A autoridade certificadora Let's Encrypt: uma oportunidade para criptografar toda a Web

*Por **Seth Schoen**, tecnólogo senior da Electronic Frontier Foundation (EFF)*

Data da publicação:

Agosto de 2015

Em uma Internet cada vez menos segura e confiável, vemos ainda muito pouco uso de tecnologias de segurança como o protocolo HTTPS para acesso seguro a sites Web. Há várias dificuldades na adoção mais ampla de HTTPS e outras técnicas, inclusive obstáculos devido ao sistema de certificação digital. Uma iniciativa da Electronic Frontier Foundation, Mozilla, Universidade de Michigan e parceiros pretende criar uma nova autoridade certificadora, chamada Let's Encrypt, para melhorar esta situação tornando mais acessível o uso de tecnologias essenciaisde segurança.

Os cientistas da computação têm tradicionalmente alertado para não depositarmos confiança na infraestrutura de rede fora de nosso controle físico. Tem-se a impressão que os dados simplesmente aparecem em nosso navegador depois que digitamos o endereço de um site Web, ou que nossos chats ou e-mails simplesmente aparecem em dispositivos de nosso amigo. Na realidade – como o jornalista Andrew Blum destaca em Tubes: A Journey to the Center of the Internet – eles são levados através do espaço físico por hardware físico que existe em algum lugar e que é possuido e gerido por alguém[1]. Na maioria das vezes não podemos ver como os nossos dados foram transportados ou o percurso dos mesmos até chegar aos nossos amigos; não podemos ver ou controlar o que aqueles que operam o hardware ao longo do caminho estão fazendo[2].

Os operadores de infraestrutura e outros que controlam partes do caminho dos nossos dados estão em condições de causar muitos danos que sequer podemos perceber. Eles podem ver nossa comunicação, podem gravá-la em bases de dados enormes, podem associá-la conosco de modo que o que fizemos ou dissemos na Internet passe a ser pesquisável. Eles podem roubar nossas senhas e passar-se por nós. Eles também podem alterar o que comunicamos, escondendo coisas de nós, impedindo-nos de dialogar sobre certas ideias, removendo ou reescrevendo enlaces ou parágrafos em nossos textos, infectando os nossos downloads de software com malware, ou colocando seus próprios anúncios no corpo das páginas Web
que visitamos.

Temos soluções técnicas baseadas em criptografia para responder à ideia que a infraestrutura de rede não pode ser confiável e devemos proteger-nos dela, mas essas soluções estão em um estado fragmentário. Eles são frequentemente frágeis e estão longe de estar implantadas universalmente. Mesmo a maioria das principais redes sociais, provedores de webmail e serviços de bate-papo até há pouco tempo não forneciam qualquer tipo de criptografia. Isso significa que era trivial para um operador de rede, um "grampeador" da Internet, ou até mesmo alguém em sua rede wi-fi gravar e procurar tudo o que você comunicou nesses espaços – e, em muitos casos, assumir o controle de suas contas. Ainda hoje, muitos serviços populares e a maioria das redes de publicidade não utilizam criptografia, permitindo que as comunicações de seus usuários sejam alvos fáceis para espionagem[3].

HTTPS

A tecnologia de criptografia mais usada e mais universalmente disponível capaz de abordar algumas dessas ameaças é HTTPS, a versão segura do protocolo HTTP. HTTPS está disponível em todos os navegadores Web, mas funciona apenas com os sites configurados para isso. Embora o HTTPS tenha sido desenvolvido há duas décadas, os sites habilitados para HTTPS ainda são u ma minoria da Web hoje, e são ainda mais raros nos países em desenvolvimento e em sites Web pessoais e não comerciais.

A maravilha da tecnologia de criptografia de chave pública, concebida na década de 1970, é que os usuários não precisam ter qualquer relação prévia para configurar uma conexão segura, mesmo se alguém estiver capturando tudo o que está sendo comunicado[4]. A tecnologia de chave pública é usada em TLS, a camada criptográfica por trás do HTTPS[5]. No entanto, um risco de captura por um interceptador ainda permanece – o assim chamado "man-in-the-middle at tack"[6] –, a menos que os dois lados da comunicação possam confirmar que estão usando as mesmas chaves de criptografia. Nós às vezes referimo-nos a isso como a garantia "que você está efetivamente visitando o site que você pensa que está" ou "que ninguém está personificando o site", mas a natureza dessa ameaça é específica da criptografia; não se trata necessariamente de "personificar" um site no sentido de criar u ma versão do mesmo falsificada do zero, mas sim intermediar criptograficamente uma conexão supostamente segura. Isso significa enganar simultaneamente ambos os lados para estabelecer conexões criptografadas com o interceptador, enquanto ambos os lados da comunicação acreditam erroneamente que estabeleceram conexões criptografadas entre si[7]. Esta ameaça é importante porque pode permitir que um invasor comprometa completamente a segurança do TLS, mas não tem equivalente exato no mundo offline.

