Criptografia

As tecnologias de criptografia permitem que os usuários de Internet protejam a integridade e a confidencialidade de seus dados e comunicações. Desde limitar o impacto de vazamento de dados até manter mensagens em confidencialidade, a criptografia é uma ferramenta essencial para a segurança digital. Como base técnica para a confiança na Internet, a criptografia promove a liberdade de expressão, o comércio, a privacidade e a segurança dos usuários, e ajuda a proteger dados e comunicações de ações de pessoas mal intencionadas.

A Internet Society acredita que a criptografia deve ser usada como padrão na proteção de dados armazenados e em trânsito na Internet.

O que é criptografia?

Criptografia eletrônica é o processo de embaralhar ou codificar arquivos e conteúdos, para que só possam ser lidos por alguém que tenha os meios de fazê-los retornarem a seu estado original. Ela é geralmente usada para proteger tanto os dados armazenados em sistemas de computadores **(dados estáticos),** quanto os dados que trafegam por redes de computadores, incluindo a Internet **(dados em trânsito)**. Dados em trânsito geralmente são embaralhados com o uso de uma chave pública e desembaralhados com o uso de uma chave privada. No caso de dados estáticos, geralmente a chave para embaralhar e desembaralhar é conhecida apenas pelo proprietário dos dados.

Criptografia ponto a ponto

Criptografia ponto a ponto (E2E, end-to-end) é qualquer forma de criptografia em que apenas o remetente e o destinatário pretendido têm as chaves para descriptografar a 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 das chaves de criptografia.

Nós usamos a criptografia todos os dias

Navegação na Internet: Navegadores e websites usam o HTTPS. um protocolo criptografado, de forma a oferecer comunicação segura, fazendo com que nossos dados não possam ser lidos por criminosos enquanto estiverem em trânsito.

Comércio eletrônico: Nós confiamos às empresas a proteção de nossas informações bancárias quando fazemos compras ou usamos o banco na Internet. A criptografia é um importante método de se obter isso

Mensagens seguras: Quando usamos um aplicativo de mensagens, esperamos que essas mensagens sejam particulares. Alguns aplicativos de mensagens usam criptografia para manter a privacidade e segurança das comunicações de seus usuários.

Outros usam até mesmo criptografia ponto a ponto, de forma que apenas o remetente e o destinatário possam ler as mensagem, por exemplo, iMessage, WhatsApp e Signal.

O que é o acesso excepcional?

Geralmente, quando as pessoas falam de acesso excepcional, elas se referem a alguma forma de permitir que autoridades tenham a capacidade de acessar o conteúdo de comunicações e dados de forma descriptografada.

Por que acesso excepcional?

Como pessoas mal-intencionadas também podem usar a criptografia para ocultar suas atividades ilícitas, autoridades e outras entidades têm preocupação em relação ao impacto negativo que a criptografia poderia ter em sua habilidade de proteger cidadãos e garantir o cumprimento das leis. Alguns argumentam que as autoridades devem ter acesso excepcional ao conteúdo de comunicações e dispositivos criptografados.

Problemas relacionados ao acesso excepcional

Não importa o método adotado, o acesso excepcional também poderá permitir que outras partes não previstas, como criminosos e outros governos, ganhem acesso a dados e comunicações protegidas. O consenso entre especialistas em segurança da informação é que mecanismos de acesso excepcional sempre agregam mais complexidade aos sistemas, aumentando a quantidade de vulnerabilidades. Essas vulnerabilidades podem servir como pontos de entrada que qualquer pessoa pode descobrir e aproveitar com fins indevidos.

As propostas de acesso excepcional dificilmente irão impedir que criminosos se comuniquem livremente em segredo. No caso de pessoas com alguma experiência em informática, é bastante fácil encontrar ferramentas alternativas de criptografia de dados estáticos ou em trânsito. Nesse caso, a comunicação de criminosos pode ficar imune à observação externa, enquanto que a comunicação dos usuários normais acabará ficando vulnerável à observação e interceptação de terceiras pessoas mal intencionadas que terão descoberto como explorar as vulnerabilidades criadas graças ao acesso excepcional.

Algumas propostas de acesso excepcional

Uma "porta dos fundos" de criptografia geralmente se refere a alguma alteração em um protocolo, aplicativo ou serviço de criptografia que faça com que pessoas autorizadas tenham acesso permitido a dados criptografados. Uma forma de fazer isso é **enfraquecer** os mecanismos de criptografia ou os sistemas que dão suporte a eles. Portas dos fundos de qualquer tipo são vulnerabilidades que podem ser usadas e descobertas por criminosos e outras pessoas mal intecionadas.

Custódia de chaves geralmente trata da ideia de chaves criptográficas armazenadas sob custódia de uma terceira parte de confiança, que possa ser usada eventualmente pelas autoridades. Porém, qualquer chave armazenada corre o risco de ser vazada e utilizada de forma ilegal por criminosos ou outras pessoas mal intencionadas.

Cadeados de bagagem – Uma metáfora para as portas dos fundos de criptografia

Os cadeados de bagagem aprovados pela TSA, a Administração para a Segurança dos Transportes dos Estados Unidos, foram projetados para permitir que os passageiros protejam suas bagagens ao mesmo tempo que dão à TSA a capacidade de abrir as malas e inspecionar seu conteúdo para fins de segurança graças ao uso de uma chave mestra pela TSA. Infelizmente, as chaves mestras não permaneceram em segredo: seu projeto foi exposto, permitindo que cópias fossem reproduzidas com uma impressora 3D ou vendidas na Internet por apenas 10 dólares. Agora, qualquer pessoa pode obter uma chave mestra para abrir cadeados aprovados pela TSA.

Considerações sobre o acesso excepcional

Se a criptografia ou outros mecanismos de segurança forem enfraquecidos para habilitarem o acesso de peritos, ficará mais fácil para qualquer pessoa obter o mesmo tipo de acesso (particularmente o crime organizado, empresas envolvidas em espionagem industrial e outros representantes governamentais, inclusive estrangeiros). Isso também prejudica os interesses legítimos de cidadãos e empresas privadas ao facilitar o furto de identidades e o acesso a informações confidenciais sobre bens, o que inclui tanto recursos financeiros quanto propriedade intelectual.

A Internet Society reconhece as preocupações das autoridades e permanece firme em sua convicção de que a criptografia é uma solução técnica importante, que todos os usuários da Internet devem usar para proteger sua comunicação e seus dados. Tentativas técnicas e legais de limitar o uso da criptografia, mesmo quando bem-intencionadas, terão impacto negativo na segurança de cidadãos cumpridores da lei e da Internet como um todo.

Propostas de acesso excepcional fazem pouco para resolver o problema da comunicação sigilosa entre criminosos e provavelmente acrescentarão uma quantidade de risco substancial aos cidadãos que respeitam e cumprem a lei. O acesso excepcional trará novos problemas sem fornecer uma solução eficaz para os problemas apontados pelas autoridades.