

[Sobre extensões de mídia criptografadas em HTML5*](#)

Timothy Berners-Lee, cientista da computação e professor do MIT, criador da World Wide Web, tendo feito uma primeira proposta para sua criação em 25 de março de 1989



Data da publicação:

Outubro 2017

Uma questão que tem sido debatida na rede é se o W3C deve endossar o padrão Extensões de Mídia Criptografada EME (Encrypted Media Extensions), que permite que uma página da Web inclua conteúdo criptografado, conectando um sistema existente de Gerenciamento de Direitos Digitais (DRM – Digital Rights Management) na plataforma subjacente. Algumas pessoas protestaram que "não", mas na verdade decidi que a resposta lógica real é "sim". Como muitas pessoas têm sido tão fervorosas em suas manifestações, sinto que devo a elas explicar a lógica. Minha esperança, como há muitas coisas que precisam ser contestadas, investigadas e monitoradas neste mundo, é de que a energia gasta em protestar contra o EME possa ser recanalizada para outras coisas que realmente precisam disso. Nas discussões ao longo do caminho também houve muitas coisas com as quais eu concordei. E, para entender o desacordo, precisamos focar na questão real: se o W3C deve recomendar o EME.

A razão para recomendar o EME é que, ao fazê-lo, levamos a indústria que primeiramente a desenvolveu a criar uma maneira simples e fácil de usar conteúdo criptografado online, de modo que haja interoperabilidade entre navegadores. Isso é uma facilidade para desenvolvedores Web e também para usuários. As pessoas gostam de assistir ao Netflix (para escolher um exemplo). As pessoas passam muito tempo na Web, gostam de poder integrar o conteúdo do Netflix em suas próprias páginas da web, gostam de poder visitá-lo. As pessoas gostam de ter discussões onde expressam o que pensam sobre o conteúdo, onde seus comentários e o conteúdo podem ser todos vinculados.

O conteúdo na Web pode ser ofertado sem DRM? Sim, uma grande quantidade de conteúdo de vídeo está na Web sem DRM. No entanto, as grandes e custosas produções de mídia colocadas na Web sem criptografia torna muito fácil copiá-las e, na realidade, o mundo utópico das pessoas que pagam voluntariamente pelo conteúdo não funciona. (Outros argumentam que todo o sistema de direitos autorais deve ser desmantelado, e eles podem fazer isso nas legislações e fazer campanha para mudar os tratados, o que será uma longa luta. Mas, enquanto isso,

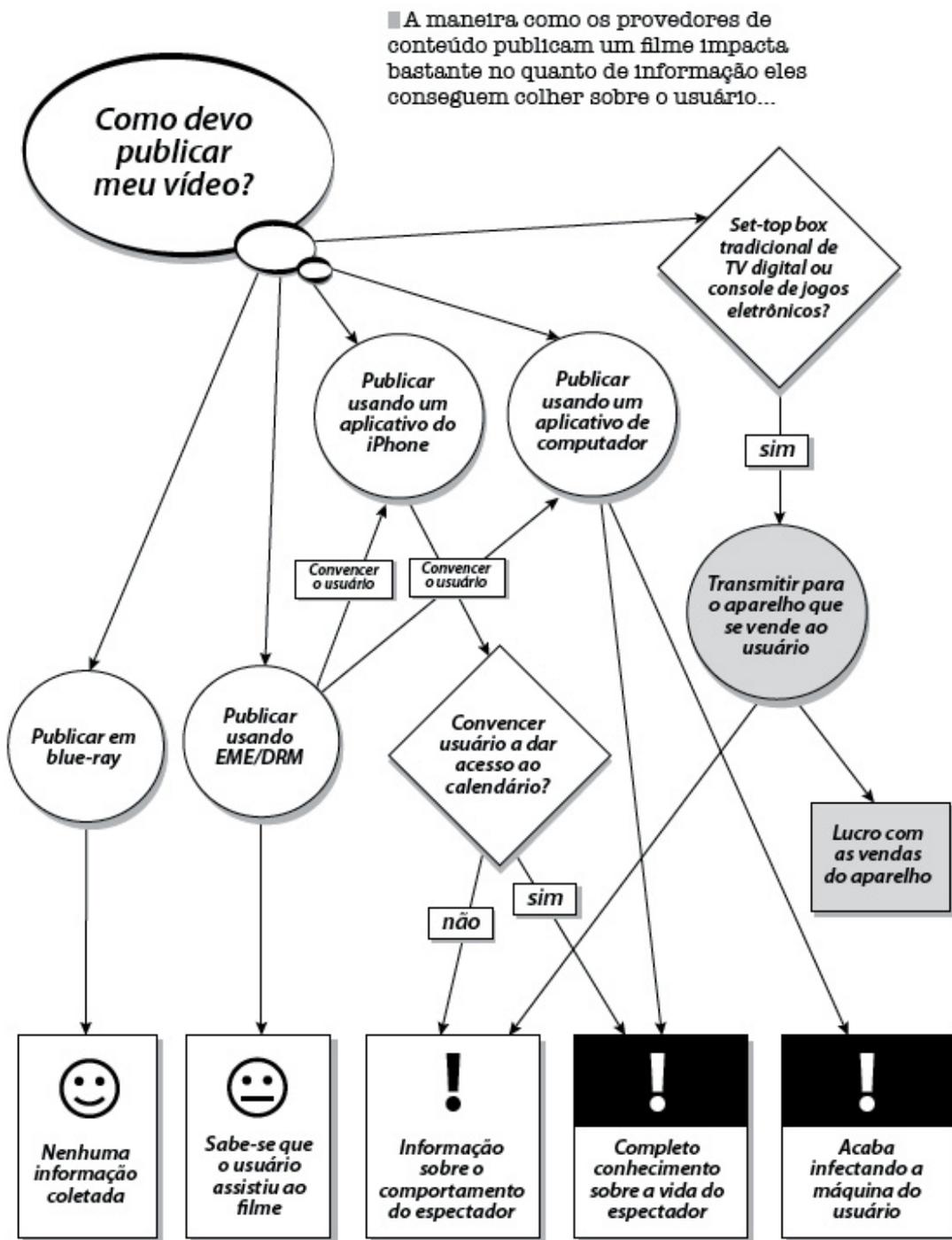
temos os direitos autorais).