A prevenção desses ataques "man-in-themiddle", garantindo que o software dos usuários saiba qual chave de criptografia realmente pertence a determinado site é o objetivo principal das autoridades certificadoras da Internet, as organizações em que os navegadores Web e outros softwares confiam para garantir tais asserções. Para estabelecer uma conexão segura com um serviço, um aplicativo de software do lado do usuário normalmente recebe cópias de certificados digitais emitidos por autoridades certificadoras confiáveis, e verifica que os certificados concordam que a chave de criptografia que o site está aparentemente usando de fato pertence ao site[8].

AUTORIDADES CERTIFICADORAS

As autoridades certificadoras aceitas pelos principais navegadores Web são centenas, e estão localizados em dezenas de países. Por convenção, a maioria das autoridades está habilitada a emitir certificados para qualquer nome de domínio da Internet[9], e os navegadores confiam plenamente nas assertivas dessas autoridades (por exemplo, as autoridades não têm de estar na mesma jurisdição que os locais para os quais elas emitem certificados). Isso significa que o sistema de autoridade certificadora só é tão forte quanto o seu elo mais fraco[10]: se uma autoridade certificadora é atacada ou induzida a emitir certificados falsos, seus certificados serão aceitos pelos navegadores, mesmo quando não houver relação prévia entre essa autoridade e o site para o qual ela emite certificados. (Em um incidente notório em 2011, a autoridade certificadora holandesa DigiNotar foi penetrada, aparentemente por um hacker iraniano ativista pró-governo[11]; em consequência emitiu certificados fraudulentos para o Gmail e outros serviços, que os navegadores dos usuários iranianos automaticamente aceitaram, mesmo que não houvesse relação entre esses sites e a DigiNotar.)

Embora existam algumas autoridadescertificadoras de governos ou empresas que operam principalmente para o uso interno dessas organizações, a maioria das autoridades certificadoras existentes cobram um preço para emitir certificados, que tem-se revelado um negócio rentável. (Por exemplo, a fortuna do filantropo Mark Shuttleworth, que foi responsável pela criação do sistema operacional Ubuntu, é um resultado do sucesso de sua empresa certificadora, a Thawte.) As autoridades certificadoras têm custos fixos elevados, especialmente com sua infraestrutura física, serviços jurídicos e de auditoria, testes de segurança e pessoal. Criar uma nova autoridade certificadora do zero é considerado um empreendimento que pode custar centenas de milhares de dólares.

A obtenção de um certificado também tem sido uma tarefa cara e complicada. O cliente precisa pagar uma autoridade certificadora e lidar com uma série de tarefas especializadas para solicitar um certificado e provar sua posse de um nome de domínio. Em nossa experiência, mesmo um administrador de sistemas experiente vai consumir mais de uma hora nessa tarefa se não for uma parte de suas responsabilidades regulares. Pessoas tecnicamente menos sofisticadas muitas vezes não conseguem completar o processo.

Muitos sites e serviços também têm sido levados a crer que não precisam de um certificado porque não lidam com pagamentos ou números de cartões de crédito, ou porque eles terceirizam pagamentos para algum outro serviço online. Sites Web que aceitam pagamentos com cartão de crédito diretamente devem exigir conexões HTTPS para este fim, com um certificado que seu navegador aceite como confiável, como resultado das regras estabelecidas no Padrão de Segurança de Dados da Indústria de Cartões de Pagamento (Payment Card Industry Data Security Standard, PCI DSS). Mas outros sites frequentemente não são oficialmente obrigados a usar HTTPS; como resultado, eles podem desativar o protocolo, ou mesmo sugerir que seus usuários ignorem os avisos de segurança do navegador. A forte associação entre HTTPS e transações financeiras tem sido difícil de

quebrar, já que muitos administradores não levam em conta que seus sites não financeiros também devem proteger a confidencialidade de seus usuários.

