ESQUEMAS SOBRE ESQUEMAS DE AUTENTICAÇÃO SEM SENHA

Palavras-Chave: SEGURANÇA, SENHAS, FIDO

Autores(as):
Leonardo da Silva Giovanelli de Santana, Engenharia de Computação – UNICAMP
Prof(ª). Dr(ª). MARCO AURELIO AMARAL HENRIQUES (orientador(a)), FEEC/DCA - UNICAMP

INTRODUÇÃO:

Desde o início da internet, a criação e o armazenamento de senhas tornaram-se tarefas rotineiras para os usuários. Para um usuário comum, utilizar uma senha padrão e fácil de lembrar parece suficiente para garantir segurança, desde que não seja compartilhada com ninguém. No entanto, sob a perspectiva da segurança da informação, o cenário é bem diferente. Com o avanço das capacidades de processamento dos computadores, a segurança da informação tornou-se uma questão cada vez mais crítica. Senhas que protegem dados pessoais e sensíveis, como informações bancárias, endereços, locais e documentos armazenados em nuvens, podem ser comprometidas rapidamente se não forem suficientemente fortes e se não utilizarem algoritmos de criptografia robustos, sendo vítimas de ataques hackers e vazamentos.

Dessa forma, com o aumento constante do número de sites e aplicativos que requerem cadastro de dados e senhas, a falta de segurança associada a essas senhas torna-se ainda mais preocupante. Para resolver esse problema, surge a tecnologia de autenticação sem senha, desenvolvida após estudos com as maiores empresas tecnológicas do mundo: a tecnologia FIDO. Esta pesquisa teve como objetivo entender o funcionamento dos três principais protocolos FIDO existentes — UAF, U2F e FIDO2 —, bem como seus principais cenários de aplicação, dificuldades e benefícios.

METODOLOGIA:

Para cumprir o objetivo deste projeto, primeiramente foram estudados os princípios da criptografia e seus diversos tipos de algoritmos criptográficos básicos, com destaque para os algoritmos de criptografia de chave pública. Especificamente, o esquema de troca de chaves de Diffie-Hellman é fundamental para a tecnologia FIDO. Segundo Stallings (2014) [1], esse algoritmo permite a geração de um par de chaves criptográficas (uma pública e uma privada), usadas para assinar mensagens trocadas em comunicações. Nesse esquema, essas chaves podem ser geradas utilizando como base outros métodos criptográficos, como o RSA e ECDSA (Criptografia por Curvas

Elípticas, método muito utilizado pela tecnologia FIDO em seus protocolos, aliados ao esquema de troca de chaves). Além disso, alternativas métodos de autenticação comuns, como autenticação em 2 fatores, também foram estudados, para efetiva comparação com os métodos de autenticação sem senha. Em sequência, foram estudados os protocolos FIDO, que serão apresentados a seguir.

A tecnologia FIDO (Fast Identity Online), criada pela FIDO Alliance, possui três principais protocolos, o UAF (Universal Authentication Framework), o U2F (Universal 2nd Factor) e o FIDO2. Segundo Angelogianni, et al. (2021) [2], o principal objetivo dessa tecnologia é o uso de um dispositivo autenticador por parte do usuário sem ter contato direto com a chave de segurança, a qual, em seu contexto, fará o papel de senha, além da autenticação do usuário fisicamente neste dispositivo. Esse dispositivo autenticador será o responsável por gerar e armazenar as chaves de segurança, que serão utilizadas para autenticação via assinatura de mensagens junto ao servidor do site/aplicação em que se está tentando realizar a autenticação. Tal dispositivo pode ser um dispositivo específico para geração e armazenamento dessas chaves geradas, eles são chamados de Chaves de Segurança (ou Tokens FIDO), os quais são comercializados por algumas empresas de tecnologia e utilizados como meio de segurança em tantas outras, porém, no protocolo mais novo, o FIDO2, o papel desempenhado por estes dispositivos pode ser feito por Smartphones e computadores atuais. O processo de autenticação física do usuário varia conforme o protocolo e o dispositivo utilizado. Pode ser realizado por meio de pressionar botões na chave de segurança, tocar na chave ou utilizar biometria. A biometria é suportada principalmente em smartphones ou tokens mais recentes, permitindo o uso de impressões digitais, reconhecimento facial ou de íris para validação da identidade do usuário.

Além disso, o principal fator relevante nesses métodos, é que o tamanho de cada chave do par é muito superior (geralmente 120 bits ou superior)[6] ao tamanho de senhas padrões em bits (sendo estes geralmente 8 caracteres, que equivalem a 48 a 64 bits), tendo ainda mais segurança devido aos algoritmos associados, como ECDSA e RSA em contrapartida com as senhas convencionais, que muitas vezes não tem.

PROTOCOLO FIDO UAF:

Conforme a documentação oficial da FIDO [3] e a Figura 1, o processo de autenticação FIDO inicia quando o usuário solicita autenticação com seus dados de login através de um Cliente FIDO no dispositivo. Este cliente se comunica com o servidor FIDO, enviando os dados e a solicitação de autenticação. O servidor busca os dados do solicitante e a chave pública armazenada durante o registro, gerando um desafio que é assinado com essa chave pública.

