HKG18-203: Overview of Linaro DRM

Peter Griffin
Agenda

● Linaro DRM
● Encrypted Media Extensions (EME)
● Content Decryption Modules (CDMs)
● Linux:
  ○ OpenCDM / CDMi architecture
  ○ Linaro CDMs
  ○ What’s new?
  ○ What’s left to do?
● Android:
  ○ ClearKey
  ○ Playready
  ○ Widevine
● Secure Data Path (SDP)
Terminology

- EME  Encrypted Media Extensions
- DRM  Digital Rights Management
- CDM  Content Decryption Module
- CENC Common Encryption
- Key System - A content protection (DRM) mechanism

- Widevine  Google DRM key system
- Playready Microsoft DRM key system
- ClearKey  key system using unencrypted key
Linaro DRM

● Provide reference DRM integrations of PlayReady, Widevine and Clear Key to our members based on open source components for Linux & AOSP.

● Typically these components include:
  ○ ARM Trusted Firmware (ATF)
  ○ OP-TEE
  ○ EDK2/U-Boot
  ○ Linux (DRM/KMS, V4L2)
  ○ AOSP & ExoPlayer
  ○ Chromium
  ○ WPE, gstreamer
Linaro DRM

- **Linux**
  - Focus on W3C EME integration with Chromium and WPE
  - Support OpenCDM for DRM interoperability
  - Support for PlayReady and ClearKey CDMs in Linux

- **AOSP**
  - Focus on DRM integration with AOSP mediadrm & mediacrypto [1] frameworks
  - Support Widevine, PlayReady and ClearKey TAs.
  - Using Exoplayer app for playback

Agenda

- Linaro DRM
- **Encrypted Media Extensions (EME)**
- Content Decryption Modules (CDMs)
- Linux:
  - OpenCDM / CDMi
  - Linaro CDMs
- AOSP:
  - ClearKey
  - Playready
  - Widevine
- Secure Data Path (SDP)
Encrypted Media Extensions

EME is a W3C proposed recommendation to extend HTMLMediaElement to enable web applications to interact with content protections systems, and allow the playback of encrypted audio and video.

Supported by almost all browsers using various DRM platforms: Widevine, Adobe Primetime, PlayReady
Encrypted Media Extensions

Web Server may handle requests or send them directly to License Server.

Dashed lines show an optional additional session (includes dotted lines) or additional round trip.

CDM implementations may return decrypted frames or render them directly.

Legend:
- Blue: Content
- Red: Encrypted Key
- Gray: Optional
- Green: Other

Platform

Content Decryption Module (CDM)

Browser

Optional

Media Stack

Net

Application

License Server

Web Server

CDN
EME Application: dash.js

LHG have been using dash.js client as test web application for Playready

- Open source project on github
EME Application: eme_player.html

- Also eme_player.html found in Chromium source.
- Used for testing ClearKey CDM
- `chromium/media/test/data/eme_player_js/*`
- `chromium/media/test/data/eme_player.html`
- [http://people.linaro.org/~peter.griffin/chrome/eme_player.html](http://people.linaro.org/~peter.griffin/chrome/eme_player.html)
Agenda

● Linaro DRM
● Encrypted Media Extensions (EME)
● Content Decryption Modules (CDMs)
● Linux:
  ○ OpenCDM / CDMi
  ○ Linaro CDMs
● Android:
  ○ ClearKey
  ○ Playready
  ○ Widevine
● Secure Data Path (SDP)
What is a CDM?

- Provides the functionality on the target hardware to implement a key system.
- Key Systems can be (but are not limited to) a commercial DRM system or even a Clear Key.
Why develop CDMs?

- Embedded CPU power
  - Zero copy
- No SoC accelerated decrypt
  - Offload to crypto IP
- No SoC buffer protection after decrypt
  - TrustZone, TZASC, RDC, Interconnect firewall

Linaro reference solutions with OP-TEE attempt to address these areas, for various key systems on member SoCs.
Agenda

● Linaro DRM
● Encrypted Media Extensions (EME)
● Content Decryption Modules (CDMs)
● Linux:
  ○ OpenCDM / CDMi architecture
  ○ Linaro CDMs
  ○ What’s new?
  ○ What’s left to do?
● Android:
  ○ ClearKey
  ○ Playready
  ○ Widevine
● Secure Data Path (SDP)
OpenCDM / CDMi architecture

- **Content Decryption Module Interface Specification** from Microsoft to allow interoperability of DRMs with open source browsers.

