As porcas e parafusos da criptografia: uma cartilha para formuladores de políticas*

Edward W. Felten, pesquisador do Centro de Políticas de Tecnologia da Informação do Departamento de Ciência da Computação, Escola Woodrow Wilson de Assuntos Públicos e Internacionais, Universidade de Princeton.

Data da publicação:

Abril de 2017

Este documento oferece uma introdução simples à criptografia, tal como ela é implementado nos sistemas atuais, em um nível de detalhe adequado para discussões de políticas. Não é assumido nenhum conhecimento prévio sobre criptografia ou segurança de dados.

A criptografia é usada em dois cenários principais. A armazenagem criptografada permite que os dados sejam armazenados em um dispositivo, com a criptografia que protege os dados caso um elemento malicioso tenha acesso ao dispositivo. A comunicação criptografada permite que dados sejam transmitidos entre dois pontos, muitas vezes através de uma rede, com a criptografia que protege esses dados em trânsito de um elemento malicioso. A criptografia é usada de maneira um pouco diferente nesses dois cenários, por isso faz sentido apresentá-los separadamente. Vamos discutir armazenagem criptografada em primeiro lugar, porque é mais simples.

Enfatizamos que as abordagens descritas aqui não são descrições detalhadas de qualquer sistema específico existente, mas descrições bastante genéricas de como os sistemas atuais funcionam normalmente. Os detalhes de produtos e normas específicas podem ter diferenças, mas basicamente são semelhantes no nível de detalhe apresentado aqui.

Armazenagem criptografada

Suponha que uma usuária, Alice, quer armazenar dados em um dispositivo, que pode ser um smartphone da usuária, ou pode ser um servidor de armazenagem operado por um provedor de serviços. Alice gera uma senha secreta que só ela sabe, e ela usa a senha secreta para criptografar os dados. A criptografia protege a confidencialidade dos dados, de modo que um elemento malicioso quem tenha acesso ao dispositivo mas não sabe a senha secreta não pode entender o conteúdo dos dados de Alice. A criptografia também protege a integridade dos dados, de modo que uma pessoa maliciosa quem tenha acesso ao dispositivo mas não sabe a senha secreta não pode alterar os dados sem que Alice perceba.

A criptografia de um dispositivo, como um smartphone, funciona tipicamente como descrito a seguir **(figura 1)**. A chave do dispositivo, que é exclusiva para o smartphone específico de Alice, é incorporada ao aparelho quando este é fabricado. Além disso, Alice digita uma senha secreta de acesso quando ela desbloqueia o aparelho[2]. A chave do dispositivo e a senha são combinadas por meio de criptografia para criar uma chave de armazenagem, que será utilizada para criptografar os dados. Daquele ponto em diante, sempre que uma aplicação pretende armazenar dados no aparelho, os dados serão criptografados com a chave de armazenagem antes de serem gravados. Sempre que um aplicativo quiser recuperar esses dados, estes são decodificados antes de ser entregues ao aplicativo. Quando o sistema decodifica os dados, também verifica a integridade dos mesmos com vistas a possível adulteração.

Porque todos os dados são criptografados antes de serem armazenados, um elemento malicioso que roube o dispositivo mas não sabe a senha secreta de Alice não pode recuperar os dados, nem pode afetar a integridade dos mesmos sem detecção.

