The New Era of Premium Content Protection

UHD Content Protection with INSIDE Secure’s DRM Solution and ARM’s TrustZone® / TEE + Secure Content Path

ARM Tech Forum
Seoul, Sept 2nd, 2015

www.insidesecure.com
DISCLAIMER

This communication does not constitute an offer to purchase or exchange or the solicitation of an offer to sell or exchange any securities of INSIDE Secure.

This communication contains certain statements that are neither reported financial results nor other historical information and other statements concerning INSIDE Secure. These statements may include financial projections and estimates and their underlying assumptions, statements regarding plans, objectives and expectations with respect to future operations, events, products and services and future performance. Forward-looking statements are generally identified by the words "expects", "anticipates", "believes", "intends", "estimates" and similar expressions. These and other information and statements contained in this communication constitute forward-looking statements for purposes of applicable securities laws. Although management of the company believes that the expectations reflected in the forward looking statements are reasonable, investors and security holders are cautioned that forward-looking information and statements are subject to various risks and uncertainties, many of which are difficult to predict and generally beyond the control of the company, that could cause actual results and developments to differ materially from those expressed in, or implied or projected by, the forward-looking information and statements, and the company cannot guarantee future results, levels of activity, performance or achievements. Factors that could cause actual results to differ materially from those estimated by the forward-looking statements contained in this communication include, but are not limited to: trends in semiconductor and wireless communication markets; the company's ability to develop new technology and the effects of competing technologies developed and expected intense competition generally in the companies' main markets; profitability of expansion strategy; challenges to or loss of intellectual property rights; ability to establish and maintain strategic relationships in its major businesses; ability to develop and take advantage of new products and software; future acquisitions and investments; the ability of the company's to integrate acquired businesses, activities and companies according to expectations; the ability of the company to achieve the expected synergies from acquisitions; and changes in global, political, economic, business, competitive, market and regulatory forces. Moreover, neither the company nor any other person assumes responsibility for the accuracy and completeness of such forward-looking statements. The forward-looking statements contained in this communication speak only as of the date of this communication and the company are under no duty, and do not undertake, to update any of the forward-looking statements after this date to conform such statements to actual results, to reflect the occurrence of anticipated results or otherwise except as otherwise required by applicable law or regulations. The products identified and/or described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.
AGENDA

● Today’s Media Distribution

● Tomorrow’s Security Challenges

● Increasing Content Protection Requirements
  • The right Security for a Standalone Software Player
  • Hardware-based Security for Premium Content
  • Future Security Requirements

● Hardware-based Content Protection
  - System level Security Approach
  - Certification
  - Embedded DRM Architecture

● DRM Content Flow and ARM TrustZone®-based Content Protection
  • Demo

● INSIDE Secure - Overview

● Summary
TODAY’S MEDIA DISTRIBUTION

- Digital Rights Management (DRM) solutions to protect Over-The-Top (OTT) streaming
- Downloadable pure software-based DRM for Android and iOS devices introduced in 2010
- Implementation includes technology like software-based anti-tampering, obfuscation, white box-crypto, jailbreak detection to protect licensing and sessions keys as well as cryptographic computations
- Enabling Content Owners to distribute content OTT to any available device
  - iOS, Android
- Since 2010, dramatic increase of OTT distribution of Content
TOMORROW’S SECURITY CHALLENGES

- Increasing value of content will demand higher levels of protection
  - More Premium Content will become available
  - Higher resolutions of 1080p and beyond
  - The costs for the content developer will increase

- Fast increase of content protection requirements

- Studios have defined additional specifications for the protection of UHD Content
  - Movielabs Specifications for Enhanced Content Protection

- DRM Providers are updating their specifications
  - Microsoft PlayReady, Google Widevine, Vidity (SCSA), ….

