

The Crisis of Standardizing DRM: The Case of W3C Encrypted Media Extensions

Harry Halpin^(✉)

Inria, 2 rue Simone Iff, 75012 Paris, France
harry.halpin@inria.fr

Abstract. The process of standardizing DRM via the W3C Encrypted Media Extensions (EME) Recommendation has caused a crisis for W3C and potentially other open standards organizations. While open standards bodies are considered by definition to be open to input from the wider security research community, EME led civil society and security researchers asking for greater protections to be positioned actively against the W3C. This analysis covers both the procedural issues in open standards at the W3C that both allowed EME to be standardized as well as for vigorous opposition by civil society. The claims of both sides are tested via technical analysis and quantitative analysis of participation in the Working Group. We include recommendations for future standards that touch upon some of the same issues as EME.

Keywords: Digital Rights Management · W3C · Security · Privacy · Standardization

1 Introduction

Encrypted Media Extensions (EME) has been recommended by Tim Berners-Lee in his role as director of the World Wide Web Consortium (W3C) as the first official Web standard for Digital Rights Management (DRM).¹ This has been a controversial decision: A large number of security researchers, ranging from Ron Rivest to Bruce Schneier, have signed a petition demanding the W3C not recommend Encrypted Media Extensions until protections for security researchers could be put into place, as suggested by a “covenant” put forward by the Electronic Frontier Foundation [8].

Encrypted Media Extensions (EME) is the only standard to enable DRM across all major web browsers (including Google, Microsoft, Apple, and Mozilla), deploying an open standards body to enable spread of DRM, a technology traditionally associated with preventing open access to information. It is also the only Web standard to lead to street protests outside of the office of W3C/MIT,² statements from civil society and academics against standardizing EME, and massive

¹ <https://lists.w3.org/Archives/Public/public-html-media/2017Jul/0000.html>.

² On a personal aside, including my resignation from W3C staff.

negative feedback on social media. Although EME was eventually in 2017 eventually approved by Tim Berners-Lee as a W3C Recommendation, overriding the objections, the repercussions of this decision could threaten the continued existence of W3C itself in the future.

The crisis brought about by standardizing DRM at the W3C goes beyond the particulars of the W3C and EME, as the entire episode shows the benefits and difficulties of an open standards process where civil society, security researchers, and the private sector all can directly participate. Open standards are defined as “open” in terms of participation, in contrast to “closed” standards bodies such as the ITU or ISO where participation requires government status. While open standards are typically required by commercial actors for anti-trust reasons, open processes also tend to be good practice from a security perspective, as the review of multiple experts typically discovers security flaws. However, when an open standards body like the W3C decides to standardize DRM at the bequest of a few actors in private industry, despite many security researchers protesting that EME will lead to increased security vulnerabilities, what can and should be done in terms of standardization?

Judging the harm to users caused by enabling a new capability that also introduces a new attack surface in a browser is not a straightforward trade-off, but requires serious analysis of both technical and social claims in the process of security standardization. After first exploring the often labyrinthine process of standardization at the W3C in Sect. 2, we’ll explore the Encrypted Media Extension standard itself, including its relationship to HTML5 in Sect. 4. This lets us analyze each of the arguments made both for and against standardizing EME in Sect. 5. Section 6 presents a data analysis of the mailing-lists to validate claims around the composition and participation of the W3C Working Group that standardized EME. Lastly, we’ll suggest ways forward to avoid the problems inherent in standardizing DRM in security standards in general in Sect. 7 before summarizing our findings in Sect. 8.

2 The World Wide Web Consortium

The World Wide Web Consortium is one of the pre-eminent standards bodies of the Internet, founded by Tim Berners-Lee in 1994 as a “break away” standards organization from the IETF (Internet Engineering Task Force) [4]. The W3C would specialize in web standards focused on the application layer in the browser, in contrast to standards focused on the networking layer as done in the IETF. The W3C is a “virtual organization” that maintains no official incorporated (non-profit or otherwise) status, and does not even have its own bank account, instead relying on its hosts and offices. This is unusual among standards bodies, as the IETF has its bank accounts ran through the Internet Society (ISOC), an officially registered non-profit. Unlike ISOC’s relationship to the IETF, the W3C is a sponsored research activity within MIT (similar to a DARPA or NSF contract). As global headquarters of W3C, MIT maintains three host agreements with Keio, Beihang, and ERCIM (France) for regional hosts. The costs of running

the consortium are paid by annual re-occurring membership dues from their (as of July 2017) 475 members, where the dues range from 77,000 USD for a large enterprise to 7,900 USD for non-profits and government agencies (although costs are lower developing countries).³ The revenue from membership dues primarily goes to pay W3C employees and the corresponding overhead costs from their host. The W3C staff are paid to be neutral technical and administrative arbiters, which the W3C states justifies the cost of membership.

3 W3C Patent Policy

A crucial advantage to W3C membership is that the W3C is in effect a patent pool for the World Wide Web.⁴ W3C standards are explicitly licensed by W3C members under a royalty-free license.⁵ In contrast, the IETF “Note Well” policy simply requires disclosure of known patents by individuals.⁶ The much stronger W3C policy essentially creates a kind of “patent war-chest” composed of all W3C standards, from XML to HTML5. This patent war-chest is then enforced by a ‘balance of terror’ so that any member that makes a patent claim on a W3C standard triggers their loss of royalty-free licensing for *all* W3C standards.

This patent policy is purported to defend W3C members against patent trolls, and as most large Silicon Valley companies (with the noticeable absence of Amazon, but including Google, Microsoft, Oracle, IBM, Apple, and the like) are members of the W3C, one likely result of the Royalty-Free licensing policy is to prevent lawsuits between W3C members as well. It can even be hypothesized that this is one explanation for the success of Javascript as a common cross-platform programming language, a role originally envisioned to be that of Java.

One of the victories of the W3C is the preservation and extension of the Web as one of the world’s largest and continually evolving programming platform that is not under the control of a single vendor. Given the history of patents stifling innovation and deployment in cryptography, ranging from the RSA to Schnorr to Certicom patents, there has been moves to even add work such as Curve 25519 to the W3C Web Cryptography API solely in order to provide patent protection.⁷

3.1 W3C Process

Another benefit of open standards bodies such as the W3C and IETF is governance. For the W3C, this is defined by the W3C Process Document, an elaborate document that is updated nearly yearly, although most of the process of standardization has remained nearly the same since the W3C was founded [15].

