The Future of Authentication: deeper look on how Authentication may look like in the future

[1]Taher A. Alwusaibie

[1]Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **Authentication has always been a predominant and inherited distraction in the area of cybersecurity. Governments, organizations, and corporations have often relied on primitive authentication methods to reduce the cost of ownership, thus continuing the lack of secure authentication technology, with the absence of seamless authentication schemes.**

Authentication has evolved, from password-based authentication in the 1980s, to the use of multifactor and transparent authentication based on biometrics and behavior-based access. This article looks at the different authentication options available, and the appropriate methods for each type of infrastructure and service. The article envisions the future of authentication given the increased technological complexity, and the demand for seamless authentication.

To overcome the shortcomings of legacy authentication methods, such as passwords, industry has established an alliance called Fast Identity Online (FIDO) that aims to establish a secure passwordless authentication. FIDO is meant to address the lack of interoperability of strong authentication. Major companies are part of this alliance to standardize authentication based on cryptography keys. FIDO provides multiple standards to support different levels of security requirements, which may require hardware-based tokens.

Authentication can furthermore be taken to a different level and include additional factors that play a critical role in verifying someone's identity. The more authentication factors, the better assurance we have in knowing that someone is who they claim to be. In addition, if these factors are seamless, the authentication method will be more acceptable to Internet users.

Keywords: **Authentication, Passwordless Authentication, Biometrics, FIDO.**

1. INTRODUCTION

Authentication is a method to establish the source of a request to access a resource. The purpose of authentication is to establish a trusted and verified digital identity that is a unique representation of a subject capable of engaging in online transactions. Because authentication is often accomplished over an open-network connection, authentication introduces a vast number of threats, such as impersonation of an identity and exposure of secrets involved in the authentication activity (NIST, 2017).

The simplest form of authentication is using something you know, such as a password, where the technology to implement such solutions is widely available and very cost-effective. To strengthen this type of authentication factor, many technical controls are enforced, e.g., password length, history, complexity, and lockout window, to protect these secrets from known password attacks, such as brute-force and dictionary-based password cracking techniques. Despite IR4.0 and advancements in AI and modern technology, passwords conitnue to be the main method of authentication.

Passwords naturally have a weakness in the way they are utilized. Taking a quick glance, passwords introduce several issues:

- The more complex our passwords are, the higher our tendency to write them in post-it notes or store them insecurely in our mobiles for quicker access. Many will leave them in vulnerable places, such as in a drawer or under their keyboards.

- There are a limited number of long secrets our brains can remember. Hence, we are inclined to use the same password on multiple systems and websites. Some might share their valuable assets' password, such as those for banks, and with highly targeted websites, such as social media. A compromise of one means the compromise of our digital identity that utilizes the same password.

- It is obvious that passwords are no longer the most favorable option to verify a subject's identity. Therefore, looking for stronger authentication methods is a must.

According to Microsoft, recent figures has shown that it was estimated that 81% of data breaches are traced back to a single compromised identity, costing $3 million per breach. These compromises are either because of stolen or weak passwords ("Password-less protection.", 2018). One can check if their digital identity and email has been compromised in recent breaches using the "Have I Been Pwned?" website. The website can check if an account has been compromised in a data breach. It is an eye opener for those who think they are using secure passwords. In response to these password issues, there has been rapid development of a solution — strong multifactor authentication.

2. EMPLOYING MULTIFACTOR AUTHENTICATION

There are three different methods that a subject can use to establish and verify their digital identity. These methods or factors include:

- Something a user knows: an example of this factor is a password or PIN. This is a secret that is only known to the user.

- Something a user is: example of this factor is fingerprint or facial recognition. This factor targets unique characteristics of the user.

- Something a user has: example is a smart card or token. The user physically holds this type of factor.

Requiring a combination of the above factors comprises multifactor authentication, which adds higher assurance for the digital identity. If implemented right, adversaries must compromise all factors to impersonate an identity. Special consideration must be made to permit an authorized user to have an acceptable method to securely recover their authentication methods for each factor, if it is forgotten or lost.

We will examine two examples of multifactor authentication. The first and most common form is the combination of passwords (something you know) and an SMS code (something you have). While many organizations believe it's secure, it has been established that SMS can be intercepted and redirected (Brandom, 2017). In addition, the service provider might have access to the one-time number in the text messages, losing full control of the authenticity of this control. While it adds value and certainly better than single-factor authentication, it is a relatively weak second factor.

Some organizations have adopted stronger multifactor authentication solutions that rely on something you have, such as a smart card, and something you know, such as the smart card's PIN. Besides the fact that such solutions are costly, the user-acceptance level and complexity of them reduced the industry adoption rate. Major components and business workflows must exist in enterprise to avail this solution, such as a public key infrastructure, key distribution, and certificate recovery and renewal.

Traditional multifactor authentication solutions have not met the expectation of the industry and acceptability of end users. Therefore, they are not widely adopted and enforced. The search for a more robust authentication continued, and the question asked "do we have a standard for secure authentication?" If we draw a graph indicating convenience versus secure, we will place a solution on the graph as shown in Figure 1. We know passwords are somehow convenient, but definitely not secure. We also know that standard multifactor authentication, such as smart cards, are secure but very inconvenient. What we are looking for is somewhere in the upper right corner of Figure 1 that meets end user acceptance and provides great security.

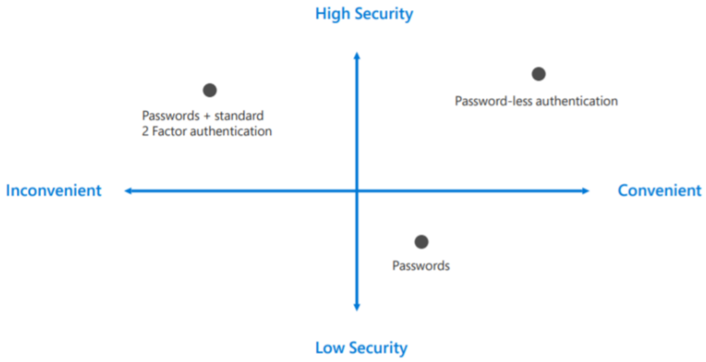

Figure 1 ("Password-less protection.", 2018)

3. FAST IDENTITY ONLINE (FIDO)

The industry realized this shortcoming and established an alliance called FIDO, to establish a secure passwordless authentication online. FIDO is meant to address the lack of interoperability of strong authentication. Major companies are part of this alliance to standardize authentication based on cryptography keys. FIDO has three main standards.

4. HOW DOES FIDO AUTHENTICATION WORK?

"The FIDO protocols use standard public key cryptography techniques to provide stronger authentication. During registration with an online service, the user's client device creates a new key pair. It retains the private key and registers the public key with the online service." ("How FIDO Works," 2019). The client needs to unlock the private key, which can be done with a user-friendly method, such as a fingerprint or facial recognition. This approach solves the two main problems introduced by traditional authentication methods:

- Cryptographic credentials are not phishable, because they are not transmitted over the network. They are basically immune to man-in-the-middle attacks ("New Report Shows Data Breaches," 2019).

- They are not based on shared secrets stored in the host server database. Therefore even if the service provider security is compromised, client credentials are protected. This allows someone to have full control over their identity ("New Report Shows Data Breaches," 2019).

For this to be fulfilled, FIDO involves two main processes. The first is to perform FIDO registration. This process involves creating the key pair to establish the identity of the user, Figure 2. The second process is FIDO Login, which involves unlocking the private key to prove the user's identity and perform authentication, Figure 3.

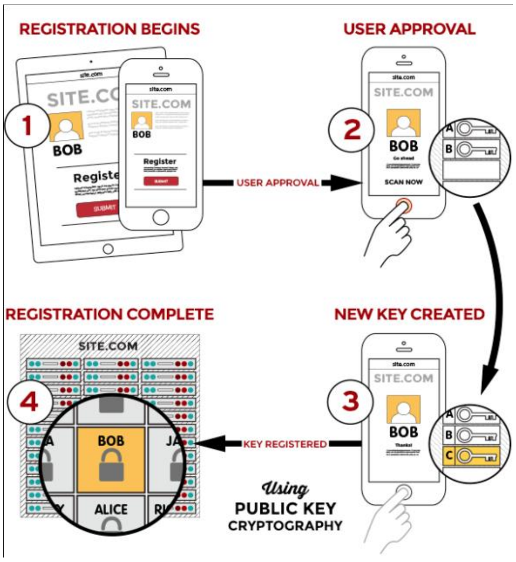

Figure 2 ("How FIDO Works," 2019)

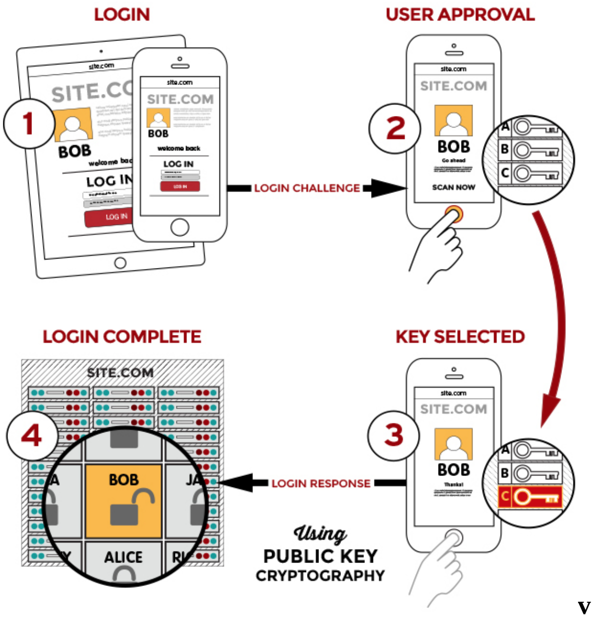

Figure 3 ("How FIDO Works," 2019)