Ativistas da privacidade, especialistas em segurança da Web e até mesmo o governo dos Estados Unidos propuseram uma utilização mais universal do HTTPS por uma gama mais ampla de sites Web[12]. A versão 2010 da ferramenta de ataque fácil de usar Firesheep (que permite que usuários de uma rede wi-fi violem contas de outros usuários online com um único clique, se as vítimas estiverem usando uma conexão HTTP insegura) ajudou a sublinhar os riscos para os serviços que permitem login em uma conta. Operadores de redes sociais e de webmail em geral reagiram ao Firesheep, tornando disponível ou obrigatório o HTTPS para seus sites. Mas sites de notícias e de referência, fóruns nãocomerciais, redes de publicidade, e até mesmo fontes de download de software têm sido mais resistentes a adotá-lo, mesmo que seus usuários também estejam em risco de censura, rastreamento e ataques de malware.

LET'S ENCRYPT

Um grupo de especialistas em privacidade e segurança na Internet da Universidade de Michigan, Mozilla e a Electronic Frontier Foundation uniram-se para criar uma nova autoridade certificadora chamada Let's Encrypt (Vamos Criptografar). A Let's Encrypt planeja estar disponível ao público em meados de setembro; a base tecnológica está sendo desenvolvida em público, incluindo o software cliente-servidor e o protocolo de rede a ser usado para comunicação mútua[13].

A ideia central da Let's Encrypt é que o nível básico de validação de identidade pela autoridade certificadora pode ser realizado automaticamente. (Esta verificação básica, chamada Validação de Domínio, confirma que a entidade que solicita um certificado na realidade tem controle sobre o nome de domínio que é objeto do referido certificado – por exemplo, verificando a capacidade da entidade de fazer alterações em serviços hospedados sob esse nome de domínio.) Já que a validação e consequente emissão de certificado pode ser realizada sem intervenção humana, não há quase nenhum custo marginal associado à emissão de um certificado para um novo domínio. Isto significa que este serviço pode ser prestado em grande escala em um modelo sem fins de lucro, sem custo para o usuário final que recebe o certificado.

A ênfase em automação também significa que os administradores de sistemas dos usuários não terão que executar a tarefa manual demorada e inconveniente de obter, instalar e renovar certificados. O software cliente da Let's Encrypt cuidará da tarefa de gerar chaves criptográficas, automaticamente autenticando o detentor do nome de domínio especificado, obtendo o certificado e até mesmo instalando o mesmo no software de servidor Web Apache ou Nginx (Contribuições de código para integrar o software cliente com outros softwares de servidor Web serão bem-vindas).

Desta forma eliminamos os obstáculos de custo, tempo e esforço que são barreiras para que sites e serviços mudem para HTTPS. Nosso objetivo é permitir que um administrador de sistemas leve menos de um minuto para obter e instalar um certificado confiável, sem nenhum custo, executando um único comando em um servidor. Os navegadores mais comuns aceitarão estes certificados automaticamente como resultado de um acordo alcançado entre IdenTrust (uma autoridade certificadora já existente) e a entidade operadora da Let's Encrypt. Usuários de navegadores Web não têm que mudar ou atualizar nada para que os certificados Let's Encrypt sejam aceitos; eles simplesmente navegam na Web como de costume e estarão automaticamente protegidos.

Para obter um certificado, o usuário da Let's Encrypt executa nosso software cliente livre (ou qualquer software de terceiros compatível com nosso protocolo ACME) em um servidor Web, selecionando os nomes de domínio para os quais será obtido o certificado, em geral a partir de uma lista gerada automaticamente. O software cliente conecta-se a nossa autoridade certificadora usando o protocolo ACME e solicita um certificado; a autoridade desafia o cliente a provar que detém os nomes de domínio, o que é feito automaticamente, fazendo alterações solicitadas no servidor Web. Quando a autoridade aprova, já emite o certificado, e o software cliente o instala automaticamente. (Na maioria dos casos, o software cliente irá renovar automaticamente o certificado quando este expirar e instalará automaticamente a versão atualizada. Isso vai reduzir a incidência dos erros irritantes no navegador Web que aparecem quando certificados expiram e não são imediatamente renovados.) Todo esse processo pode ser concluído em um minuto ou menos.