³ <https://www.w3.org/Consortium/membership>.

⁴ Note that a patent holder can still claim patent infringement even if an idea is embodied in a standard (such as an IETF RFC) and in open source code.

⁵ <https://www.w3.org/Consortium/Patent-Policy-20040205/>.

⁶ <http://www.rfc-editor.org/rfc/rfc3979.txt>.

⁷ <https://www.w3.org/2014/08/18-crypto-minutes.html>.

In contrast to the IETF's slogan of "We reject kings, presidents, and voting ... we believe in rough consensus and running code," the W3C is ran as a sort of parliamentary monarchy, with all decisions ultimately resting on the authority of the Director, who has always been Tim Berners-Lee. There is no way to nominate another Director or transition plan if he departs from the role. Although the Director ultimately makes all decisions, his decisions are ratified and voted on by the W3C Advisory Committee, where each W3C member gets a single vote regardless of the type or size of the member. For example, in the Advisory Committee, both Google and the EFF have a single vote. The goal of the W3C is to make decisions by consensus, with the Director being able to override any lack of consensus, although members can launch a "formal objection" that requires the Director and W3C staff to provide an official written comment on why the objection has been overridden in their decision-making.

In order to create a new standard, the W3C runs workshops with open invitations (as the "open invitation" is needed to recruit new dues-paying members) in order to determine if there is enough momentum for standardization. If successful, the W3C staff and Director create a charter for a new W3C Working Group, with the charter going out to the Advisory Committee for approval via voting. If the vote garners a substantial amount of approval, the Working Group is launched and W3C members may join, as long as they commit their patents to the charter of the Working Group (as the standard itself does not yet exist yet). Eventually, a draft of the standard is matured by the Working Group to be a Candidate Recommendation after the text of the standard is considered complete in terms of features by the Working Group and interoperability has been shown for each feature by at least two implementations.

If the membership agrees with continuing the standardization process, the standard becomes a Proposed Recommendation, which is expected to be stable (as textual stability is needed for the royalty-free patent licensing) and presented for an Advisory Committee vote. During this stage, it is expected that each W3C member that votes on the standard is prepared to commit its patents to the Proposed Recommendation. If the vote is successful, the finalized standard is published as an official W3C Recommendation.⁸ In order to update a standard, the Working Group must be rechartered and the another vote must go on, although the Working Group may begin again directly at the Candidate Recommendation phase [15].

3.2 HTML and EME at the W3C

While having democratic features, the power of determining what precisely to standardize in the traditional W3C process lies entirely with the W3C staff and the Director, as there is no ability for members to vote to create a new Working

⁸ Note that patent protections are not given by all W3C member companies, but only those that commit to the final vote. Therefore, this considerably weakens the patent protections, as they are effectively "opt-in."

Group Charter.⁹ After the success of W3C XML, the W3C decided to stop development of HTML in 2000 and replace HTML with XHTML. Although the XHTML 1.0 W3C Recommendation was finished in 2002 with modest deployment, the work started at W3C on a XHTML 2.0 standard had no backing or implementation from browsers. As the W3C HTML standards increasingly diverged from the reality of browser implementations, all browser vendors except Microsoft started the informal WHATWG (Web Hypertext Application Technology Working Group), an informal “standards” body to curate the future of the HTML in 2004.¹⁰ Rather than follow the cumbersome W3C process, HTML was considered to be a “living standard” that reflected consensus amongst browser implementations. Berners-Lee and the W3C focused primarily on standardizing Semantic Web technologies, which are considered irrelevant by the browser vendors to the future of the Web. Yet when Berners-Lee saw the rapid uptake of WHATWG’s version of HTML, the W3C decided to formally “fork” the WHATWG HTML standard into HTML5 by putting the text of the WHATWG HTML specification through W3C Process in 2007 and ending work on XHTML 2.0 in 2009. As there was concern from browser vendors that the W3C was too slow-moving and the rechartering process would limit the ability of HTML to be extended, two new processes were made. The first was a fully automated system for creating W3C Community Groups meant for pre-standardization work.¹¹ The second process, unique to the W3C HTML Working Group, was to allow HTML Extensions to be defined without rechartering in order to speed up the W3C HTML Working Group and counter criticisms from WHATWG that W3C Process made it impossible for the W3C HTML Working Group to evolve HTML in an agile manner.¹²

Although there had been workshops on standardizing DRM at the W3C since 2001,¹³ the W3C had never managed to create a DRM Working Group until 2012. Technically, the reason had been due to the W3C’s desire to build on work such as MPEG-4 IPMP but add a more flexible (and likely in RDF or XML) language for expressing “intellectual property rights.” Legally, standardizing DRM in HTML was mired in the vast number of patents on the DRM systems themselves.¹⁴ With the rising popularity of streaming video in 2012, new W3C member Netflix

⁹ Instead, W3C members may submit “Member Submissions” of potential standard, but the only requirement is that the W3C staff provide textual feedback on the maturity and suitability of the work as a W3C standard, and historically very few eventual W3C Recommendations have been Team submissions.

¹⁰ <https://whatwg.org>.

¹¹ <https://www.w3.org/community/>.

¹² <https://www.w3.org/html/wg/wiki/ExtensionSpecifications>.

¹³ In particular, the highly attended “Workshop on Digital Rights Management for the Web” hosted by W3C Staff Rigo Wenning in January, see <https://www.w3.org/2000/12/drm-ws/>.

¹⁴ Personal communication with Daniel Weitzner in 2016, W3C Staff Counsel in 2000.

proposed “Encrypted Media Extensions” in 2012 as an HTML Extension. This was approved as an extension by the chair of the HTML Working Group, Paul Cotton (Microsoft), and work proceeded on EME in a unofficial “task force” of the W3C HTML Working Group, unnoticed by the outside world.

