Next-Gen Media Content
Protection with TZMP2

Ashwin Matta
Senior Product Marketing Manager

ARM Tech Symposia India
December 7th 2016

©ARM 2016
Media content protection use cases

Mobile/Consumer

- Digital Rights Management (DRM) for audio/video content
  - Smartphones, tablets, laptops
  - DTVs and STB
- Surveillance, drones and cameras

Automotive

- Connected Vehicle and 5G
  - High bandwidth data transmission
  - Enable rich media streaming
- Camera/Display Innovations
  - High Resolution display
  - Transparent OLED windscreen and windows
- The Smartphone Spillover Effect
  - Audio and Video Streaming
  - Proximity information / advertisement relay
Problem statement
Evolution of media protection system architecture

Current ARM®-based devices

- Provide content protection based on robust hardware-based security
  - TrustZone® technology for management of root of trust, control of cryptographic operations
  - Hardware-based isolation to protect media pipelines

Changing landscape

- Premium content
  - Resolutions to 4k and beyond, increasing memory pressure
  - Quality enhancement technologies (e.g. HDR) evolving faster than the Silicon lifecycle

- Developments in SoC technology
  - Coherency

- Evolving RichOS requirements
  - Advanced UI use cases
  - Demand for more complex, programmable video / graphics pipelines
Media content protection

Client device

Decryptor

License

DRM client

Content provider

DRM server
Media content protection

The client device must protect
- The DRM client and associated assets
- The license and associated decryption key(s)
- The plaintext data, throughout the pipeline
Problem statement

- Prevent unauthorised access to plaintext media content
  - From output of decryptor to final destination
    (directly connected sink, or remote endpoint)

- Minimise size of trust domain
  - Avoid need to trust the entire media stack

- Allow flexible sharing of resources between protected and non-protected tasks
  - Media devices
  - Memory

- Design for compatibility with future evolution of memory systems
  - Coherency between masters
  - Distributed caches
Threat profile

Cost / effort of attack vs Value to attacker

Software Attacks
- Malware & viruses
- Social engineering

Non-invasive Hardware Attacks
- Side channels (DEMA, DPA)
- JTAG
- Bus probing
- IO pins
- TEST

Invasive Hardware Attacks
- Laser
- FIB

Media Protection
GlobalPlatform™ TEE

SmartCards / HSMs
TZMP architecture
TZMP specification

Abstract system architecture

- Security model
- Principle of isolating the media pipeline
- Access control policy
- Software authentication requirements

Concrete embodiments

- Alternative realisations of the system architecture
- Utilise different mechanisms to isolate the media pipeline
- All targeting identical security levels
Data flow restrictions
High-level system architecture

Protected world
- DRM

Non-secure state
- Video codec
- GPU
- Display

Data

Trusted world
- Trusted Execution Environment
  - RNG
  - Key store
  - Crypto

Rich OS
- TEE comms
- Device drivers

Non-trusted world
- Video player application

Control
Example media pipeline
# Protected memory footprint

Example: **2160p video playback with overlay**

## Displayable layers

<table>
<thead>
<tr>
<th>Layer</th>
<th>Resolution</th>
<th>Bits per pixel</th>
<th>Number of buffers</th>
<th>Footprint /MB *</th>
<th>Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>3840 × 2160</td>
<td>16</td>
<td>12</td>
<td>192</td>
<td>Yes</td>
</tr>
<tr>
<td>Overlay</td>
<td>3840 × 2160</td>
<td>32</td>
<td>3</td>
<td>96</td>
<td>No</td>
</tr>
</tbody>
</table>

* Rounded up to 2MB
TZMP1

- Initiator identified by a sideband signal propagated with each transaction
- Protection is enforced by slave-side TZC
- Combining with coherency is complex
- Access permissions defined on a small number of physically contiguous regions
- Requires a carve-out
- Filter programmed by Secure state software
TZMP2

- Protection enforced by a master-side filter(s)
- Filter is capable of protecting physically discontiguous memory
- Protected memory allocated from system heap
  - Carve-out no longer required
- Software which programs the master-side filter(s) is called the Protected Media Manager (PMM)
Evolution of TZMP

