INSE 6150 – Security Evaluation Methodologies

Usability, Deployability, and Security Analysis of FIDO2 Protocol

PriyaDharshan Muthu - 40196410
Pavithran Koteeswaran - 40196178
Vishal SK - 40193983

Introduction:

It is widely acknowledged that traditional username and password authentication mechanisms are no longer enough to ensure online security, as they are vulnerable to various attacks such as phishing and credential stuffing. Phishing assaults have significantly increased since the COVID-19 outbreak, which emphasizes the need for alternate security-enhancing measures. Researchers have come up with a variety of alternative procedures throughout the years, but most of them haven't gained much popularity because of the compromise between usability and security. But FIDO2 stands out because it offers a high level of security while also being simple to use and deploy. FIDO2 is a protocol developed by the FIDO alliance, an industry association committed to providing a more user-friendly and secure alternative to password-based web logins.

FIDO2 offers a more convenient and safe method of authentication than password-based authentication. Key flaws in password-based authentication, such as weak or reused passwords, frequently result in online data breaches. Despite efforts by researchers and practitioners to provide password-free alternative authentication methods, only a small number of these methods have found widespread use. For instance, even though single sign-on (SSO) federated identity systems like SSO make it easier to remember multiple passwords and are more secure by limiting password reuse, their usage outside organizational contexts is still limited in part because of consumers' privacy concerns. Similar to password managers, although they have become more popular as a result of security experts' advice, adoption rates have remained low. For password-less authentication, FIDO2 provides a standardized method for websites to employ hardware tokens or gadgets like mobile phones and security keys. FIDO2 credentials are a reliable substitute for conventional password authentication since they cannot be stolen through phishing attempts and are immune to database hacks and replay assaults. Most browsers and operating systems, including Android and Windows, support the open web authentication standard FIDO2.

The FIDO2 framework offers more benefits compared to other alternative mechanisms. It not only provides a high level of security but also offers a better user experience, lower costs, and scalability. Moreover, FIDO2 is compatible with existing systems, making it easier to adopt and implement.

FIDO2:[1]

FIDO2 is a standard that uses modern authentication technology to enable strong password-less authentication. A joint project of the FIDO Alliance and the W3C, FIDO2 combines the Client to Authenticator Protocol (CTAP) with the Web Authentication API (WebAuthn).

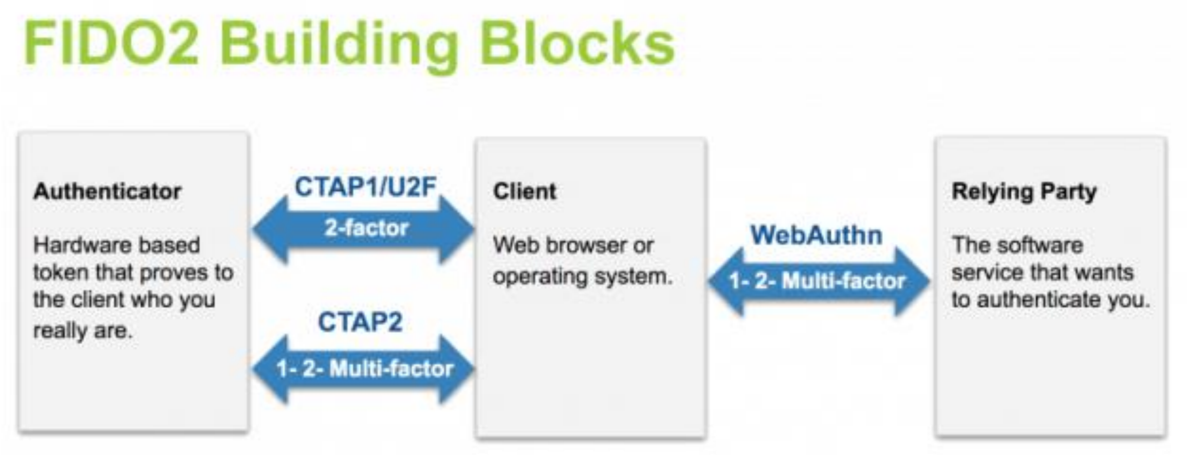
Examples of FIDO 2:

1. Biometric-capable devices and platform authenticators: These are built-in authenticators that require a biometric, PIN, or passcode. Examples include Apple's Touch ID and Face ID, Windows Hello, and Android fingerprint and face recognition.
2. Roaming authenticators or security keys: FIDO2-capable hardware tokens use USB, NFC, or BLE to communicate user verification via biometrics or PIN.

FIDO2 Framework = WebAuthn + CTAP2, and there are a few options for FIDO2-specific authentication methods. Passwordless authenticators can also come in the form of mobile applications, like Duo Mobile.