- As security will be included at the system level there is an increasing demand for system level certifications

- Good Digital Right Management solutions
  - Efficient though transparent to the user
## INCREASING CONTENT PROTECTION REQUIREMENTS

<table>
<thead>
<tr>
<th></th>
<th>Level A</th>
<th>Level B</th>
<th>Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximal Video Resolution</strong></td>
<td>Standard (SD) 480 - 720</td>
<td>Premium (HD) 720 - 1080</td>
<td>Ultra-Premium (UHD/4K) 1080-2160</td>
</tr>
<tr>
<td><strong>Content Processing Path</strong></td>
<td>Not Protected</td>
<td>Protected against Software attacks</td>
<td>Protected against Software and Hardware attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Bus protection</td>
<td>Higher level of Data Bus protection</td>
</tr>
<tr>
<td><strong>Execution Security Requirement</strong></td>
<td>Software protection</td>
<td>Trusted Execution Environment</td>
<td>Trusted Execution Environment with dedicated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Crypto Hardware blocks</td>
</tr>
<tr>
<td><strong>Overall Security Level</strong></td>
<td>Pure Software Protection against code and secret software attacks</td>
<td>Hardware assisted Protection against code, secret and data bus attacks</td>
<td>Hardware secured Protection against code, secret and data bus attacks</td>
</tr>
<tr>
<td><strong>Output Protection</strong></td>
<td>HDCP DTCP</td>
<td>HDCP DTCP</td>
<td>Additional requirements for links using HDCP / DTCP</td>
</tr>
</tbody>
</table>

**Note:**
The applicable security level not only depends on the resolution but also on the age and value of the content.
TYPICAL DRM IMPLEMENTATION

Browser

Content Server (CDN)  License Server

Application (Java Script)

Media Source Extensions  HTML5 engine  Encrypted Media Extensions

Media Stack

Content samples

CDMi

Content Decryption Module (CDM)

Platform

TEE  Or  CPU  Or  GPU

(Optional) Secure Video Path

Legend:

Browser  JavaScript API  INSIDE Secure  Chipset vendor
PROTECTION LEVEL A: THE RIGHT SECURITY FOR A STANDALONE SOFTWARE PLAYER

- Implementations are studio approved with possible third party certification
- Full software-based implementation
  - Using software-based protection techniques to protect keys and cryptographic computations: anti-tampering, obfuscation, white box crypto, jailbreak detection
- Fully downloadable from app-stores
- Full flexibility & full cross platform compatibility
- Possible immediate over-the-air enhancements and upgrades
  - Fast delivery of new features
- Protection level more than enough for SD content / “small” screens (mobile phones, tablets)
PROTECTION LEVEL B: HARDWARE-BASED SECURITY FOR PREMIUM CONTENT

- Smart mix of Rich OS software (powerful, fast, flexible… but unsecure) and Trusted Applications (limited functions, cryptography centric… and very secure)

- Execution of the sensitive operations inside a hardware-based Trusted Execution Environment (TEE) supported by e.g. ARM TrustZone®

- Protection against software attacks
  - Keys are stored and protected by the TEE
  - Cryptographic functions are running inside the TEE

- Protected Video Path to protect the plain content after decryption and before display

- Standardization, Trusted Application Managers and (Trusted) App Stores will help to gain the same flexibility as available for full software solutions

- Platform dependent certification
PROTECTION LEVEL C: FUTURE SECURITY REQUIREMENTS

- Secure Video Path
  - Higher level of protection requirements against software as well as hardware-based attacks
  - Bus encryption / scrambling
- Devices must be resistant against software and hardware attacks
- Tamper resistant to protect the device keys, licensing keys as well as the session keys
  - SCA countermeasures
- Certification is required
  - GlobalPlatform
  - DRM protection providers
  - FIPS 140-2 level 1/2/3
HIGH-LEVEL DATA FLOW FOR DRM

Legend:
- INSIDE Secure component
- Interface
- Third-party component

Secure Content Path
- Enable
- Secure drivers: Decryption, Memory allocation and copy, Secure storage, Logging

DRM Agent
- Normal world
- GP Client API
- Secure world
- TA Loader
- Session Manager / TA Loader
- Main Event Loop
- Secure OS API
- Licenses and Key Storage
- PlayReady Decryption
- Command Processor
- DRM Agent TA

Payload data R/W

OS Shared Memory

Send command
Receive response

Load TA
Open session
ARM TRUSTZONE®-BASED CONTENT PROTECTION

Normal World

1. Encrypted content
2. License acquisition
3. License (with protected keys)
4. License request
5. License (with protected keys)
6. License (with protected keys)
7. License (with protected keys)
8. License (with protected keys)
9. License (with protected keys)
10. Licensing keys
11. Keys
12. Encrypted content
13. Video fragments (clear + encrypted)
14. Buffer handle (TrustZone protected)
15. Buffer handle (secure decoder)
16. Encrypted video samples + buffer handle
17. Encrypted video samples + buffer handle
18. Encrypted video samples + buffer handle
19. Encrypted video + buffer handle
20. Check output to apply OPL policy
21. Write decrypted samples to W/O memory area
22. Buffer ready (buffer handle)
23. Decode buffer handle
24. Read decrypted samples

Secure World

PlayReady® License Management
HDCP DTCP-IP
PlayReady® Interface & Protection Manager
TEE Support functions (TRNG, Secure Storage, AES, etc.)
TEE Internal API (Global Platform)
TEE Support functions (Global Platform)

Linux OS Layer

MediaCrypto
MediaDRM
INSIDE Secure DRM

Mali OMX Layer
(i.e.: OMX.ARM.h264.decoder.secure)

Mali Driver

TEE Supplicant
TEE Driver

Android OS component
DRM Agent component
Customizable component
Vendor driver
Protected Content
Content flow
Key Management
Communication flow

Platform HW/FW component

MediaRenderer
MPEG-DASH, SS, HLS Extractor

MediaCodec

TrustZone Address Controller

Memory Config

Secure Memory
Mali Video / Display Processor

Output Controller
HDMI

ExoPlayer

16. Encrypted video samples + buffer handle
17. Encrypted video samples + buffer handle
18. Encrypted video samples + buffer handle
19. Encrypted video + buffer handle

TEE Supplicant
TEE Driver

14. Buffer handle (TrustZone protected)
15. Buffer handle (secure decoder)
16. Encrypted video samples + buffer handle
17. Encrypted video samples + buffer handle
18. Encrypted video samples + buffer handle
19. Encrypted video + buffer handle

20. Check output to apply OPL policy
21. Write decrypted samples to W/O memory area
22. Buffer ready (buffer handle)
23. Decode buffer handle
24. Read decrypted samples

21. Write decrypted samples to W/O memory area
22. Buffer ready (buffer handle)
23. Decode buffer handle
24. Read decrypted samples

25. Decoded image

Hardware Security Module - VaultIP (Key Management + Secure Storage + Decryption)
## FUTURE CONTENT PROTECTION REQUIREMENTS

<table>
<thead>
<tr>
<th></th>
<th>Level A</th>
<th>Level B</th>
<th>Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximal Video Resolution</strong></td>
<td>Standard (SD) 480 - 720</td>
<td>Premium (HD) 720 - 1080</td>
<td>Ultra-Premium (UHD/4K) 1080-2160</td>
</tr>
<tr>
<td><strong>Content Processing Path</strong></td>
<td>Not Protected</td>
<td>Protected against Software attacks</td>
<td>Protected against Software and Hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Bus protection</td>
<td>attacks and Hardware attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Higher level of Data Bus protection</td>
</tr>
<tr>
<td><strong>Execution Security Requirement</strong></td>
<td>Software protection</td>
<td>Trusted Execution Environment</td>
<td>Trusted Execution Environment with dedicated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Crypto Hardware blocks</td>
</tr>
<tr>
<td><strong>Overall Security Level</strong></td>
<td>Pure Software Protection against code and</td>
<td>Hardware assisted Protection against code,</td>
<td>Hardware secured Protection against code,</td>
</tr>
<tr>
<td></td>
<td>secret software attacks</td>
<td>secret and data bus attacks</td>
<td>secret and data bus attacks</td>
</tr>
<tr>
<td><strong>Output Protection</strong></td>
<td>HDCP DTCP</td>
<td>HDCP DTCP</td>
<td>Additional requirements for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>links using HDCP / DTCP</td>
</tr>
</tbody>
</table>

**Note:**
The applicable security level not only depends on the resolution but also on the age and value of the content.
HARDWARE-BASED CONTENT PROTECTION

- System-level security approach starting at the silicon level
  - Trusted Execution Environment (TEE)
    - Hardware Root of Trust
    - Secure Boot
    - ARM TrustZone® + Secure OS
  - Content Path
    - All decrypted content must be protected against software and hardware attacks from decryption up-to display
  - Side Channel Attack Protected Cryptography

- To reduce Risk and Time-to-market a layered integration and pre-certification should be done in order to reduce risks and time-to-market
  - Module (Secure OS + Hardware security + Secure Content Path)
  - SoC
  - Device
  - Application
A WORLD LEADER IN EMBEDDED SECURITY FOR MOBILE AND CONNECTED DEVICES

A world leader securing millions of devices and identities from the chip to the cloud.