- OpenCDM and cdmiservice projects are a reference implementation of this.
  - No longer maintained by fraunhoferfokus
  - Has led to several forks (Linaro, WPE)

- Linaro involvement
  - Port to ARM and integrations with Chromium
  - Support for OP-TEE
  - Unification of WPE & Linaro forks to support both browsers.
OpenCDM / CDMi architecture

Browser

OpenCDM [1]

CDMi Service [2]

cdmi.h
Interface for various key systems.

ClearKey
OpenSSL CDM

ClearKey
OP TEE [3]

PlayReady CDMi [4]

LHG using Chromium & WPE

OpenCDM plugin

Divided into three layers: browser glue, core and communication. Allowing other browsers or RPC mechanisms to be easily added. LHG supports Chromium and WPE (used in Comcast RDK).

[1] Note: Currently different key systems are selected at compile time via autotools --enable-playready or --enable-aes-ta.

Open Embedded integration

LHG has two OE layers, *meta-lhg* and *meta-lhg-prop*.

**Ambition** is to keep LHG OE layers as small as possible, and upstream as many changes to the upstream projects and other OE layers (e.g. meta-rpb).

1. **meta-lhg**: [https://github.com/linaro-home/meta-lhg](https://github.com/linaro-home/meta-lhg)
   a. Contains everything that can be public, and can’t be sent upstreamed to other layers.
      *meta-lhg-integration* dir contains ‘in flight’ patches which in an ideal world wouldn’t exist.
      ./recipes-security/optee/optee-aes-decryptor.bb
      ./recipes-security/ocdm/ocdmi_git.bb

   a. Contains recipes for proprietary components such as PlayReady and bbappends for public recipes to enable proprietary components e.g..
      ./recipes-browser/chromium: chromium_%.bbappend
      ./recipes-security/ocdm: ocdmi_%.bbappend
      ./recipes-security/optee: optee-playready.bb
      ./recipes-security/playready: files playready_3.3.4472.bb playready.inc
Open Embedded integration

#Build Chromium with OpenCDM plus OP-TEE ClearKey TA
> repo init -u https://github.com/linaro-home/lhg-oe-manifests.git -b morty
> repo sync
> . setup-environment
> bitbake rpb-westonchromium-image

#Force re-compile of Playready & optee-playready libs
bitbake playready -f -c do_compile; bitbake playready -f -c do_install;
bitbake playready -f -c do_populate_sysroot; bitbake playready -f -c
do_package;

#Force re-compile of ocdmi
bitbake ocdmi -f -c do_clean; bitbake ocdmi -f -c do_compile; bitbake ocdmi
-f -c do_install;

See blog post https://www.linaro.org/blog/lhg-updates-w3c-eme-solution-96boards-hikey-platform/
Debugging OpenCDM & CDMiService

**CDMiService**

Use `--enable-debug` configure option to enable logging and build with debug symbols.

```
meta-lhg/meta-lhg/recipes-security/ocdm/ocdmi_git.bb
```

Use GDB as usual to debug user binary.

**Chromium & OpenCDM**

Enable debug build of OpenCDM shared object

```
Set OCDM_CHROMIUM_BUILD_TYPE=Debug in
```

```
meta-lhg/recipes-browser/chromium/chromium-wayland_%.bbappend
```

Use additional

```
--ppapi-plugin-launcher='gdbserver localhost:4444' cmd argument to chrome to launch plugin inside gdbserver.
```
Agenda

- Linaro DRM
- Encrypted Media Extensions (EME)
- Content Decryption Modules (CDMs)
- Linux:
  - OpenCDM / CDMi architecture
  - Linaro CDMs
  - What’s new?
  - What’s left to do?
- AOSP:
  - ClearKey
  - Playready
  - Widevine
- Secure Data Path (SDP)
Linux: What’s new?

