SANS

A SANS Whitepaper

Authentication: It's All About the User Experience

Written by **Matt Bromiley**

May 2019

Sponsored by:

Yubico

Introduction

How can you prove you are who you say you are? That is one of the most fundamental questions asked of anyone utilizing an electronic device. In a world where compromised user credentials can cost an enterprise millions of dollars, the importance of being able to validate user accounts is a crucial enterprise requirement. Therefore, the obvious solution is to wrap as many protections around our users as we possibly can. At least, that's the way it *should* be.

To validate user identity, we have seen a myriad of authentication schemes made available, ranging from security tokens to phone apps that provide one-time codes.

However, even with these technologies, a significant number of organizations still utilize only usernames and passwords for employees and customers. We have to ask: **Why, when the technology is available, does implementation still lag?**

In this paper, we propose that authentication sometimes remains an afterthought due to three key issues:

1) A lack of understanding
2) A concern about interrupting the user experience
3) The cost of implementation

We also argue that modern authentication techniques actually allow for better user experiences as well as stronger authentication. We examine how these techniques

can be applied within your organization for your employees—the other custodians of your data. We believe that although your organization may not yet have taken advantage of enhanced authentication techniques, you are in the right spot to consider implementations.

We wrap up with a brief comparison case study that introduces the new WebAuthn specification, recently approved by the W3C. This specification allows for authentication via public key cryptography and a choice of hardware security keys and built-in authenticators as opposed to standard passwords. Get ready to be launched into the future!

As you read this whitepaper, we encourage you to consider the current state of authentication at your organization for both your users *and* your employees. We provide multiple "Actionable Pro Tips" throughout the paper that can be put into action plans immediately.

Authentication: A Double-Edged Sword

Even with a myriad of advanced authentication techniques available, many organizations still deploy legacy authentication mechanisms. Sadly, these implementations leave open a massive attack surface. Simple password-based authentication provides a lucrative attack vector. For example, in July 2018, the FBI announced that business email compromise (BEC) attacks had amounted to a total of $12.5 billion in global losses over an approximately five-year period.[1]

Simple password-based authentication provides a lucrative attack vector. If attackers need to clear only one hurdle to initiate their attack, they will focus heavily on phishing and credential theft to gain access into the environment.

So why do organizations still rely on easy-to-defeat mechanisms? In breaches where single-factor is at play, SANS' experience is that attackers often have a higher level of success. One would think that if a more secure solution came along that kept out attackers, upgrades would occur overnight. Unfortunately, this is rarely the case.

In our experience, we've found three key roadblocks to implementation:

- Authentication remains a bit of a mystery or is not perceived as being as important as other security issues.
- Authentication is perceived as potentially having a negative impact on the user experience.
- Security experts have a perception that there is significant cost to overhauling authentication to make it effective.

Let's examine each roadblock and discuss how your organization can navigate around all three of them.

[1] FBI, "Business E-mail Compromise the 12 Billion Dollar Scam," www.ic3.gov/media/2018/180712.aspx

In many organizations, the word *authentication* is met with, "I'm not sure what that means." And humans often resist what they don't know or understand. After all, many security professionals throw around terms such as *multifactor authentication*, *smart cards* and *biometrics* as if they were as easy to grasp as a fork at mealtime. However, for complex organizations running multiple applications across multiple services across multiple countries, these terms have complex implications. Unfortunately, in too many situations, organizations are simply installing and using applications without understanding the authentication considerations. Or they ignore the issue, assuming that other security tools will make up for the lack of effective authentication.

It's easy to get lost in authentication terms and to misunderstand what the technology is doing. When evaluating, remember to ask how the authentication mechanism validates the user. This question gets at the heart of preventing attacker spoofing and credential theft. You don't need to be a cryptography expert—you just need to know that simple passwords won't work anymore!

Additionally, some organizations get wrapped up in their own complexities of authentication. In nearly every organization, user account needs differ by users and their permissions and/or job roles. As teams battle out who needs access to what, it's easy to get lost in the confusion, and this further slows down the process. Thus, prior to any advanced implementation, privileged and non-privileged accounts may be treated the same, which again opens up doors for attackers.

Unfortunately, many organizations get lost in these terms or deem them to be too complicated to implement. (We'll address the user experience side of this in the next section.)

Table 1. Key Authentication Terms and Types

Term	Meaning
OTP	One-time password—A password that is valid for a single session or transaction. Typically generated using a predefined mathematical algorithm (housed on a smart card or hardware security key), OTPs may be combined with a PIN or password for two-factor authentication.
MFA	Multifactor authentication—An authentication routine that typically involves more than just a username and password, often in the form of a token or code. By adding multiple "factors" (often only one more, which results in two-factor authentication), you make it harder for attackers to steal credentials and take over accounts.
Strong Single-Factor Authentication (Passwordless)	With the recognition that user passwords are often highly insecure, passwordless login focuses on other authentication techniques to secure accounts.
FIDO	The Fast ID Online Alliance—A consortium designed to create specifications for enhanced authentication techniques to move away from an overreliance on passwords. Many authentication terms are ported into FIDO specifications, such as *FIDO2*, *U2F* and *UAF*, all of which rely on public key cryptography (something we will examine in our case study).
WebAuthn	A new W3 standard, incorporating FIDO's U2F and FIDO2 standards, that relies on public key cryptography, as opposed to usernames and passwords. WebAuthn has increasing support from all the leading browsers and platforms.

No doubt many organizations have heard of more secure authentication techniques but perhaps didn't understand the terminology. For example, you may have heard the acronyms OTP and MFA but weren't sure what the terms mean. Let's examine some key authentication terms and types in Table 1.

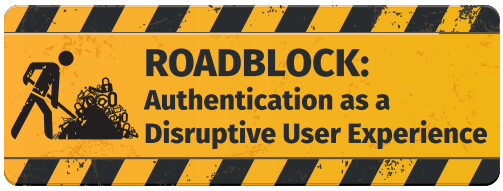
If you find yourself lost in a sea of authentication, turn to the W3C and the FIDO Alliance to help explain key authentication terms and how they may apply to your organization.

Actionable Pro Tip

In a world of complex terms and acronym soup, it's easy to get lost in what type of authentication you should be implementing within your organization.

You may not have to make the choice. Lean on your vendors to see what they offer and integrate appropriately within your browsers.

As you upgrade and enhance the technology within your organization, seek out methods that utilize public key cryptography as opposed to usernames and passwords.



Some of the pervasive roadblocks to strong authentication implementations are rooted in concern about disrupting the user experience. This is a complex topic, but basically, each organization has two types of users that must be considered in all authentication discussions: customers and employees.

From a **customer** perspective, some organizations are *extremely* sensitive to how their users interact with their various services. In fact, depending on their business model, user interaction may be the crux of the service itself. With revenue at stake, many organizations are hesitant to introduce any security mechanism that may disrupt the user experience or, even worse, cause users to seek services elsewhere. Unfortunately, within many industries, it is possible to lose customers for being *too secure*.[2]

There are two types of users who interact with your systems: customers and employees. Both can cause harm to the organization and/or result in data loss. Strong authentication should be wrapped around both.

However, the customer experience is already changing, independent of your organization. With the introduction of internal authenticators on mobile devices (think Apple's TouchID and FaceID), more and more users are becoming familiar with streamlined authentication routines. The new WebAuthn specification, for example, will allow for users, applications and web browsers to take advantage of both external hardware security keys and built-in authenticators to bypass the risk of weak user passwords. Many organizations are also taking advantage of built-in payment mechanisms, such as Google Pay, to allow for easy, verified payments using strong security standards.

Actionable Pro Tip

Many users are now more familiar with biometric authentication techniques, such as fingerprint or face recognition. Most computer and mobile device hardware today ships with built-in support for strong authentication. Take advantage of this and (re)develop your applications accordingly. Users will appreciate the integration of additional authenticator options into their current authentication routines, and your organization will enjoy the newer security techniques.