FIDO2 Architecture:[2]

With WebAuthn, servers can integrate with authenticators such as the YubiKey, a USB token, a smartphone, Apple's Touch ID, and Windows Hello. The server stores the user's public key and generates challenges for the authenticator to sign. The authenticator stores the user's private key and signs the challenge using it. This way, the server can verify that the user owns the private key without actually knowing it. WebAuthn provides a secure and user-friendly way to authenticate without passwords, using devices that users already have and trust.


FIDO2 Building Blocks
Authenticator
Hardware based token that proves to the client who you really are.
CTAP1/U2F
2-factor
CTAP2
1- 2- Multi-factor
Client
Web browser or operating system.
WebAuthn
1- 2- Multi-factor
Relying Party
The software service that wants to authenticate you.

Risk Mitigation:

The FIDO2 protocol introduces new components on both the end-user device and the server, and organizations considering FIDO2 must evaluate these components to ensure compatibility and security. The FIDO2 protocol eliminates the traditional password-based authentication method, but it requires that the authenticator on the user's device is pre-registered with FIDO. This can create risks if the user loses or switches their device, as they may not be able to access FIDO2-compliant services securely.

To mitigate this risk, organizations can use roaming or external authenticators that allow users to authenticate themselves with multiple devices. However, the diversity of authenticator devices can make it difficult to ensure a uniform degree of security and usability across all devices.

FIDO Certification can help users measure compliance and ensure interoperability among services that support FIDO specifications. However, it is important to note that FIDO specifications do not require the FIDO authenticator to be implemented within an embedded secure component. Therefore, users should consider the security of the generated keys when selecting a FIDO2 authenticator device. FIDO2 authenticators that are not physically isolated from the rest of the operating system may be vulnerable to sophisticated attacks, and users should ensure that their chosen authenticator is sufficiently secure. Technologies like TPM, Trusted Execution Module, and IOS Secure Enclave can help to isolate the FIDO authenticator from the rest of the operating system and provide additional security.

Advantages of FIDO2:

Some of the key benefits of FIDO2 comparing FIDO. FIDO2 provides several advantages over FIDO, including wider compatibility, support for multiple authentication methods, stronger phishing resistance, password-less authentication, and compliance with industry standards.

FIDO2 is designed to support password-less authentication, which means that users don't have to remember passwords. This makes the authentication process more convenient and user-friendly, while also improving security by reducing the risk of password-based attacks. FIDO, on the other hand, still requires users to remember a password in addition to using a security key.

FIDO2 is designed to comply with the WebAuthn and CTAP2 (Client to Authenticator Protocol 2) standards, which provide a more consistent and interoperable user experience. FIDO, on the other hand, is not based on any specific standard

STRIDE:

STRIDE analysis is a threat modeling technique used in software engineering and computer security to identify and mitigate potential threats to a system or application.

Spoofing:

The ability of an adversary to steal the identity of the FIDO key user can be used to evaluate this attribute. It is a perfect 2FA because users can't log in without the keys (unlike other 2FA techniques). Both FIDO protocols are more secure and spoofing-proof than SMS- and time-based 2FA methods because UAF uses smartphone features like biometric authentication and facial recognition for its security and U2F devices use biometric authentication for logging in. Individual authenticators with both UAF and U2F keys are indistinguishable during the manufacturing process, and the underlying cryptographic authentication keys are exclusive to each user and device combination.

Tampering:

The ability of an attacker to modify information in the FIDO authentication protocol can determine its security level. The FIDO authentication method can utilize hardware (U2F) or software (UAF) keys, with hardware keys having extra protection through features like the Trusted Platform Module (TPM). Hardware keys, such as Yubikeys, can safeguard sensitive information like private encryption keys and are not easily cloned or replaced. In contrast, software keys like the Authenticator app are theoretically more susceptible to cloning without user awareness.

Repudiation:

This characteristic can be assessed based on the ability to trace the originator of a transaction. FIDO authentication offers better non-repudiation compared to other password alternatives. The cryptographic authentication key is unique to the FIDO Authenticator, User, and Relying party. The FIDO metadata service contains information about the Authenticator certification status. Certified authenticators are required to implement a trusted path for all user/Authenticator interactions, depending on the certification level.

Information Disclosure:

When evaluating a protocol, information disclosure analysis can be categorized into Verifier Leak Resilience and Authenticator Leak Resilience. Verifier Leak Resilience measures how well the protocol resists data leaks from the user's perspective. With FIDO keys, cryptographic keys are stored at the device level for U2F, and data submitted for authentication is different every time, making it difficult for the verifier to accidentally reveal it to anyone. Authenticator Leak Resilience, on the other hand, focuses on preventing information leakage from the Authenticator's perspective.