- Rebase of OpenCDM/CDMi integrations from Chromium v43 to Chromium v53.
- Integration of WPE browser glue into Linaro OpenCDM.
- Jenkins OE Playready build with Gerrit integration.
- Common Android/Linux TA branches.

In Progress?

- Rebase to Chromium v65 currently in progress.
- OpenCDM / CDMiservice github integration with Jenkins.
- WPE with Linaro OpenCDM reference builds.
- Automated Playready LAVA playback test.
Agenda

- Linaro DRM
- Encrypted Media Extensions (EME)
- Content Decryption Modules (CDMs)
- Linux:
  - OpenCDM / CDMi architecture
  - Linaro CDMs
  - What’s new?
  - What’s left to do?
- AOSP:
  - ClearKey
  - Playready
  - Widevine
- Secure Data Path (SDP)
Linux: To Do?

- Replicate SDP work from Android to Linux
- Linux Widevine OP-TEE support
- CDMiService multi DRM support
- LHG-282: Playready porting kit migration to CDMi API
- Become OpenCDM “upstream”
- CI & Testing
  - Better linaro-home github CI
  - Better validation with LAVA
Agenda

● Linaro DRM
● Encrypted Media Extensions (EME)
● Content Decryption Modules (CDMs)
● Linux:
  ○ OpenCDM / CDMi architecture
  ○ Linaro CDMs
  ○ What’s new?
  ○ What’s left to do?
● AOSP:
  ○ mediadrm / mediacrypto architecture
  ○ ClearKey
  ○ Playready
  ○ Widevine
  ○ SDP updates
AOSP

- DRM integrations focused on **ClearKey**, **Widevine** and **Playready** TA’s with AOSP mediadrm & mediacrypto frameworks.

- Try to build on LMG / SWG work e.g. use a OP-TEE enabled AOSP board like HiKey).
  
  https://github.com/linaro-swg/optee_android_manifest

- Recent focus on ClearKey and SDP support in all three TAs.
AOSP mediadrm mediacrypto arch

- DRM on AOSP uses a plugin based architecture

*(diagram from https://developer.android.com/reference/android/media/MediaDrm.html*)

Need implementation for each supported DRM scheme.
Agenda

● Linaro DRM
● Encrypted Media Extensions (EME)
● Content Decryption Modules (CDMs)
● Linux:
  ○ OpenCDM / CDMi architecture
  ○ Linaro CDMs
  ○ What’s new?
  ○ What’s left to do?
● AOSP:
  ○ mediadrm / mediacrypto architecture
  ○ ClearKey
  ○ Playready
  ○ Widevine
  ○ SDP updates
AOSP: ClearKey OPTEE plugin

- LHG developed OP-TEE ClearKey mediadrm & mediacrypto plugin (forked from OpenSSL ClearKey in AOSP source).
- Modified to use OP-TEE TA for AES decryption.
- Enhanced to support secure buffers.
- SDP_PROTOTYPE test code for SoC’s awaiting “secure codecs”.
- Creates `libdrmclearkeyopteeplugin.so` installed under `/vendor/lib/mediadrm`

- Allows fully open source SDP reference solutions (no proprietary code).

[https://github.com/linaro-home/clearkeydrmplugin](https://github.com/linaro-home/clearkeydrmplugin)
AOSP: ClearKey TA

- Common branch shared between Linux and Android.
- Modified to support TA decryption into trustzone secured buffer.
- Zero copy optimisation (removes 2x memcpy from decrypt path).
- Tested on 32 & 64bit TAs/SoCs.
- Tested on HiKey, TI X15 HS, iMX8M and Juno boards.
- Tested using ExoPlayer player.
- ClearKeyOPTEEDrmUnitTest available.

https://github.com/linaro-home/optee-clearkey-cdmi
Agenda

- Linaro DRM
- Encrypted Media Extensions (EME)
- Content Decryption Modules (CDMs)
- Linux:
  - OpenCDM / CDMi architecture
  - Linaro CDMs
  - What’s new?
  - What’s left to do?
- AOSP:
  - mediadrm / mediacrypto architecture
  - ClearKey
  - Playready
  - Widevine
  - SDP updates
AOSP: Playready plugin

- LHG have developed a PlayreadyCryptoPlugin and PlayreadyDrmPlugin for Microsoft Playready, which is a glue layer between Android and Playready Porting kit APIs.

