WINMAGIC

WHITE PAPER

PASSWORDLESS AUTHENTICATION

What you should know about this new approach to secure remote access

INTRODUCTION

Data breaches have been the number one security concern for businesses for many years. According to the Verizon Data Breach Investigations Report (DBIR), 81% of hacking-related data breaches are caused by compromised, weak and stolen passwords. Identity theft is also among the biggest concerns for users, and the many long passwords, while cumbersome and very annoying, don't really help much against password phishing and other cyberattacks. What can the industry do?

PASSWORDLESS AUTHENTICATION is gaining traction due to market demand and advances in technologies.

In this white paper, WinMagic shares its viewpoints on the following topics and key findings:

01

Industry efforts with passwordless authentication will most likely eradiate identity theft and thus the main source of online data breaches

02

Users will no longer struggle with many long, complex passwords

03

We are in the early stages of the passwordless era

04

Considering the attacks, passwordless solutions might be easily done on the client-side (for example, via the deployment of software tokens)

05

The server-side will follow much faster than the progress made in the past several years

THE AUTHENTICATION SCENARIO IN QUESTION

Let us examine the various actions in the authentication scenario that the "passwordless" movement intends to change. If you are using a computing device – say a laptop – and you want to log in to Gmail (the "server"), two distinct actions need to take place:

REMOTE AUTHENTICATION

This occurs between the server and the device. Among others, the verification takes place on the server, remote from where the user or the device sits.

LOCAL GESTURE

On the local device, the user might use some local gesture to prompt the device to perform the authentication with the server.

REMOTE AUTHENTICATION

Traditional remote authentication method leveraging a username and password

The current "username and password" authentication is:

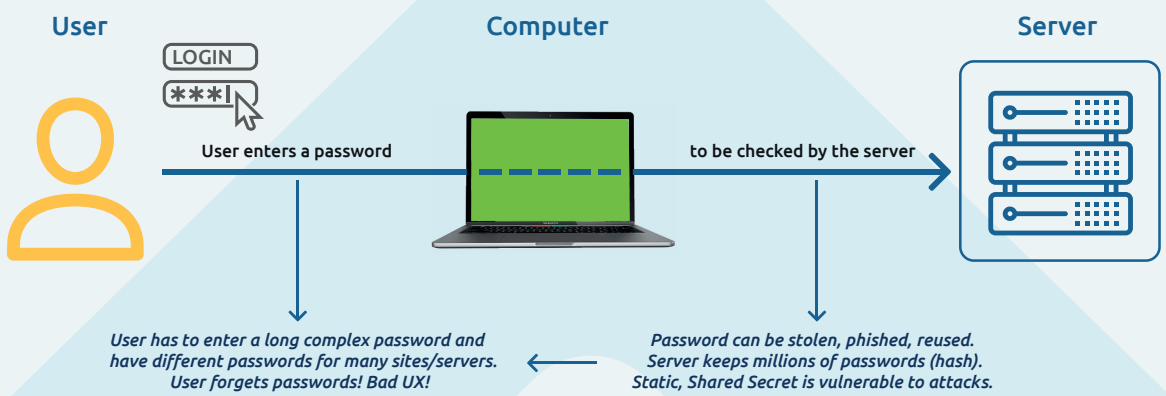
01

Agree on a password

02

Have the server compare its version
e.g., a hash – with what the user entered.

"Username and Password" Authentication



In this scenario, attackers can get your current password – through phishing or other attacks. They can log in from some device somewhere on the Internet and get access to the website just as you do, despite how difficult or strong you made the passwords. Having a long, complex password and different passwords for different websites or servers can reduce the effectiveness of some attacks, but not by much. This, despite your heroic effort to remember those passwords without writing them down.

