Comunidade Internet Defende a Criptografia?
Criptografia Para Todos

Junho 2020

Comunidade Internet Defende a Criptografia

A criptografia desempenha um papel vital no aumento da confiança geral na Internet - e deve ser a norma para o tráfego Internet e para o armazenamento de dados.

A *Internet Society*, os seus capítulos e outras organizações defendem a criptografia, tomando medidas para tornar a Internet mais segura e confiável para todos os seus utilizadores.

Eis o Que Estamos a Fazer e Como Você Também Pode Participar

Para promover o uso e a da criptografia e o seu incremento na Internet, a Internet Society apoia e encontra-se envolvida em projetos que contribuem para o desenvolvimento ou implantação da criptografia.

Alguns destes incluem:

Iniciativas da Online Trust Alliance

O *Cyber Incident and Breach Readiness Guide* (Guia de Prontidão e Resposta a Ciber Incidentes e Falhas de Segurança) e o *Trust Audit and Honor Roll* (Auditoria de Confiança e Lista de Honra) da *Online Trust Alliance* (OTA), ambos sublinham a criptografia como uma prática de segurança crítica para as empresas.

Deploy360

A *Internet Society* está a promover a implementação do protocolo DNSSEC (*Domain Name System Security Extensions*), o protocolo DANE (*DNS Based Authentication of Named Entities*) e o uso do TLS em aplicações através do seu programa Deploy360. O Deploy360 oferece introduções, com recursos de formação aprofundados, para facilitar a implementação das principais tecnologias da Internet.

O Projeto CryptTech

A *Internet Society* apoia o projeto Cryptech, que "está a desenvolver um projeto de mecanismo criptográfico de *hardware* de código aberto que corresponda às necessidades de sistemas de infraestrutura da Internet de elevada fiabilidade que usam criptografia".

Let's Encrypt

A *Internet Society* apoia a iniciativa Let's Encrypt, que fornece certificados gratuitos para sítios *web* para *Transport Layer Security* (TLS), automatizando o processo, tornando mais fácil e barato para os sítios *web* usarem TLS.

Defendendo um Futuro Confiável

A *Internet Society* estabeleceu como objetivo garantir que os promotores de políticas públicas, legisladores e o público em geral entendam a importância da criptografia e os riscos associados ao seu enfraquecimento ou à limitação do seu uso. As políticas que apoiam em vez de enfraquecer a criptografia são críticas para criar uma Internet segura e confiável.

A *Internet Society* é signatária da *Secure the Internet*, que insta os governos a apoiar o desenvolvimento e o uso de ferramentas e tecnologias de comunicação seguras e a rejeitar políticas que impeçam ou prejudiquem o uso da criptografia forte.

Em abril de 2019, a *Internet Society* assinou a *Joint Call to World Leaders for a Healthy Digital Society* (Apelo Conjunto Por Uma Sociedade Digital Saudável), apelando aos Ministros do Interior do G7 se lembrarem que as promessas de que a criptografia não seria afetada pelo "acesso legal" simplesmente não se podem manter. Em agosto de 2019, a *Internet Society* e mais de 30 organizações assinaram uma carta aberta pedindo aos líderes do G7 para protegerem e promoverem a criptografia forte que é a base para nossas economias digitais, sociedades digitais e vidas interdependentes.

Recursos

Resumo de Políticas: Criptografia

O Resumo da Política de Criptografia inclui as principais considerações, desafios e princípios orientadores que um governo deve seguir ao lidar com a criptografia.

Leia *online* ou faça o *download*

Criptografia e Acesso Excecional

Uma explicação da criptografia, além de como as propostas de acesso excecional funcionam e afetam a Internet.

Leia *online* ou faça o *download*

6 Formas Como o "Acesso Legal" Coloca a Segurança de Todos Nós em Risco

Uma ficha informativa para legisladores explicando como as medidas de "acesso legal" enfraquecem a segurança da Internet.

Leia *online* ou faça o *download*

Criptografia Essencial Para a Comunidade LGBTQ+

Para algumas comunidades, como as comunidades LGBTQ +, a criptografia é especialmente crucial para manter as pessoas seguras *online* e na vida real.

Leia *online* ou faça o *download*

Afirmações

- G7 Leaders: Protect Strong Encryption for a Secure World
- The Internet Society's Concerns on the Recent Government Action in Kazakhstan Regarding Encrypted Internet Traffic
- Internet Society Signs Open Letter Opposing GCHQ Ghost Proposal For Weakening Encrypted Communications
- Andrew Sullivan: The False Promise of Lawful Access to Private Data
- Constance Bommelaer de Leusse: «Laisser les Etats décrypter et filtrer Internet peut créer un préjudice pour les citoyens et l'économie»
- Leaders of the G7: A Safer World Means Strong, Secure Communication
- Encryption Is Critical for the Australian Economy
- Encryption Is Key to Safety of Journalists
- Encryption and Law Enforcement Can Work Together
- Statement to the G20: Securing our Digital Economy
- Strong Encryption is Essential to Our Security, Not a Barrier
- Statement by the Board of Trustees: Internet Society Commends Internet Architecture Board Recommendation on Encryption by Default for Internet

Relatórios e Submissões

- Internet Society submission to the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Expression and Opinion regarding the use of encryption and anonymity in digital communications
- Internet Society-Chatham House Roundtable on Encryption and Lawful Access
- IGF 2015 Workshop Report: Law Enforcement in a World of Pervasive Encryption
- CEOs and Encryption: The Questions You Need to Ask Your Experts

Rumo a uma solução para o debate da criptografia sobre acesso excecional

Os criminosos também podem usar criptografia. Algumas forças policiais estão preocupadas que a criptografia as impeça de obter os elementos probatórios ou informações que necessitam. Para resolver essas preocupações, alguns governos estão a tentar fazer com que as empresas lhes criem maneiras de aceder ao conteúdo cifrado pelos sistemas das empresas (uma prática conhecida por "acesso excecional").

A *Internet Society* reconhece as preocupações das forças policiais e permanece firme na sua convicção de que a criptografia é uma solução técnica importante que todos os utilizadores da Internet devem usar. Para aproximar o debate da criptografia e do acesso excecional a uma solução bem sucedida, a *Internet Society* está a trabalhar para desconstruir os desafios enfrentados pelas forças policiais e explorar como o conflito percebido entre a criptografia e a aplicação da lei pode ser tratado.

Em outubro de 2017, a *Internet Society*, em parceria com a *Chatham House*, realizou uma mesa redonda sobre criptografia e acesso legal. Durante a mesa redonda, os especialistas identificaram as principais nuances à volta do uso da criptografia, além de áreas específicas em que é possível fazer progressos. Os especialistas também dividiram o problema em partes geríveis, fornecendo um conjunto claro de questões que exigirão esforços futuros concentrados por parte das entidades interessadas para as resolver.

Como os membros da comunidade técnica da Internet defendem a criptografia

Após as revelações de 2013, onde foi descoberta a extensão da monitorização generalizada do estado-nação, muitos membros da Comunidade da Internet tomaram medidas para tornar a Internet e seus utilizadores mais seguros.

Fortalecendo os Protocolos da Internet

Em maio de 2014, a ***Internet Engineering Task Force*** **(IETF)** lançou o seu RFC 7258, afirmando que a monitorização generalizada representa um ataque contra a Internet. Em resposta, o ***Internet Architecture Board*** **(IAB)** lançou sua própria declaração (*IAB Statement on Internet Confidentiality)*, reconhecendo também que a aspiração da implementação da criptografia generalizada levanta alguns problemas práticos e desafios técnicos.

Desde 2014, a Comunidade IETF desenvolveu vários novos protocolos e continua a trabalhar noutros que visam fortalecer e tornar a criptografia o padrão para a Internet. Um desses protocolos é o TLS 1.3, também conhecido como *Transport Layer Security* versão 1.3, que fornece maior segurança ao tráfego Internet à medida que este passa pelas redes.

Em setembro de 2019, o ***Internet Architecture Board*** **(IAB)** divulgou a declaração sobre "*Avoiding Uninted Harm to Internet Infrastructure*" que "discute os possíveis efeitos não intencionais que as politicas e as propostas regulamentares podem ter na Internet".

O ***World Wide Web Consortium*** **(W3C)** partilhou as descobertas *Securing the Web* e *End-to-End Encryption and the Web*, que destacam a importância da criptografia ponto-a-ponto e da confiança para o sucesso da Web.

Em 2015, um grupo de cifradores e especialistas em segurança divulgou o relatório *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. Este é um influente no debate sobre a criptografia e acesso das forças policiais, e os seus autores continuam a ser fortes defensores da criptografia.

A **InternetNZ** publicou dois documentos sobre criptografia: um iniciador de discussão, Encryption: what it is and why it's important, e um documento de posicionamento, ways forward that protect the Internet's potential.

A ***World Information Technology And Services Alliance*** **(WITSA)**, que representa associações do setor de TI em mais de 80 países, deixou claro, tanto numa declaração quanto num discurso do seu *Chairman*, que se opõe fortemente a *backdoors* na criptografia.

Como os Capítulos da *Internet Society* Defendem a Criptografia

Do desenvolvimento de documentos e vídeos à realização de eventos e campanhas nacionais de defesa de direitos, os capítulos da *Internet Society* defendem a criptografia a nível nacional e internacional. Abaixo estão apenas

algumas das atividades que os Capítulos da *Internet Society* têm levado a efeito:

- Em outubro de 2019, a **Internet Australia** divulgou um comunicado de imprensa expressando preocupação ao notar a solicitação do governo australiano ao Facebook - para interromper os planos de introdução da criptografia forte ponto-a-ponto nos seus sistemas de mensagens - numa carta aberta assinada pelo Ministro da Administração Interna da Austrália, Peter Dutton, juntamente com seus colegas dos EUA e do Reino Unido.
- Em resposta à legislação anunciada relacionada com a criptografia e acesso legal, a **Internet Australia** e a *Internet Society* realizaram uma Sessão de Especialistas em Criptografia em 20 de agosto de 2018, em Canberra, na Austrália. A **Internet Australia** também publicou um comunicado de imprensa destacando as suas preocupações com o projeto de lei.
- O Capítulo Canadiano da ISOC, em sua apresentação à *Public Safety Canada* e à Consulta sobre Segurança Nacional do Departamento de Justiça, enfatizou a importância da criptografia e instou a indústria e o governo a procurar melhorar os padrões da criptografia em vez de os enfraquecer.
- O **Capítulo da Grande Washington, DC (ISOC-DC)** criou o vídeo *The Internet Exposed: Encryption, Backdoors and Privacy - and the Quest to Maintain Trust*, para explicar ao público em geral os problemas com a criptografia.
- Membros de 22 Capítulos Europeus da Internet Society em 20 países reuniram-se para discutir questões políticas específicas que afetam vários países da Europa, criptografia e filtragem de conteúdos.
- O **Capítulo de Delhi na Índia** organizou um seminário *online* sobre o projeto de lei *Information Technology [Intermediary Guidelines (Amendment) Rules] 2018,* proposto pelo Ministério Indiano de Eletrónica e Tecnologias da Informação. O Capítulo também enviou *feedback* ao governo indiano durante o período de comentário público e incentivou os seus membros e instou outras entidades Indianas interessadas a fazerem o mesmo.