Secure Coding.
Practical steps to defend your web apps.

SANS

A SANS Spotlight

Bye Bye Passwords: New Ways to Authenticate

Written by **Matt Bromiley**

July 2019

Sponsored by:

Microsoft

Passwords Are Making You Weak

Time and time again we see user passwords treated with minimal to no security. They are kept in plaintext, reused again and again by employees, and left to fend for themselves in the form of single-factor authentication. This practice has resulted in billions of dollars stolen and enormous data breaches from which it takes organizations months, sometimes years, to recover. Or even worse, threat actors sell your legitimate credentials over and over, meaning your organization never has time to recover and is constantly on the defense. Sound familiar? If we know the problem, we can begin to work toward the solution.

Remember: we don't want to protect passwords. We want to get rid of the threats they bring!

In this paper, we help you work toward that solution. We begin by examining the problem of passwords and password mismanagement, and we show how letting password security slip can cause significant problems. Some of our security concerns may sound familiar; don't worry, you're not alone.

But talk is easy. Action gets results. We also provide tips and suggestions for increasing your organization's account security using modern industry standards. The "passwordless movement" is upon us now.

Passwords as Attack Vector

Before we begin discussing ways to change password handling and implement more secure authentication, it's important to understand one surprising fact: Multiple attack types have been highly successful without the use of advanced technology. This fact only highlights how critical password security is—even the best-designed networks can be brought to their knees with single-factor authentication.

Single-factor authentication leaves a massive attack vector open in your organization, which may lead to a significant loss of money or data as well as legal and compliance consequences.

Business Email Compromise

One of the more prolific and profitable attacks over the past few years is known as Business Email Compromise, or "BEC." There's a good chance you've heard about these attacks—the FBI has been warning against the threat actors behind them for many years, and with good reason. In July 2018,[1] it was reported that these attacks stole more than $12 billion in a little less than five years, and that's just reported cases!

These attacks have been very profitable, but they are remarkably low tech. They often involve phishing user credentials and abusing platforms such as office productivity suites with single-factor authentication to steal address books and build target lists.

Attackers will also subvert trust to embed themselves in the wire transfer process and steal hundreds of thousands, if not millions, of dollars. Unfortunately, an organization that protects its address books and email accounts with single-factor authentication means it is only one spearphish attack away from significant potential damage.

Legacy Protocols

Attacks such as BEC, amongst a plethora of others, have also achieved success in areas where enhanced authentication is not an option. Unfortunately, there are limitations in the technology used by organizations today, primarily in the deployment of email. Legacy protocols, such as SMTP, were created in simpler times wherein MFA was not needed, let alone a push-button away from implementation.

Attackers are aware of these protocol limitations and will find ways to force a downgrade in protocols and authentication. Attackers may use outdated browsers or email applications to force your secured, enhanced authentication environment to resort to less secure protocols.

One attacker technique is to force your organization into less secure legacy protocols. Disable them as soon as possible within your organization, and move toward applications that force modern authentication.

The Hidden Threat: Third-Party Password Reuse

Users are notorious for reusing passwords, and this behavior poses grave risks to an organization using single-factor authentication. This behavior is true not only between password resets but also between different sites and organizations. Even with good,

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

strong no-reuse policies, you are still fighting against other third parties where users may have reused their passwords. Thus, if your users are reusing passwords, their security becomes your security.

This security concern is compounded by some recent mega-breaches that have yielded hundreds of millions, if not *billions* of accounts. Haveibeenpwned, a site that tracks credentials compromised as a result of a data breach, has multiple data breaches within its records that encompass hundreds of millions of user accounts. If any of your users have reused a password on a breached site, it's a guarantee that attackers will obtain and try that password against your organization as well. Figure 1 depicts some of the ways that an attacker can arrive at your login screen prepared for the next step.

Notice there are certain ways to ascertain a password (marked by the green star) that have nothing to do with your defenses!

In a better-case scenario, a threat actor may arrive at your login screen with old or outdated credentials. Depending on how your users create their passwords, however, the threat actor still may be able to review user password history and figure out any patterns the user may employ. This technique may allow them to predict the next password in line. Using password managers is a good way to introduce randomness and break out of user habits, but the goal of this white paper is to break you out of single-factor authentication, not make single-factor more reliable.