Eventualmente esperamos ter parcerias com empresas de hospedagem Web populares e CDNs ("content-delivery networks"[14]) para gerar e instalar automaticamente os certificados disponíveis para todos os seus clientes, e esperamos também que o software cliente Let's Encrypt seja incluído em todos os principais sistemas

operacionais de servidor Web. (Os nossos serviços continuarão a ser de uso livre para os clientes em qualquer escala, sejam pessoas físicas ou grandes corporações. Estamos financiados por doações de nossos parceiros e de indivíduos que entendem que o nosso serviço constituiu ma parte importante para tornar a Internet mais segura.)

TRANSPARÊNCIA

Preocupações consideráveis têm sido levantadas que autoridades certificadoras possam ser atacadas por hackers (como aconteceu com DigiNotar, Comodo, e outros) ou sejam forçadas pelos governos a emitir certificados fraudulentos para facilitar a interceptação (como foi sugerido por Soghoian e Stamm[15]; o caso Lavabit também aumentou as preocupações que os governos usariam seu poder para obter chaves criptográficas sensíveis, embora a ordem judicial, nesse caso, tenha sido direcionada a um serviço específico, não a uma autoridade certificadora)[16]. Hoje as autoridades certificadoras têm um poder considerável, uma vez que qualquer autoridade pode emitir um certificado para qualquer site, facilitando a vigilância sobre seus usuários[17]. Existem inúmeras certificadoras que operam em uma ampla variedade de jurisdições, e nenhuma é formalmente obrigada a dizer ao público quais certificados foram emitidos. O setor insiste que autoridades certificadoras devem sujeitar-se a um processo de auditoria, mas este geralmente concentra-se na análise dos controles de políticas, burocráticos e organizacionais em vez da auditagem técnica. Os processos de auditoria também examinam os procedimentos gerais da certificadora, em vez de sua decisão de emitir certificados específicos.

Nós não consideramos que Let's Encrypt seja um alvo particularmente atraente para qualquer hacker ou coerção legal; algumas autoridades certificadoras existentes provavelmente são mais vulneráveis a isso do que nós. Mas os sites devem ser capazes de defender-se contra a emissão de certificados fraudulentos, e o público deve ser capaz de verificar que as certificadoras estão fazendo seu trabalho corretamente.

Felizmente existem novos meios técnicos já disponíveis para responsabilizar as certificadoras e aumentar a transparência das suas operações. Entre estes, o CAA permite que sites informem as certificadoras que não têm contrato com eles para não emitir certificados para estes sites; o HPKP permite que os sites informem o navegador Web sobre quais certificadoras estão autorizadas a emitir certificados para os mesmos; e o sistema de Transparência de Certificados do Google permite que as certificadoras mantenham um registro público de todos os certificados já emitidos, que não pode ser retroativamente alterado[18]. Estas tecnologias reduzem o poder das certificadoras de emitir certificados fraudulentos e não detectáveis como tal, e o nível de confiança que os usuários da Internet são forçados a ter sobre as mesmas. Isso é uma boa coisa.

O Observatório SSL da EFF e o projeto ZMap da Universidade de Michigan também catalogam os certificados em uso nos servidores visíveis publicamente[19]. Além de definir os procedimentos internos de detecção de fraudes, a Let's Encrypt compromete-se a cooperar com as tecnologias que aumentem a transparência das atividades de certificadoras, além de publicar registros detalhados de todos os certificados emitidos por nós e por que decidimos emitir cada um deles. Também incentivaremos sites a usar tecnologias como HPKP para defenderem-se contra certificados fraudulentos. Esperamos estabelecer um exemplo para o resto do setor de certificação, fazendo o que pudermos para garantir que os ataques contra certificadoras não tenham êxito, ou sejam detectados de imediato.

CONCLUSÃO

O TLS e sua infraestrutura de chave pública, constituídos por um grande número de autoridades certificadoras, são sistemas complexos criados às pressas na década de 1990. Eles têm sofrido pressão considerável e falharam de várias maneiras, mas o escrutínio de peritos ao longo dos últimos anos tornou-os cada vez mais seguros e resilientes. O maior problema com TLS e HTTPS hoje não é alguma falha técnica; é o fato de não serem utilizados pela maioria dos sites e assim exporem as comunicações de seus usuários a uma Internet cada vez mais hostil e amplamente vigiada.

