Encrypted Media Extensions
HTML5 con DRM

Gabriel Carballude

Universidad Católica "Nuestra Señora de la Asunción"
Asunción, Paraguay

Resumen En este documento se analiza la especificación EME (*Encrypted Media Extensions*) hecha por la W3C (*World Wide Web Consortium*) que fue añadida al estándar de la web en Septiembre 18 del 2017. Se comienza explicando el concepto y uso de la especificación, luego se explica la parte técnica de esta y por último se presentan las distintas posturas de las organizaciones sobre la especificacion con sus motivos respectivos. El siguiente texto no busca presentar su propia postura sino explicar el contexto, la tecnología y mostrar las posturas existentes para informar al lector.

1. Introducción

En el año 2013 la W3C (*World Wide Web Consortium*) empezó a trabajar en la especificación EME (*Encrypted Media Extensions*) la cual se agrego como un estandar en Septiembre del 2017.

La especificación EME especifica una API (*Application Programming Interface*) para habilitar a aplicaciones web poder interactuar con sistemas de protección de contenido sin utilizar Plugins, la idea de EME viene de que poco a poco se estan incluyendo al estandar funcionalidades que hoy solo se pueden agregar mediante Plugins, y así como antes de HTML5 se requerían Plugins para ver videos (HTML5 introdujo el Tag de "video" y los componentes usados para reproducir dichos videos) antes de esta especificacion no se podían ver videos en tiempo real (Streaming) sin utilizar Plugins.

El problema de usar Plugins el cual esta especificación y varias otran eliminan es que se debe ejecutar en un contexto distinto y por ende sale de las revisiones de seguridad de los browsers que deja que cada Plugin implemente su propio sistema de DRM (*Digital Rights Management*), que serian los metodos utilizados para proteger los archivos pasados.

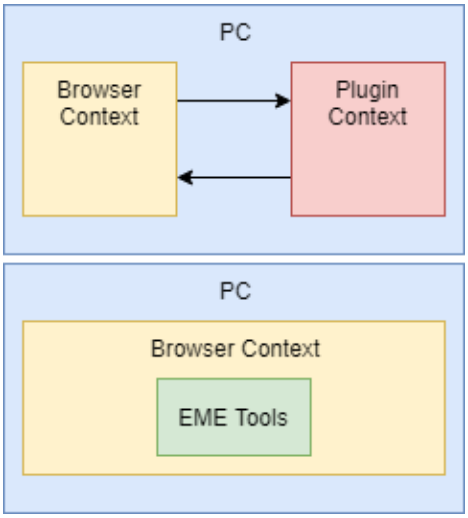

Figura 1. Diferencia entre el contexto al usar un Plugin y al usar las herramientas de la especificación EME

2. Bases de EME

2.1. World Wide Web Consortium

La organización W3C es una comunidad internacional donde las organizaciones que son miembros, un grupo de empleados de tiempo completo y el público trabajan juntos para desarrollar estándares de la web, liderado por uno de los inventores de la web Tim Berners-Lee y su CEO (*Chief Executive Officer*) Jeffrey Jaffe con la misión de llevar a la Web a desarrollar su potencial completo.[1]

2.2. Digital Rights Management

DRM (*Digital Rights Management*) se refiere a una colección de sistemas que son usados para proteger el derecho de autor de medios electrónicos como música digital, películas así como otros tipos de datos que se transfieren digitalmente. DRM es entonces el modo en que las compañías se aseguran que sus archivos fueron obtenidos legalmente y disminuyen la distribución ilegal de sus productos, agregando una capa de protección DRM que puede ser uno de muchos métodos para asegurar que el contenido está siendo visto por el que lo compro.[2]

DRM es un tópico con mucha controversia, se suele decir que a pesar de que uno compra el archivo, uno no es dueño de este, porque al final queda en manos del creador decidir cómo y cuándo el que compro puede utilizar los archivos lo que lleva a que mucha gente que se entera de cómo funcionan las tecnologías DRM a que se sientan que se están violando sus libertades civiles.[3]

Un ejemplo que abrió los ojos a la gente sobre cómo no son realmente dueños de lo que compran fue cuando Amazon en el 2009 accedió remotamente a los

Kindles (Lector de libros electrónico) de sus usuarios y elimino libros de su librería sin el permiso de sus dueños porque la persona que inserto el libro para ser vendido no tenía derechos de venderlo, y si bien anunciaron tras el evento que su sistema se cambiaría para no tener que eliminar los libros de sus usuarios el hecho que este evento fuera completamente legal y posible gracias a las herramientas de DRM creo grandes controversias sobre privacidad y propiedad en cuanto a los archivos digitales.[4]