Já que o DRM existe...

Quando uma empresa decide distribuir conteúdo que deseja proteger, ela tem muitas opções. Isto é importante lembrar.

Se o W3C não recomendar o EME, os navegadores simplesmente o terão de qualquer modo. Se o EME não existisse, os vendedores poderiam simplesmente criar novas versões baseadas em Javascript. E, sem usar a Web, é muito fácil convidar os espectadores a mudar para visualizar o conteúdo em um aplicativo proprietário. E se as plataformas fechadas proibissem o DRM em aplicativos, os grandes fornecedores de conteúdo simplesmente distribuiriam seus próprios set-top boxes e consoles de jogos como a única maneira de assistir suas produções.

Se o diretor do Consórcio decretasse que não haverá mais DRM, de fato, nada mudaria, já que o W3C não tem poder para proibir nada. O W3C não é o Congresso dos EUA, nem a OMPI, nem um tribunal.



O W3C poderia assumir uma posição e só porque o DRM é uma coisa ruim para os usuários poderia simplesmente recusar-se a trabalhar nele e retardar os trabalhos neste campo? Isso não teria qualquer efeito, porque, ao contrário de um tribunal ou uma agência de execução, o W3C é um lugar para as pessoas conversarem e forjarem o consenso sobre as novas tecnologias para a Web. Sim, há um argumento que, em qualquer caso, o W3C deve apenas opor-se ao DRM, mas nós, como Canuto¹, entendemos que nosso poder é limitado. Mas mais importante que isso, existem razões pelas quais afastar as pessoas da Web é uma má idéia: é melhor para os usuários que o DRM seja feito através do EME do que via outras formas.

1) Quando o conteúdo está em uma página Web, ele faz parte da Web.

2) O sistema EME pode manter o código DRM em um ambiente de testes² protegido para limitar o dano que poderia causar ao sistema.

O sistema EME pode isolar o código DRM em uma sandbox³ para limitar o dano que poderia causar ao sistema do usuário; pode restringir o código DRM a aplicativos específicos para limitar o dano que poderia causar à privacidade dos usuários. Como mencionado acima, quando um fornecedor distribui um filme, ele tem muitas opções, com diferentes vantagens e desvantagens. Uma questão importante aqui é o quanto o editor pode aprender sobre o usuário:

- Se eles vendem um disco de DVD ou Blu-ray, eles nunca saberão se o usuário verá o vídeo. Do ponto de vista do usuário, o vídeo pode ser visto quantas vezes ele quiser, sem a sensação de que está sendo observado.

- Se eles colocarem a mídia na Web usando EME, eles poderão registrar quando o usuário desbloqueia o filme. No entanto, o navegador, no sistema EME, pode limitar o nível de acesso do código DRM e pode impedir que este busque mais detalhes na máquina do usuário. (A página da Web também pode monitorar e informar sobre o usuário, mas isso pode ser detectado e monitorado, pois esse código não faz parte da "bolha DRM").