A Let's Encrypt vai ajudar a corrigir isso, tornando rápido, fácil e sem custos para os sites em qualquer escala obter certificados que os navegadores mais usados aceitam, e que são renovados automaticamente, de modo que os administradores de sistemas possam considerar esse problema resolvido e dedicar seu tempo a outros desafios. Nossa tecnologia será baseada em software livre e padrões abertos da Internet disponíveis para adoção e aperfeiçoamento de todos. Até o final deste ano, a Let's Encrypt estará fazendo uma contribuição para uma Internet mais segura e universalmente criptografada.

--

1. Ver Andrew Blum, Tubes: A Journey to the Center of the Internet (Ecco, 2013).

2. É importante notar que estas preocupações não se aplicam apenas aos atos volitivos de nossos próprios prestadores de serviços de Internet comerciais. As ameaças à comunicação são muito diversificadas. A sabotagem no tráfego da Internet pode ser realizada por outras pessoas em nossas redes wi-fi (digamos, em um café ou em uma escola), por alguém que pode invadir nossos roteadores wi-fi (que normalmente têm software desatualizado que raramente recebem atualizações depois de fabricados), por provedores de serviços Internet que anunciam rotas espúrias, por aqueles que controlam partes da infraestrutura de nomeação DNS, por espiões que grampeiam cabos de fibra óptica, e por governos que obrigam os provedores a conceder-lhes acesso ao hardware de rede ou secretamente exploram suas vulnerabilidades.

3. Os usuários não têm que identificar-se em um site (ou mesmo estar cientes que o site existe) para que este seja usado para espionagem. Reportagens do The Intercept e do Washington Post com base em documentos fornecidos por Edward Snowden mostraram que as agências de inteligência criam sistemas de rastreamento de usuários que interceptam os cookies de redes de publicidade em conexões HTTP não criptografadas para identificar dispositivos móveis e assim localizar usuários da Internet, e até mesmo direcionar ataques contra eles.

4. Esta propriedade da segurança é baseada em problemas matemáticos com uma estrutura assimétrica ou de alçapão ("trapdoor"), que são fáceis de resolver dado algum conhecimento secreto, mas muito difícil de resolver sem ele. Entre outras possibilidades, isto significa que o conhecimento de como criptografar uma mensagem pode ser distinto do conhecimento de como decifrá-la; o primeiro pode, então, ser tornado público, enquanto o último é mantido em segredo.

5. O protocolo TLS (Transport Layer Security) era anteriormente conhecido como SSL (Secure Sockets Layer), um termo que ainda está em uso generalizado. O TLS também pode ser usado para proteger os serviços de Internet e protocolos que não sejam HTTP, e os certificados descritos neste artigo também servem para serviços além do HTTP. Este artigo irá discutir apenas o uso de TLS para proteger HTTP, mas os certificados emitidos pela Let's Encrypt também podem ser usados com outros protocolos de Internet.

6. Forma de ataque em que os dados trocados entre duas partes, por exemplo entre o usuário e o seu banco, são de alguma forma interceptados, registrados e possivelmente alterados pelo atacante sem que as vítimas percebam. Durante o ataque "man-in-the-middle", a comunicação é interceptada pelo atacante e retransmitida por este de uma forma discricionária. Os participantes legítimos da comunicação não percebem que os dados podem estar adulterados e podem fornecer informações ou executar instruções por ordem do atacante. Fonte: https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle

7. Um atacante do tipo "man-in-the-middle" poderia permitir comunicação entre as partes sem interferência aparente; ao fazer isso, o atacante pode no entanto ler o conteúdo dessas comunicações, o que seria impedido pela criptografia. Uma analogia é uma agência de correios que às vezes consegue abrir envelopes, examinando (e talvez alterando) os seus conteúdos e em seguida fechá-los de modo que pareçam intactos para os destinatários dos envelopes. A vulnerabilidade a um ataque criptográfico "man-in-the-middle" é semelhante à impossibilidade de detectar quando e se os selos foram violados; isso não significa que todas as comunicações serão sempre interceptadas, mas que alguns atacantes poderiam interceptá-las sem ser percebidos.

