Technical Alternatives to Encrypted Media Extensions and Diversity Analysis

Harsh Gupta

12MA20017

Table Of Content

Introduction and Motivation

The arrival of internet and digital technologies have made it is very easy and cheap to create perfect copies of digital media. This has produced serious difficulties to produce and distribute media using the pre internet era business models. To continue with their old ways media companies have tried to make it hard for people to make copies of digital media and working with hardware manufacturers and software platform providers they have various types of copy restrictions in hardware and software that is used to play the media. These technologies are largely known as Digital Rights Management or Digital Restriction Management or simply DRM. DRMs have remained controversial since their inception, by media companies DRM is seen as something essential to preserve their business models and continue operating profitably whereas many digital rights activist see DRM as something fundamentally opposed to user's ability to own and control their devices. DRM also opens up serious issues regarding serious issues Modern DRM usually works by storing and transmitting the media in encrypted formats which is usually decrypted only while the playing or rending of the media on end user's devices. On the world wide web the existing way use DRM for videos is through party plugins like Adobe's Flash Player and Microsoft silverlight. There is an ongoing draft proposal by W3C to standardize this in HTML5 with a standard called Encrypted Media Enhancements(EME). EME has remained controversial since 2013 when the work on the standard started.
The aim of my study during the internship was two fold:

- Study the debate that happened about EME, and identify if any better standard could have been prepared.
- Figure out if the interests of all the stakeholders were well represented at W3C.

Detailed Methodology

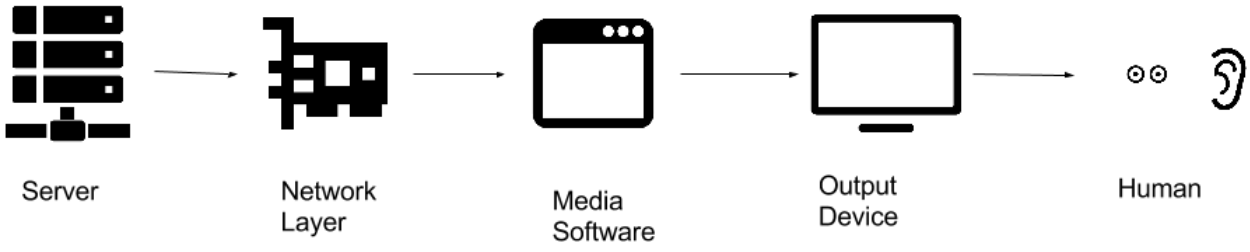
Methodolgy for Comparison of Technical Alternatives to EME

In the early stages of the research I read all emails sent between 21st February 2012 to 1st March 2012 about EME on the public-html mailing list. There were more 100 such emails discussing the various aspects of the proposed EME standard. Then I identified major themes of the discussion and the several alternatives to EME that were proposed.
In the next stage, I evaluated the proposed standards on six dimensions identified in the discussion. These are

- technical copy protection
- legal copy protection
- interoperability and entry barriers for browsers
- accessibility
- privacy of the user
- security of user's system.

Overview of 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 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[1] 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

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

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.[2]
Legal protection against infringement is high in DRM system if:

- High: Circumventing the DRM and creating tools to enable that is illegal unconditionally
- 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:[3]

- 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.

---

2 Section 1201, US Digital Millennium Copyright Act
3 https://github.com/w3ctag/eme/blob/master/EME%20Proposal.md#accessibility-1

We say accessibility in a DRM system is:

- High: If all the of the guidelines are met
- 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.[4] 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.[5] 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.

4 https://lists.w3.org/Archives/Public/public-html/2012Feb/0328.html
5 Section 1201, Digital Millennium Copyright Act

HTTPS and JS encryption

Tab Atkins proposed using JS encryption using browser and <video> element[6]. Since the technique requires the a malicious user to implement the full <video> 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.[7] As a concrete example he talked about protected .m4p audio files from iTunes library, which plays just fine on Safari.[8]

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[9].

Diversity Analysis Methodology

Any emails with EME, Encrypted Media or Digital Rights Management in the subject line is considered to about EME. Then each of the participant is categorized on the basis of region of the world they belong to and their employer's interest to the debate.

Region Categories

- Asia
- Australia and New Zealand
- Europe
- Africa
- North America
- South America

Region Methodology

- Look up their personal website and social media accounts (Twitter, LinkedIn, Github) and see if it mentions the country they live in. (Works in Most of the cases)
- If the person's email has uses a country specific top level domain, assume that as the country
- If github profile is available look up the timezone on last 5 commits.

6 https://lists.w3.org/Archives/Public/public-html/2012Feb/0456.html
7 https://lists.w3.org/Archives/Public/public-html/2012Feb/0422.html
8 https://lists.w3.org/Archives/Public/public-html/2012Feb/0433.html
9 https://lists.w3.org/Archives/Public/public-html/2012Feb/0427.html

- For people who have moved from their home country consider the country where they live now.

Work Categories

- Foss Browser Developer
- Content Provider
- DRM platform provider
- Accessibility
- Security Researcher
- Other W3C Employer
- Privacy
- None of the above

Work Methodology

- Look up their personal website and social media accounts (Twitter, LinkedIn, Github) and see if it mentions the employer and categorize accordingly.
- 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.

Knowledge/Skills Acquired

The skill I acquired through this internship are varied and complex. In specific I learned how does video on a modern browser work, how are content protection systems implemented and how to download mailing list conversations and analyze them. On a higher level I learned how web standards are made, the politics that goes inside it and how non-profit research organizations work.

Results And Discussion

Techinical Alternatives

Technical Alternative	Copy Protection Technical	Interoperability	Copy Protection Legal	Accessibility	Privacy	Security
Obfuscation (Arbitrary Codec)	Medium	High	Low	Depends on Implementation Details	High	High
Encryption using video tag	Medium to High[10]	Medium	High	Depends on Implementation Details	Depends on Implementation Details	Depends on Implementation Details
HTTPS and JS decryption	Medium	High	High	Depends on Implementation Details	High[11]	High
EME	Depends on CDM[12]	Low	High	Depends on CDM	Depends on CDM	Depends on CDM
Plugin (Flash)	High[13]	Medium	Medium	Medium[14]	Low[15]	Low

10 Using HDCP is possible with compatible hardware
11 The implementation itself doesn't require additional cookies
12 The Spec allows CDMs which do not act as DRM, but the content providers may not support them.
13 Adobe's new Flash DRM comes with selective output control
http://arstechnica.com/business/2010/05/adobes-new-flash-drm-comes-with-selective-output-control
14 Flash Player provides some accessibility functionalities
https://www.adobe.com/accessibility/products/flash/captions.html
15 Soltani, Ashkan and Canty, Shannon and Mayo, Quentin and Thomas, Lauren and Hoofnagle, Chris Jay, Flash Cookies and Privacy (August 10, 2009). Available at SSRN: http://ssrn.com/abstract=1446862 or http://dx.doi.org/10.2139/ssrn.1446862

Diversity Analysis

Region

Region	Participants per Region	Emails sent per Region
Asia	0	0
Europe	13	146
Australia and New Zealand	5	16
Africa	0	0
North America	30	310
South America	0	0
Total	**48**	**472**

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

Stakeholder Community	Participants per work category	Emails sent per work category
FOSS browser developer	5	56
Digital Content Provider	9	186
DRM Platform Provider	15	100

Accessibility	4	47
Security Researcher	0	0
Privacy	2	2
Other W3C Employee	3	10
None of the Above	10	71
Total	**48**	**472**

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.

Gender

Gender	**Participants per Gender**	**Emails sent per Gender**
Female	1	6
Male	47	466
Total	**48**	**472**

Summary Of The Outcome

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[16].

We found that there are vaible technical alternatives to Encrypted Media Extensions specification which can provide sufficient content protection without compromising on privacy, accessebility, interoperability or security.

In the diversity analysis we found out that there was a serious lack of representation on all fronts in questions, region, gender and the stakeholder communities.