Yet when EME was brought up to be part of the official W3C HTML Recommendation as an extension, a number of members issued concerns over EME and the Electronic Frontier Foundation joined W3C in order to organize against what they considered the dangerous addition of DRM to Web standards; this first took the place of an argument over the extension of the HTML Working Group’s charter to include the use-case of “content protection.”¹⁵ After objections from the HTML Working Group that the controversial and (at the time) unimplemented EME standard would slow the development of HTML5, EME and MSE (Media Source Extensions¹⁶), were spun off from the HTML Working Group into the separate HTML Media Extensions Working Group in 2013. This new Working Group was joined by all major browser vendors, including Mozilla. The Electronic Frontier Foundation (EFF) and others filed formal objections to the creation of the Working Group after I wrote, as a W3C employee at the time, that it was “now or never to save the open web.” [13]. However, the work continued and EME was soon deployed later in 2013 by Netflix. The standard soon reached the point where it was a Candidate Recommendation in 2016, with all major browser vendors (Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari) demonstrating interoperable support of EME.

As it became clear that EME would move from Candidate Recommendation to Proposed Recommendation, the EFF circulated a petition in January 2016 stating that all work on EME should be halted until a “covenant” could be put in place to defend users and security researchers from prosecution under Chap. 12 of the DMCA [8]. At the Advisory Committee meeting in April 2016 at Cambridge, the W3C decided not to go forward with an official vote on the adoption of the covenant and to progress Encrypted Media Extensions to a Candidate Recommendation regardless. This led to the first-ever street protest against the W3C organized by the Free Software Foundation (FSF). I threatened to quit if W3C continued to approve EME, and at the time I was the staff contact for both the Web Cryptography and Web Authentication Working Groups.¹⁷ A number of objections were filed by W3C members, W3C employees (including both myself and staff legal counsel Wendy Seltzer¹⁸), and ordinary programmers (with no official W3C affiliation) to the continuation of EME. Despite the protest and even staff resignation from the W3C, the W3C approved the transition to a Proposed Recommendation in July 2016. The issue finally started to gain attention

¹⁵ <https://www.eff.org/deeplinks/2013/10/lowering-your-standards>.

¹⁶ MSE is standard needed to select the source of streaming media.

¹⁷ https://motherboard.vice.com/en_us/article/jpgpjx/we-marched-with-richard-stall-man-at-a-drm-protest-last-night-w3-consortium-MIT-joi-ito.

¹⁸ <https://lists.w3.org/Archives/Public/public-html-media/2016Aug/0007.html>.

from outside the W3C, with civil society organizations ranging from UNESCO to the JustNet Coalition (NGOs from the Global South) filing statements asking Berners-Lee not to approve EME. After a nearly tied W3C vote on whether or not to approve W3C EME as a Recommendation (and thus, quite far from consensus), Tim Berners-Lee in his role of W3C Director finally approved EME as a Recommendation in July 2017. Given that more than 5% of W3C members were against W3C, the EFF triggered the never before used option to repeal a Director’s decision.¹⁹ The recall vote was divided, but the majority (108) of W3C members approved of the progress towards Recommendation while a substantial minority (57) objected and (20) abstained.²⁰ Therefore, EME is now an official W3C Recommendation.

4 Encrypted Media Extensions

EME is a Javascript API that provides access to a Content Decryption Module (CDM) in order to restrict the playback of video to only those who possess an authorized cryptographic secret key on their own client device. Without this key, the encrypted media stream cannot be decrypted and so can not be displayed on the video output of the user’s client device. EME does not mandate a single CDM to decrypt encrypted video media. This allows the various patent pools around CDM itself to be avoided while applying the W3C patent royalty-free licensing to the API itself, allowing interoperability between “plug and play” CDMs. In terms of EME support, Microsoft Edge supports the PlayReady DRM system, Google supports the Widevine CDM, and Mozilla has removed Adobe Primetime for Windows and switched to Google’s Widevine CDM.²¹

EME is an extension to the standard `HTMLMediaElement` element. In brief, this element unifies both popular `video` and `audio` elements into a single framework, as well as defining text tracks for subtitles via `track` attribute. EME extends `HTMLMediaElement` (and thus both audio and video) to include a new `MediaEncryptEvent`, so that there can be encrypted blocks waiting for decryption or playback but blocked due to waiting for a key. EME defines the framework for the use of these decryption keys for DRM systems, and consists of the following components, whose relationship is given in Fig. 1.

- **Content Decryption Module:** The component in the platform or browser that provides decryption for a Key System.
- **Key System:** A uniquely identified CDM that is bound to the server that served the request for a key.
- **License:** Licenses are an array of one or more `MediaKeys` IDs that can be used to decrypt the media.

¹⁹ <https://boingboing.net/2017/07/12/save-the-web.html>.

²⁰ <https://lists.w3.org/Archives/Member/chairs/2017JulSep/0154.html>.

²¹ <https://www.ghacks.net/2017/01/10/firefox-52-adobe-primetime-cdm-removal/>.

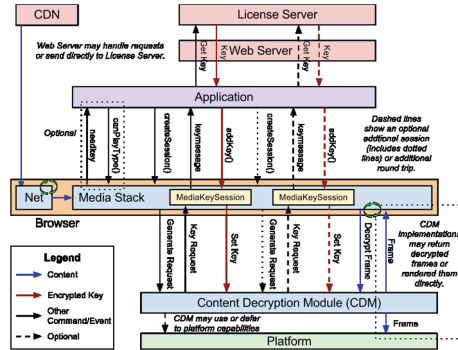


Fig. 1. Encrypted Media Extensions (from W3C Recommendation [9])

- **MediaKeys:** One or more uniquely identified decryption keys needed to decrypt encrypted media data and bound to a session. These can be manually loaded into a CDM via an explicit `update` call.
- **MediaKeySession:** An ID for a series of uses of a **MediaKeys** object to decrypt media. License information and associated **MediaKeys** are cleared from the browser after the end of a session, but may be re-used across sessions.