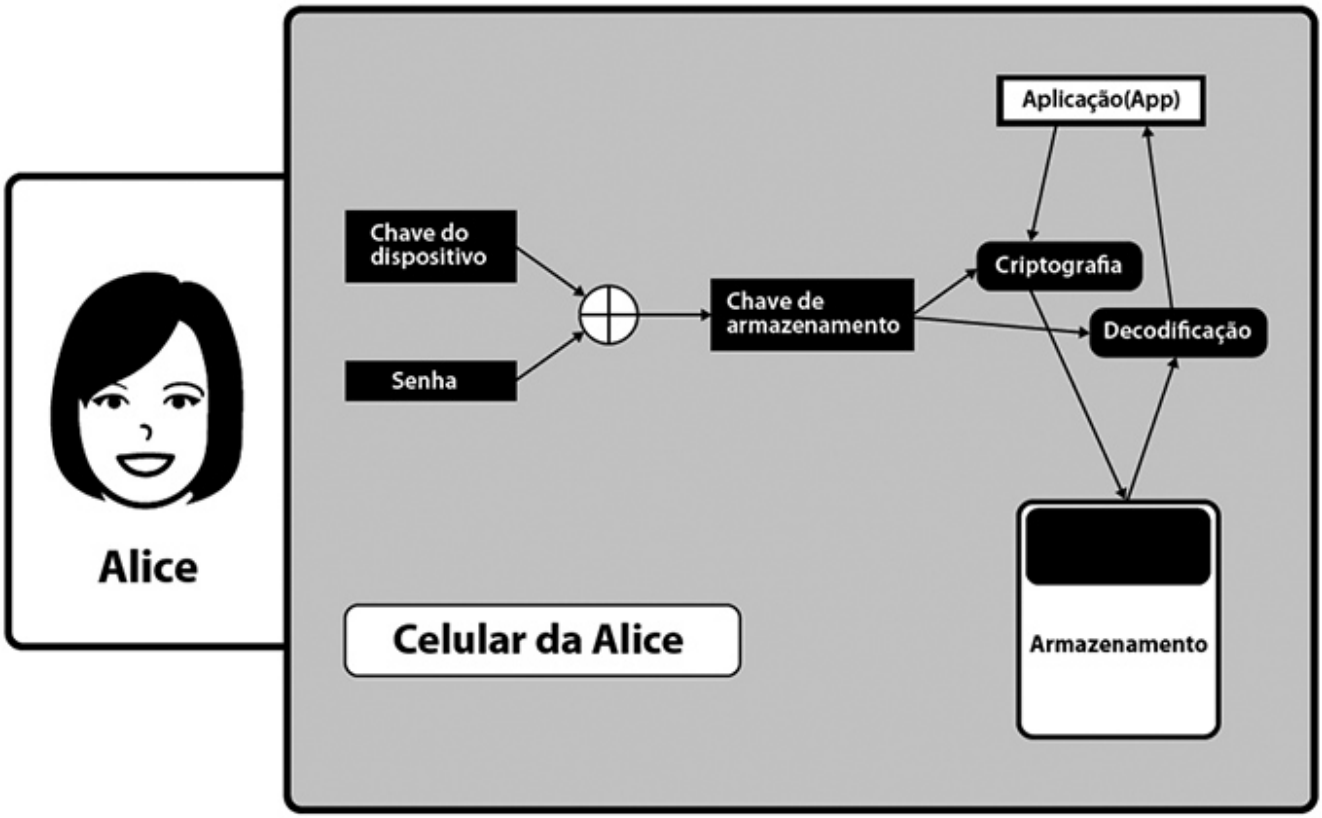

FIGURA 1

A segurança dos dados do dispositivo depende basicamente duas chaves. O uso da chave do dispositivo garante que os dados podem ser decifrados apenas no aparelho específico de Alice – e o telefone normalmente tem proteção interna forte, de modo que é muito difícil para uma pessoa maliciosa extrair a chave do dispositivo. O uso da senha de Alice para gerar a chave de armazenagem assegura que Alice deve executar uma ação explícita – digitar sua senha – para permitir a decodificação ou modificação autorizada de dados.

Quando Alice bloqueia o telefone, ou quando o telefone ficar sem energia, a senha de Alice e a chave de armazenagem são apagadas do telefone. Neste estado o telefone já não contém a chave que permite que a informação nele contida seja recuperada ou modificada sem detecção. Decodificação e adulteração não são possíveis porque a chave de armazenagem não está presente. A chave de armazenagem não pode ser recriada porque a senha de Alice não está presente. Só com esta senha pode ser possível novamente a decodificação e modificação autorizada dos dados.

Mas essas proteções serão inúteis se um elemento malicioso puder obter a senha de Alice. Na prática, os usuários costumam escolher senhas que são de fácil adivinhação por um computador que pode fazer um grande número de tentativas muito rapidamente. Um sistema seguro deve ter defesas adicionais contra quebra de senha. Normalmente, isso envolve fazer com que o sistema imponha um atraso depois de uma tentativa fracassada de inserir o código e pare de aceitar tentativas de quebra de senha completamente após um determinado número de tentativas. Isso tornará inviável a quebra do código, a menos que Alice escolha uma senha excepcionalmente fraca, como 0000 ou a data de seu aniversário.

Comunicação criptografada

A comunicação criptografada funciona de forma diferente. Suponha que dois parceiros, Alice e Beto, querem trocar uma série de mensagens. Eles querem usar criptografia para proteger a confidencialidade das mensagens (para que ninguém mais possa entender o conteúdo das mensagens) e a integridade das mesmas (de modo que ninguém possa alterar mensagens sem detecção); e eles querem usar a criptografia para autenticar-se mutuamente (de modo que ambos saibam que não estão comunicando-se com um impostor).