O servidor envia de volta ao aplicativo as políticas de autenticação, incluindo os tipos de autenticadores permitidos e a necessidade de verificação do usuário. O Cliente FIDO recebe essas informações e as envia ao autenticador FIDO no dispositivo, que busca o registro do usuário e inicia a verificação da presença do usuário, seja por PINs ou biometria.

Após a verificação bem-sucedida, o autenticador resolve e assina o desafio com a chave privada, enviando-o de volta ao Cliente FIDO, que repassa os dados ao servidor. O servidor verifica a assinatura e o desafio usando a chave pública. Se a verificação for bem-sucedida, o usuário é autenticado.

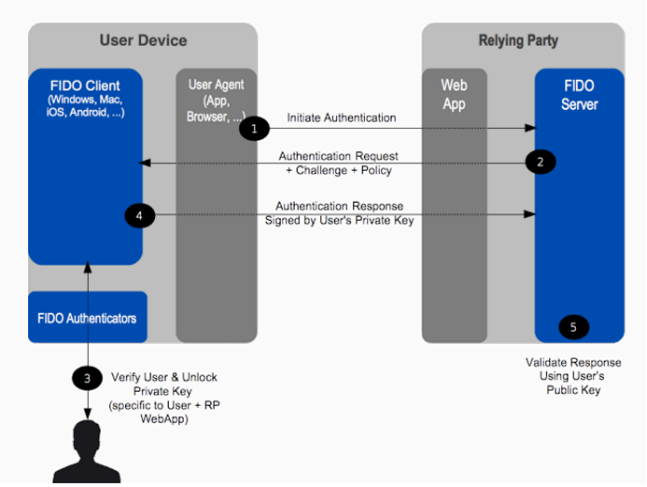

Figura 1: Fluxo de autenticação UAF (fonte: https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/FIDO-UAF-COMPLETE-v1.0-ps-20141208.pdf)

PROTOCOLO FIDO U2F:

O FIDO U2F foi desenvolvido como o protocolo seguinte ao UAF. Segundo Angelogianni et al. (2021) [2], a principal diferença do U2F em relação ao UAF é que ele não elimina o uso de senhas, atuando como um segundo fator de autenticação para garantir maior segurança ao método tradicional. O principal dispositivo autenticador nesse protocolo são as chaves de segurança externas. O usuário ainda precisa gerar e usar uma senha tradicional ao se registrar ou autenticar, mas após a utilização da senha, ocorre um segundo processo de autenticação sem o uso de senhas, utilizando o protocolo e o autenticador de maneira semelhante ao UAF.

Conforme a Figura 2, o fluxo de autenticação do U2F é semelhante ao do UAF, incluindo tipos de dados transmitidos, com algumas adições como contadores de tempo de execução (para limitar o tempo de comunicação e evitar possíveis ataques) e hashes para garantir a segurança do processo. De forma que a principal diferença é que, antes do início do processo, ocorre o login via senha padrão.

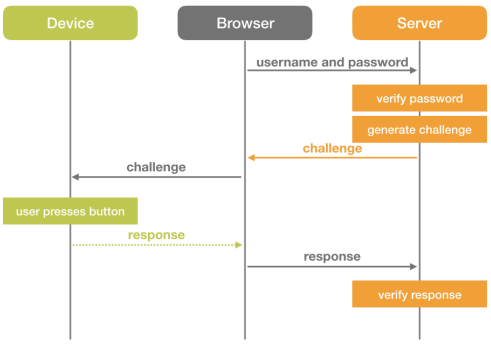

Figura 2: Fluxo de registro do U2F(fonte: https://github.com/makerdiary/nrf52-u2f)

PROTOCOLO FIDO2:

O mais recente dos protocolos é o FIDO2, que foi desenvolvido para facilitar e popularizar a autenticação sem senhas. De acordo com a FIDO Alliance (2018) [6], seus principais diferenciais incluem uma maior variedade de dispositivos externos que podem atuar como autenticadores, como smartphones, smartwatches e chaves de segurança. Além disso, o FIDO2 utiliza tecnologias wireless de curta distância, como NFC e Bluetooth, para comunicação entre dispositivos (por exemplo, entre PCs e smartphones). Esses novos dispositivos autenticadores oferecem maior segurança, permitindo diversos tipos de autenticação do usuário, como biometria facial, de íris e digital, garantindo que a operação só seja realizada pelo legítimo dono do dispositivo.

O FIDO2 também apresenta novas especificações para maior compatibilidade, como a API WebAuthn, desenvolvida pela W3C em JavaScript para navegadores e sistemas atuais, facilitando o uso da autenticação FIDO, e o CTAP2 (Client-to-Authenticator Protocol 2), que define protocolos para a comunicação entre o autenticador e o cliente FIDO, simplificando o uso dos dispositivos externos como autenticadores.

Conforme a Figura 3, o fluxo de registro e autenticação do FIDO2 é semelhante aos protocolos anteriores, com a WebAuthn e o CTAP2 sendo os principais diferenciais. O restante do fluxo de comunicação e das informações transmitidas é similar aos outros protocolos, mas com a melhoria significativa de usar diferentes tipos de hashes nas mensagens para garantir a confiabilidade e integridade da comunicação entre servidor e cliente, uma melhoria em relação ao UAF que suporta apenas um tipo de hash [4][6].