Simplified code of an example usage of EME using a single key (and license requested from a server and data to discover the key) is given below in Fig. 4. The typical flow of EME is as follows to decrypt media from an **MediaEncryptEvent** is as follows:

1. Call the `requestMediaKeySystemAccess` with a `licenseUrl` variable that designates the URL where the license with the needed **MediaKey** IDs is. The license is retrieved using the `licenseRequestReady` function either from the URL (which the Web Server redirects to a License Server) or from a licenses stored locally on the Web Server.
2. This license request is passed via the browser to the CDM. If the key IDs requested by the license are returned to the browser from the CDM, new **MediaKeys** are created via the `createMediaKeys`, where the keys are bound with a Web Server using a server certificate.
3. After a **MediaKeySession** is created, these **MediaKeys** are sent to the CDM where, if they fulfill the license, they can be used. If needed, the license is updated and provided to the CDM in order to request more keys and thus a new **MediaKeySession**. This step may repeat one or more time in the form of multiple **MediaKeySessions**.
4. Once all **MediaKeySessions** have been created that fulfill the license, the media is decrypted by calling the originating **HTMLMediaElement** with a **MediaKey** as well as any needed initialization data.


```

<script>
var licenseUrl;
var serverCertificate;

function createSupportedKeySystem() {
  someSystemOptions = [
    { initDataTypes: ['keyids','webm'],
      videoCapabilities: [
        { contentType:'video/webm; codecs="vp8"' }
      ]
    }
  ];
return navigator.requestMediaKeySystemAccess('com.example.keysystem',x-options).then(
  function(keySystemAccess) {
    licenseUrl = 'https://example.com/getkey';
    serverCertificate = new Uint8Array([ 0x01111fef010 ]);
    return keySystemAccess.createMediaKeys();
  }
).catch(
  console.error.bind(console, 'Needed DRM system not present or license not supported')
);
promise.then(
  function(createdMediaKeys) {
    return video.setMediaKeys(createdMediaKeys);
  }
).catch(
  console.error.bind(console, 'Unable to set MediaKeys')
);
promise.then(
  function(createdMediaKeys) {
    var initData = new Uint8Array([...]);
    var keySession = createdMediaKeys.createSession();
    keySession.addEventListener('message', handleMessage,
      false);
    return keySession.generateRequest('webm', initData);
  }
).catch(
  console.error.bind(console,
    'Unable to create or initialize key session')
);
});
}

function handleInitData(event) {
  var video = event.target;
  createSupportedKeySystem().then(
    function(createdMediaKeys) {
      video.mediaKeysObject = createdMediaKeys;
      if (serverCertificate)
        createdMediaKeys.setServerCertificate(serverCertificate);
      for (var i = 0; i < video.pendingSessionData.length; i++) {
        var data = video.pendingSessionData[i];
        makeNewRequest(video.mediaKeysObject, data.initDataType, data.initData);
      }
      return video.setMediaKeys(createdMediaKeys);
    }
  ).catch(
    console.error.bind(console, 'Failed to create and initialize a MediaKeys object')
  );
}
}
</script>
<video autoplay onencrypted='handleInitData(event)''></video>
}

```

5 Objections to W3C EME

The arguments for EME is that the Web itself needs to be extensible to include “access to protected content” without the use of a plug-in.²² As many content producers require DMCA-compliance, platform providers such as Netflix believe that enabling DRM in the browser is necessary for streaming video in order to “say goodbye to third-party plugins, making for a safer and more reliable web”²³. The W3C holds the position that EME is necessary for a Web without plug-ins for DRM: “Developers who use HTML5 for video can create play back video directly without external dependency on third party apps (like Adobe Flash or Microsoft Silverlight) and without inheriting security vulnerabilities from those third party apps.”²⁴ The W3C maintains that EME improves security and privacy without impacting accessibility negatively.

The general argument against the standardization of Encrypted Media Extensions at W3C is that DRM contradicts the W3C’s official mission to lead to “Web to its full potential”, in particular to the make benefits of the Web “available to all people, whatever their hardware, software, network infrastructure, native language, culture, geographical location, or physical or mental ability” via open standards.²⁵ Objectors like EFF and FSF believe that DRM by design is meant to prevent users from accessing content that is encrypted via DRM in a manner that by definition discriminates against both security researchers and users, including those lawfully exercising their rights. A more broad objection to adding DRM is that by making DRM a W3C standard, the amount of DRM on the Web will increase, as DRM will now work seamlessly in a cross-platform manner across all major browsers, which previously led DRM systems to be too cumbersome to use by many video content providers. The lack of cross-platform compatibility was one of the major reasons why DRM systems were ultimately not adopted by the music industry [17]. As EME makes it much easier for content providers to add DRM, there is concern that the Web itself may eventually become a “pay-to-play” closed space similar to pre-Web services [13].

Although Encrypted Media Extensions only covers media, the proposed W3C Digital Publishing Working Group includes general purpose DRM for text in HTML in its use-cases for future W3C standardization.²⁶ Although the W3C has stated that “EME is not DRM for HTML” as EME “defines a common API that may be used to discover, select and interact with such systems as well as with simpler content encryption systems,” it is unclear what other purpose EME could possibly serve except to enable DRM-based systems inside of HTML. The concerns therefore are with DRM on the Web. The concerns can be given in terms of (1) user control and fair-use (2) accessibility (3) privacy and (4) security. For each of these arguments, first we will first state the W3C argument for standardizing EME and then summarize the arguments against standardizing EME.

²² <https://www.w3.org/2013/09/html-charter.html>.

²³ <https://www.w3.org/2017/09/pressrelease-eme-recommendation.html.en>.

²⁴ <https://www.w3.org/2016/03/EME-factsheet.html>.

²⁵ <https://www.w3.org/Consortium/mission>.

²⁶ https://www.w3.org/dpub/IG/wiki/DRM_UC#DRM-1.