The TZMP specification defines two recommended embodiments

Architectural differences

The same level of media asset protection, targeted at different generations of device design

<table>
<thead>
<tr>
<th>TZMP1</th>
<th>TZMP2</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Protection enforced by slave-side filtering</td>
<td>- Protection enforced by master-side filtering</td>
</tr>
<tr>
<td>- Protection of contiguous physical memory</td>
<td>- Protection of scattered physical memory</td>
</tr>
<tr>
<td>- Protection managed from Secure state</td>
<td>- Protection managed from EL2</td>
</tr>
<tr>
<td>- Already implemented today</td>
<td>- Aimed at next generation of SoC designs</td>
</tr>
</tbody>
</table>
Rationale for TZMP1 → TZMP2 evolution

Integration with shared caches

In TZMP1, protection is enforced by a target filter

When coherency is added

- Access constraints must be applied to data in shared caches
- Protected snoop transactions must be forced via DRAM

This approach becomes increasingly difficult as complexity of the memory subsystem increases

In TZMP2, protection is enforced before transaction enters the interconnect
Implementation of TZMP2 in ARM IP
ARM’s System MMU (SMMU)

- SMMU handles translation of virtual addresses to physical addresses
- Scalable TBU (translation buffer unit)
  - Does translation on un-translated requests
  - Holds the translation look aside buffer (TLB)
  - Request translation for virtual → physical from the TCU
  - Security/access checks on address from devices
- TCU (translation control unit)
  - Does table walks of translation tables
  - Communicates to TBU and remote device to invalidate a cached transaction
  - May contain additional caches to handle partial misses
- Local AXI-Stream interconnect
  - Free-flowing transport layer between TBU and TCU
  - Enables distributed TBU and reduced congestion/routing
Delivering performance with TZMP2

- Real-time displays and GPUs sensitive to PTW overhead
- Memory protection cache (MPC) for storing 2-bit protection attributes for entire memory space
  - Provides fast protection attribute lookup
- Limits protection granularity to 2MB to keep MPC size manageable
- Linux CPA (Compound Page Allocator) helps aggregate smaller pages into 2MB continuous chunk for protection
TZMP2 software requirements
Key TZMP2 software components

- **Protected Media Manager**
  - Enforce a memory access policy, restricting access to protected media assets
  - Apply the policy by programming hardware filter(s)

- **REE memory allocator**
  - Capable of allocating memory at a granularity appropriate to the filter
TZMP2 software topology

- PMM executes at EL2 as a bespoke software stack only managing media protection
- No other software executes at EL2
Protected media manager (PMM)

- TZMPx requires a trusted management component
  - Enforce a memory access policy, restricting access to protected media assets
  - Apply the policy by programming hardware filter(s)

- In TZMP1, the management component is in the Secure state
  - Implemented as part of the TEE
  - Changes memory protection status and access permissions based on request from REE

- In TZMP2, the Protected Media Manager executes in EL2
  - Authenticated during secure boot
  - Tracks protection status of each memory location
  - Changes memory protection status and access permissions based on request from REE
PMM ≠ Hypervisor

- TZMP2 leverages a subset of the hardware features which are required for virtualization
  
  ✓ Memory protection  
  ✓ Static interrupt routing  
  ✓ Basic exception handling

  ✗ Memory management (translation)  
  ✗ Device allocation and sharing  
  ✗ Scheduling

- These can be managed by a simpler EL2 software stack than a full hypervisor
Summary

- Escalating need for media content protection with growth in streaming audio/video content in mobile/consumer/automotive devices
- ARM’s TZMP architecture addresses content protection in devices subject to non-invasive hardware attacks
- TZMP1 and TZMP2 are successive embodiments of TZMP architecture providing same level of content protection for evolving use cases
- TZMP2 provides master-side protection without requiring a memory carveout enabling coherent operation at reduced BoM costs
- TZMP2 solution from ARM includes both hardware IP and software components - protecting content while continuing to deliver highest performance at lowest cost
Thank you

(For more information on TZMP architecture and HW/SW support from ARM contact ashwin.matta@arm.com)