8. Os certificados também podem conter outras afirmações sobre a identidade do mundo real de alguma entidade, por exemplo, afirmando que um site é operado por uma determinada empresa ou organização, em um endereço físico específico. Esse tipo de verificação é menos importante para a segurança em geral. A maioria dos usuários finais raramente ou nunca consulta essa informação, e a capacidade dos navegadores em estabelecer ou não uma conexão segura é determinada apenas pela verificação de que as chaves criptográficas são válidas. O navegador não verifica se o certificado diz que google.com.br é operado pela Google Inc., de Mountain View, Califórnia, mas apenas se a chave criptográfica de curva elíptica 045cf96e6579eb74ed905a60fdee882a1 290e8c5c2e85ecfe14b047085193df9d b0c61a803a894729b6d22583ef83da80b 7d396809b54600f4bb21d742ad079448 pertence de fato ao operador do domínio google.com.br.

9. Existem meios técnicos para restringir os nomes de domínio para os quais uma certificadora pode emitir certificados, mas estes meios são usados raramente.

10. Hoje em dia, sites especialmente preocupados com a segurança podem reduzir o risco com tecnologias como

"public-key pinning" (HPKP), extensão do HTTP que alerta os navegadores para rejeitarem alterações inesperadas de um certificado; no entanto, cada site tem que optar por ativar essa proteção.

11. Ver os detalhes do caso em https://www.eff.org/pt-br/deeplinks/2011/09/post-mortem-iranian-diginota...

12. Ver, por exemplo, http://www.w3.org/2001/tag/doc/web-https e https://https.cio.gov.

13. Ver https://www.letsencrypt.org, site oficial da Let's Encrypt, que inclui enlaces para o código-fonte e o rascunho do padrão ACME.

14. Designação de grandes sistemas distribuidos de servidores instalados em múltiplos datacentros na Internet para entregar conteúdo a usuários finais com alta disponibilidade e desempenho. Hoje os CDNs fornecem uma grande parte do conteúdo da Internet, incluindo textos, gráficos, software, serviços de e-comércio, mídia em tempo real, mídia sob demanda, redes sociais e outras aplicações. Fonte: https://en.wikipedia.org/wiki/Content_delivery_network

15. Ver Christopher Soghoian e Sid Stamm, "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL" (em https://s3.amazonaws.com/files.cloudprivacy.net/ssl-mitm.pdf) (sugerindo, com base na literatura da indústria de vigilância, que "agências do governo exigem – via mandato judicial ou outro processo legal – que uma certificadora emita certificados para serem usados por agentes policiais e de inteligência para secretamente interceptar e sequestrar a comunicação segura de indivi?duos").

16. Lavabit era um provedor de webmail seguro baseado nos EUA. Em julho de 2013, o governo dos EUA exigiu judicialmente que o provedor entregasse suas chaves criptográficas secretas. O Lavabit não levantou objeções formais às demandas a tempo e acabou tendo que cumprir a demanda por ordem judicial e revelar suas informações de chaves secretas. Os tribunais, de acordo com resumo da EFF sobre o caso, "não decidiram conclusivamente se ou como o governo pode obrigar um provedor de e-mail a fornecer suas chaves de criptografia privadas ao governo"; ver https://www.eff.org/cases/lavabit (descrevendo o envolvimento da EFF no caso).

17. As preocupações sobre o abuso do poder das autoridades certificadoras para fins de vigilância foram levantadas quando o China Internet Network Information Center (CNNIC) solicitou em 2009 ser reconhecido por desenvolvedores dos navegadores Web como uma certificadora confiável; analistas temiam que o governo da República Popular da China usaria seu controle sobre o CNNIC para forçar a emissão de certificados fraudulentos e espionar as conexões HTTPS. Essa ansiedade reflete uma percepção da República Popular da China como uma praticante particularmente agressiva do vigilantismo (e a certificadora do CNNIC acabou sendo removida da lista de certificadoras confiáveis de alguns navegadores em 2015 depois de um escândalo envolvendo uma delegação indevida de autoridade para uma empresa egípcia). No entanto, certificadoras já existiam em dezenas de jurisdições, e muitas são controladas diretamente por entidades governamentais ou por empresas estatais de telecomunicações. É concebível, como Soghoian e Stamm descrevem, que qualquer governo poderia tentar obrigar secretamente qualquer certificadora dentro de sua jurisdição a emitir certificados falsos.

18. Ver https://en.wikipedia.org/wiki/DNS_Certification_Authority_Authorization, https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning e http://www.certificate- transparency.org.

19. Ver https://www.eff.org/observatory e https://scans.io.

Categoria:

- poliTICs 21