Análise da aplicação da tecnologia FIDO (Fast Identity Online) como segundo fator de autenticação de usuários

Leone Vinícius de Oliveira , Marco A. A. Henriques
{l1178685@dca.unicamp.br, maah@unicamp.br}

Departamento de Engenharia de Computação e Automação (DCA)
Faculdade de Engenharia Elétrica e de Computação (FEEC)
Universidade Estadual de Campinas (Unicamp)
Campinas, SP, Brasil

Resumo – A necessidade de corrigir as falhas ao autenticar usuários é uma urgência cada vez maior conforme o uso da internet aumenta. Métodos como login e senha, biometria e envio de senhas únicas já são amplamente utilizadas, mas possuem falhas na segurança em determinados contextos. Com a intenção de resolver esse problema, a *FIDO Alliance* desenvolveu o sistema de autenticação FIDO (Fast Identity Online). Esse método utiliza um par de chaves pública e privada, onde a chave pública é distribuída aos clientes e a privada é armazenada no autenticador, que pode ser o smartphone (com NFC ou Bluetooth) ou um token USB. A principal diferença da FIDO com os outros métodos é que a autenticação acontece apenas na presença de um dispositivo que guarda chaves criptográficas de forma segura, impedindo ataques como *phishing* (obtenção de senhas por meio da indução do usuário ao erro) e *man in the middle* (interceptação de comunicação e alteração de mensagens), já que o atacante precisaria ter acesso físico ao dispositivo para poder se passar por um usuário legítimo. Neste trabalho estamos avaliando as diferentes formas de emprego dessa tecnologia e os custos, vantagens e desvantagens de cada uma delas, de maneira a identificar possíveis aplicações no contexto de autenticação em sistemas sensíveis na universidade.

Palavras-chave – chaves criptográficas, autenticação, *Fast Identity Online*, autenticação de múltiplos fatores

1. Introdução

A constante evolução da internet demanda a agilização e a garanta de segurança ao autenticar usuários. O método mais utilizado para isso ainda é com a verificação através de um *login* e de uma senha. Este método tem sérios problemas de segurança e de usabilidade, uma vez que o usuário pode esquecer da sua senha, criar várias contas com a mesma senha, sofrer ataques como *phishing* (obtenção de senhas por meio da indução do usuário ao erro) e *man in the middle* (interceptação de comunicação e alteração de mensagens), entre outras inconveniências.

Outros métodos de autenticação surgiram com a intuição de solucionar essas falhas. A utilização da biometria para autenticar os usuários soluciona alguns dos problemas do método anterior, mas o custo para sua implementação é alto e tem um menor alcance aos usuários. Outro método de autenticação foi através do uso de senhas únicas, que poderiam ser enviadas por SMS, email ou aplicativos específicos com essa funcionalidade, como *Google Authenticator*. Estes, por sua vez, podem ter problemas ao transmitir a senha única e podem gerar dificuldades ao usuário para a compreensão de como utilizar corretamente. Considerando todos esses pontos, a *FIDO Alliance* desenvolveu protocolos para o método de autenticação FIDO(*Fast Identity Online*).

2. Chaves criptográficas

As chaves criptográficas são um conjunto de informações (bits, números, letras, etc.) que representam a identidade de um usuário. Com elas, é possível codificar e decodificar mensagens. Existem as chaves simétricas, onde a chave para codificar é a mesma para decodificar, e as assimétricas, que são chaves diferentes para codificar e decodificar uma mesma mensagem.

O método de criptografia que utiliza chaves assimétricas também é chamado de criptografia por chave pública. Nele a chave privada deve ser armazenada com sigilo e somente o usuário dono deve ter acesso à ela. Já a pública pode ser distribuída aos serviços que a requisitarem para autenticar o usuário que possui seu par privado. Uma mensagem criptografada por uma chave privada só pode ser decodificada pela chave pública que compõe o seu par, e vice-versa.

Utiliza-se o método de criptografia por chave pública para prover sigilo à mensagem que deve ser enviada e para garantir sua autoria. Ao criptografar a mensagem utilizando a chave pública, apenas o usuário que possuir sua chave privada par tem a capacidade de decodificá-la, garantindo assim o sigilo. Já quando a mensagem é criptografada pela chave privada, qualquer um que possuir a chave pública par pode ler a mensagem, mas o destinatário saberá que somente o dono da chave privada par foi capaz de escrever aquela mensagem codificada.

