervisor Mode

The Architecture for the Digital World®
Virtualization on ARM

- Latest ARM cores provide support for virtualization extensions using HYP mode
- MMU/HYP and Hypervisor provide isolation
- Result is a protected area for sensitive code and data
- System MMUs can be added to non CPU DMA masters for system wide virtualization
TrustZone® based TEE

- Hardware root of trust
- Trusted Boot
- Trusted Execution Environment
- Small security boundary
- Assured/Certifiable security

Hardware Isolation provided by

- TrustZone provides system wide, hardware security isolation: processor, fabric, internal/external memory, interrupts, debug
GlobalPlatform TEE

Primary device environment runs as normal, including other security mechanisms

GlobalPlatform APIs ensure portability across handsets & platforms

Security critical code and resources protected by TEE applications

TEE provides the constant security foundation independent of OS choice

Integrity and trust underpinned by SoC hardware

Control of secure resources (e.g. UI, SE)

GlobalPlatform TEE

Rich OS Application Environment

Client Applications

GlobalPlatform TEE Functional API

GlobalPlatform TEE Client API

Rich OS

Trusted Execution Environment

Trusted Application DRM

Trusted Application Payment

Trusted Application Corp.

GlobalPlatform TEE Internal API

Trusted Core Environment

Trustcore Function

TEE Kernel

HW Secure Resources

HW Keys, Secure Storage, Trusted UI (Keypad, Screen), Crypto accelerators, NFC controller, Secure Element, etc.
## Comparison of Hypervisor and TEE

<table>
<thead>
<tr>
<th></th>
<th>Type 1 Hypervisor</th>
<th>TrustZone based TEE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boot</strong></td>
<td>Boots after TEE and before guest OS’s</td>
<td>TrustZone provides Root of Trust and isolated boot code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TEE normally part of Trusted Boot</td>
</tr>
<tr>
<td><strong>Isolation</strong></td>
<td>Each OS in a separate VM = separate view of memory</td>
<td>Built into architecture, extends across SoC with NS bit</td>
</tr>
<tr>
<td></td>
<td>Provided by “HYP”+hypervisor</td>
<td></td>
</tr>
<tr>
<td><strong>Integration</strong></td>
<td>Requires no OS modification for new cores with “HYP”</td>
<td>Needs to be integrated by silicon partner and OEM</td>
</tr>
<tr>
<td><strong>Secure debug</strong></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Combined VM &amp; TEE</strong></td>
<td>Hypervisor is optionally the gatekeeper for secure world</td>
<td>Can provide integrity checking to the hypervisor</td>
</tr>
</tbody>
</table>
Spectrum of Security Solutions

Virtualisation

User space & OS Separation: Enterprise & Mobile

Trusted Execution Environment + TrustZone

Protection from Software attack: Trusted Apps

Secure Element

Protection from Hardware attack: Tamper proof

Example solutions

Red Bend Software

Mentor Graphics

OK Labs

SOLACIA

TRUSTONIC

SC300

Content isolation
Platform abstraction
Environment separation
Platform management

Typical use cases
Payment
Identity management
Operator services
Content Protection

Secure Storage
Network Identity
Wallet

The Architecture for the Digital World®
Spectrum of Security Solutions

Virtualisation

User space & OS Separation: Enterprise & Mobile

Trusted Execution Environment + TrustZone

Protection from Software attack: Trusted Apps

Secure Element

Protection from Hardware attack: Tamper proof

Example solutions

Red Bend Software

OK Labs

Mentor Graphics SOLACIA

TRUSTONIC

SC300

Content isolation
Platform abstraction
Environment separation
Platform management

Typical use cases
Payment
Identity management
Operator services
Content Protection

Secure Storage
Network Identity
Wallet

Rich area for business growth & innovation

Typical use cases
Payment
Identity management
Operator services
Content Protection

Secure Storage
Network Identity
Wallet

Rich area for business growth & innovation

Typical use cases
Payment
Identity management
Operator services
Content Protection

Secure Storage
Network Identity
Wallet

Rich area for business growth & innovation
Spectrum of Security Solutions

Virtualisation
User space & OS Separation: Enterprise & Mobile

Trusted Execution Environment + TrustZone
Protection from Software attack: Trusted Apps

Secure Element
Protection from Hardware attack: Tamper proof

Example solutions
Red Bend Software
OK Labs
Mentor Graphics
TRUSTONIC
SC300

Content isolation
Platform abstraction
Environment separation
Platform management

Typical use cases
Payment
Identity management
Operator services
Content Protection

Secure Storage
Network Identity
Wallet

Rich area for business growth & innovation
Content Protection: TEE & NSAID*

TrustZone based TEE protects:
- DRM
- Keys
- Crypto setup

TZASC400 uses NSAID to provide isolated memory regions:
- Decrypted content
- Decoded content
- Display processors

*Non-Secure Access ID
TZC-400 TrustZone® Controller

- Controls access by Masters to different memory regions using NSAID*
- Provides access control to 8 memory regions
- Can filter NSBIT or NSAID accesses
- Can filter READ or WRITE accesses
- Fast Path for ZERO cycles latency
- Extends Trusted Memory to cheap external DRAM

![Address Map](image)

**Address Map**

- Master A: Write
- Master B: Read, Write
- Master C: Read, Write
- Master D: Read

**Regions**

- Region 0
- Region 1
- Region 2
- Region 7

**Access Control**

- Interconnect CCI/CCN/NIC
- Memory Controller - DMC
- TZASC400

**CoreLink**

- NSAID = A
- NSAID = B
- NSAID = C
- NSAID = D
- NSAID = E
- NSBIT = 0

**Access Filtering**

- Fast Path for ZERO cycles latency
- Extends Trusted Memory to cheap external DRAM
Content Protection: HYP, SMMU & TEE