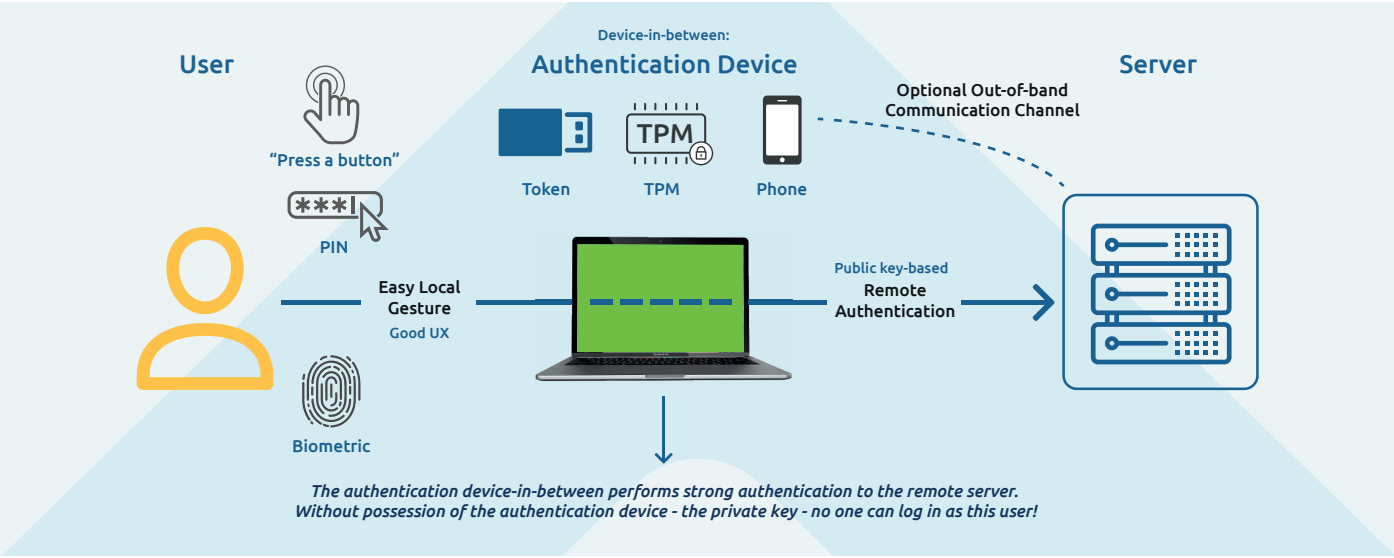
For more secure remote authentication, newer solutions make it so that even if the attacker has all the computing power in the world – all clouds, data centers and the billions of computing devices combined – it will take him millions of years before he can successfully fake the authentication.

Authentication using public-key cryptography

With public-key cryptography, the user can sign some data with the private key. The server, having the user's public key, can verify that the signature comes from the user – the only one who has the private key. The authentication, including the verification, can be done without a shared secret, without the user sharing the private key.

"Passwordless" Authentication

Passwordless: No centrally managed passwords.



The function of the "device"

At this time, we observe:

01

In the old "username and password" method, the device is only the communication channel, and the authentication is between the user and the server. The password represents the "knowledge" in the MFA.

02

The main change in the new passwordless solution is that the device actively does the authentication – no longer the user. When we mention the "user" in the cryptography-based actions above, we mean the (authentication) device. The device must be able to perform public-key cryptographic operations and must have the private key for the corresponding public key on the server. Since the private key cannot be copied out of the device, no one can authenticate without the device.

03

So, the "device" enables the remote authentication to be secure – thousands or even millions of times more secure than your longest and most complex password. If somehow this "device-in-between" could also enable you not to have to remember many, long, complex and different passwords, it would be perfect.

NIST has deprecated some methods or devices even though they are "passwordless"

Some solutions today involve a device and cryptography, but they are deemed unsuitable against modern attacks. We expect "SMS push" (sending a message to a smartphone) or one-time passwords (OTP) to be deprecated over time.

In this white paper, we consider only public key-based methods. FIDO is a prominent one today, but other methods with PKI, smartcard and cert are also prevalent and offer similar security levels.