5.1 User Control and Fair Use

The W3C has stated that users demand protected content, and any attempt to halt the standardization of DRM on the Web is effectively limiting their rights to watch DRM-protected content [3]. In contrast, EFF holds the position that DRM systems seek to take away control from users of what Doctorow calls “general purpose computing” in order to enforce copyright restrictions.²⁷ This is the same concern brought up by free software advocates, namely that DRM restricts user control over their own computer and thus violates user freedom. Even under laws like the DMCA that DRM systems are meant to enforce, a user often has “fair use” rights to copy even copyrighted material, such as for educational purposes, parody, or sharing the same media across multiple devices [19]. However, the “fair use” doctrine cannot be implemented via the strictly technically enforced key-based decryption enabled by DRM systems, as “fair use” depends on knowledge of social context that cannot be accessed by the purely technical capabilities of DRM systems. There are a wide variety of limitations and exceptions to copyright law across various nation-states, and any purely technical system such as EME is unlikely to be able to justice to all of these heterogeneous legal regimes. As W3C is a global standards body, it is surprising that various national legal regimes are ignored. For example, there are even heterogeneous limitations and exceptions between European nations as shown by the fact that re-streaming certain content may be legal in Greece but not in the United Kingdom [2]. Due to this reason, EME has caused a motion in the European Parliament to determine if EME violates limitations and exceptions to European copyright law.²⁸ Some countries like India had for years copyright protection that did not clearly “criminalise the manufacture and distribution of circumvention tools” and still today give courts more leeway than in the DMCA [18].

5.2 Accessibility

DRM has been thought to damage accessibility, but accessibility experts at W3C have claimed that EME is compatible with accessibility goals,²⁹ as EME only encrypts the media content and `HTMLMediaElement` has a separate `track` for textual descriptions (such as subtitles) that is not encrypted by EME. Therefore, EME does not present any obstacles for the playing of subtitles, although it also offers no improvement per se over HTML5 without EME. However, this feature shows a potential weakness in EME as a DRM system, as EME may not fully satisfy the needs for copyright control if the copyright claims include the text given by subtitle tracks. More importantly, EME cannot support access to audio and video media for accessibility reasons, because the media itself can still only be decrypted only by EME. This prevents accessibility tools that can automatically create accessible subtitles from the media content directly using

²⁷ <https://www.youtube.com/watch?v=gbYXBJOFgeI>.

²⁸ <https://juliareda.eu/2017/04/open-letter-to-the-european-commission-on-encrypted-media-extensions/>.

²⁹ <https://www.w3.org/2017/03/eme-accessibility.html>.

automatic speech detection and other machine-learning techniques that require access to video and audio before it is played. These tools for the automatic creation of accessible media are likely to become more widespread in the future.³⁰

5.3 Privacy

Tim Berners-Lee wrote that “the EME system can sandbox the DRM code to limit the damage it can do to the users privacy” [3]. As given in Sect. 4, EME functions in virtue of the request and retrieval of uniquely identified keys (**MediaKeys**). In this way, EME could violate privacy for a single origin. The EME specification states that “key IDs may contain any value” and thus “these data items could be abused to store user-identifying information” [9]. Furthermore, EME key systems “may access or create persistent or semi-persistent identifier(s) for a device or user of a device” and thus as “identifiers are present in Key System messages, then devices and/or users may be tracked” [9]. Although care is taken to note that CDM instances should abide by the same origin policy by associating only one **MediaKey** for a CDM per origin and usage identifiers “must ensure that... session data is not shared between **MediaKeys** objects or CDM instances,” these goals are nowhere enforced in EME, as the naming control and duration of **MediaKey** objects are entirely left to the control of the content provider. EME even admits that **MediaKey** objects are likely to be used for tracking, as “within a single origin, a site can continue to track the user during a session, and can then pass all this information to a third party” [9].³¹

Despite these vague recommendations not to use personally identifiable information to attach a user to key material, these gestures towards privacy are not technically enforced in the specification. For example, EME states that “user agents must take responsibility for providing users with adequate control over their own privacy” although the W3C rejected a formal objection that would disable the CDM without user consent.³² Although the EME specification clearly outlines the privacy dangers of the technique of associating a user with a uniquely identified key, given the functioning of DRM requires uniquely identified keys to be associated with a uniquely identified CDM in order to see if a user has fulfilled the licensing conditions, there is no testing to see if the various guidelines given by EME to enforce user privacy will be respected in EME implementations.³³ Even if they were respected, these privacy properties are not tested for conformance in the W3C test suite, possibly due to fears of violating the anti-circumvention provisions of the DMCA, which may apply not just to the CDM but to handling of key material by EME. In this way, the statements in the specification about EME respecting user privacy appear to be red herrings that are contradicted by the real-world functioning of DRM.

³⁰ <https://www.technologyreview.com/s/603899/machine-learning-opens-up-new-ways-to-help-disabled-people/>.

³¹ Although if they are used, they “must be encrypted, together with a timestamp or nonce, such that the Key System messages are always different” [9].

³² <https://github.com/w3c/encrypted-media/issues/386>.

³³ <https://w3c.github.io/test-results/encrypted-media/all.html>.

5.4 Security

The EFF and other opponents clam that the DMCA makes it illegal to discuss the security of the underlying CDM. While the DMCA’s 1201 clause does state that “no person shall circumvent a technological measure that effectively controls access to a work protected under this title” and EME enables such a technological measure across web browsers, there are explicit exemptions for security research in the DMCA [7]. However, these exemptions are difficult to enforce in practice, because while it is legal under the DMCA to reveal “information derived used solely to promote the security of the owner or operator of the tested computer system” as long as that “information obtained is shared directly with the developer of the system,” this information becomes illegal as soon as “information obtained distributed in a way that might enable copyright infringement or other legal violations” [7]. This final restriction essentially forces the vulnerability to only be disclosed to the DRM system manufacturer, even if the DRM system manufacturer does not fix the flaw. This law was used against security researchers first in the threats to Snosoft by Hewlett-Packard in 2002,³⁴ and over fifty court-cases have been launched against security research as of 2016.³⁵ Unfortunately, legal precedent also shows academic publications on vulnerabilities in DRM systems violate the DMCA and so result in the censorship of the academic work, as shown by the Felten case over Sony DRM [12]. Although no known DRM case has involved EME and browser-based DRM, it is reasonable to hypothesize that security audits by researchers on browser-based DRM systems will suffer a “chilling effect” due to the DMCA and that there will be increased DRM circumvention cases if DRM on the Web grows.

The W3C recognizes the possible security threats of CDMs in the EME specification as well, noting that “user agent implementers must ensure CDM implementations can and will be quickly and proactively updated in the event of security vulnerabilities” [9]. However, the W3C also claims that, unlike browser plugins that have privileges for every origin in an entire browser, EME is restricted per origin and that the CDMs may be sandboxed, providing “security and privacy superior to native platform alternatives.”³⁶ In particular, the W3C continues to note that sandboxing may at least limit the damage as “DRMs under EME can be sandboxed” to enforce the requirement of the EME specification that “the CDM must not make direct out-of band network requests” [9].

