Criptografia

Um documento informativo da Internet Society sobre políticas públicas

3 de junho de 2016

Introdução

A criptografia está por toda parte. Ela é usada para proteger dados enviados por meio de todos os tipos de dispositivos em todos os tipos de redes. Além de proteger os "chaveiros" eletrônicos que guardam tanto nossas senhas nos computadores como documentos que devem ter "acesso restrito", a criptografia é usada para proteger as informações que são trocadas sempre que uma pessoa usa um caixa eletrônico, faz uma compra usando um smartphone, realiza uma chamada de celular ou aperta um botão no chaveiro para abrir as portas do carro. Trata-se de uma tecnologia versátil cada vez mais disseminada nas nossas vidas cotidianas e muito importante para a segurança de muitas das nossas atividades.

A criptografia eletrônica, ou seja, o processo de embaralhar ou codificar dados para que só possam ser lidos por alguém que tenha a capacidade de decifrá-los, é bastante usada para proteger tanto dados armazenados em sistemas de computadores quanto dados transmitidos em redes computacionais, incluindo a Internet. Para a comunicação de dados em uma rede, a criptografia moderna codifica os dados usando um código secreto ou chave, conhecida apenas pelo remetente e destinatário. No caso de dados armazenados, o código secreto geralmente é conhecido apenas pelo proprietário dos dados.

A criptografia e outras técnicas relacionadas são também empregadas para aumentar a segurança de transações financeiras e proteger a comunicação privada de usuários finais. Ela é usada para determinar se os dados foram manipulados (integridade de dados), aumentar a confiança dos usuários de que eles estão realmente se comunicando com o destinatário pretendido (autenticação) e integrar protocolos que fornecem a evidência de que as mensagens foram enviadas e recebidas (não repúdio).

Considerações importantes

Na prática, a criptografia é realizada basicamente destas formas:

- **A criptografia simétrica** usa chaves idênticas para criptografar e descriptografar a mensagem. Tanto o remetente quanto o destinatário têm acesso à mesma chave. Embora seja rápida e eficiente para computadores, a criptografia

As tecnologias de criptografia permitem que os usuários da internet protejam a confidencialidade de seus dados e comunicações contra observações e intrusões indesejadas. A criptografia também é um dos fundamentos técnicos da confiança na internet. Ela promove a liberdade de expressão, comércio, privacidade, confiança do usuário e também ajuda a proteger os dados das ações de pessoas mal-intencionadas. Por essas razões, a Internet Society acredita que a criptografia deve ser o padrão usado no armazenamento de dados e tráfego de internet.

Uma vez que pessoas mal-intencionadas podem usar a criptografia para ocultarem suas atividades ou sequestrarem dados de usuários (por ex., via ransomware[1]), integrantes tanto de agências governamentais de segurança quanto de órgãos de policiamento demonstraram preocupação sobre o impacto negativo da criptografia em sua capacidade de proteger os cidadãos e zelar pelo cumprimento das leis.

A Internet Society reconhece o as preocupações das autoridades e permanece firma em sua convicção de que a criptografia é uma solução técnica importante que todos os usuários da internet: indivíduos, órgãos governamentais, empresas e outras comunidades devem usá-la para proteger sua comunicação e seus dados. Acreditamos que as tentativas técnicas e normativas de limitar o uso da criptografia, bem intencionadas ou não, terão um impacto negativo na segurança dos cidadãos que cumprem as leis.

simétrica deve garantir que a chave seja entregue de forma confiável para o destinatário e não caia em mãos erradas.

- **A criptografia assimétrica**, também chamada de criptografia de chave pública, é uma forma de criptografia de mão única. As chaves são geradas em pares e as informações criptografadas com a chave pública só podem ser descriptografadas com a chave privada correspondente. O destinatário divulga publicamente sua chave pública para que os remetentes a empreguem para criptografar uma mensagem. O destinatário, então, usa uma chave privada correspondente para descriptografar os dados. Isto é semelhante a uma caixa de correio trancada na qual as cartas podem ser inseridas por meio de uma abertura para entrega, mas só podem ser acessadas pelo proprietário que tem a chave. A criptografia de chave pública é mais segura do que a criptografia simétrica, pois a chave privada não precisa ser transferida a terceiros.

- **A criptografia ponto a ponto** é qualquer forma de criptografia em que apenas o remetente e o destinatário pretendido podem ler determinada mensagem. O aspecto mais importante da criptografia ponto a ponto é que terceiros, até mesmo a empresa que fornece o serviço de comunicação, não têm conhecimento da chave de criptografia. Entre os exemplos de criptografia ponto a ponto estão os protocolos Pretty Good Privacy (PGP) e Off-the-Record Messaging (OTR). Exemplos de serviços de comunicação com criptografia ponto a ponto são o iMessage da Apple, o Telegram e o Threema. A Electronic Frontier Foundation publicou uma avaliação de aplicativos de mensageria seguros,[1] que traz informações sobre as características de vários serviços.