THE LOCAL GESTURE

As discussed above, on a local device, the user might employ some local gesture to tell the device to perform the authentication with the server. This local gesture is not and does not have to be authenticated to the local device. You are already using it!

So, in a typical scenario, the local gesture is completely up to you or your company policy. Unlike the old case of "username and password," your local gesture has nothing to do with the strong authentication between your device and the remote server! So, yes, the device-in-between does wonders for you! It makes the remote authentication very strong and, at the same time, your local gesture simple. You simply need to have that device!

FURTHER CONSIDERATIONS

What can be used as the authentication device?

The security of the public key crypto-based authentication relies strongly on the protection of the private key, secure storage and **secure execution when operating**. If the key cannot be copied out of the device, then the only way to get the private key is to steal the device – and know the means to unlock it.

Typically, a crypto chip offers both secure key storage and a secure execution environment protected within the chip. With this "hardware-based" crypto, in no circumstance will the private key be exposed.

More and more hardware today is equipped with features to help protect data (USB). Crypto tokens, smartcards, and TPM typically contain crypto chips and should do this job well. The smartphone and computer increasingly have features for secure execution and storage.

What is the communication channel between the authentication device and the server?

We feel compelled to focus on the communication channel between the authentication device and the (authentication) server at this time. As the world is moving to passwordless authentication at this early stage, we like the Gartner recommendation to "craft a cohesive strategy that combines the fewest moving parts to implement passwordless authentication across key use cases."[1] We believe this communication channel plays an important role and that we will see changes and adaptations along the way.

The changes to the new, passwordless era include the following distinct changes:

01

The use of the device-in-between.

02

Instead of the current separated client-server applications authentication, the authentication is now sometimes off-loaded to an authentication server. The uncoupling can have security ramifications.

03

The communication channel for the authentication is no longer just between the computing device and the server. The use of the smartphone instead of the computing device via a different communication channel can have several ramifications.

[1]Gartner "Top Five Midsize Enterprise Security Projects for 2020," Paul Furtado, Brian Reed, 6 May 2020

We will discuss the communication channel below.

Using the smartphone in a different communication channel

Recently, the use of the smartphone in the authentication process has gained in popularity. SMS push and OTP will be deprecated someday, but FIDO will grow.

Using a token or the computing device as the authentication device

We lump together all methods that use the communication channel between the computing device and the authentication server. Note that the smartphone can also talk to the laptop via Bluetooth®, for example, and thus, the smartphone can be the authentication device with the same communication channel as well.

We believe that with the laptop, equipped with the TPM chip, and the use of a USB token, a Bluetooth smartphone offers a very secure solution, and keeping the same communication channel – to the laptop – gives a good association between the application and the authentication. At this time, we feel this communication channel offers the fewest moving parts.

Still fewer moving parts?

Modern laptops are equipped with memory encryption and secure execution. Identity theft is typically done via phishing, online attacks and, at times, with malware. Few attackers steal laptops for typical identity theft. And if so, SecureDoc™ full disk encryption and file encryption can help secure the laptop.

Considering the attacks and the technologies on the PC, it seems to us a software-based token can more than adequately protect the private key and would help businesses ease into the passwordless era with few moving parts. WinMagic's "SecureDoc token" supports TPM, FIDO tokens, non-FIDO tokens like smartcard/PIV card (uniquely), and the most flexible software token – no hardware or management and maintenance costs.

A SecureDoc token could be used not only as one of the many tokens that retailers give their customers to do online businesses but also for the workforce for various applications, including Windows login, websites, SaaS and VPN. It enables easy entry now and is future-proof, offering the highest-end and most secure solution where applicable.

SOME OBSERVATIONS RELATED TO MULTI-FACTOR AUTHENTICATION (MFA)

Authentication is often associated with multi-factor authentication. MFA includes knowledge (something the user and only the user knows, such as a password); possession (something the user and only the user has, such as a hardware token); inherence (something the user and only the user is, such as biometrics or the speed/cadence with which the user types).