Unfortunately, there is more sand than box in ‘sandboxing’ on the Web. Although a browser may be sandboxed from the rest of the computer in the same way any other computer program, origins are not defended adequately from each other inside the browser. Javascript is constrained per origin, but security flaws are not constrained per origin in browser memory. In modern web browsers, there are a limited number of content processes (Firefox recently went up to 4 or 5, while mobile browsers often have one). Normally, each origin does not have its

³⁴ <https://www.cnet.com/news/security-warning-draws-dmca-threat/>.

³⁵ https://www.eff.org/files/2016/03/17/1201_reported_case_list_revised.xls.

³⁶ <https://lists.w3.org/Archives/Public/public-html-media/2017Jul/0000.html>.

own content process, as that would cause a performance slowdown and so each content process shares memory. Therefore, if there is a flaw in the underlying CDM that has access to the browser via EME, its access will not be limited to the origin, but to the entire shared memory space of the content process. As security flaws are simply more likely in a CDM that can't be inspected to see if it has flaws or follows EME security's guidelines and by default this CDM will be sharing a content process, thus the CDM is not sandboxed in any actual sense of the word if there is a security vulnerability.

Another concern is the scope of the DMCA and whether or not it can be implemented in open source. EME provides a technique to keep the key material unencrypted in the browser, called "clear key" that can be implemented without a CDM in order to keep compliance possible for open-source browsers and browsers without CDMs, as the keys are generated locally and stored in cleartext in the browser take the place of the license server. However, one danger is that the "clear key" technique is subject to DMCA, and thus the EME specification inflicts an inherently insecure yet DMCA-compliant system on all browsers due to the "clear key" option.

In order to protect security researchers, the EFF created a "covenant" modelled on the W3C Royalty-Free Licensing Policy that would allow W3C members to make a legally binding commitment not to prosecute security researchers investigating EME-related DRM systems. In a petition, over 100 security researchers as well as many W3C staff members [8]. The EFF covenant stated that: "Each participant irrevocably covenants that it will not bring or join suit against any person under 17 U.S.C 1203, or under any other law of any jurisdiction that regulates the circumvention of technological measures that effectively control access to a work protected by copyright, where the act complained of relates to (a) the circumvention of any implementation of the specification; (b) the publication of any non-compliant implementation of the specification; or (c) the publication or disclosure of any vulnerability in the specification or in any implementation of the specification" [10]. The issue of security also caused interventions from civil society, with UNESCO pointed out that the same infrastructure used by DRM to control content could also be used for censorship and surveillance.³⁷ However, the W3C stated that "despite much work those efforts were not successful and consensus among the W3C Membership was not achieved" on the covenant. Yet the EFF covenant was never formally put forward to an actual vote by W3C, so the EFF called for a revocation of the W3C Director's decision to make EME a W3C Recommendation through a repeal process that requires 5% of the Advisory Committee to uphold. As of July 2017, the process of appeal is underway. However, as it has historically never happened at W3C, it is unclear if the result will be the removal of EME as a Recommendation and its patent status.

³⁷ <http://en.unesco.org/news/be-careful-about-proposed-technical-change-web-says-unesco-s-rue>.

6 Quantitative Analysis

Two claims have been made by opponents of EME standardization at W3C that touch upon actual involvement in “open standards.” The Free Software Foundation has claimed that the W3C is controlled by content providers and browser vendors without suitable representation from wider civil society and security researchers: “It looks like a select few organizations are pushing and influencing their power unduly.”³⁸ The JustNet Coalition (JNC) has called EME a form of “digital colonialism,” as JNC claimed that EME excludes those in the Global South who are struggling for access to information at the expense of a few North American and European corporations.³⁹

In terms of participation, the total number of members in the group is 273, with 70 invited experts. Using the origin country of the member to determine a rough estimate of the geographical breakdown of the Working Group (and thus excluding Invited Experts), there was a majority participation from the United States (66%) and less from Asia (33%). Asian representation did not include anyone from India. There were a few representatives from South America (1%), one member from Australia, and none from Africa. In terms of the types of participation (excluding Invited Experts), the majority of the Working Group consisted of browsers and DRM manufacturers (53%) with smaller representation from civil society (4%) and accessibility experts (4%), and these being roughly balanced by pro-DRM trade associations (4%), as given in Fig. 2. The amount of email sent on the list is 3,427, with clear spikes of activity that correspond to debates where civil society tried to stop progress on EME advancing in the formal W3C process, as given by Fig. 3. There was indeed little participation from the Global South outside large companies like Baidu from China, Samsung from Korea, and

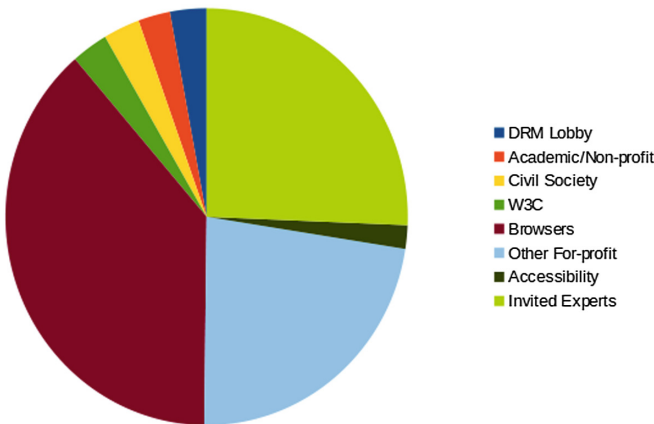


Fig. 2. Categories of members of the EME Working Group

³⁸ <https://www.youtube.com/watch?v=SPfdOOiuOHL>.

³⁹ https://justnetcoalition.org/2017/W3C_EME_objection.pdf.