- **A criptografia de dados estáticos ("data-at-rest")** é qualquer forma de criptografia que protege dados armazenados fisicamente em formato digital (por exemplo, em computadores, unidades de disco, dispositivos móveis ou dispositivos de internet das coisas).

Na prática, a criptografia é aplicada em uma abordagem por camadas. Por exemplo, um usuário criptografa o conteúdo de seu e-mail usando PGP ou extensões S/MIME (Secure/Multipurpose Internet Mail Extensions) e o provedor de e-mail (por exemplo, Gmail) criptografa a transmissão de dados entre servidores usando HTTPS.

É importante observar que a criptografia não faz com que todos os dados relacionados à comunicação fiquem necessariamente inacessíveis. Por exemplo, metadados de comunicações - incluindo identificadores de remetente e destinatário, tamanho da mensagem, local, data e hora, além de dados usados pelas autoridades - podem estar expostos em texto legível.

Desafios

O aumento da disponibilidade da criptografia, sua natureza versátil e seu uso por diversos tipos de atores vêm acompanhados de vários desafios.

1 Acesse https://www.eff.org/secure-messaging-scorecard.

- **Liberdade de expressão, anonimato e possíveis abusos.** As tecnologias de criptografia facilitam a comunicação anônima, um possível instrumento para a proteção de cidadãos e ativistas vivendo em regimes opressores e pessoas vulneráveis, como vítimas de abuso doméstico, pessoas em programas de proteção a testemunhas e policiais disfarçados. A mesma tecnologia, no entanto, pode ajudar pessoas mal-intencionadas a ocultar atividades e comunicações com o uso de ferramentas de anonimato, por exemplo para praticar *bullying digital* ou outras formas de assédio na internet.

  A Internet Society reconhece o objetivo legítimo que os estados têm de protegerem seus cidadãos, mas adverte quanto a tentativas de regular a tecnologia para impedir que criminosos se comuniquem de forma confidencial. Essa abordagem faz com que haja o risco real de impossibilitar que os cidadãos que respeitam as leis protejam a confidencialidade de seus dados e comunicações, gerando riscos a seus direitos de privacidade, liberdade de expressão e opinião. Conforme descrito em nosso relatório "Segurança Colaborativa"[2], o objetivo geral de políticas de segurança deve ser o de aumentar a confiança na internet e garantir o sucesso continuado da internet como um agente incentivador de inovações econômicas e sociais.

- **O dilema segurança–privacidade.** O debate de políticas relacionadas à criptografia geralmente apresenta a questão como um conflito entre segurança e privacidade, uma questão de equilibrar a responsabilidade dos governos de protegerem seus cidadãos *versus* o direito dos cidadãos de protegerem sua privacidade de intrusões de agentes governamentais, comerciais, criminosos, etc. A Internet Society afirma que segurança e privacidade não são necessariamente conceitos mutuamente excludentes. Pelo contrário, eles podem se reforçar mutuamente: a confiança do usuário é fruto da sensação de ter tanto sua segurança quanto sua privacidade protegidas Nesse sentido, a confiança de que uma mensagem está protegida (só será lida pelo destinatário pretendido) ajuda uma variedade de serviços de internet a se expandir, mais notavelmente o comércio eletrônico.

- **Backdoors (ou "portas dos fundos") de criptografia.** O termo se refere à ideia de uma ferramenta capaz de auxiliar uma pessoa não autorizada a decodificar e obter acesso a dados criptografados sem ter acesso às chaves criptográficas. Tais portas dos fundos dissimulam o acesso de terceiros ao conteúdo. O consenso técnico[3] é que o uso de portas dos fundos por quaisquer das técnicas propostas atualmente colocaria usuários legítimos sob risco e dificilmente impediria criminosos de se comunicarem clandestinamente. Pessoas mal-intencionadas provavelmente encontrarão formas alternativas de comunicação, enquanto os usuários medianos talvez não consigam ter acesso às mesmas ferramentas. Isso pode fazer com que comunicações criminosas deixem de ser

2 Acesse http://www.internetsociety.org/collaborativesecurity.

3 Acesse Chaves embaixo do tapete: insegurança decorrente de acesso exigido pelo governo a todos os dados e comunicações, Manifesto da IAB sobre a confidencialidade na internet, Descoberta da W3C TAG: a criptografia de ponta a ponta e a web, Descoberta da W3C TAG: a web mais segura, Postagem no blog da M3AAWG: MAAWG apoia recomendações de criptografia de ponta a ponta "Chaves embaixo do tapete" e Comunicado de imprensa da WITSA: setor global de ICT se opõe à descriptografia de backdoor.

observadas, enquanto comunicações de usuários se tornem vulneráveis à observação e interceptação por governos ou pessoas mal-intencionadas que eventualmente tenham descoberto como explorar essas portas traseiras.

- **Tecnologia resistente a adulterações.** De modo a dificultar e a dissuadir que criminosos façam modificações na tecnologia, a criptografia é uma tecnologia que resiste a adulterações e é capaz de apontar que elas foram efetuadas. Usadas em conjunto com o emprego da criptografia, essas medidas podem ajudar a impedir (1) o acesso a um dispositivo após muitas tentativas repetidas de login e (2) a instalação de portas dos fundos, *rootkits* (código malicioso desenvolvido para acessar diferentes áreas de um computador sem autorização) e outros tipos de software malicioso. Nos últimos anos, tem havido uma tendência de aumento na utilização de tecnologia de resistência a adulterações e de mecanismos que automaticamente apagam dados em casos de manipulação (por ex., após dez tentativas sem sucesso de conectar-se com uma senha inválida). Embora a tecnologia de resistência a adulterações ajude a proteger a integridade da tecnologia, ela também pode oferecer dificuldades às autoridades que precisam obter acesso às comunicações e dados de pessoas mal-intencionadas mediante ordem judicial[4].

Princípios de orientação

A Internet Society oferece estes princípios para orientação de políticas relacionadas com o tema:

- **Confidencialidade e anonimato.** Para apoiar o exercício ilimitado de direitos humanos, incluindo a privacidade e a liberdade de expressão, as pessoas devem poder se comunicar de forma confidencial e anônima na internet.

- **Segurança de dados.** Assim como as pessoas têm o direito de proteger seus bens e propriedades físicas, elas devem ter o direito de usar a criptografia e outras ferramentas para proteger seus dados, ativos digitais e atividades on-line. Nós incentivamos o desenvolvimento aberto e a disponibilidade ampla de tecnologias de proteção de dados.

- **Confiança.** A confiança do usuário é essencial para a expansão e evolução continuadas da internet e um número cada vez maior de usuários está se dando conta das vantagens de utilizar aplicativos e serviços que respeitam a privacidade. Nós incentivamos o fornecimento de mecanismos confiáveis de autenticação, confidencialidade de dados e integridade de dados como componentes técnicos vitais para a criação de produtos e serviços de confiança. Também acreditamos que os marcos legais devem dar apoio aos direitos humanos, incluindo o direito à privacidade.

- **Criptografia.** A criptografia deve ser a norma para todo tráfego de internet. Trabalhar para esse objetivo é um importante complemento aos esforços atuais

4 Esta questão está em um caso recente de um tribunal de federal de primeira instância da Califórnia, envolvendo o FBI e a Apple.

da comunidade técnica no sentido de tratar do excesso de monitoramento. Projetistas e desenvolvedores de produtos e serviços digitais são fortenemente incentivados a garantir que os dados dos seus usuários, armazenados ou comunicados, sejam criptografados por padrão. Sempre que possível, soluções de criptografia ponto a ponto devem ser disponibilizadas. Além disso, operadores de rede e serviços são incentivados a empregar criptografia em todos os lugares onde ela ainda não estiver disponível e os encorajamos a permitir tráfego criptografado em suas políticas operacionais.

- **Tecnologia de resistência a adulterações.** A tecnologia de resistência a adulterações deve continuar a ser desenvolvida e implantada de forma a dar apoio à criptografia. Órgãos governamentais não devem exigir a colocação de vulnerabilidades em quaisquer ferramentas, tecnologias ou serviços. Da mesma forma, órgãos governamentais não devem exigir que ferramentas, tecnologias ou serviços sejam desenvolvidos ou projetados de forma a permitir que terceiros acessem o conteúdo de dados criptografados. Os órgãos governamentais devem também dar apoio ao trabalho de pesquisadores de segurança e outros que tenham como objetivo identificar e divulgar de forma responsável vulnerabilidades de segurança e de privacidade na tecnologia.

- **Implantação.** A implantação cada vez mais comum de mecanismos de segurança, como a criptografia, trará desafios em projetos de gestão, desenvolvimento, administração e usabilidade de redes. A gestão de redes, detecção de intrusos e prevenção de spam terão novos requisitos funcionais; nesse sentido, desafios políticos e econômicos devem ser esperados nesse contexto.

- **Soluções definidas multissetorialmente.** Criminosos podem se comunicar de forma confidencial e anônima. Confrontar a implicações dessa realidade com sucesso exige a ação conjunta de vários interessados. A Internet Society reafirma seu compromisso de facilitar o engajamento de todos os atores interessados, dos múltiplos setores, e de desempenhar um papel ativo e tecnicamente informado em contribuição ao desenvolvimento de soluções.

Além disso, a Internet Society assinou a petição "Mantenha a internet segura" [5] como forma de demonstrar o seu apoio aos princípios nela estabelecidos, mais precisamente para destacar que os órgãos governamentais não devem:

- Banir ou limitar de qualquer forma o acesso de usuários à criptografia ou proibir a implementação e/ou o uso das diversas técnicas de criptografia, independentemente do tipo ou características.

- Exigir o desenvolvimento ou a implantação de portas dos fundos ou vulnerabilidades em ferramentas, tecnologias ou serviços.

5 Acesse https://www.securetheinternet.org/.

- Exigir que ferramentas, tecnologias ou serviços sejam projetados ou desenvolvidos para permitir que terceiros tenham acesso a dados não criptografados ou chaves de criptografia.

- Procurar enfraquecer ou prejudicar padrões de criptografia, ou influenciar de forma intencional o desenvolvimento desses padrões, exceto quando se tratar da promoção de um nível mais alto de segurança de informações.

- Obrigar a adoção de algoritmos de criptografia, padrões, ferramentas ou tecnologias inseguras.

- Constranger ou pressionar entidades – por meio de medidas públicas ou sigilosas - a realizarem atividades incompatíveis com os princípios acima.

Recursos adicionais

A Internet Society publicou uma série de documentos e conteúdos adicionais relacionados a este tema. Eles estão disponíveis gratuitamente no site da Internet Society e muitos podem ser encontrados em nossa página principal sobre criptografia, no endereço https://www.internetsociety.org/encryption

Boletins de notícias da Internet Society

- Internet Society reage a relatórios do governo americano sobre violações da tecnologia criptográfica, https://www.internetsociety.org/news/internet-society-responds-reports-us-government's-circumvention-encryption-technology

- Internet Society faz recomendação ao Comitê de Arquitetura da Internet a respeito de criptografia , https://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default

- Parecer da Internet Society sobre o uso da criptografia e do anonimato em comunicações digitais dirigido ao Relator da ONU para a proteção e promoção do direito de liberdade de expressão e de opinião, http://www.internetsociety.org/doc/internet-society-submission-un-special-rapporteur-protection-and-promotion-right-freedom

Postagens do blog

- Liberdade de expressão: repensando o papel da criptografia, https://www.internetsociety.org/blog/2013/05/freedom-speech-rethinking-role-encryption

- Portas do fundo de criptografia reduzem confiança na internet, https://www.internetsociety.org/blog/tech-matters/2015/05/encryption-backdoors-decrease-trust-internet

- Apoio ao anonimato e à criptografia do Relator da ONU David Kaye , http://www.internetsociety.org/blog/public-policy/2015/06/strong-support-un-special-rapporteur-david-kaye-anonymity-and-encryption

- Não deixe a chave embaixo do tapete, https://www.internetsociety.org/blog/public-policy-tech-matters/2015/08/no-keys-under-doormat-please

- A tensão fundamental entre segurança e privacidade (e a proposta de banimento da criptografia no Reino Unido), https://www.internetsociety.org/blog/public-policy/2015/01/fundamental-tension-between-safety-and-privacy-and-uks-proposed

- Internet Society apoia iniciativa "Vamos criptografar" para aumentar a criptografia de ponta a ponta, https://www.internetsociety.org/blog/tech-matters/2015/10/isoc-supports-lets-encrypt-initiative-increase-end-end-encryption

- Imagine um mundo criptografado! Um workshop na IGF, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/11/imagine-encrypted-world-workshop-igf-2015

- Criptografia e autoridades policiais: em busca de confiança, https://www.internetsociety.org/blog/tech-matters-public-policy/2015/12/encryption-and-law-enforcement-aiming-trust

- "Vamos criptografar" lança em versão beta para aumentar a criptografia na internet, https://www.internetsociety.org/blog/tech-matters/2015/12/lets-encrypt-enters-public-beta-increase-encryption-internet

- Internet Society assina a petição on-line "Mantenha a internet segura", http://www.internetsociety.org/blog/tech-matters/2016/02/internet-society-signs-secure-internet-online-petition

- Portas do fundo de criptografia de todos os tipos: uma reação à carta ao cliente emitida pela Apple, https://www.internetsociety.org/blog/public-policy/2016/02/encryption-backdoors-come-all-guises-reacting-apples-customer-letter

Artigos e relatórios de workshops

- Barreiras ao desenvolvimento: experimentando as potenciais diferenças entre a infraestrutura desenvolvida e a que está desenvolvimento, https://www.iab.org/wp-content/IAB-uploads/2015/08/MaRNEW_1_paper_27.pdf