For the described authentication, we observe:

The only thing the server can use is data, which comes from the device over the network (Internet included). The server cannot physically verify the possession or biometrics. We could think "what you have" refers to something like the physical key. But we can leave the exact definition to the best minds.

In any case, we see some deviations from the desire for strong MFA in the described scenario. On the one hand, it is understandable that MFA can be a requirement to access someremote servers. On the other hand, the local gesture here can be minimal to give a positive user experience, mainly because the user is already using the computing device and won't need to re-authenticate to the device again.

(Strong) Multi-Factor Authentication in turn should apply when it comes to the authentication to a local device – for example, the laptop. The laptop itself is equipped with USB ports for tokens, smart card readers or biometric sensors like fingerprint readers, microphones and cameras.

WinMagic offers MFA for pre-boot authentication for its full disk encryption and on top of BitLocker, but many businesses use PIN or even no authentication – no PBA – at all. But this is another story. Note that for remote authentication, an out-of-band communication channel can be used, and the same idea applies that the only thing the server sees is data.

The term 'Passwordless' in Passwordless Authentication

We concluded that "passwordless" means there won't be any centrally managed or centrally stored passwords! Passwordless Authentication refers to authentication to the server. It does not mean that the user can no longer use passwords for the local gesture.

Updated: June 2022 WinMagic Inc.

AUTHENTICATION AS PART OF THE APPLICATION – NEXT STEPS

As we move to the passwordless era, the industry will add these authentications to applications like VPNs and others, including legacy applications. Some websites have added support for FIDO. We are excited to see strong authentication gaining traction; we believe it will make identity theft a thing of the past. We hope our viewpoints and explanations are useful to you and that you enjoyed this read.

CONCLUSION

01

Industry efforts with passwordless authentication will most likely eradicate identity theft and, thus, the main source of online data breaches. Users will also no longer struggle with many long, complex passwords.

02

The communication channel for authentication is more secure with the computing device than an out-of-band channel like the smartphone. Not using the smartphone is easier, too!

03

We are in the early stages of the passwordless era. There is some support from the largest players, for example, for FIDO on websites and SaaS today, but not everywhere. Vendors of most popular applications – servers – will offer passwordless solutions within the next few years, and standards will make this mostly a plug-and-play affair between application and authentication, server and clients.

04

We believe WinMagic will contribute first with comprehensive multi-platform client software, supported from the lowest to the highest end. The computing device – mainly the laptop – offers a built-in crypto-chip in TPM or, even when without TPM, secure execution that allows businesses an easy entry to the passwordless era with the fewest moving parts.

Note: SecureDoc token also supports the existing (PIV) smartcard for FIDO authentication – with no token at all!

05

WinMagic's SecureDoc Endpoint Encryption – endpoint presence – and now passwordless authentication can offer the best user experience on everything encryption and authentication on the endpoint. SecureDoc uniquely offers single sign-on from an MFA pre-boot authentication to passwordless authentication servers.

WINMAGIC

AUTHENTICATE. ENCRYPT. ACHIEVE.

Contact WinMagic to Learn More

WinMagic is a leading developer of cybersecurity solutions that, over the course of 20 years, has raised the bar for endpoint encryption. As a result of extensive experience with securing the endpoint – and a commitment to continuous innovation – WinMagic is trusted by over 2,500 businesses and government agencies around the world and has over 3 million active licenses globally. WinMagic's authentication and encryption suite of products protects data within any laptop, physical or virtualized data center, on-premise or in the cloud. The company's solutions are platform-independent, able to secure data on devices using Windows, Linux, and Mac systems. WinMagic has earned wide recognition for protecting against threats and data loss while helping businesses meet privacy and regulatory compliance requirements. WinMagic delivers a secure, seamless authentication and encryption experience and offers solutions that free customers to think, share and achieve their goals, knowing employees and data are protected. For more information, visit winmagic.com.

WINMAGIC

US & Canada
+1 888 879 5879

EMEA
+49 69 175 370 530

Japan
+03 5403 6950

For more information, click here or contact WinMagic