# Technical Alternative to Encrypted Media Extensions (EME)

## Introduction

Encrypted Media Extensions (EME) are a draft specification[1] to standardize digital rights management (DRM) for audio and video at the browser level.

The specification has been very controversial in the software community since it was first drafted in 2012. It was proposed by content providers and streaming service operators to ensure that content delivered to legitimate users is inaccessible to pirates.

However, the proposed solution raised salient questions about interoperability, privacy, accessibility and implementation in Free and Open Source (FOSS) software.

Several parties have, over the course of the discussion at W3C, proposed several alternate technical alternatives. This report aims to analyze these alternatives and the proposed EME specification along six dimensions; technical copy protection, legal copy protection, interoperability/entry barriers for browsers, privacy, accessibility, and user security.

## Aims of the Specification

- Make it technically hard for a malicious user to pirate a particular media
- Have sufficient legal barriers to deter infringement

At the same time:

- Ensure interoperability and make sure there are no entry barriers for new browsers
- Protect privacy of users
- Make sure the system doesn't bring about security vulnerability
- Maintain accessibility for a person with disabilities

## Metrics of Comparison

### Technological Copy Protection :

During the transfer of video content from the web server of the content provide to the user, there are multiple points where a malicious entity can capture the copyrighted content.

We classify the technical strength of a DRM system depending on the point in transition where the capture can take place. Assuming the server is itself secure, the first point where the adversary can capture the media is during the transition from the server to the user's device. Preventing such kind of interception is a

[1] Encrypted Media Extensions W3C Candidate Recommendation *https://www.w3.org/TR/encrypted-media/*. For a general overview see https://hsivonen.fi/eme/

standard problem and is in solved by the use of HTTPS. After the media stream reaches the device of the intended user, she can capture the before it is played on the media software. For example in case of images or text, the user can usually save the media without the need of any special software or specialized technique. So the next step from content providers side is build restrictions in the software playing the media. The usual way to do this is by making sure that the media can be played only on certain software which doesn't allow the user to copy the media. The software restrictions can be implemented using arbitrary codecs, scrambling or encryption. Technical restrictions at software level are always prone to be captured by screen capturing softwares, and hardware emulators which appears as output devices to media software but are used to save the media instead. To prevent capturing at software level there exists technologies such as HDCP[2] which protects the media during its transition from the media software to the output device. Although such technologies are also fallible to a user holding a video camera in front of the monitor. This weakness of the DRM systems is known as Analog Hole.

Technological Copy Protection is:

- High: Infringer needs specialized hardware to capture the copyrighted content.
- Medium: Infringer needs specialized Software to capture the copyrighted content
- Low: Infringer needs only commonly available software and hardware to capture the copyrighted content

Copy Protection (Legal)

Jurisdictions across the world have laws which make it illegal to circumvent technological protections methods for the protections of Copyright. The most famous of them is the Section 1201 of the United States Digital Millennium Copyright Act (DMCA). For content providers who wish to use TPMs to prevent piracy of their copyrighted work, these laws provide additional layers of protection. DMCA disallows circumventing a technical measure which effectively control access to copyrighted work, also it disallows the "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component" which is primarily designed to circumvent a DRM. DMCA has an exception that allows the reverse engineering of a DRM when solely done to provide interoperability.[3]

Legal protection against infringement is high in DRM system if:

- High: Circumventing the DRM and creating tools to enable that is illegal unconditionally

[2] HDCP Whitepaper, *https://web.archive.org/web/20080920191718/http://www.digital-cp.com/files/documents/04A897FD-FEF1-0EEE-CDBB649127F79525/HDCP_deciphered_070808.pdf*

[3] Section 1201, US Digital Millennium Copyright Act

- Medium: Circumventing the DRM and creating tools to enable that is illegal depending the intent and circumstances
- Low: Circumventing the DRM and creating tools to enable that is legal.

Security

DRM systems have been criticized for leaving users' devices vulnerable.

Security of a user using the DRM system is:

- High: The system don't require any elevated permissions
- Medium: The system only requires elevated software permissions
- Low: The system requires both elevated hardware or software permission

Privacy

Privacy of user using the DRM systems is:

- High: The system doesn't collect minimal information
- Medium: The system only collects non personally identifiable information
- Low: The system collects personally identifiable information

Accessibility

DRM systems can turn out to be problematic for providing accessibility for disabled persons. In case of video service can be made accessible by providing access to closed captions for a video and by modifying the stream to make it accessible to color blind people. However, a DRM system could present unnecessary barriers for people trying to provide accessibility solutions. There can be technical barrier in the process of handling the video stream

W3C Technical Architecture Group (TAG) suggested following guidelines to maintain accessibility in Encrypted Media Extensions:[4]

- ensuring that media content may be redirected to certain system services;
- ensuring that every piece of digital content is available in its original form (for example, subtitles are not blended into video, etc);
- ensuring that standard operations (adjusting contrast, using third-party subtitles or audio-stream) may be applied to restricted media;
- ensuring that restricted media from different sources provided by different EME systems (for example, video from one source and sign-language interpretation of that video from another source) may be used simultaneously.

We say accessibility in a DRM system is:

- High: If all the of the guidelines are met

[4] https://github.com/w3ctag/eme/blob/master/EME%20Proposal.md#accessibility-1

- Medium: If two more points in the guideline are met
- Low: If less than points of the guideline are met

Interoperability

Interoperability of any system is important to keep the entry barriers low for a new producer to enter the market. Interoperability of a DRM system for browsers is:

- High: The full spec is available for implementation on royalty free basis
- Medium: The full spec is not available, but can be implemented through reverse engineering without legal barriers.
- Low: Third parties may restrict new browsers from implementing the spec through legal means.

Specifications

EME Specification

EME specification only defines the javascript component of the system and the large component called Content Decryption Module(CDM) is left undefined. The CDM can be hardware based using technologies like HDCP, which prevents screen capture. The CDM can be software based and can return the decrypted video to the browser to render, or it can use its own media stream and render it by itself. Most of the CDMs in use are proprietary but there can exist CDMs which are fully specified and are open source. The implications for copy protection, privacy, accessibility and security depends on the CDM used. Interoperability of EME spec is very low because there are not only technical barriers due lack of full specification but also legal barriers as browsers may need to get into a contract with the dominant CDM providers to add support for their CDM.

Obfuscation (Arbitrary Codec)

Charles Pritchard pointed out the HTML5 video specification is codec agnostic, hence the content providers can stream the media using an arbitrary codec which only supported by the media provider.[5] So even if the user captures the video stream it cannot be pirated without reverse engineering the codec. Although reverse engineering is usually allowed by DRM laws hence the legal protection is low.[6] Since the codec support is provided through OS, there is no need to modify the browser and the system can be supported by any browser without any technical or legal barriers.

HTTPS and JS encryption

Tab Atkins proposed using JS encryption using browser and <video> element[7]. Since the technique requires the a malicious user to implement the full <video>

[5] https://lists.w3.org/Archives/Public/public-html/2012Feb/0328.html

[6] Section 1201, Digital Millennium Copyright Act

[7] https://lists.w3.org/Archives/Public/public-html/2012Feb/0456.html

spec to decrypt the video, the scheme provides moderate technical copy protection.

Encryption using video tag

According to David Singer encrypted video can be played through the existing <video> tags where the content file says its content-ID and is marked as protected, someone who has the DRM to play the content installed and has brought the keys to play it can watch the video.[8] As a concrete example he talked about protected .m4p audio files from iTunes library, which plays just fine on Safari.[9]

Plugin System (Flash)

Existing plugin system, mainly Flash is be used to as a technical measure to prevent copyright infringement. It is more interoperable than EME because any browser with a correct implementation of NPAPI can provide support for Flash[10].

@@

Diversity Analysis

We considered that any email on the public-html mailing list of W3C with " EME ", "Encrypted Media" or "Digital Rights Management" in the subject line is about the Encrypted Media Extensions draft specification. Then we manually tagged every participant by their gender, the region they belong to and their stakeholder community.

Region

@@

We found that there were no absolutely participants from Asia, Africa or South America.

The Internet is lived differently in different parts of the world. The IP laws in many countries in the global South are very different to those in the USA or Europe. In addition, many internet users in these countries use connections with relatively low bandwidths. The lack of representation of people from the global South means that their concerns -- technical, cultural, and legal -- are not being considered at all in this debate.

Stakeholder Community

@@

We observe that there was no participation from the Security Researcher community and negligible participation from privacy community. Voice of Digital Content Provider was overrepresented with almost 40% of emails sent by them.

[8] https://lists.w3.org/Archives/Public/public-html/2012Feb/0422.html

[9] https://lists.w3.org/Archives/Public/public-html/2012Feb/0433.html

[10] https://lists.w3.org/Archives/Public/public-html/2012Feb/0427.html

Methodological remarks:

- Participants are categorized on the basis stakes of their employer and not specifically on the work they do. For example someone who works on privacy in Google will be placed in “DRM platform provider” instead of “Privacy”.
- W3C and Universities are considered to neutral and their employees are categorized by the work they do.
- Google’s position is very interesting, it is a DRM provider as a browser manufacturer but also a content provider in Youtube and fair number of Google Employers are against EME due to other concerns. Therefore Christian Kaiser has been paced as Content provider because he works on Youtube, and everyone else has been placed as DRM provider.

Gender

@@

There was only one women participating in the discussing contributing 1.3 % of the emails sent. The numbers reflects widely discussed lack of gender diversity in Tech and Open communities[11].

[11] http://geekfeminism.wikia.com/wiki/FLOSS