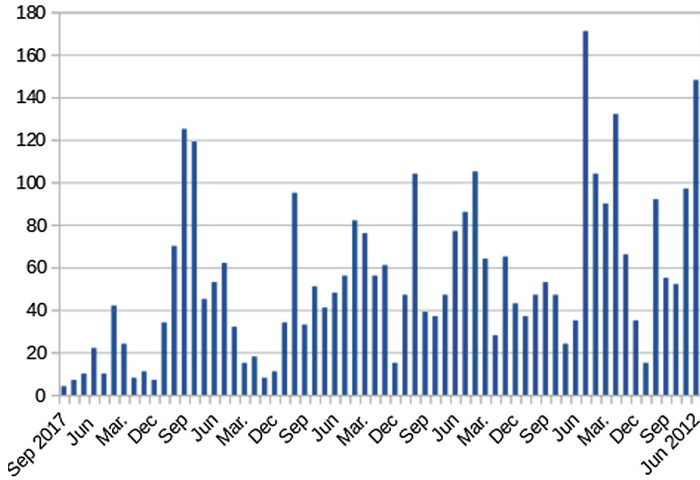


Fig. 3. Email frequency to EME mailing list

Sony from Japan. There was domination by browsers and for-profit corporations in the Working Group, but there was significant if much smaller representation from civil society and accessibility experts, with civil society (in particular EFF) being active in bursts. This analysis of the HTML Media Extensions Group is in line with similar analysis done of participation in the HTML Working Group that also noticed a lack of participation from the Global South [11].⁴⁰

7 Is Harm Reduction for DRM Possible?

Is there a solution towards standardizing DRM that can avoid the problems of the EME specification that the W3C has encountered? As explored in Sect. 5, standards bodies should recognize that there are legitimate concerns with privacy and security with DRM systems for end-users. Both legal and technical approaches can be applied to reduce the harm of EME, but to the generic problem of the need for DRM standards. While it is too late to pursue these approaches for EME at W3C, applying these approaches should be best practices for future standards.

Technically, DRM has the potential to be privacy-invasive and possible security issues, but this is true of all software. However, modern DRM implementations in the consumer market essentially work by violating Kerckhoffs' principle, namely that the security of cryptosystem should rely only on the protection of key material, so that the cryptosystem must be secure even if everything else

⁴⁰ Note these numbers are preliminary, and a more detailed and careful analysis is under preparation that also takes into account the origins and roles of Invited Experts and git repo of EME is underway.

about the system is public. To ignore Kerckhoffs’ principle produces broken systems, as cryptographic history has shown [16]. It is in the best interest in terms of security for standards bodies, content providers, and users to base standards on security reductions to well-studied cryptographic primitives and securing cryptographic key material. There exist many alternatives to classical DRM, such as traitor tracing, have been well developed in the research literature and do not require security by obscurity [6]. Lastly, there has been a corresponding growth of “trusted computing” environments in consumer deployment, such as the ARM Trustzone, and increasing research into making these trusted computing platforms capable of remote attestation [1]. This research into attestable “trusted computing” is not ready for market: The ill-fated Microsoft Next-Generation Secure Computing Base that was canceled after having been found to have security vulnerabilities [5]. Still, research into more secure and auditable computing systems for access control is ongoing [14].

Access control, of which DRM systems attempt to enforce by obscurity on the client device should be based *only* on having any key material on the client under user control. This key material can be stored in a trusted and attestable way, including the usage of hardware tokens or “trusted computing” with secure enclaves. In terms of usability, users can correctly handle private user-centric key material and this key material can respect the same origin policy, as shown by a new generation of standards like the W3C Web Authentication API.⁴¹ Future standards may avoid the controversy of DRM systems as long as (1) the key is under user control and (2) the security of the DRM system is reducible to the security of the key and the publicly known cryptographic primitives.

As current DRM systems are not deployed following Kerckhoffs’ principle and thus there are possible security bugs that cannot be detected by an audit of the CDM, DRM systems should simply be installed only when officially requested by a user, and should be not installed by default. A user can be empowered to take the risk of installing and activating a CDM, but a DRM system should be disabled by default. At least with plug-ins, a user had the chance to refuse to install the plug-in, so standards should not remove that user choice. A modification enforcing “opt-in” of DRM could be easily added to W3C EME by forcing a dialogue with the user warning them that they are installing or activating a CDM, similar to the user interaction needed to install Adobe Flash-based DRM systems pre-EME as well as the use of a user-prompt to access the potentially privacy-invasive microphone and video as needed by WebRTC.⁴² Although the W3C Working Group claimed that a one-time user-centric privacy prompt would defeat usability (as “being able to visit a site and watch video without annoying and confusing consent prompts is a user experience benefit”), but no evidence of prompts causing retention issues was provided.⁴³ A “one time” prompt at first use of EME-encrypted video seems unlikely to reduce usage, and is less restrictive than WebRTC’s usage of `getUserMedia`). This standpoint risks being

⁴¹ <https://www.w3.org/TR/webauthn/>.

⁴² <https://www.w3.org/TR/webrtc/>.

⁴³ <https://lists.w3.org/Archives/Public/public-html-media/2017Apr/0013.html>.

hypocritical, as the W3C has argued that controversial privacy-invasive features to web browsers should require user interaction, and this would logically include EME. At least with a DRM plug-in, a user could refuse to install the plug-in if they had security concerns.

On the legal framework, there is a long-term gain for security to be made by supporting reform of the DMCA. The primary reason for the controversy around EME is not due to the technical details of the specification itself, but the legal framework that prevents reasonable security audits. The EFF has claimed to W3C that DMCA ends up handing too much power to the companies in terms of their control of the disclosure of vulnerabilities.⁴⁴ On a larger note, the EFF has also started a court-case arguing that the DMCA should be overturned as it violates the free-speech of researchers, stifles innovation, and damages cybersecurity.⁴⁵ The Copyright Office of the United States has recently issued a statement agreeing that the provisions of the DMCA restrictions requiring the need for security researchers to require authorization from vendors, stating that “the exemption for encryption research under section 1201(g) may benefit from similar revision, including removal of the requirement to seek authorization and clarification or removal of the multifactor test.”⁴⁶

Times have changed since the DMCA has been passed: Today, security should be more important than copyright enforcement. As it the best of interest of any security standard to have open review, security standards bodies should provide legally binding guarantees that there can be open and legal audits of the standard (as well as of the implementations of a standard) that do not require permission in order to check conformance to specified normative security and privacy properties. More concretely, although the W3C created a “W3C Security Disclosures Best Practices” document, it failed to have any support (much less adoption), as most companies already have security disclosure policies.⁴⁷ While it is possible the DMCA will be revised to allow open security audits, the EFF covenant was likely unacceptable to many vendors as it would override their existing commitments to enforce the DMCA without clear benefits, such as that provided by W3C Patent Policy. However, if each member changed their existing security disclosure policy to agree to not prosecute with both security researchers engaged in audits of implementations and users who are not violating copyright law, as well as co-operate with security disclosures, then concrete harm reduction could be done around the possible security vulnerabilities introduced by DRM systems.

