INDUSTRY FORUM

VR-IF Security Guidelines
CES2018 Master Class

Mick O'Doherty – Irdeto
Technical Solutions Manager
VR-IF – Security Task Force Chair

Security

INDUSTRY FORUM

- The security sections in the guidelines focus on protecting Virtual Reality (VR) content.
- VR content includes not only 360 Video, but also associated assets such as CGI graphics.
- This draft of the guidelines focuses on VR 360 Video, building on existing best practice for traditional content security.
- Traditional threats and security problems are outlined along with VR specific threats.
- Security mechanisms such as encryption, secure media pipelines and secure platforms, are discussed in the VR context.
- Topics for further discussion, in particular focusing on viewport dependent profiles are identified.

Security – MovieLabs ECP

INDUSTRY FORUM

- The MovieLabs Specification for Enhanced Content Protection (ECP) describes a set of high-level requirements for securing content.

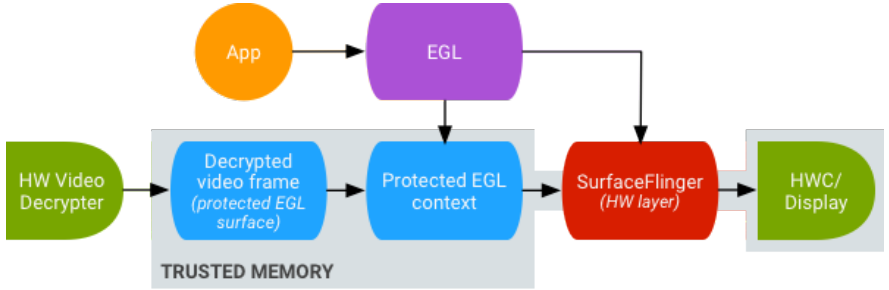
- They are intended to be general enough to be applicable to any content distribution system (including future ones), but specific enough to serve as a template for evaluating a specific instance of such a system.

- Although the ECP is a good starting point for defining guidelines for systems distributing VR content, additional work is required because VR is a fundamentally different media type than traditional audio-visual content. Some of these differences require new mechanisms (or modifications of existing ones) to secure the VR content.

- The guidelines follow the format of the ECP document and highlight the deltas that VR introduces.

Security – Encryption

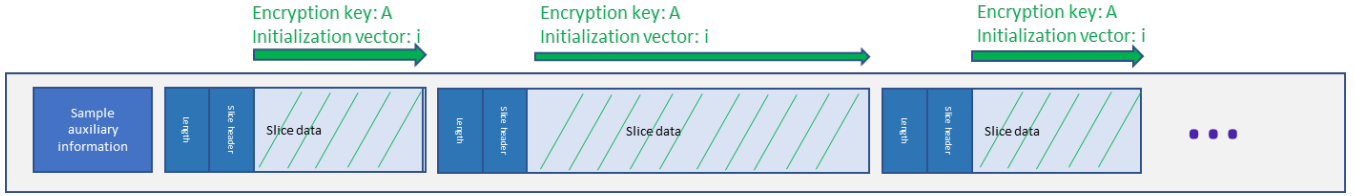
- The Viewport Independent Media Profile is fully compatible with all commonly deployed DRM functionalities and encryption work flows which makes it simple and easy to deploy - current DRM and encryption technology allow a Viewport Independent Media Profile video to be encrypted, transported, decrypted and made available for rendering. The rendering process may differ across players and platforms, some of which may impose some restrictions, however testing on major mobile OS's has shown full support and it is expected this will extend across major platforms and players. Example guidelines for the usage of DRM and security in DASH are provided in the DASH-IF interoperability guidelines [DASH-IF IOP], clause 7. This provides a good overview of widely deployed adaptive streaming DRM and encryption systems.



Example of rendering transformation on protected video memory from Android online documentation - https://source.android.com/devices/graphics/arch-st

Security – Encryption cont.

- For Viewport Dependent Baseline Media Profile, content encryption has some new requirements.
- When the DASH Access engine in the VR Service Platform performs DASH sub-segment concatenation, it will construct a single ISOBMFF file.
- This file will contain encrypted data from individual DASH streams for each tile that will make up the frame, concatenated into the single ISOBMFF file.



- This restricts the AES encryption mode that can be used – ctr and cbc1 cannot be used. For this reason the recommended encryption mode for viewport dependent media profile VR at this time is cbcs.

- Note this area remains a work in progress and further investigation is required to verify the operation of VR Players and to analyse the performance implications of this approach.

Security – further focus areas

INDUSTRY FORUM

- Verification of VR player capabilities across platforms and of encryption performance implications.
- VR 360 Video watermarking.
- CGI content protection.
- Sensor and return path data security guidelines.