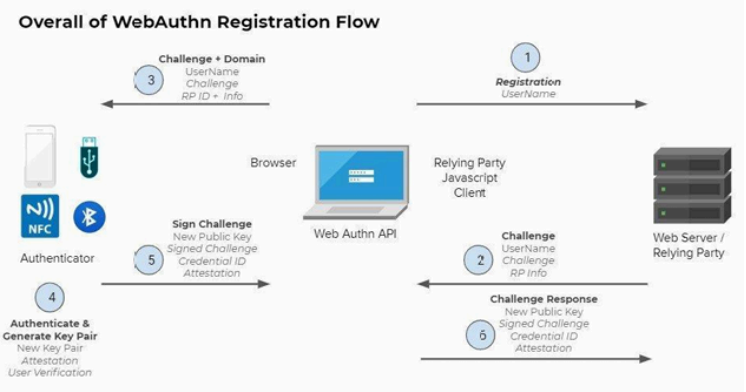

Figura 3:Fluxo de registro do FIDO2(fonte: https://how-to.vertx.io/fido2-webauthn-howto/)

Assim, além dos protocolos, foi feito também um estudo dos preços das chaves de segurança no mercado brasileiro, onde foi possível observar que a loja com maior variedades e melhores preços na época da pesquisa, foi a loja Amazon, na qual foram encontrados apenas 4 modelos de chaves com poucas funcionalidades (sem opções biométricas como uso de digitais e bluetooth), todos da mesma fabricante: A YUBICO. De forma que seus preços variavam de 250 a 700 reais.

RESULTADOS E DISCUSSÃO:

O uso da tecnologia FIDO como alternativa para problemas relacionados a senhas é promissor, oferecendo maior segurança para os dados do usuário. O FIDO2, em particular, é relevante para sistemas de grande escala devido ao suporte a vários dispositivos autenticadores, como smartphones, e sua compatibilidade com sistemas web atuais. Ele proporciona uma segurança superior aos sistemas tradicionais, que geralmente usam senhas de 8 a 16 caracteres, comparadas aos pares de chaves de mais de 120 bits oferecidos pelo FIDO2. A segurança do FIDO2 é acentuada pela criptografia de alto nível, como o ECDSA, que protege contra ataques de força bruta e criptoanálise, diferentemente das senhas tradicionais que podem ser baseadas em informações fáceis de lembrar. O FIDO2 também se destaca em relação ao método de autenticação de dois fatores convencional, que é mais suscetível a ataques de rede e phishing, enquanto o FIDO2 evita esses problemas mantendo o autenticador e a chave privada fora da rede.

Como resultado principal desta pesquisa, temos que entre os protocolos FIDO, o FIDO2 se sobressai ao UAF e ao U2F devido à sua atualidade e versatilidade, combinando o uso de dispositivos autenticadores variados e sistemas diversos. Sua capacidade de comunicação sem fio de baixa distância e a integração com dispositivos pessoais tornam o FIDO2 uma solução atraente tanto para empresas quanto para usuários, proporcionando segurança reforçada e facilidade de implementação em larga escala.

CONCLUSÕES:

Durante a pesquisa, foram analisados artigos, livros e documentações sobre segurança da informação e criptografia, compreendendo a importância dos problemas relacionados às senhas e seu impacto na segurança digital. A tecnologia FIDO, com seus sistemas de autenticação sem senha, oferece uma alternativa segura ao uso de senhas, utilizando algoritmos como ECDSA, hashes e evitando contato direto das chaves com a rede. O FIDO2, em particular, é versátil, fácil de adaptar e tem potencial para crescimento e popularização. Foi constatado que a adoção do FIDO2 traz benefícios significativos, oferecendo maior segurança em comparação às senhas tradicionais e autenticações de dois fatores. Embora os protocolos FIDO anteriores tenham sido avanços importantes, o FIDO2 apresenta funcionalidades e especificações muito mais atualizadas.

BIBLIOGRAFIA

[1] Stallings, William. Criptografia e segurança de redes: princípios e práticas. 6ª edição. São Paulo: Pearson Education do Brasil, 2014.

[2] Anna Angelogianni, Ilias Politis, Christos Xenakis. How many FIDO protocols are needed? Surveying the design, security and market perspectives, 2021.

[3] FIDO Alliance. FIDO Specifications. <<https://fidoalliance.org/specs/>(acesso em 04/02/2024).

[4] FIDO Alliance . 2014. FIDO UAF specification. https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/FIDO-UAF-COMPLETE-v1.0-ps-20141208.pdf).

[5] FIDO Alliance. 2017. FIDO U2F specification.
<https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/FIDO-U2F-COMPLETE-v1.2-ps-20170411.pdf> (acessado em 22/02/2024).

[6] FIDO Alliance. 2018. FIDO2 specification- Client to Authenticator Protocol CTAP. FIDO-COMPLETE-v2.0-id-20180227.