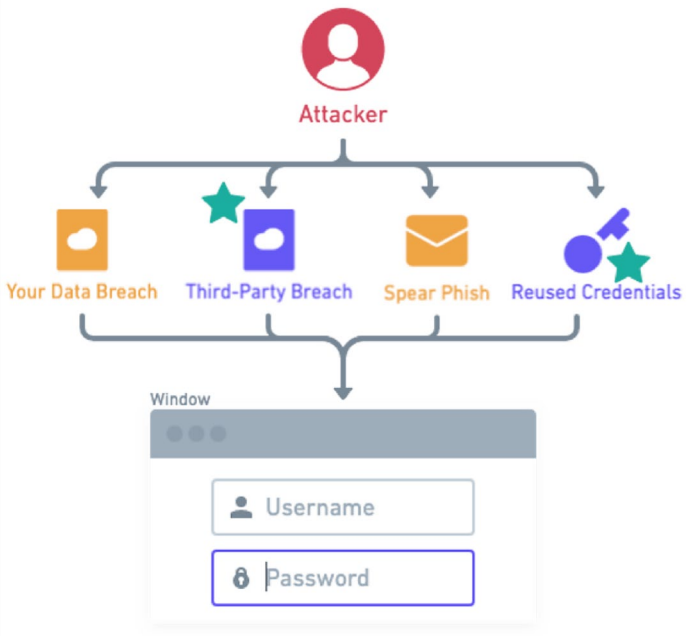

Figure 1. Ways an Attacker Can Arrive at Your Login Screen Poised to Do Damage

Join the Passwordless Movement

The chief concern with single-factor authentication is that once a threat actor obtains credentials, they can simply "walk" into the organization and appear to be a legitimate user. This possibility foils a detection strategy. How would one detect for legitimate logins? We need to build detections around additional factors or, more importantly, implement stronger authentication mechanisms and/or additional factors.

MFA: Implement Now

Time to implement multi-factor authentication! Multi-factor authentication (MFA) often involves a username, password and some other mechanism to prove the user identity. This verification is often done in the form of a One-Time Passcode (OTP) served up by an authenticator app or a "push" from the authenticating service. (We'll look at passwordless authentication in the next section, so don't confuse that here.)

Multi-factor authentication is meant to secure your organization, not break it. Develop an implementation plan to protect your most important accounts or devices now, with a longer-term goal of securing the entire organization.

[2] "Have I Been Pwned: Check If Your Email Has Been Compromised in a Data Breach," https://haveibeenpwned.com

We see two primary obstacles to adopting MFA implementations today. First, there's a misconception that MFA requires external hardware devices. While external tokens or other hardware tools are an option and offer strong security benefits, now there are secure and easily-implemented software-based MFA tokens that can be used and integrated with smart devices, such as a cell phone, that users may already own.

Second, some organizations put off implementing MFA because of potential user disruption or concern over what may break (meaning they don't have their account movement mapped out, which is yet another issue). To us, this comes across as another excuse. There are multiple ways to implement stronger authentication within your organization; it doesn't have to be an all-or-nothing approach. In Figure 2, we examine some potential approaches your organization could use to limit the disruption while moving to a more advanced state of authentication.

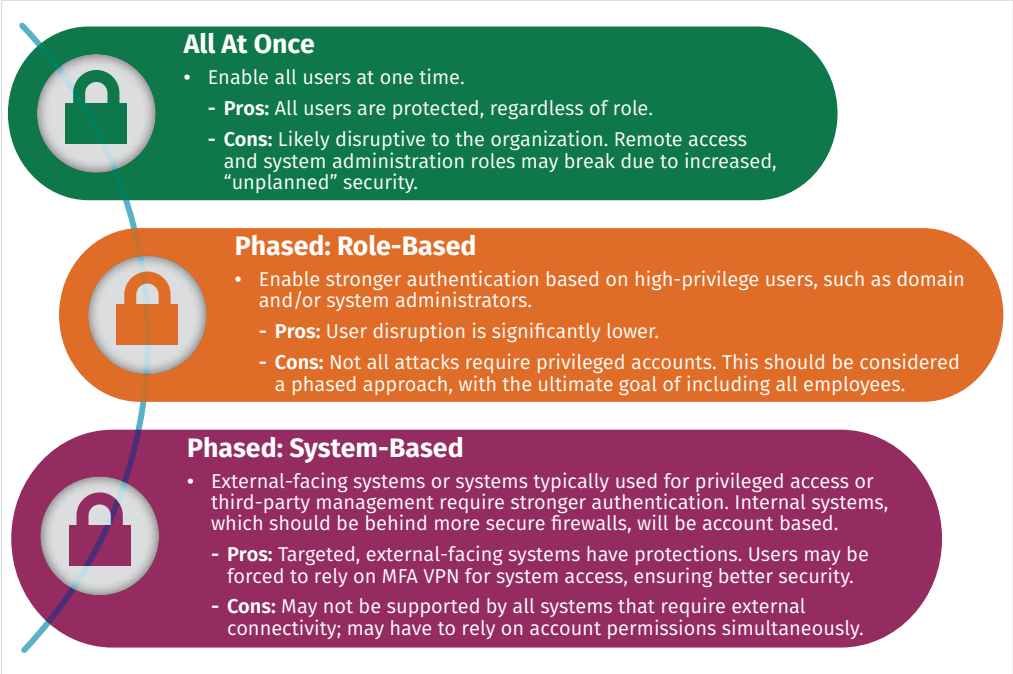

Figure 2. Enhanced Authentication Implementation Approaches that Limit Disruption to the Organization

The New News: Going Passwordless

The previous section focused on ways to strengthen user authentication via multiple login factors. Some organizations, however, are looking to move to even stronger techniques—especially those that are inherently multi-factor, such as biometric and public/private keys working together—without any knowledge or impact to the user. Luckily, the past is here to deliver the future.