Denial of service:

This characteristic can be evaluated by checking if attackers can manipulate registration information to prevent legitimate users from logging in during the next phase. In the UAF protocol, both the server and client supply nonces, while in U2F, only the server provides nonces. The use of nonces in the protocol ensures that any additional random information inserted by attackers as a Man-in-the-Middle (MiTM) attack is rejected.

Elevation of privilege:

This property pertains to the ability of an attacker to gain unauthorized access to a FIDO key and use it for authentication. Both UAF and U2F keys provide access as 2FA, which involves using a combination of something you know (i.e., password) and something you have (i.e., FIDO key). In case the mobile or FIDO device is stolen, the attacker would still need to know the password and other login information for the FIDO key, such as biometric or facial scans. However, with FIDO2, which involves only 1FA, an attacker gaining physical access to the device may result in unauthenticated privilege.

Security evaluation criteria:

S1 – Physical theft: Resilient to Physical security in terms of theft or lost
Half Dot – Though Mobile phones and FIDO Keys can be stolen; the adversary still needs a password or pin the access them. So, something to steal but needs access to them.

S2 – Password Guessing
Full Dot - Because the password is generated inside the UAF and U2F keys and cannot be removed, cryptographic keys are impossible to guess and prevent the user from mistakenly sharing them.

S3 - Data Privacy: Providing confidentiality
Full Dot – The system provides Data privacy and not storing or displaying any personal information of the customer

S4 – Availability: Available to be accessed all the time
Half Dot – The system is unavailable for certain times but the backup system is available

S5 - Explicit Consent: Consistent and reliable
Full Dot - The principal user of a FIDO key must repeatedly press the buttons to authenticate. FIDO keys always require the user's explicit permission, unlike some other password substitutes where a token or SMS can be used even by a third party or at a different time.

Usability evolution criteria:

U1 – Nothing to carry: Requires some device to be carried always
No Dot: There is always a second key to carry with hardware-based authenticator keys like U2F and FIDO2. Users' devices are equipped with UAF software keys.

U2 – Recovery: Not easy to recover the device
No Dot - When FIDO keys are lost or stolen, the user must apply for new ones and change their authentication settings since the cryptographic keys carried by the new keys differ from those carried by the lost keys.

U3 - Time efficient: The authentication process is carried out quickly
Full Dot – The system is fast, responsive, and reliable

U4 - User-friendly: The system must be user-friendly
Full Dot - The Security Key is simple to use and easy to master because all you have to do is insert it and push a flashing button when the browser asks you to.

U5 – Nothing to remember: Users don’t need to remember the passwords
Full Dot - On U2F/FIDO2 keys, users only need to press the capacitive button, or they can use their smartphone's biometric login to access the UAF software key. No security question or pin to remember as part of the login procedure.

U6 – Scalability: Can be used without any breakdown of the system
Full Dot - Single Authenticator can be used for hundreds of accounts.

Deplorability criteria:

D1 – Compatibility: the system must be compatible with all devices and software
Half Dot – The system needs some specific components to be used, for example, any mobile device can be used and at the same time some specific FIDO key device must be used.

D2 - Deployment Cost: Cost efficient
Half Dot - Although UAF keys are configured over the user's smartphone devices, U2F and FIDO2 keys have a one-time cost involved.

D3- Maturity: The system is free of bugs and deployed on a large scale for availability
Full Dot - With the industry's wide adoption of FIDO2 by organizations like Google, Microsoft, Amazon, Apple, Mastercard, VISA, and American Express, it may be said to be a well-matured 2FA and 1FA protocol with significant consumer growth anticipated in the years to come.

D4 - Browser Compatibility: Easy implementation
Full Dot - FIDO2 if deployed with WebAuthn utilizes the W3C standard which is implemented in all browsers

D5- Computational Complexity: The system does not require any large process to access the information
Full Dot – Simple press of a button is enough

Systemization of knowledge

Paper 1:[3]

The paper discusses the FIDO2 formal security model, which considers the different protocol elements such as the user's device, the service provider, and the authentication server. The model outlines the security requirements that must be met by the protocol, including secrecy, integrity, and authenticity, and it describes the security game that an attacker can engage in to undermine the protocol's security.

Overview:

They start with an analysis of the Security of WebAuthn which is a simple basic protocol. They have defined the class of password-less authentication (PlA) protocols that capture the syntax of WebAuthn. The PlA model takes into account the registration and authentication phases of communication between an authenticator, a server (relying party), and a client. The tamper-proof authenticator stores the joint state created during the registration phase, which is utilized to confirm the authenticator's identity during the authentication phase. subsequently applies this model to demonstrate WebAuthn's security under the presumption of collision-resistant hashing and unalterable signatures.