The latest standard of FIDO, named FIDO 2, "enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments." ("How FIDO Works," 2019). The standard provides security, scalability, privacy, and usability. Through FIDO2, "WebAuthn enables online services to use FIDO Authentication through a standard web API that can be built into browsers and related web platform infrastructure." In addition, Client-to-Authenticator Protocol (CTAP) "enables external devices such as mobile handsets or FIDO security keys to work with browsers supporting WebAuthn, and also to serve as authenticators to desktop applications and web services." ("How FIDO Works," 2019).

5. WHAT OTHER FACTORS ARE MADE POSSIBLE?

This is what the industry has delivered so far around authentication. This can be taken to a different level, and includes additional factors that can play an essential role in the authentication method. An example is Geolocation Identification. We are already being tracked by applications that require access to our phone location services. Can we add this factor to ensure the physical presence of the user at the time authentication is required?

For example, assume customers are shopping at grocery stores and their banks need to authenticate them. One option could be to use the physical location of the customers through their mobile phone, to verify the user is at the same location as the point of sale processing the transaction. Authorizing the transaction could be very transparent to the user with this method.

6. CONTINUOUS AUTHENTICATION

Authentication has always been thought of as gate or entry to what a subject is authorized to perform. Authentication happens once, then the subject has all authorized resources available at their disposal. This has made attacks such as session hijacking possible when the subject leaves the authenticated session unattended. This scenario is commonly involves an insider threat or trusted person. If you leave your computer unlocked, the malicious hacker has bypassed all controls and multifactor authentication that your organization spent millions to deploy.

The concept of continuous authentication requires relying on technologies and methods to maintain the authenticated characteristics of a subject, and validate them on a periodic basis. The easiest and cheapest option in a password-based authentication system is to require the user to enter their password every 5 minutes to verify the user's identity. The down side of this approach is that the user will not tolerate the frequent requests for authentication, which definitely affects usability and productivity.

If we attempt to bring this concept to our lives, we notice that we are always authenticating others. Based on this seamless authentication, the way we speak to our parents is different than how we speak to our coworkers. Naturally, we are making authentication decisions on a continuous basis. The way we are authenticating others is based on their biometric characteristics. For an authentication system to perform continuous authentication, it must utilize a combination of biometric data to keep that specific user's session authenticated. Once the user cannot be authenticated, the user is denied access. This approach enforcese end-to-end continuous authentication (Lech, 2018).

7. CONCLUSION. THE ULTIMATE OBJECTIVE: INVISIBLE AUTHENTICATION

The ultimate objective of authentication is to have it happen in the background and be completely invisible to the user. As biometric identifications are advancing, we want to reach a stage where it requires no active participation from the user. Biometrics must combine many factors and authenticate the user every second, using a combination of different dynamic biometrics, such as facial, voice, and keystroke dynamics. This is the future of passwordless authentication.

REFERENCES

[1] "NIST Special Publication 800-63B." June 2017, Pages.nist.gov, pages.nist.gov/800-63-3/sp800-63b.html.

[2] "Password-less protection." 2018, query.prod.cms.rt.microsoft.com, query.prod.cms.rt.microsoft.com /cms/api/am/ binary/RE2KEup

[3] Brandom, Russell. "This Is Why You Shouldn't Use Texts for Two-Factor Authentication." The Verge, The Verge, 18 Sept. 2017, www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin.

[4] "New Report Shows Data Breaches, Phishing and Regulations Driving Rapid Adoption of Strong Authentication." FIDO Alliance, 24 Jan. 2019, fidoalliance.org/new-report-shows-data-breaches-phishing-and-regulations-driving-rapid-adoption-of-strong-authentication/.

[5] "How FIDO Works - Standard Public Key Cryptography & User Privacy." FIDO Alliance, 25 Jan. 2019, fidoalliance.org/how-fido-works/.

[6] Lech, Olga. "Behave Yourself - Continuous Authentication Method Presented by Digital Fingerprints." Digital Fingerprints, 12 Dec. 2018, fingerprints.digital/behave-yourself-continuous-authentication-method-presented-by-digital-fingerprints/.