From an **employee** perspective, enhanced authentication techniques should become a "must," not a "maybe." Nonetheless, some organizations work hard to justify not moving beyond usernames and passwords.

Excuses such as "We've always done it this way" or "We don't have time for codes or additional hardware" serve as psychological escape hatches that put authentication out of sight and out of mind. Even worse, though, are the organizations that say, "We don't have anything worth stealing anyway." That's an extremely dangerous viewpoint.

[2] Note that some industries, such as finance, typically have better authentication implementations than others. Within those industries, however, some organizations still have less-than-ideal implementations in place.

When we hear these excuses, we have to ask: If your team doesn't have time to enter a second code or learn to use new types of authenticators, then how will you have the time to investigate a breach? This stance of "We'll do it later" ends up snowballing into an incomplete security program easily penetrated by an opportunistic attacker. And believe us, no businesses are out of attackers' crosshairs.

Attackers find success in businesses of all sizes, in every industry. If your business conducts financial transactions or has a list of customers (and almost all do), then you are a target. Attackers have known for a long time that the fastest way into an organization is to steal a legitimate account. Earlier in this paper we discussed BEC breaches, which are largely predicated on the abuse of single-factor authentication following a successful spearphishing expedition. The attackers behind such breaches know no boundaries and don't care about business size.

Organizations that are concerned about resistance from employees should consider that they are becoming more familiar with enhanced authentication techniques all the time, because those techniques are now widely deployed in consumer devices such as phones and tablets. These techniques present unique opportunities for organizations to help secure their assets—employees can be requested to utilize hardware tokens or multifactor options such as phone PIN codes or "pushes," which verify the user is who they say they are.

Actionable Pro Tip

Your employees are often your weakest line of defense if they are equipped with legacy authentication and/or simple usernames and passwords. However, you have the ability to change these events and morph your users into the strongest line of defense on the network by making their accounts almost impossible to steal. **Implement strong authentication as policy,** educate users appropriately, and empower them to defend your organization.

The last key area where effective deployment of authentication suffers greatly is in the perception of cost to the organization. Despite the strengths of enhanced authentication, many organizations will simply look at dollar signs and decide that user security costs too much. This decision robs your users of the chance to be an actionable, empowered line of defense within your security posture.

Many organizations will get hung up by the idea that multifactor authentication security key fobs or app-based implementations may have a hardware cost *on top of* the subscription or per-seat fees. But just consider the cost of an eventual breach. A 2018 survey from Ponemon found that the global average cost of a data breach was $3.86

million, which of course scales up or down based on organization size.[3] If you decide to go with "We'll take our chances," that could end up costing more than prevention.

And how many organizations even think about the real costs of their single-factor authentication? Password resets can eat up a lot of help desk time, and that costs money. A 2018 survey from LastPass and Forrester found that the average help desk cost for a single password reset was $70.[4] Multiply this by the number of employees in your organization, and the costs can quickly reach beyond the purchase of secure authentication devices for all of them.

In any event, smart cards or security key fobs are no longer requirements for enhanced authentication, as we'll illustrate in our next case study. Built-in hardware security devices nowadays can be harnessed to ensure your users (whether employees or customers) are truly who they say they are.

Actionable Pro Tip

When weighing the cost of enhanced authentication, don't stop at the dollar amount on the invoice. Consider how your organization would respond to a breach of employee or—even worse—customer data. That cost could easily be much higher than an investment in enhanced authentication.

Case Study: The Old vs. the New

As we mentioned earlier, significant gaps are being created in enterprise security postures due to reliance on or use of single-factor (username/password) authentication. Let's examine a case study where a user wishes to create an account for a website, and the various security concerns associated with that act. We'll then examine how this process can be streamlined and made more secure using the new WebAuthn specification.

The Old

In an all-too-familiar situation, imagine a user who wishes to create an account and utilize a particular web service. Figure 1 provides an overview of this situation, with a focus on key points of the transaction.

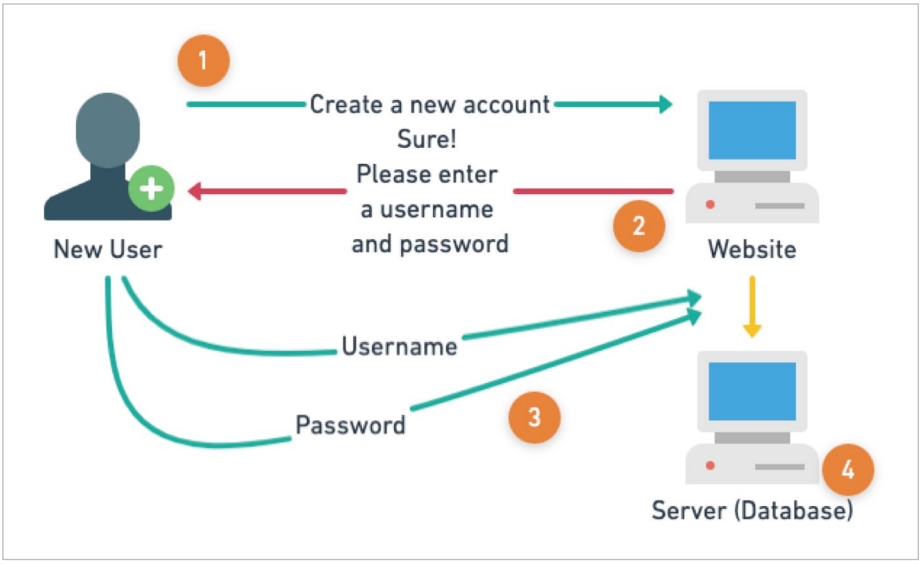


Figure 1. Steps for Typical User-Created Accounts

[3] "The Average Cost of a Data Breach," https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx

[4] "Stolen credentials cause 1/3 of external security breaches," https://blog.lastpass.com/2018/05/new-forrester-report-real-cost-password-risks.html

Typically, the process goes as follows:

1. The user wishes to sign up and create a new account. The web server, configured to utilize legacy authentication, begins the process of registering the new account.
2. The user is redirected to a registration page to create a username and password. Here is the first area of concern—things such as password strength are left to the user's technical capabilities. *Even if your website offers features such as password-strength meters, users want something memorable, not strong.*
3. Upon form submission, the user sends the desired username and password to the web server.
4. The organization must store the username and password somewhere, often on a back-end server or database that provides secure and robust credential storage.

Unfortunately, this tried-and-true method of registering accounts has multiple security weak spots, the first being reliance on the user as part of the authentication process. The user is required to create a password, which can introduce problems such as password reuse (always a tempting option to users who want something memorable).

The outcome might be better if the user utilizes a password manager, which will create a truly unique and pseudo-random password for your site. Ironically, however, password managers themselves are often accessed by a single password (and, we hope, strong authentication!). The core problem lies in the responsibility being placed on users to create, maintain and protect their own pieces of challenge-response authentication.

Even if your website offers features such as password-strength meters, users want something memorable, not strong.

The second security concern—and the direst—is the necessity for the server to store usernames and passwords. The need for this is fairly obvious; the server must have something to compare and validate the user login. Unfortunately, this places all user credentials at risk of theft from an attacker who figures out just the right way to break in and steal user credentials. With a trove of usernames and passwords, attackers can log in and masquerade as anyone they choose.

Now, some of you may be thinking of techniques that have been implemented to defeat these types of attacks. And it's true that most software will encrypt stored passwords so attackers cannot simply use them. Encrypted passwords may be crackable, though, so this may serve as only a temporary stopgap for a skilled attacker. Other web servers may introduce additional tracking mechanisms that do not "recognize" an attacker system, and prompt for an additional authentication factor. This technique isn't entirely useless—as long as the true user is the one who must perform the validation. Be warned, though: Attackers have worked around these mechanisms as well.