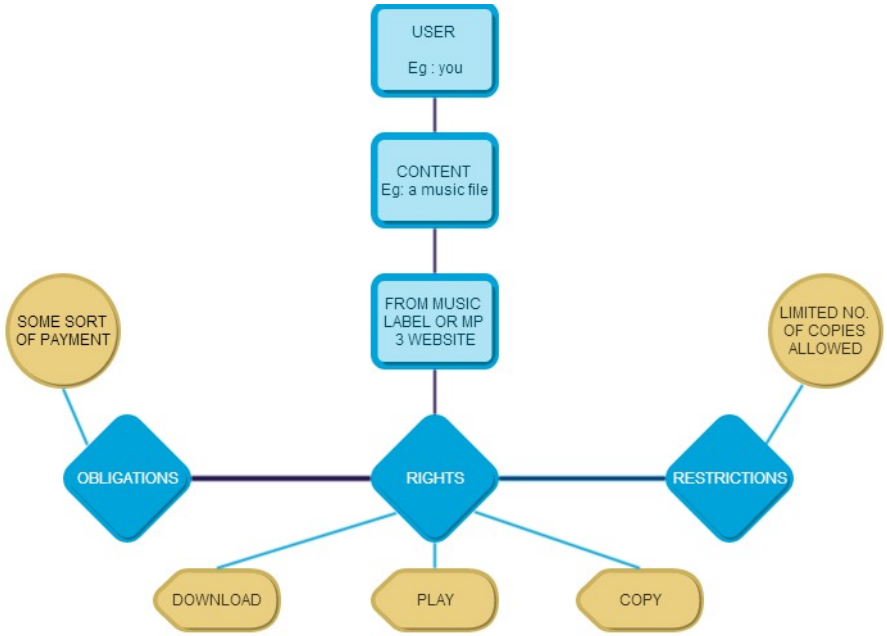

Figura 2. Ejemplo de sistema DRM aplicado a una canción

2.3. Application Programming Interface

Una API (*Application Programming Interface*) es un tipo de arquitectura de programa que busca mantener oculta la forma en la cual funciona el programa y solo provee los comandos, funciones, etc. simples a sus usuarios, efectivamente transformando al programa en una caja negra que tiene funcionalidades que ofrece al mundo, entonces el usuario solo debe conocer que funcionalidades se le ofrece y que datos debe proveer a la funcionalidad en caso de que necesite algo, similar a la interacción entre dos objetos y sus métodos públicos en la programación orientada a objetos. Es una arquitectura muy útil para la reutilización de código y simplificación a la hora de conectar un programa con otro.[5]

Figura 3. Visualización de una API

2.4. Surgimiento

Ver películas en la web se volvió un sector grande de la vida moderna, y es por esto que muchas compañías que ofrecen ver películas en tiempo real nacieron alrededor del mundo. Se estima que en el 2017 la cantidad de personas en Estados Unidos usando servicios pagados y gratis de vista de videos tiempo real sobrepaso a los DVD, a las descargas e inclusive al cable por primera vez y que para el 2021 trafico de video será del 82 por ciento de todo el tráfico de Internet, comparado con el 73 por ciento en el 2016. El uso de servicios de videos tiempo real está creciendo exponencialmente por todo el mundo y cientos de millones de usuarios ya usan EME en servicios como Netflix u otros similares, donde este último mencionado ya anuncio más de 100 millones de usuarios en Abril del 2017.[6]

Dada la gran cantidad de usuarios que querian ver cosas online y el hecho que casi todas las compañías online requieren que el video sea encriptado para ser servido legalmente en la web, miembros de la W3C pidieron a la organización que se investigue cual seria la forma mas segura de ver videos online[6] y de esta petición se incluyo en la especificación EME el sistema de DRM, que busco como se podrían aplicar las tecnologías de seguridad en el navegador (Sin uso de alguna aplicación externa) y producirla de forma:

- Accesible
- Segura
- Privada

3. Funcionamiento

EME es una extensión a la especificación *HTMLMediaElement*, al ser una extensión esta no es requerida para estar conforme a HTML, pero bien es requerida para reproducir contenido encriptado en el navegador.

La extensión aumenta la API de *HTMLMediaElement* proveyendo la capacidad de reproducir el contenido protegido, la API habilita varios casos de uso para

esto pero no define un sistema de DRM ni CDM (*Content Decryption Module*) sino funciona como un explorador, selector e interactuante para estos sistemas.