References

- *Chromium Design Documents Video* https://www.chromium.org/developers/design-documents/video
- Mark Pilgrim, *Dive into HTML5, Video*: http://diveintohtml5.info/video.html

16 http://geekfeminism.wikia.com/wiki/FLOSS

- *HDCP White Paper*: https://web.archive.org/web/20080920191718/http://www.digital-cp.com/files/documents/04A897FD-FEF1-0EEE-CDBB649127F79525/HDCP_deciphered_070808.pdf
- Section 1201, Digital Millennium Copyright Act
- Soltani, Ashkan and Canty, Shannon and Mayo, Quentin and Thomas, Lauren and Hoofnagle, Chris Jay, Flash Cookies and Privacy (August 10, 2009). Available at SSRN: http://ssrn.com/abstract=1446862 or http://dx.doi.org/10.2139/ssrn.1446862

Appendix

Code for diversity analysis

```
import bigbang.mailman as mailman
import bigbang.process as process
from bigbang.archive import Archive


import pandas as pd
import datetime

from commonregex import CommonRegex

import matplotlib.pyplot as plt
%matplotlib inline
def filter_messages(df, column, keywords):
        filters = []
        for keyword in keywords:
        filters.append(df[column].str.contains(keyword, case=False))

        return df[reduce(lambda p, q: p | q, filters)]
# Get the Archieves
pd.options.display.mpl_style = 'default'  # pandas has a set of preferred graph formatting options

mlist = mailman.open_list_archives("https://lists.w3.org/Archives/Public/public-html/",
archive_dir="./archives")

# The spaces around eme are **very** important otherwise it can catch things like "emerging", "implement"
etc
eme_messages = filter_messages(mlist, 'Subject', [' EME ', 'Encrypted Media', 'Digital Rights Managagement'])
eme_activites = Archive.get_activity(Archive(eme_messages))

# XXX: Bugzilla might also contain discussions
eme_activites.drop("bugzilla@jessica.w3.org", axis=1, inplace=True)

# Remove Duplicate senders
levdf = process.sorted_matrix(eme_activites)

consolidates = []
# gather pairs of names which have a distance of less than 10
for col in levdf.columns:
  for index, value in levdf.loc[levdf[col] < 10, col].iteritems():
        if index != col: # the name shouldn't be a pair for itself
        consolidates.append((col, index))

# Handpick special cases which aren't covered with string matching
consolidates.extend([(u'Kornel Lesi\u0144ski <kornel@geekhood.net>',
                u'wrong string <kornel@geekhood.net>'),
                (u'Charles McCathie Nevile <chaals@yandex-team.ru>',
                u'Charles McCathieNevile <chaals@opera.com>')])
```

```
eme_activites = process.consolidate_senders_activity(eme_activites, consolidates)
sender_categories = pd.read_csv('people_tag.csv',delimiter=',', encoding="utf-8-sig")

# match sender using email only
sender_categories['email'] = map(lambda x: CommonRegex(x).emails[0].lower(),
sender_categories['name_email'])

sender_categories.index = sender_categories['email']
cat_dicts = {
        "region":{
        1: "Asia",
        2: "Australia and New Zealand",
        3: "Europe",
        4: "Africa",
        5: "North America",
        6: "South America"
        },
        "work":{
        1: "Foss Browser Developer",
        2: "Content Provider",
        3: "DRM platform provider",
        4: "Accessibility",
        5: "Security Researcher",
        6: "Other W3C Empoyee",
        7: "Privacy",
        8: "None of the above"

        }
}

def get_cat_val_func(cat):
        """
        Given category type, returns a function which gives the category value for a sender.
        """
        def _get_cat_val(sender):
        try:
        sender_email = CommonRegex(sender).emails[0].lower()
        return cat_dicts[cat][sender_categories.loc[sender_email][cat]]
        except KeyError:
        return "Unknow"
        return _get_cat_val
grouped = eme_activites.groupby(get_cat_val_func("region"), axis=1)
print("Emails sent per region\n")
print(grouped.sum().sum())
print("Total emails: %s" % grouped.sum().sum().sum())
print("Participants per region")
for group in grouped.groups:
        print "%s: %s" % (group,len(grouped.get_group(group).sum()))
print("Total participants: %s" % len(eme_activites.columns))
grouped = eme_activites.groupby(get_cat_val_func("work"), axis=1)
print("Emails sent per work category")
print(grouped.sum().sum())
print("Participants per work category")
for group in grouped.groups:
        print "%s: %s" % (group,len(grouped.get_group(group).sum()))
```