- Se a mídia for incorporada a um sistema fechado como um iPhone, então eles conseguem ativar o DRM que preferirem. Eles também conseguem registrar exatamente como e onde o usuário observa quais partes do filme. Se eles podem persuadir o usuário a permitir-lhes outro acesso, como ao calendário do usuário, eles podem construir um perfil completo do usuário e correlacionar isso com seus hábitos de exibição de filmes.

- Se eles distribuírem a mídia usando um aplicativo em um sistema aberto, como Android ou Mac OS X, então eles podem obter o mesmo feedback que em um aplicativo para iPhone. No entanto, como o sistema operacional não é um sistema bloqueado, o aplicativo pode abusar ainda mais do usuário, possivelmente extraindo mais informações e também, como no caso do Sony Rootkit⁴, instalando spyware no sistema.

- Se eles distribuírem a mídia em seu próprio sistema fechado, como um console de jogos ou um set-top box, então o computador do usuário estará protegido. O distribuidor terá o controle completo das informações que são enviadas de volta sobre a reprodução e a pausa do usuário, e assim por diante. Isso de nenhum modo interfere na presença Web do usuário.

Portanto, em resumo, é importante apoiar o EME como um ambiente online relativamente seguro para assistir a uma mídia, bem como o mais conveniente, e que o torna parte do discurso interconectado da humanidade.

É preciso mencionar que a proteção do usuário ao limitar o código DRM a uma sandbox não está definida pela especificação EME, embora as implementações atuais, pelo menos no Firefox e no Chrome, incluam o sandbox do DRM.

O alcance a outros meios

Devemos preocupar-nos com o fato de que, colocando filmes na Web, os provedores de conteúdo desejarão também usar o DRM para outras mídias, como música e livros? Para a música, não penso assim, porque vimos a indústria mover-se conscientemente de um modelo baseado em DRM para um modelo não criptografado, onde muitas vezes o endereço de e-mail do comprador pode ser colocado em uma marca d'água, mas não há DRM.

Para livros, sim, isso pode ser um problema, porque tem havido uma grande quantidade de dispositivos fechados for a da Web, aos quais as pessoas estão acostumadas, e para as quais os distribuidores comumente usam o DRM. Em muitos casos os dispositivos físicos foram substituídos por aplicativos que incluem DRM, em dispositivos de propósito geral como telefones fechados ou computadores abertos. Esperamos que a indústria, ao mudar para um modelo Web, também desista do DRM, mas isso não está claro.

Problemas com DRM

Falamos sobre as vantagens das diferentes formas de usar o DRM na distribuição de filmes. Agora vamos discutir alguns dos problemas com os sistemas DRM em geral.

Muito deste texto inclui a perspectiva técnica do W3C sobre o EME, que eu reproduzo usando meu chapéu de diretor – mas no que segue sobre DRM e DMCA, que é uma questão de política, expresse minhas opiniões pessoais.

Problemas para os usuários

Há muitos problemas com DRM, do ponto de vista do usuário. Estes foram documentados em outros lugares. Aqui, deixe-me listar estes:

- não é possível fazer uso “justo” do material, como a abertura de exceções para comentários, propósitos educacionais, e assim por diante;
- isso impede o remix (a recombinação) em trabalhos derivados;
- o usuário não pode fazer uma cópia de backup;
- ter uma bolha de DRM no computador é uma ameaça de segurança, que poderia atacar os sistemas da máquina.

Os sistemas DRM geralmente são frustrantes para os usuários. Parte disso pode ser agravado por coisas como códigos regionais em uma licença para que o usuário só possa utilizar quando estiver em um determinado país, confusão entre "comprar" e "alugar" algo por um período fixo e problemas que surgem quando fornecedores de conteúdo deixam de existir e todas as licenças "compradas" ficam inacessíveis. Apesar desses problemas, os usuários continuam a comprar conteúdo protegido por DRM.

Problemas para os desenvolvedores

O DRM impede que desenvolvedores independentes criem diferentes sistemas de reprodução que interagem com o fluxo de vídeo, por exemplo, para adicionar recursos de acessibilidade, como acelerar ou diminuir a velocidade da reprodução.

Problemas para a posteridade

Há uma possibilidade de que acabemos em décadas com nenhuma mídia utilizável desses filmes, porque estão criptografados ou porque as pessoas não se preocuparam em tirar cópias na época, porque as cópias teriam sido inúteis para eles. Uma das minhas sugestões favoritas é que qualquer um que detenha direitos autorais de um filme e o distribua criptografado de qualquer forma deve depositar uma cópia não criptografada em um conjunto de bibliotecas de direitos autorais que incluem a Biblioteca Britânica, a Biblioteca do Congresso e o Arquivo da Internet⁵.