EME utiliza los siguientes componentes externos:

- Key System: Un mecanismo de DRM.
- Content Decryption Module: El software o hardware del lado del cliente para reproducir el contenido protegido.
- Interactúa con el CDM para proveer las llaves para desencriptar, negociar con el servidor de licencias queda a cargo de la aplicación.
- Encripta y cifra los datos para distribuir/consumir

La siguiente imagen muestra un caso de uso de la API seguido de un paso a paso de que se hace desde que llega el dato encriptado hasta que se reproduce:

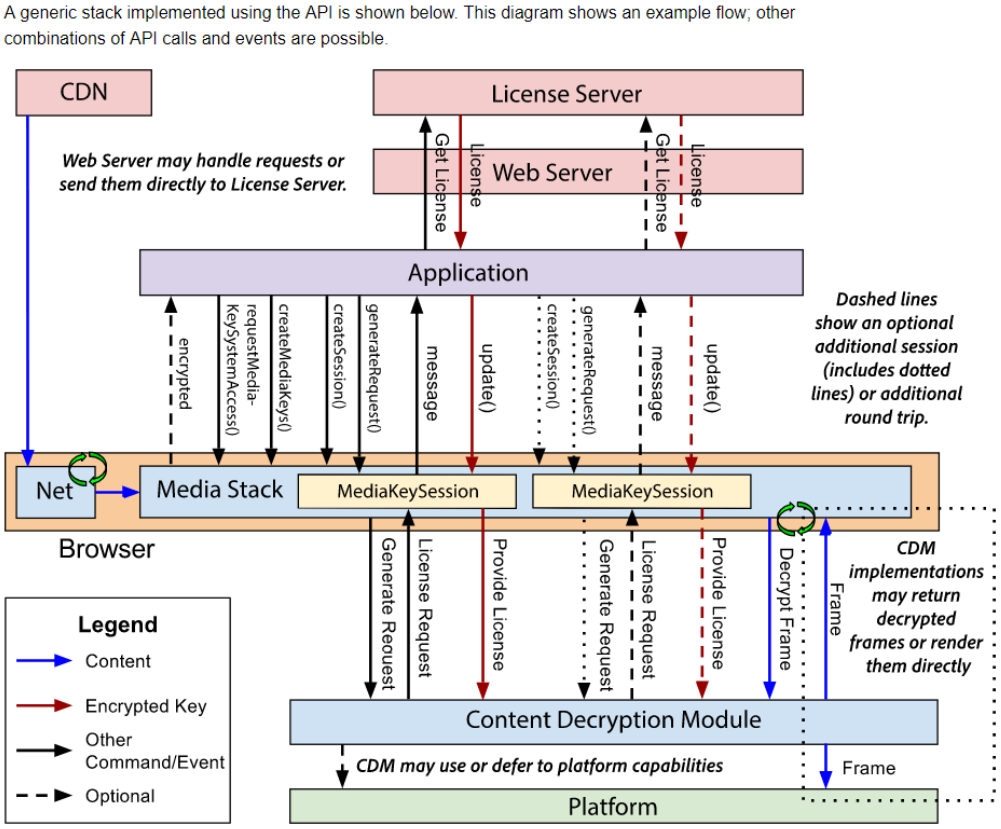

Figura 4. Caso de uso de EME
[7]

1. La aplicación trata de reproducir audio o video que tiene uno o más canales encriptados.
2. El navegador reconoce que el *media element* esta encriptado y dispara un evento *encrypted* con metadata obtenido de los datos.
3. La aplicación maneja el evento *encrypted* de modo que si no tiene un objeto *MediaKeys* asociado al *media element* primero selecciona un Key System y luego crea un objeto *MediaKeys* que termina asociando al *HTMLMediaElement* para que la llave se pueda usar para decodificar los datos.
4. La aplicación crea una *MediaKeySession* llamando el método *createSession()* del objeto *MediaKeys* asociado, este nuevo objeto representa la vida de la licencia y sus llaves.
5. La aplicación genera un pedido de licencia pasando la *media data* obtenida en el *encrypted handler* al CDM usando el método *generateRequest()* del objeto *MediaKeySession* asociado.
6. El CDM dispara un evento *message* que es un pedido para adquirir una llave de un servidor de licencias.
7. El objeto *MediaKeySession* recibe el evento *message* y la aplicación manda el mensaje al servidor de licencias.
8. La aplicación recibe la respuesta del servidor de licencias y pasa los datos al CDM usando el método *update()* del objeto *MediaKeySessions*.
9. El CDM decodifica los datos usando las llaves en la licencia.
10. Se reproduce.

4. Utilidad

La utilidad viene dada para las grandes compañías como Netflix[8] u otras que trabajan en el negocio de streaming de alta calidad. Debido a reglas impuestas por los dueños de las series y películas se requiere que la transmisión de los datos sea necesariamente encriptado y pasados por un sistema DRM, esto causa que se tenga que utilizar algún sistema DRM mediante algún plugin como los que ofrece Flash o Microsoft Silverlight, lo cual no solo molesta al cliente por tener que instalar estos componentes sino que hacen a la interoperabilidad más costosa y complicada, este problema se resuelve con la extensión dado que agrega la interoperabilidad al utilizar la API y remueve el uso de plugins, removiendo toda molestia al usuario en cuanto a la aplicación de los sistemas DRM.

5. Críticas

5.1. Practica Anticompetitiva

Una de las críticas a la especificación EME es que es una práctica anticompetitiva, lo cual se define como una rama de prácticas de negocio las cuales una compañía o grupo de compañías pueden aplicar de modo a restringir la competencia entre sus competidores para mantener o aumentar su posición relativa en el mercado sin tener que necesariamente proveer productos o servicios a menor

precio o de mejor calidad[9], en este caso, dado que las leyes en cuanto a saltarse el sistema DRM estarán siendo aplicadas sobre los browsers mismos y no sobre los plugins se tiene miedo de que los browser se vuelvan herramientas de uso para prácticas anticompetitivas, esto se debe a que en los Estados Unidos las prácticas anticompetitivas que se lograban en situaciones similares fueron catastróficas, y no solo lo que se pensó que podría aparecer como mala práctica termino ocurriendo sino que aparecieron prácticas que nadie se imaginó, causando serios daños al sector, lo cual es algo que se piensa que causara grandes daños a la web.[10]

5.2. W3C se "vendió"

Se critica a la W3C por haberse "vendido" al pasar esta especificación porque se considera que esta traiciona los principios de la web mundial, dado que no añade realmente nada y solo ayuda a limitar el potencial de la web y que por ende toda esta cuestión es tan solo un intento de atraer a más compañías para que se vuelvan miembros y aporten dinero dado que esta especificación les ayuda mucho a estas.[11]

5.3. Perjudica a la Investigación

El uso de la especificación EME deja expuesto a los usuarios a las leyes de sistemas DRM que en varias partes incluyen leyes que hace ilegal el intento de romper el sistema, lo cual es terrible para los buenos usuarios que requieren romper estos sistemas como pre-requisito como los investigadores de seguridad que ya ni quieren meterse en temas que involucren esquemas DRM por miedo a ser demandados, entonces a medida que más tecnología implemente sistemas DRM más insegura se vuelve la tecnología debido a que menos investigadores estarán mirando estas.[11][12]

5.4. La W3C no manejo a las objeciones de forma correcta

Muchos de las críticas mencionadas fueron temas que se presentaron ante el grupo que estaba a cargo del desarrollo de la especificación e inclusive se presentaron soluciones a algunos de estos problemas pero todas fueron descartadas por motivos que no siempre fueron correctos, a veces usando argumentos que son "ciertos pero injustos" como "Uno no está obligado a usar HTML5", lo cual es cierto pero para dar una comparación es como que una compañía que tiene el monopolio completo de un producto diga "No están obligados a comprar de mi". O insistían que traerían buenos beneficios como en cuanto a accesibilidad y privacidad pero estos beneficios dependen de que el público pueda ejercer ciertos derechos que se les removía a entrar en el campo legal de los DRM.[12]

6. Conclusion

La especificación EME de la W3C fue pasada con mucho descontento y cuyo aporte fue minimo mientras que el daño causado a la web mundial fue alto, dado esto habrá que ver cómo responde la W3C en cuanto a la cantidad de investigadores que hoy ya no quieren investigar temas relacionados a algún sistema DRM y la repercusión que tendrá esto en la seguridad de la web, posiblemente terminen incluyendo algún tipo de seguridad para los investigadores que los proteja de las leyes que están perjudicando su investigación o bien este podría ser solo el comienzo de las "malas decisiones" de la W3C.

Referencias

1. https://www.w3.org/Consortium/: About w3c (2017)
2. https://techterms.com/definition/drm: Drm (2017)
3. https://www.lifewire.com/why-is-drm-so-controversial-2483185: Why is drm so controversial with music and movie artists? (2017)
4. http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?mcubz=0: Amazon erases orwell books from kindle (2009)
5. https://techterms.com/definition/api: Api (2016)
6. https://www.w3.org/2017/07/EME-backgrounder.html: Backgrounder on encrypted media extensions (eme) at the world wide web consortium (w3c) (2017)
7. https://www.w3.org/TR/encrypted-media/: Encrypted media extensions (2017)
8. https://medium.com/netflix-techblog/update-on-html5-video-for-netflix-fbb57e7d7ca0: Update on html5 video for netflix (2017)
9. https://stats.oecd.org/glossary/detail.asp?ID=3145: Anticompetitive practices (2003)
10. https://boingboing.net/2017/04/28/two-tims.html: An open letter on drm to the inventor of the web, from the inventor of net neutrality (2017)
11. https://blog.whatwg.org/drm-and-web-security: Drm and web security (2017)
12. https://www.eff.org/deeplinks/2017/09/open-letter-w3c-director-ceo-team-and-membership: An open letter to the w3c director, ceo, team and membership (2017)