- Plugin used in conjunction with Linaro Playready PRiTEE TA.

- Recently added support for multiple KIDs (allows decryption of streams encrypted with multiple keys e.g. 1x audio 1x video).

- SDP_PROTOTYPE test code for SoC’s awaiting “secure codec” support.

lhg-review.linaro.org:29418/android/playreadydrmplugin
Reference implementations by LHG.

[1] Playready MediaDrm & MediaCrypto plugins (LHG/Linaro)  
ssh://lhg-review.linaro.org:29418/android/playreadydrmpplugin

ssh://lhg-review.linaro.org:29418/lhg/playready

[3] PRiTEE TA (PlayReady Interface for Trusted Execution Environments)  
ssh://lhg-review.linaro.org:29418/optee-playready
AOSP: Playready TA updates

- Update to v3.3 Microsoft porting kit release
- Shared branch for Linux and Android development.
- Enablement of MS “Handle backed memory” API’s
  - Allows Playready TA decryption into a secure buffer.
- Removal of 2xmemcpy() in “non secure” decrypt call flow.
- OEM_CopySecureMemory() TA command added.
- Better multi-DRM support
  - Removal of some temporary scratch buffer allocations, which allows better co-existence with other DRM TA’s like Widevine & ClearKey.
AOSP: Playready TODO

- To be fully compliant some areas need further work.
  - Implementation of secure clock OEM APIs. (LHG-221)
  - Enforcement of Output protection levels (HDCP etc).
  - Override porting kit OEM cryptographic calls with GlobalPlatform APIs
  - More documentation of the “OP-TEE Intermediate Product”.
  - Upgrade to v4.0 MS porting kit (supports CBCS).
  - Upstream ARM porting kit changes to Microsoft.

- CI & Automated test
  - Jenkins & Gerrit integration for Android (in progress).
  - LAVA playback verification tests (in progress)
  - More unit tests e.g. pritee_test_utility.exe (LHG-222)
Agenda

- Linaro DRM
- Encrypted Media Extensions (EME)
- Content Decryption Modules (CDMs)
- Linux:
  - OpenCDM / CDMi architecture
  - Linaro CDMs
  - What’s new?
  - What’s left to do?
- AOSP:
  - mediadrm / mediacrypto architecture
  - ClearKey
  - Playready
  - Widevine
  - SDP updates
AOSP: Widevine

- Google provides Widevine mediadrn & mediacrypto plugins to Widevine licensees.

- Linaro has an OP-TEE oemcrypto reference implementation.


AOSP: Widevine

- OEMCrypto is an interface to the trusted environment that implements the functions needed to protect and manage keys for the Widevine content protection system.

- SWG/Linaro have implemented the OEM_Crypto_* v11 library for OP-TEE.

- Replacing oemcrypto.so with the op-tee reference library, moves the key management and decryption operations into the TEE.
AOSP: Widevine: OEMCrypto

The OEMCrypto interface provides:

1. mechanism to **establish a signing key**. Used to verify the authenticity of messages to and from a license server.

2. mechanism to **establish a key encryption key**. Used to decrypt the key material contained in the messages.

3. mechanism to **load encrypted content keys** into the trusted environment and decrypt them.

4. Mechanism to **use the content keys** to produce a decrypted stream for decoding and rendering.
AOSP: Widevine

- Google provide many unitary test code. Main one used currently is `oemcrypto_test`. Which tests the `oem_crypto` library.

- Also unitary tests are provided for mediadrm & mediacrypto level, and also APK level.

- Currently using ExoPlayer at application level for video playback testing.
oemcrypto_test

LOAD_TEST_KEYBOX: Call LoadTestKeybox before deriving keys.
Note: Google Test filter = *-ForceKeybox:*CastReceiver:*Performance*
[==========] Running 251 tests from 21 test cases.
[----------] Global test environment set-up.
[----------] 18 tests from OEMCryptoClientTest
[ RUN ] OEMCryptoClientTest.VersionNumber
  OEMCrypto Security Level is L1
  OEMCrypto API version is 11
  OEMCrypto supports usage tables.
[ OK ] OEMCryptoClientTest.VersionNumber (72 ms)
[ RUN ] OEMCryptoClientTest.CheckHDCPCapability
[ OK ] OEMCryptoClientTest.CheckHDCPCapability (79 ms)
[ RUN ] OEMCryptoClientTest.CheckMaxNumberOfSessionsAPI10
  Max Number of Sessions: 50.
[ OK ] OEMCryptoClientTest.CheckMaxNumberOfSessionsAPI10 (62 ms)
[ RUN ] OEMCryptoClientTest.NormalGetDeviceId
  NormalGetDeviceId: dev_id = HiKey02_L1_00000001 len = 19
[ OK ] OEMCryptoClientTest.NormalGetDeviceId (66 ms)
[..]
AOSP: Widevine updates

- Support added for decryption into trustzone secure buffers and the `OEMCrypto_BufferType_Secure` buffer type.

- Last remaining `oemcrypto_test` test failure fixed [SWG-194](#).

- Migration to 64bit TA on 64bit SoCs

- New README.md to help new developers.

- Secure decryption support being used by ARM Juno & NXP iMX8M platforms.
AOSP: Widevine TODO

- Update to OEMCrypto v13 API.
  - HDCP system renewability message
  - Provisioning 3.0

- Enforcement of HDCP protection in TEE.

- Better documentation for members.

- Better automated CI & testing
  - oemcrypto_test, and others unitary code converted into LAVA tests.

- Provide reference provisioning?
SDP updates

- All 3 DRM TA’s now provide support for decryption into secure buffers.

- In Android platforms like iMX8M or Juno whose OMX implementations enable secure codecs, TA’s decrypt into the secure buffer passed by OMX layer.

- PlayReady & ClearKey plugins also have additional SDP_PROTOTYPE test code.

- Very hard to enable full SDP pipeline without close collaboration with member company engineers.
  - Often requires changes in video firmware. In-depth knowledge of SoC required. LHG has very limited resources.
**Boards / SoCs**

<table>
<thead>
<tr>
<th>Board / SoC</th>
<th>ClearKey DRM</th>
<th>PlayReady DRM</th>
<th>Widevine DRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiKey 96</td>
<td><strong>Yes</strong> Linux + Android</td>
<td><strong>Yes</strong> Linux + Android</td>
<td><strong>Yes</strong> Android</td>
</tr>
<tr>
<td>NXP iMX8M</td>
<td><strong>Yes</strong> Android *</td>
<td><strong>Yes</strong> Android *</td>
<td><strong>Yes</strong> Android</td>
</tr>
<tr>
<td>TI X15 HS</td>
<td><strong>Yes</strong> Android</td>
<td><strong>Yes</strong> Android</td>
<td>No</td>
</tr>
<tr>
<td>Poplar 96</td>
<td>Android (in progress)</td>
<td>Android (in progress)</td>
<td>Android (in progress)</td>
</tr>
</tbody>
</table>

* Linux support in progress

- New boards to consider in the future. HiKey960.
WE NEED YOU!
Thank You

peter.griffin@linaro.org
#HKG18
HKG18 keynotes and videos on: connect.linaro.org
For further information: www.linaro.org
This Slide is for when Two Columns are Needed

- You can use this for two columns of bullets
- Or you can replace one column with an image or diagram

- This could be a second column of bullets
- Or it could be a table, image or graphic
Useful Logos

Download Hi Res logos from here* to use on your slides

*http://link.linaro.org/logos
Some Images

- Download Hi Res photos from [here](http://link.linaro.org/groupphotos) to use on your slides

* [http://link.linaro.org/groupphotos](http://link.linaro.org/groupphotos)