Para a comunicação criptografada, cada um dos parceiros gera uma chave de identidade de longo prazo, que será

mantida em segredo. Um parceiro pode usar sua chave de identidade de longo prazo para provar sua identidade para outros parceiros.

Tal como ilustrado **abaixo**, uma comunicação criptografada opera em duas fases. Na primeira fase, conhecida no jargão técnico como handshake (aperto de mão), os dois parceiros trocam uma série de mensagens especialmente criadas. Se tudo correr bem, o handshake inicial tem dois resultados: cada parceiro recebe a confirmação da identidade do outro (ou seja, que o outro parceiro é realmente Alice ou Beto, e não um impostor), e Alice e Beto concordam em usar uma chave de sessão secreta que é conhecida apenas pelos dois. Os detalhes de como o processo de handshake inicial obtém estes resultados são complexos, mas não diretamente relevantes para a discussão de políticas.

Tendo completado o handshake inicial, Alice e Beto podem então trocar mensagens em segurança. Se Alice quer enviar uma mensagem a Beto, ela criptografa a mensagem com a chave de sessão e envia os dados criptografados resultantes a Beto. Beto usa a chave de sessão para decifrar a mensagem e assim recuperar a mensagem original e confirmar que não houve adulteração enquanto a mensagem esteve em trânsito.