Problemas com legislação

Muito da rejeição contra o EME é derivada da resistência ao DRM, que por sua vez está baseada em problemas específicos importantes com certas leis. A lei mais discutida é a Lei de Direitos Autorais do Milênio Digital dos EUA (DMCA)⁶. Outras leis existem em outros países que, em maior ou menor grau, assemelham-se ao DMCA. Algumas delas têm sido consideradas nos debates, mas não temos uma lista ou análise exaustiva das mesmas. Vale a pena notar que os EUA gastaram muita energia usando os vários acordos bilaterais e multilaterais para persuadir outros países a adotarem leis como a DMCA. Não vou considerar a legislação em outros países. No entanto, sinalizo que isso não pode ser desconsiderado como se fosse um problema só dos EUA. Dito isto, vejamos mais detalhes do DMCA.

Seja o que for que você gostaria de mudar no sistema de direitos autorais como um todo, existem partes específicas do DMCA, especificamente a seção 1201, que coloca pesquisadores de segurança inocentes em risco de uma punição severa se forem acusados de terem feito revelações sobre qualquer sistema DRM.

Em um momento do processo no W3C, houve uma tentativa de impedir a divulgação das especificações EME até que todos os participantes do grupo de trabalho concordassem em isentar os pesquisadores de segurança nesta seção. Para encurtar uma história muito longa, a tentativa falhou e os historiadores podem apontar para a falta de vantagem no uso das especificações EME daquela forma, e para a diferença entre o conjunto de empresas do grupo de trabalho e o conjunto de empresas que poderiam abrir processos com base no DMCA, entre outros motivos.

Investigadores de segurança

Atualmente⁷, há um esforço relacionado no W3C para encorajar as empresas a criar programas de “caça aos bugs” que pelo menos garantam imunidade de perseguição a pesquisadores de segurança que encontram e relatam erros em seus sistemas. Embora o W3C possa encorajar isso, ele só pode fornecer diretrizes e não pode

alterar a lei. Eu encorajo aqueles que pensam que isso é importante para ajudar a encontrar um conjunto comum de diretrizes de melhores práticas que as empresas poderão adotar. Um primeiro rascunho de algumas diretrizes foi anunciado⁸. Por favor, ajude-os a torná-los efetivos e aceitáveis e a sua empresa a adotá-los. Por exemplo, algo mais lógico seria mudar a lei, mas a comunidade técnica parece ter se resignado a não incidir positivamente no sistema legislativo dos EUA devido a problemas bem documentados com esse sistema. Isso é algo em que a pressão pública sobre as empresas para que concordem em adotar essas diretrizes pode ajudar, para não mencionar a mudança na causa raiz do DMCA. O W3C gostaria de saber sobre exemplos de pesquisadores de segurança que tenham esse tipo de problema, para que todos possamos acompanhar.

A futura Web

A Web tem que ser universal, para funcionar de alguma forma. Tem que ser capaz de conter ideias alucinadas do momento, mas também as ideias bem estruturadas do século. Ela deve ser capaz de lidar com qualquer idioma e cultura. Deve poder incluir informações de todos os tipos e mídia de muitos formatos. Nessa universalidade deve incluir a capacidade de lidar com material gratuito e pago, pois todos fazem parte deste mundo. Isso significa que é bom para a Web poder incluir filmes e, por isso, é melhor para o HTML5 ter EME do que não ter.

* Publicado originalmente em 28-2-2017 em <https://www.w3.org/blog/2017/02/on-eme-in-html5>

1. A fábula do rei Canuto, que explicou a sua corte que não tinha o poder de deter as ondas do mar, pode ser lida aqui:

<https://contadoresdestorias.wordpress.com/2007/09/10/o-rei-canuto-a-beir...> [n.ed.] 2. Nota do editor: no original, o termo utilizado foi sandbox que, no ramo de desenvolvimento de softwares, designa um ambiente online no qual se pode testar a mudança em códigos, programas e conteúdos sem que isso afete o sistema original.

3. Nota do editor: No ramo de desenvolvimento de softwares, *sandbox* é um ambiente online no qual se pode testar a mudança em códigos, programas e conteúdos sem que isso afete o sistema original.

4. Refere-se ao escândalo do sistema de proteção de CDs da Sony em 2005, que tornava a máquina do usuário vulnerável a ataques. Ver https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal [n.ed.]

5. Refere-se ao Internet Archive. Ver <https://archive.org> [n.ed.]

6. Ver, por exemplo, https://pt.wikipedia.org/wiki/Digital_Millennium_Copyright_Act [n.ed.]

7. Este texto foi escrito em fevereiro de 2017 [n.ed.].

Categoria:

- [poliTICS 26](#)