Hardware-based authentication is nothing new; systems have been shipping with the Trusted Platform Module, or TPM chips, for years. These hardware devices allow for storage of encryption keys that help validate user identity. But the embedded TPMs have been underutilized by many organizations for user authentication, primarily because of a lack of easily understood and non-proprietary solutions to enable authentication.

Industry standards, such as WebAuthn,[3] have made critical strides recently in utilizing hardware for true passwordless authentication that works across platforms and is much more easily deployed. WebAuthn is going a step further by incorporating web browsers and platforms to ensure that the most common user application—the web browser—is an integral part of authentication. The standard also allows websites to incorporate stronger authentication in their processes, thus ensuring that user credentials are protected end-to-end and strengthening the entire security chain.

[3] WebAuthn.io, https://webauthn.io

If you're worried that this may be too complex for your users, fear not. Many users these days have become familiar with facial recognition technology and fingerprint readers, for example, thanks to implementation in many notebook computers and phones. Some desktop operating systems are also using facial recognition to validate user identity by requiring a user to simply look at a screen. There's an even better inherent security advantage: These techniques make authentication theft a very costly, and extremely difficult, route to compromise someone's system.

The WebAuthn standard allows websites to incorporate stronger authentication in their processes, thus ensuring that user credentials are protected end-to-end and strengthening the entire security chain.

Hybrid Environment? Even Better!

While we could've easily floated a hybrid environment as a roadblock for implementing stronger authentication, in these times we actually consider this to be a benefit. Most cloud-providers, for example, have multi-factor authentication already built into their systems. In some cases it's as simple as checking a box, and now your organization is better protected. If your organization is utilizing cloud resources, we recommend at a *minimum* you place privileged accounts behind strong authentication. If you can do this for all accounts, by all means, do so.

Speaking of the cloud, don't forget about your third parties. Many organizations are using single sign-on aggregators to help manage their various company resources. With central points of access, strong authentication such as multi-factor should not even be a question. Enable it!

For the areas of your organization that are on-premises, you can easily enhance authentication by reaching out to vendors offering after-market authentication upgrades. Free and open source software can be used to help implement newer standards on current, existing services. Depending on the technology you are utilizing on-premises, you may be able to be up and running in a matter of hours!

What Are You Waiting For?

Unfortunately, user passwords and authentication management have been too often ignored. Some organizations may view stronger authentication mechanisms as a hindrance because users shouldn't be bothered to effectively maintain a second factor. We've seen organizations abstain from multi-factor authentication simply because a couple of C-suite members found token codes to be an inconvenience. These trends need to be broken. Now.

In this paper, we identified reasons why single-factor authentication only hurts the organization when used to secure priority assets and/or privileged accounts. Single-factor opens up a massive attack vector—one that could and should be easily prevented. If you're currently living in a single-factor world, consider moving toward multi-factor authentication or passwordless options. Newer standards and built-in hardware give you the tools for stronger and simpler, industry-standard ways to enable MFA with minimum hassle.

Concerned about any user disruption? Consider how to prioritize your user base and account usage, and phase in MFA appropriately. There simply is no longer a good excuse to keep using simple passwords.

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 a principal 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:

Microsoft

Last Updated: August 22nd, 2019

Upcoming SANS App Sec Training

SANS Brussels September 2019	Brussels, Belgium	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Network Security 2019	Las Vegas, NV	Sep 09, 2019 - Sep 16, 2019	Live Event
Network Security 2019 - DEV522: Defending Web Applications Security Essentials	Las Vegas, NV	Sep 09, 2019 - Sep 14, 2019	vLive
Mentor Session - DEV522	Novi, MI	Sep 16, 2019 - Nov 18, 2019	Mentor
SANS Paris September 2019	Paris, France	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS London September 2019	London, United Kingdom	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WA	Oct 14, 2019 - Oct 19, 2019	Live Event
Cloud & DevOps Security Summit & Training 2019	Denver, CO	Nov 04, 2019 - Nov 11, 2019	Live Event
SANS San Francisco Winter 2019	San Francisco, CA	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Jeddah March 2020	Jeddah, Kingdom Of Saudi Arabia	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS San Francisco Spring 2020	San Francisco, CA	Mar 16, 2020 - Mar 27, 2020	Live Event
SANS London March 2020	London, United Kingdom	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS 2020	Orlando, FL	Apr 03, 2020 - Apr 10, 2020	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced