Whitepaper

SecureDoc™ by WinMagic

PASSWORDLESS AUTHENTICATION
Some WinMagic Viewpoints

Introduction

Data breaches have been the number one security concern for businesses in many years. According to the Verizon Data Breach Investigation 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 user; and the many and long passwords, while cumbersome and very annoying, didn'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 whitepaper, WinMagic shares our viewpoints on these topics/key findings:

- Industry effort with passwordless authentication will most likely eradicate identity theft and thus the main source of online data breaches
- Users will no longer struggle with many and long complex passwords
- We are in early stage of passwordless era
- Considering the attacks and all, Passwordless solutions might be easily done on the client side (for example, via the deployment of software tokens)
- And the server side will follow, much faster than the progress in the last several years

The Authentication Scenario in Question

Let us examine the various actions in the authentication scenario the "passwordless" movement intends to change. You are using a computing device – say the laptop – and you want to login a website, say Gmail – the "server". Two distinct actions take place here:

1. **The remote authentication**, occurring between the server and the device. Among others, the verification takes place in the server, remote from where the user or the device sit.
2. **The local gesture:** On the local device, the user might use some local gesture to prompt the device to perform the authentication with the server.

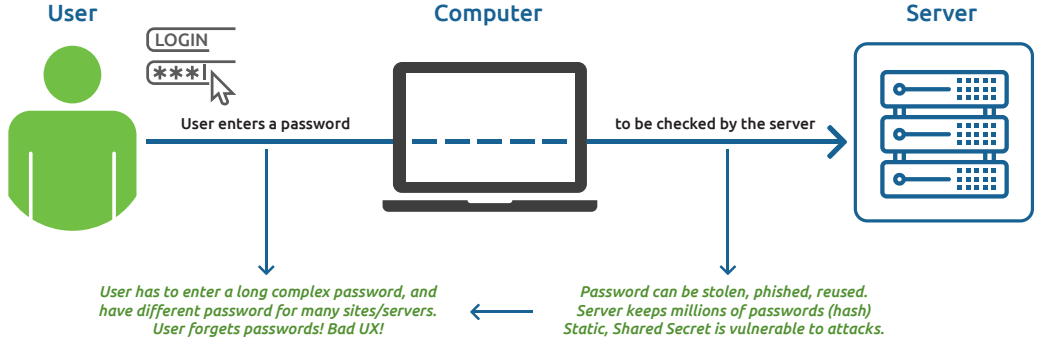
The Remote Authentication

Current Remote Authentication with username and password

The current "username and password" authentication is:

1. Agree on a password, and
2. Have the server compare its version – e.g. a hash - with what the user entered.

"Username and Password" Authentication

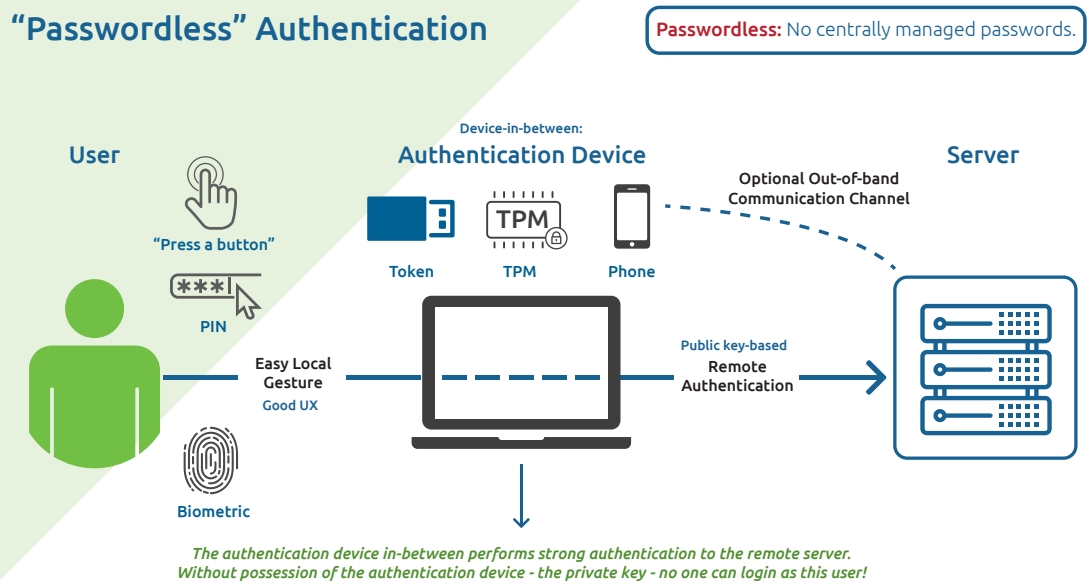


Attackers can get your current password – through phishing or other attacks. They can login from some device somewhere on the Internet and get access to the website as if you do it, often regardless of how difficult or strong you made the passwords. Having a long, complex password, and different passwords for different websites or servers reduce some effectivity of some attacks, but not much more. This, despite your heroic effort to remember those passwords without writing them down.

For secure remote authentication, the new solution makes it so that even if the attacker has all the computing power of the whole world the authentication is still considered unbreakable.

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 must come from the user, the only one who has the private key. The authentication including the verification can be done without a shared secret; without user sharing the private key.



The function of the "device":

At this time, we observe:

- 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.
- 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 operation, must have the private key for the corresponding public key on the server. And, if the private key cannot be copied out of the device, no one can authenticate without the device.
- So, the "device" enables the remote authentication to be secure, very secure indeed, e.g. zillions of times more secure than your longest and most complex password. If somehow this "device-in-between" can also enable you not 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 phone), or One Time Password (OTP) to be deprecated over time.

In this whitepaper, we only consider 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 level.

The Local Gesture

As discussed above, on the local device, the user might use 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, an authentication to the local device. You are already using it!

So, in the typical scenario, the local gesture you need to do, 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, the secure storage and when operating (secure execution). 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 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 are equipped with features to help protect data. Crypto tokens (USB), smartcards, and TPM typically contain crypto chips and should do this job well. The phone and the 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 and at this early stage, we like Gartner's recommendation to "Craft a cohesive strategy that combines the fewest moving parts to implement passwordless authentication across key use cases". 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:

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

We will discuss the communication channel below.

Using the cell phone in a different communication channel

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

We believe that the laptop, equipped with the TPM chip, and the use of a USB token, a Bluetooth phone 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, secure execution. Identity theft is typically done via phishing, online attacks and at times with malware. Few attackers steal the laptops for typical identity theft. And if so, SecureDoc full disk encryption and file encryption 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 passwordless era with few moving parts. WinMagic's "SecureDoc token" supports TPM, FIDO tokens, non-FIDO token like smartcard/PIV card (uniquely), and the most flexible software token – no hardware, managing and maintenance cost.

A SecureDoc token could be used not only as one of the many tokens retailers give their customers to do online businesses, but also for the workforce for various applications including Windows logon, Website, SaaS and VPN. Easy entry now and future proof with highest-end and most secure solution where applicable.

Authentication as a part of the Application – Next Steps

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

Conclusions

- Industry effort with passwordless authentication will most likely eradiate identity theft, and thus, the main source of online data breaches. Users will also no longer struggle with many, and long complex passwords.
- The communication channel for the authentication is more secure with the computing device than an out-of-band channel like the phone. Not using the phone is easier, too! To be precise, if you use an Internet café's device then that device is not your authentication device and some out-of-band solution like the phone would be useful.
- We are in early stage of passwordless era. There is some support from the largest players, for example, for FIDO on website, 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.
- We believe WinMagic will contribute firstly with a comprehensive multi-platform client software supporting from the easiest to the highest end. The computing device – mainly the laptop – offers built-in crypto-chip in TPM, or even when without TPM, secure execution that allow businesses an easy entry to the passwordless era, with fewest moving parts. Note: SecureDoc token also support the existing (PIV) smartcard for FIDO authentication, and no token at all!
- 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.

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 one hand, it is understandable that MFA can be a requirement to access some remote 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 exactly 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 Reader, or biometric sensors like fingerprint readers, microphones and cameras. WinMagic offers MFA for preboot authentication for its full disk encryption and on top of BitLocker, but many businesses uses PIN or even no authentication – no PBA – at all. But this is another story.

Note that for remote authentication 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 for the local gesture user no longer can use passwords.

July 2020, WinMagic Inc.

US & Canada +1 888 879 5879 | **United Kingdom** +44 0148 334 3020 | **Germany** +49 69 175 370 530 | **Japan** +03 5403 6950 | **APAC** +65 9634 5197