TrustZone based TEE protects:
- DRM
- Keys
- Crypto setup
- Integrity check to hypervisor

Hypervisor protects:
- Software components e.g. software video codec
- System MMU (MMU-400) provides:
  - Memory protection to masters
  - Handles fragmented buffers
ARM System IP for Media Protection

- ARM Cortex-A CPUs
- ARM v8 Crypto Extension
- ARM CoreLink Interconnects (CCI)
- ARM CoreLink DMC-400
- ARM CoreLink TZC400
- ARM CoreLink MMU400
- ARM CoreSight Debug
- ARM Mali-V500 Video Decoder
- ARM Mali GPU
- ARM SecurCore
CHARACTERISTICS OF SECURE PLATFORMS
Characteristics of Secure Platforms

- How can an ARM based Application Processor provide the characteristics of a secure platform?

  And how can it meet the standard of security required by government?

- In the UK the UK Government's National Technical Authority for Information Assurance (IA) provides openly published recommendations on how to secure computing environments and platforms and how to design systems to be “secure by default”. We’ll use this as a publicly available source of best practice.
Characteristics of Secure Platforms

- Processor Security Controls Limit Access and Cannot be Bypassed
  - TrustZone Monitor provides a single point of entry into the Trusted World which cannot be bypassed. It acts as gatekeeper and can control the interaction between the two worlds
  - Mechanisms to enter into the secure state are well defined
  - Within the Trusted World, Privileged and User states exist, and can have separate page tables from the Normal world so Trusted Applications within the Trusted World need not necessarily have access to all secure peripherals allowing a further hierarchy of control
Characteristics of Secure Platforms

- Direct Memory Access (DMA) is Limited and Controlled
  - Access to secure peripherals by bus masters is limited to only on-chip bus masters
  - Bus masters can be restricted to be non-secure only by configuration, preventing their access to secure assets
  - The process of deciding what peripherals and bus masters are capable of being within the Trusted World is an important aspect of the system design and directly influences the robustness of the security design
Characteristics of Secure Platforms

- DMA from External Devices is Additionally Protected
  - The AXI secure control signal is not carried off chip, thereby protecting on-chip Trusted World assets from external attack

- Central Processor Access From Other Processing Elements is Minimised and Controlled
  - Only secure bus masters can access Trusted World assets
Characteristics of Secure Platforms

- Processes Consuming Platform Resources can be Identified and Controlled
  - Resource allocation can be securely controlled and supervised by a Trusted Application running within the TEE
  - Alternatively, a Trusted Application can be used to monitor and supervise the OS in arbitration of system resources
Characteristics of Secure Platforms

- **Debug Functionality Does Not Compromise Security**
  - TBSA requires debug be correctly managed in production devices

- **I/O Control**
  - Secure I/O can be controlled from with the Trusted World. All secure peripherals can be selectively chosen to be secure or non-secure as required
  - Secure paths for video, audio and user input can be configured by the Trusted World depending on operation
Characteristics of Secure Platforms

- Secure Device Identity
  - The Trusted World can be used to securely store keys, and to protect secure identification assets such as serial numbers for IMEI or MAC addresses
  - This allows strong authentication at the application layer, or when network drivers are placed in the Trusted World, can also allow secure authentication lower down the network stack and preventing spoofing of unauthorised identification numbers

- Secure Credential Storage
  - The Trusted World can be used to securely store private keys. Cryptographic operations can then occur within the Trusted World by applications in the Normal World, without compromising the security of the keys
Characteristics of Secure Platforms

- Measured/Verified Boot
  - The Trusted Base Boot Requirements specification (TBBR) recommends how to construct a Trusted Boot sequence
  - In addition, a Trusted Application executing within the Trusted Execution Environment can provide a secure means to store measurements to provide virtual TPM functionality. This can be used in booting the Rich OS, to secure it’s boot process

- Secure Update/Recovery
  - Secure Firmware update is specified as part of the Trusted Base Boot Requirements specification (TBBR)
Characteristics of Secure Platforms

- **Control Flow Integrity**
  - The ARM C Compiler/DS-5, provides stack checking functionality for protecting the integrity of system and application software
  - The MMU provide a XN/eXecute Never bit, to ensure data pages cannot be executed

- **Security Primitives**
  - The ARMv8 architecture provides additional instructions for AES and SHA-1 and SHA-256
  - TBSA specifies RNG
TrustZone® Ready Program

- These recommendations are documented, and made available as part of ARM’s TrustZone Ready Program.

The security recommendations are contained in the documents:

- Trusted Base System Architecture (TBSA)
- Trusted Board Boot Requirements (TBBR)
TrustZone® Ready Program

- Market Requirements
- Desired Services
- Industry Factors

TrustZone®
System Security by ARM

SoC Platform Definition
- Security Docs: Trusted Base
- System Arch & Trusted Boot
- TEE Integration
- Interoperability
- Standard APIs

Industry Certification

SoC Platform Assurance

SoC Checklist

GLOBAL PLATFORM

The Architecture for the Digital World®
Conclusion

- TrustZone® security extensions together with the GlobalPlatform Trusted Execution Environment can provide a strong and robust secure platform.

- These recommendations can be applied to many common use cases:
  - Secure delivery of Premium Content
  - Online and mobile banking and payment
  - Securing platforms for Enterprise use

- TrustZone® Ready Program and ARM’s System IP can simplify the implementation of system wide security.
Questions?