3. O protocolo SSH

O protocolo SSH é um conjunto de regras que determina diretrizes de como conectar dois computadores de forma segura utilizando a criptografia com um par de chaves pública-privada. Para configurar a criptografia como SSH, três requisitos devem ser alcançados: sigilo, autenticação da origem e integridade da mensagem. Os dois primeiros requisitos já caracterizam uma comunicação por par de chaves assimétricas. O terceiro requisito define que a mensagem deve ser entregue sem sofrer nenhuma alteração.

Neste protocolo, o computador local requisita uma conexão com a máquina remota desejada, que já deve ter um *software* com o protocolo SSH. Então esta máquina, que é o servidor SSH, envia um desafio para o computador local, que deve resolvê-lo e confirmar sua identidade criptografando a mensagem com a chave privada. O servidor SSH verifica então a resposta utilizando a chave pública par para descriptografar a mensagem e então permitir o acesso do usuário. Toda essa conversa entre os computadores acontece de forma que o usuário não necessite realizar nenhuma ação [1].

4. *FIDO Alliance*

A *FIDO Alliance*, consórcio de empresas que pretende mudar a forma como a autenticação online é feita, desenvolveu três conjuntos de especificações e regras: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) e FIDO2. Juntos, estes protocolos têm o objetivo de mostrar como alcançar uma comunicação mais simples, mais segura e mais robusta para o usuário.

4.1. FIDO U2F

Esse conjunto de protocolo tem como objetivo assegurar a segurança ao utilizar o protocolo FIDO como segundo fator de autenticação. Para isso, um dispositivo que seja compatível com os protocolos FIDO deve ser utilizado, que chamaremos de dispositivo U2F. Ele pode ser um token USB ou um smartphone que tenha como se comunicar com as tecnologias Bluetooth ou NFC. Quando o usuário se cadastra em um serviço, ele deve conectar o dispositivo U2F, que gera o par de chaves público-privado, armazenando localmente a chave privada e registrando a chave pública par no servidor do serviço requisitado. Quando o usuário se identificar novamente, o serviço o identifica através do dispositivo U2F. Esse conjunto de protocolos também definem qual a criptografia utilizada e como a comunicação com o dispositivo será realizada [2]. Ao utilizar um dispositivo U2F, é garantido que o usuário está fisicamente em posse do dispositivo, impedindo que alguém que possua seus *login* e senha possa se passar por ele.

4.2. FIDO UAF

Esse conjunto de protocolos tem como objetivo fornecer um mecanismo de autenticação unificado que substituam as senhas. Os protocolos FIDO UAF determinam como devem ser feitos o registro, a autenticação, a confirmação da transação e a exclusão de cadastro de usuários [3].

4.3. FIDO2

FIDO2 é a junção de dois conjuntos de protocolos: *Client-to-Authenticator Protocols* (CTAP) e *W3C Web Authentication* (WebAuthn). Elses se complementam para garantir a segurança na autenticação em aplicativos web. O CTAP foi desenvolvido pela *FIDO Alliance* e tem como objetivo determinar como a interface autenticadora deve receber e passar os parâmetros e desafios necessários para a autenticação, como as mensagens devem ser criptografadas e como o meio de transporte assegura a integridade das mensagens enviadas [4].

5. O protocolo FIDO

O protocolo FIDO determina como devem ser feitos o registro e a autenticação do usuário utilizando a criptografia por um par de chaves pública-privada. Tanto no registro quanto na autenticação, são determinadas as especificações entre três sujeitos: o Autenticador FIDO, que pode ser um token USB ou um smartphone com NFC ou Bluetooth; o cliente FIDO, que é o navegador que requisita o cadastro; e o servidor FIDO, que verifica se a autenticação é bem sucedida ou não.

5.1. Registro

Quando o cliente pede para se cadastrar no servidor FIDO, ele retorna ao cliente informações da conta, um desafio e informações opcionais de segurança que ajudam a evitar ataques. No pacote de autenticação, o cliente determina qual vai ser o método de autenticação e adiciona também informações de segurança necessárias para o autenticador. O cliente então envia esse pacote ao autenticador para ele verificar o usuário, criar um par de chaves pública e privada e a credencial, e retornar ao cliente um pacote com a sua credencial para aquele serviço específico, a chave pública e informações sobre o sucesso ou a falha na autenticação do usuário. O cliente envia esse pacote ao servidor, que armazena a chave pública e a credencial do cliente. Vale notar que o usuário apenas teve que se autenticar localmente com o autenticador, sem a necessidade dele enviar nenhuma informação online [5].

5.2. Autenticação

Ao desejar acessar o serviço novamente, o usuário se identifica e então é realizada a autenticação. Nesse processo, o servidor FIDO envia uma mensagem ao cliente com um desafio e dados opcionais de segurança. O cliente então cria um pacote com os dados do cliente e com o desafio, e o envia para o autenticador. Este então verifica o usuário e depois busca a chave privada para resolver o desafio, verificando também se apenas um acesso foi realizado, aumentando assim a segurança na comunicação. Após isso, o autenticador retorna ao cliente um pacote onde indica se a autenticação do usuário foi bem sucedida e, caso positivo, envia a resposta do desafio. O cliente repassa o pacote ao servidor, que busca a chave pública da credencial do cliente no banco de dados e verifica a resposta do desafio. Caso a resposta esteja correta, o usuário estará autenticado. Nota-se que mais uma vez o usuário precisou se autenticar apenas localmente com o autenticador [5].

6. Conclusões e próximos passos

Através de um exemplo básico de funcionamento, foi possível perceber a praticidade da autenticação. Após se identificar, o usuário deve realizar uma pequena ação requisitada pelo dispositivo autenticador, que pode ser um toque no sensor ou apertar um botão. Como todo o processo de autenticação acontece apenas localmente, com o cliente enviando ao servidor FIDO informações de sucesso ou de falha, foi concluído que a segurança é maior utilizando os protocolos FIDO, quando comparado com outros métodos de autenticação. Apesar disso, esse método de implementação ainda não está amplamente utilizado por três principais fatores: (i) nem todos os dispositivos são compatíveis com a tecnologia FIDO; (ii) uma dependência aos dispositivos autenticadores, que leva ao investimento para a aquisição de tokens USB ou às inconveniências de garantir que o usuário esteja com um smartphone compatível sempre com a bateria carregada; (iii) e explicar aos usuários o passo adicional para a autenticação, que, mesmo sendo mais prático que verificar uma senha única em um aplicativo próprio ou em outros canais, ainda é existente e menos robusto que a simples identificação por *login* e senha.

A continuação deste trabalho tem como objetivo mostrar como a tecnologia FIDO pode substituir os métodos tradicionais de segundo fator de autenticação, utilizando como exemplo a comunidade existente na Unicamp, onde o público alvo é diversificado. Deve ocorrer primeiramente uma identificação do método já existente e determinar suas dificuldades. Após isso deve-se determinar como realizar a substituição e verificar se ela é plausível ou não. Por fim deve-se justificar os resultados obtidos.

7. Agradecimentos

Eu tenho uma enorme gratidão ao meu professor orientador Marco Amaral Henrique, que me passou todas as principais orientações e direcionamentos para que a pesquisa pudesse ser concluída. Além disso, agradeço sua paciência e didática para me passar seus conhecimentos fundamentais para a melhor compreensão dos resultados obtidos. Agradeço também meus pais e amigos, Lilian Margareth da Silva Oliveira, Jânio José de Oliveira e João Vitor Tobias da Silva, que sempre se colocaram a disposição para apoiar minha pesquisa e não deixar faltar motivação para concluí-la.

Referências

[1] D. J. Barrett and R. E. Silverman, *SSH, the Secure Shell: The definitive guide*. O'Reilly and Associates, 2001.

[2] D. Balfanz, S. Srinivas, and E. Tiffany, "Universal 2nd factor (u2f) overview," *FIDO Alliance*, 2014.

[3] R. Lindemann and E. Tiffany, "Fido uaf protocol specification," *FIDO Alliance*, 2020.

[4] J. Bradley *et al.*, "Client to authenticator protocol (ctap)," *FIDO Alliance*, 2022.

[5] G. Prado, M. Landi, and A. Shikiar, "Introdução à autenticação fido," 2019.