An innovator with unique security assets, essential IP portfolio (>650 patents) and strong R&D focus.

$125.4M revenue in FY 2014

Global organization of about 250 employees with European & U.S. development centers.

With more than 100 blue chip customers, INSIDE Secure serves a multi-billion unit TAM across non-cyclical, growing and diversified end-markets. Products incorporating INSIDE Secure are shipping in over 300M devices per year. More than 25 years of experience in data security.
A COMPREHENSIVE SET OF PRODUCTS THAT PERFECTLY MATCHES MARKET SECURITY REQUIREMENTS

Threats

• Loss of application control, denial of service, ….
• Loss of user privacy and control of data
• Fraud
• Terrorism attacks
• Loss of revenue
• Liability issues
• Brand damage
• Health hazard
• …..

Security needs

• Device Identity and Authentication
• Root of Trust
• Secure Communication
• Secure Data Storage
• Trusted Execution Environment (TEE)
• Secure Boot
• Secure Updates
• Device Integrity
• …..

Solutions

Silicon IP cores and modules for SoCs
- High performance
- FIPS pre-certified / countermeasures
- Ultra low gate count and low power consumption
- Security Module for Mobile and IoT (VaultIP)

Highly tamper resistant ICs
- Proven security (CC EAL5+ IC, FIPS140-2 Level 3)
- Cryptographic & Security Functions
- Java OS GP2.2 & EMVco certified

Secure Application Software toolkits
- Content Protection – DRM, HDCP, DTCP-IP
- Application Protection and Data Security - for data in transit or at rest
- Proven security in financial applications: Software Protection, software secure element..

Secure Communication Software toolkits
- Tiny SSL/DTLS stack (10kb /600 bytes RAM)
- SSL / DTLS, IPsec, MACsec Software toolkits

Secure Personalization & Provisioning Services
- High Secure Environment
- High Security Level (EMV, Common Criteria)
A COMPLETE PRODUCT PORTFOLIO FOR CONTENT PROTECTION

Client side

**Downloadable DRM Agent**
*Streaming SDK for Apps in stores*
- PlayReady® DRM
- HLS, Smooth Streaming, DASH
- Android and iOS

**Embedded DRM Agent**
*Streaming SDK for OEM platforms*
- Integration with ARM TrustZone®, TEE and SCP
- Silicon crypto IP cores, modules and chips
- Supports most features from « Downloadable Agent »
- Android and Linux

**Embedded HDCP & DTCP-IP**
*Protection for media sharing*
- Stand-alone and ARM TrustZone®, TEE-based
- Support for multiple interfaces

Server side

**DRM Fusion Server**
*DRM license server*
- Running on Java
- DRM: PlayReady® and OMA2
- Target customers: media companies, system integrators, DRM clearinghouses
- Many active deployments

**DRM Batch Protector**
*Command-line DRM batch of content encryption tool*
- Running on Java
- Target customers: media companies, system integrators
- Many active deployments
SUMMARY

● Due to the success of OTT streaming and the increasing value of premium content, Hollywood studios are specifying higher security requirements to protect their high-value content

● Highest security levels can be achieved only by a system level security approach

● ARM TrustZone®/TEE + ARM’s Secure Content Path together with a hardware-based DRM implementation is a perfect combination for solving today’s and future content protection requirements

● INSIDE Secure provides all the expertise and technology related to multi DRM integration as well as providing security modules in pre-certified silicon IP format or as CC EAL5+ certified chips

● ARM and INSIDE Secure are working together at the system level by implementing DRM on the latest ARM reference platform to significantly reduce risk and time-to-market for SoC/platform vendors and OEM’s
THANK YOU

Henk Pruim
hpruim@insidesecure.com

http://www.insidesecure.com/Contact-us