The New

Now let's examine the same type of transaction using the new WebAuthn specification. As we described, WebAuthn allows for authentication via a cryptographic key exchange, much as you would expect to see when connecting via HTTPS to an encrypted site. Figure 2 provides a walkthrough of the initial account registration.

Figure 2. Walkthrough of Initial Account Registration

The process works like this:

1. The user visits the same website, this time enabled with WebAuthn. The user wishes to register a new account.
2. Utilizing the WebAuthn specification, the server responds by asking for a public key that is *unique to this user and this website.* Via a strong external authenticator device, such as a hardware security key, the user generates the appropriate public/private keypair for this website.
3. The public key is provided back to the website, and is associated with the particular user account. Usernames and passwords never cross the network, and thus are never stored.

One of the critical steps of authentication is assertion, where users prove their identity by validating that they own the private key. Without it, the website can assume that this is not the original user, who will thus not be allowed access to the site.

Let's examine the second step of this process, in which the user returns to the site. Figure 3 walks us through these steps.

1. After successfully creating an account at some point in the past, the user wishes to return to the site. Upon doing so, the website recognizes the user account and asks the user to sign a randomized string of data.

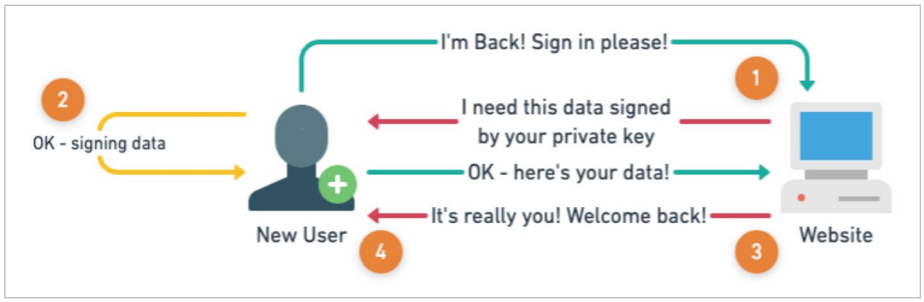


Figure 3. User Authentication Steps with Private Key

2. The user receives the data and signs it utilizing the private key that was provided during the initial account setup. The whole authentication process is centered on the cryptographic key exchange. **This is the most critical stage of authentication, in which users prove that they have the private key, thus proving they are who they say they are. This is called "assertion."**
3. The website receives the signed data, which is then compared against the public key.
4. Upon validating that the user owns the private key and is *who she says she is*, she is permitted to sign into the website.

Notice that all of the above was performed without user passwords, providing a seamless approach and user experience. Next time you're considering whether enhanced authentication can impact your user experience, remember that it can actually make the experience faster, easier and more secure!

Closing Thoughts

Organizations often spend large sums implementing hardware and software security mechanisms in order to prevent attackers from gaining unauthorized access to their sensitive data and/or employees. Unfortunately, many of these same organizations still rely on simple password-based authentication for their users, both customers and employees. With access dependent on a single password, you may be voiding all of the security benefits you think you have in place.

It's time to make a shift, as an organization, to more secure authentication mechanisms. In this paper, we examined the top three reasons for lack of advancement in authentication: ignorance, user experience and flat-out cost. While these are not insignificant considerations, they may pale in comparison to the damage caused by lack of truly secure authentication. We also examined how moving toward a passwordless world helps protect your users, employees, data and, ultimately, your organization.

Make the change to strong authentication that is easy to use. Your customers will thank you with business.

But you may be thinking that all of the above is easier said than done. "Simply rewrite your applications" is not an easy task and may require significant investment. Supplying physical devices to facilitate attestation may require another financial outlay, and all those costs may be tough to justify if you haven't experienced a breach. With that in mind, moving toward secure authentication may come across as more of a culture shift than a security precaution.

Our advice: Make the change. Your customers, who are silently demanding strong authentication, will thank you with business. Your employees will become your strongest line of defense.

And, for once, you may begin to build an organization that attackers shy away from instead of gravitating toward.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also an incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

yubico