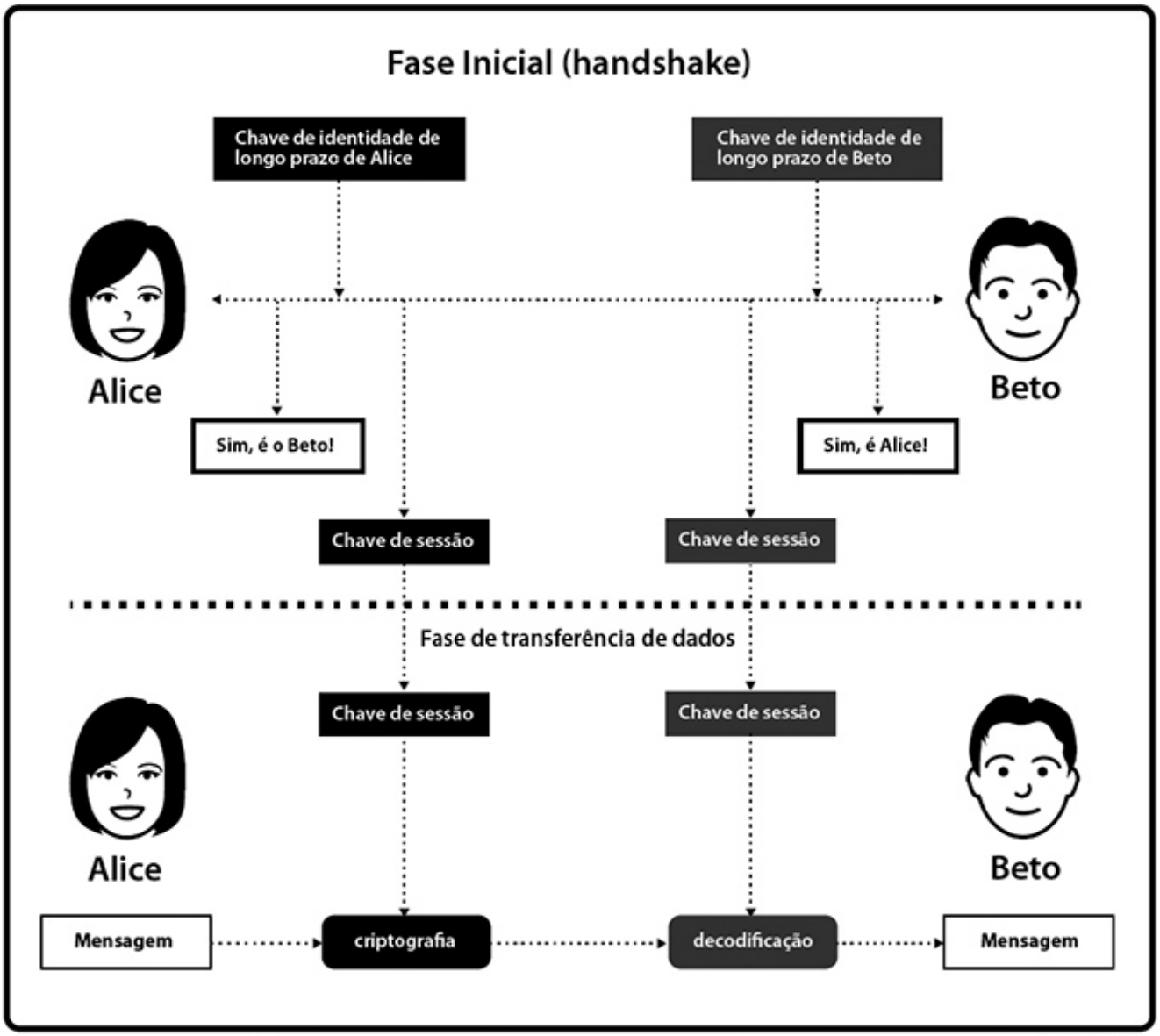

FIGURA 2

Os sistemas de comunicação criptografada usam diferentes chaves criptográficas para diferentes fins. Cada um dos parceiros na comunicação tem uma chave de identidade de longo prazo, que é usado na fase inicial de handshake para autenticar a identidade do parceiro e negociar uma chave de sessão inicial. Se um elemento malicioso obtiver a chave de identidade de longo prazo de Alice, isso permitirá que esse elemento possa passar-se por Alice no futuro, mas que não permitirá decodificação ou adulteração de mensagens enviadas em sessões

seguras.

As chaves de sessão são utilizados para proteger as mensagens individuais que transitam entre dois parceiros. Se um elemento malicioso obtém uma chave de sessão, ele pode decodificar ou adulterar mensagens criptografadas com a chave de sessão. Os sistemas comumente trocam as chaves de sessão com frequência, para limitar os danos que poderiam resultar da perda de uma chave de sessão específica. Muitos sistemas geram uma nova chave de sessão para cada troca de mensagem, de modo que a perda de uma chave de sessão compromete apenas a respectiva mensagem. Uma vez que uma nova chave de sessão é gerada, todas as cópias das chaves de sessão anteriores são apagadas.

Na comunicação criptografada, as consequências de um elemento malicioso ter acesso a uma chave secreta vai depender de qual chave é comprometida. Um elemento malicioso que de alguma forma tenha acesso à chave de identidade de longo prazo de um usuário será capaz de passar-se por ele no futuro, mas não será capaz de decifrar as mensagens antigas. Um elemento malicioso que de alguma forma tenha acesso a uma chave de sessão será capaz de decifrar todas as mensagens que foram criptografados com essa chave de sessão, mas não será capaz de decifrar as mensagens enviadas com chaves de sessão anteriores ou posteriores, e não será capaz de passar-se por outra pessoa. A utilização de várias chaves e a prática de mudar as chaves de sessão com frequência limitam o dano resultante do possível comprometimento de qualquer das chaves.

Discussão: tendências comuns em práticas de criptografia modernas

Vários tópicos são comuns aos projetos atuais de aplicações de criptografia:

- A criptografia faz mais do que apenas manter segredos. Além de proteger a confidencialidade dos dados, protege a integridade, permitindo a detecção de qualquer tentativa não autorizada de mexer com os mesmos. Em algumas aplicações, a integridade é a principal razão para a utilização de criptografia.
- A comunicação criptografada faz mais do que apenas proteger a própria mensagem de decodificação ou adulteração. Ela também permite que os dois parceiros que estão se comunicando autentiquem suas identidades mutuamente. Em algumas aplicações, a autenticação da identidade e da fonte de mensagens é a principal razão para o uso de criptografia.
- A informação é protegida muitas vezes pela destruição de todas as cópias da chave usada para criptografá-la. Na armazenagem criptografada, a chave de armazenagem e senha de Alice são apagadas quando o dispositivo está bloqueado, garantindo assim que um elemento malicioso com acesso ao dispositivo bloqueado não possa decodificar os dados. Na comunicação criptografada, a chave de sessão usada para criptografar uma mensagem é apagada logo que a mensagem foi decodificada pelo destinatário, garantindo assim que um elemento malicioso que registrou os dados criptografados não terá como obter a chave que permitiria decifrá-la.

--

2. Esta senha pode ser gerada por um sensor de impressão digital, uma sequência numérica ou outros métodos [n.ed.].

Categoria:

- poliTICs 25