In terms of the W3C EME standard, this would require not signing a single covenant, but to engage with each member of the Working Group to ensure that their security disclosure document included suitable language that prioritized

⁴⁴ <https://www.eff.org/deeplinks/2017/02/indefensible-w3c-says-companies-should-get-decide-when-and-how-security>.

⁴⁵ <https://www.eff.org/press/releases/eff-lawsuit-takes-dmca-section-1201-research-and-technology-restrictions-violate>.

⁴⁶ <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf>.

⁴⁷ <https://w3c.github.io/security-disclosure/>.

the security of the Web in terms of CDM implementations for EME, where the decision over whether a particular security policy complied was left to a neutral third party, such as the independent policy council of the W3C. As there are only three major EME systems supported by the four major browser vendors (Microsoft, Google, and Apple, as Mozilla has dropped support for Adobe's CDM in favor of simply using Google's Widevine CDM) and one non-browser system (Netflix), there are only four major security disclosure policies to be taken into account.

8 Conclusion

In conclusion, the W3C EME standard has garnered unheard of controversy, but the security standardization community should learn from their example in order to determine how to successfully deal with the standardization of DRM systems that present possible security and privacy threats. We have shown that the controversy is founded due to the privacy concerns inherent in uniquely identifying keys and CDMs, and that there are also real dangers posed in terms of security and the prevention of open security audits by the DMCA. Otherwise, no actual technical guarantees can be given about the security and privacy properties of a system. Quantitative analysis shows that the critiques of the large amount of influence by vendors and content providers from Europe and North America is indeed correct. We have suggested two ways forward that have not been considered by the W3C but that are easily considered by future standards. Security standards should indeed be open to inspection and depend only on the security of the key material, which should remain under the control of the user. If there is any reason to believe a system may introduce privacy and security issues, explicit user consent should be required. Lastly, companies should expand their security disclosure policies to include co-operation and explicit non-prosecution of security researchers. By taking these steps, security standards can regain the trust of the general public, and have that trust validated by scientific research.

References

1. Bai, G., Hao, J., Wu, J., Liu, Y., Liang, Z., Martin, A.: TRUSTFOUND: towards a formal foundation for model checking trusted computing platforms. In: Jones, C., Pihlajasaari, P., Sun, J. (eds.) FM 2014. LNCS, vol. 8442, pp. 110–126. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-06410-9_8
2. Batchelor, B., Jenkins, T.: FA premier league: the broader implications for copyright licensing. *Eur. Compet. Law Rev.* **33**(4), 157–164 (2012)
3. Berners-Lee, T.: On EME in HTML5 (2016). <https://www.w3.org/blog/2017/02/on-eme-in-html5>
4. Berners-Lee, T., Fischetti, M.: *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor*. Harpers Information, New York (2000)
5. Brumley, D., Boneh, D.: Remote timing attacks are practical. *Comput. Netw.* **48**(5), 701–716 (2005)

6. Chor, B., Fiat, A., Naor, M.: Tracing traitors. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 257–270. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48658-5_25
7. US Congress: Digital millennium copyright act. Pub. Law **105**(304), 112 (1998)
8. Doctorow, C.: Security researchers: tell the W3C to protect researchers who investigate browsers (2016). <https://www.eff.org/deeplinks/2016/03/security-researchers-tell-w3c-protect-researchers-who-investigate-browsers>
9. Dorwin, D., Smith, J., Bateman, A., Watson, M.: Encrypted Media Extensions (2017). <https://www.w3.org/TR/encrypted-media/>
10. EFF: Objection to the rechartering of the W3C EME group: Covenant (2016). <https://www.eff.org/pages/objection-rechartering-w3c-eme-group>
11. Gupta, H.: (Lack of) representation of non-western world in process of creation of web standards (2016). <https://arxiv.org/pdf/1609.01996.pdf>
12. Halderman, J.A., Felten, E.W.: Lessons from the Sony CD DRM episode. In: USENIX Security Symposium, pp. 77–92 (2006)
13. Halpin, H.: DRM and HTML5: it's now or never for the Open Web. Guardian (2013). <https://www.theguardian.com/technology/2013/jun/06/html5-drm-w3c-open-web>
14. LaMacchia, B.A.: Key challenges in DRM: an industry perspective. In: Feigenbaum, J. (ed.) DRM 2002. LNCS, vol. 2696, pp. 51–60. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-44993-5_4
15. McCathie-Neville, C.: W3C process document (2016). <https://www.eff.org/deeplinks/2016/03/security-researchers-tell-w3c-protect-researchers-who-investigate-browsers>
16. Mercuri, R.T., Neumann, P.G.: Security by obscurity. Commun. ACM **46**(11), 160 (2003)
17. Petrick, P.: Why DRM should be cause for concern: an economic and legal analysis of the effect of digital technology on the music industry. Berkman Center for Internet and Society at Harvard Law School Research Publication (2004)
18. Prakash, P.: Technological protection measures in the Copyright (Amendment) Bill 2010 (2016). <http://cis-india.org/a2k/blogs/tpm-copyright-amendment>
19. Rosenblatt, B.: DRM, law and technology: an American perspective. Online Inf. Rev. **31**(1), 73–84 (2007)

Security, Privacy, and Applied Cryptography Engineering
7th International Conference, SPACE 2017, Goa, India,
December 13-17, 2017, Proceedings
Ali, S.S.; Danger, J.-L.; Eisenbarth, Th. (Eds.)
2017, XXIV, 295 p. 55 illus., Softcover
ISBN: 978-3-319-71500-1