Then they studied CTAP2 which is a complex protocol. Authenticator setup, binding, and access channel are the three stages of the protocol's PIN-based access control for authenticators (PACA) concept. The paper establishes two security concepts—unforgeability (UF) and strong unforgeability (SUF)—and suggests two additional extensions of these concepts—UF-t and SUF-t—that place higher trust assumptions on the protocol's binding phase. The study demonstrates that CTAP2 is insecure regarding the three stronger ideas and only achieves the weakest UF-t security. The paper points out weaknesses in CTAP2's design and makes suggestions for fixes.

Execution Model:

They have considered protocols involving four parties: users, authenticators, clients, and servers. The communication channels are represented as double-headed arrows, and human communications are assumed to be authenticated and private. They assume that authenticators contain good sources of random bits, as well as volatile and static storage, and are impervious to tampering. The user's responsibility is to confirm the token, check the client's inputs, and perhaps check both the client's inputs and the token. A public gesture predicate G that encapsulates the semantics of the user's choice is used to model this. The security experiments hardwire user actions as direct inputs to either a client or a token

Limitations:

The paper's main objective is to examine the security of various FIDO2 user authentication systems. The prospect of attacks through alternative attack surfaces, such as supply chain attacks, side-channel attacks, or attacks that take advantage of flaws in the hardware or software used in the protocols, is not taken into account by the research. Furthermore, the study makes the unavoidable assumption that communications between a human user and an authenticator device or client terminal will always be physically secure. The security of the protocols in real-world settings may be impacted by elements not taken into account in the study.

Paper 2:[4]

The security and usability advantages of employing smartphones as FIDO2 roaming authenticators were investigated in this study. As a result of worries about phone availability, account recovery/backup, and setup challenges, participants judged using a smartphone as a roaming authenticator to be significantly less convenient than using a password, even if they acknowledged the high-security benefits. This shows obstacles to smartphone adoption as FIDO2 roaming authenticators as well as opportunities.

Overview:

The three particular implementations of simFIDO, caBLE, and Neo are highlighted. Android devices can act as hardware authenticators thanks to SimFIDO, which uses a TPM based on SIM cards. To enable mobile devices to act as roaming mobile authenticators, CaBLE suggests expanding CTAP2. Neo is a prototype that connects to a Chrome browser through a QR code and uses push notifications for authentication, allowing mobile devices to act as roaming authenticators. The list of CTAP2 transports will soon include an HTTPS-based transport thanks to ongoing work. Account sharing poses a possible security problem, and there is disagreement over when user presence or verification should be necessary for authentication.

The recruited varied pool of candidates can be affordable by using MTurk for recruitment. Participants can be made trustworthy and dependable by validating their locations and needing a high approval rating on MTurk. To further guarantee that participants are capable of completing the research activities accurately and efficiently, it may be necessary to specify some technological prerequisites, such as the need for an Android phone and Google Chrome.

Execution Model:

To evaluate the usability of Neo authentication vs conventional passwords, they recruited 247 participants from Amazon Mechanical Turk and randomly split them into two groups, one using passwords and the other using the Neo authentication technique. Over two weeks, participants were expected to complete several tasks on a hypothetical banking application. They were also asked to rate the System Usability Scale (SUS) of the given login method. After the trial, participants from both groups also filled out an exit survey.

To evaluate the login experience and users' perspectives over time, the researchers ran a longitudinal study in which they collected timing data and first impressions from participants for each phase of the setup procedure. They compared the Neo and Password groups using both qualitative and quantitative data analysis techniques, including content analysis and regression models, to comprehend how authentication success, processing time, and Likert-scale responses evolved. The study's findings revealed that participants thought FIDO2 authentication using a smartphone was more user-friendly and safe than conventional password-based authentication.

Limitations:

The relatively small sample size of participants is one potential drawback of this study. 248 people participated in the study, which is a respectable quantity for a user study but might not be typical of the general populace. The findings may not apply to other authentication techniques or circumstances since the study only examined one particular use case (using a smartphone as a FIDO2 roaming authenticator). Finally, the study did not evaluate security outcomes or performance indicators, simply user impressions of usability and security.

Reference:

[1] https://duo.com/blog/webauthn-passwordless-fido2-explained-componens-passwordless-architecture

[2] https://developers.yubico.com/WebAuthn/

[3] Manuel Barbosa, Alexandra Boldyreva, Shan Chen, and Bogdan Warinschi [May 26, 2022]. Provable Security Analysis of FIDO2

[4] Kentrell Owens, Duo Security, University of Washington; Olabode Anise and Amanda Krauss, Duo Security; Blase Ur, University of Chicago [Aug 9, 2021]. User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators