TWO-FACTOR AUTHTICATION:

WHAT YOU NEED TO KNOW

White Paper November 2021
By Christopher Birkbeck

Contents

Executive Summary

Today, a critical computer security issue facing all organizations is authentication, the verification of the identities of people interacting with the organization's computer systems. Since the beginning of computing, systems have used passwords as their sole authentication method. However, passwords have revealed their flaws, resulting in many security breaches. In response, security researchers have developed Two-Factor Authentication (2FA) systems that attempt to addresses these faults.

This paper will examine the shortcomings of passwords, explain how Two-Factor Authentication (2FA) addresses those shortcomings and the pros and cons of a few 2FA systems available. Finally, it makes a few comments on which systems should or should not be implemented and how organizations can integrate those systems to an overall security strategy.

Introduction

Authentication is the process of determining if somebody is who they say they are, that is, the confirmation of an identity. Any serious business on the Internet requires all parties to have an identity, such as a consumer buying a product on webstore, or a caller entering a conference call.

The standard authentication method is the password, a secret string of letters, numbers and punctuation (or characters) that only the user knows, but the user has recorded in the machine beforehand. The first usage of passwords in computing is in 1961, when computers were massive machines shared between users. The presence of multiple users on a single machine required identities to differentiate between users. The system works as follows:

1. When a person first starts using a computer, they create a new account with a unique username and password.
2. To use the computer, they must first login and authenticate their identity. At the login screen, they must enter their username and then the password. If what they typed matches what the computer has stored on the machine, the system authenticates that user and allows access to the machine. If it does not match, it will not authenticate and allow no access to the machine.

When the World Wide Web became popular in the 1990's, the same authentication scheme was carried over to accounts created and accessed over the web. This is now the predominate use of passwords today.

The Defects of Passwords

In the decades since the introduction of passwords, security experts have discovered their numerous faults:

- Short passwords can be defeated easily with brute force, by simply going through all possible combinations of characters that a password can have. As computers have become faster and faster, the size of the longest password that can be brute forced has increased. At time of writing, hackers can crack any password with less than 8 characters.

Number of Characters	Numbers only	Upper or Lower case letters	Upper or Lower case letters mixed	Numbers, Upper & Lower case letters	Numbers, Upper & Lower case letters, Symbols
3	instantly	Instantly	Instantly	instantly	instantly
4	Instantly	Instantly	Instantly	Instantly	instantly
5	instantly	instantly	instantly	3 secs	10 secs
6	instantly	instantly	8 secs	3 mins	13 mins
7	instantly	instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1 qt years

Figure 1. Time to brute force a password.

- Hackers often do not need to randomly guess at passwords, because some passwords are far more common than other passwords, as examination of hacked password databases show. Common passwords include strings of numbers ('1234567890'), letters ('qwertyuiop'), common words ('monkey') or some variation of these words ('passw0rd'). Hackers can preform a dictionary attack, going through the most common, and thus more likely, passwords first.
- Early security advice suggested using longer, complicated passwords with occasional forced password resets. These suggestions lead to users reusing the same password for different accounts. So, if a hacker gets access to one password, if they know the person's username on other sites, they can breach those accounts as well.

Most common passwords in 2021:

1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 1234567890
9. qwerty123
10. 1234567

Source: https://nordpass.com/most-common-passwords-list/

To address these faults, security researchers recommend that organizations move beyond (just) passwords towards Two Factor Authentication (2FA).

What is 2FA?

2FA uses two factors instead of the single factor of traditional password authentication. Typically, this mean using password as one of the factors alongside another factor. An authentication factor is something that confirms an identity. These can be grouped into three major types:

1. Knowledge factors (something you know): passwords, PINs, secret questions.
2. Possession factors (something you have): SMS passwords, Time-based One Time Password (TOTP), Universal 2nd Authentication (U2F), Push notifications.
3. Inherence factors (something you are): biometrics like fingerprints or voice recognition.

Some security experts also include location factors (somewhere you are) and time factors (sometime you are). But these factors are only useful in limited circumstances, so they are not covered in this paper.

During the 2FA process, users must verify their identity with both factors, and failure to authenticate one identity means the system will deny access. The most widely used and familiar application of 2FA is ATMs. An ATM customer requires both:

1. Knowing the PIN to their account (a knowledge factor).
2. Possessing a bank card (a possession factor).

Thus, even if an account's password is breached, a hacker cannot access the account without also breaking the security of the other factor. Not all factors are made equal, however. The following sections will show the advantages and disadvantages of each method.

Knowledge Factors

Besides passwords, systems will sometimes use other knowledge factors for authentication:

- Secret questions: at account creation, the user will choose one or more questions (often from a set of pre-chosen questions, such as "What is your mother's maiden name?", or "What hospital

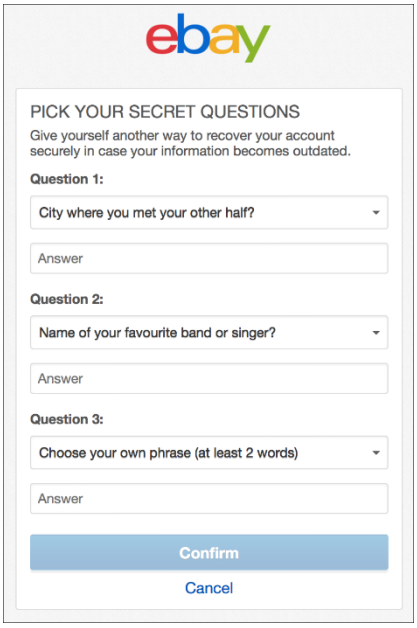


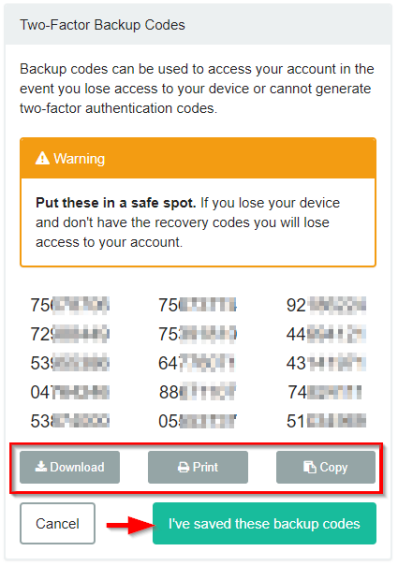
Figure 3. Secret questions.

were you born in?") and enter in answers. At login, the system will authenticate only if the questions are answered correctly.

- Pre-generated codes: at 2FA setup, the system will generate a set of passwords, all being random strings of between 6 to 8 characters. The user stores these codes in a secret location.

Generally, these are used as a backup for other factors: secret questions for password resets and pre-generated codes for a non-password factor. They suffer from the same flaws of passwords.

Figure 2. Secret codes.



Recommendations

Most 2FA schemes use passwords as one of the authentication factors, so both customers and employees should follow good password practices, such as:

- Prefer longer over complex passwords. They should m
- Each account should have its own password.
- Ideally, password should be randomly generated.
- There should be no mandatory password changes, as they encourage password reuse. Passwords should only be changed if either there has been a password breach or the user forgetting the password.
- Encourage the use of password managers, databases which will store passwords so that users do not have to manual remember and type each password. This allows them to use long, random and unique password for each account. Customers can use a simpler personal password manager, while employee should use enterprise password manager, which have additional features like session monitoring.

zzPossession Factors

This paper will focus mostly on possession factors, which prove identity with providing some item that only the account's owner should have.

SMS Passwords

What is it?

When making an account with 2FA enabled, the user enters a cellphone number. At each login, the server will send a text message with a short string of numbers to that cellphone. The user has to enter that code to successfully login.

Advantages:

- SMS Passwords are convenient, as cellphones with text messaging have become common throughout the world.
- No extra cost for users (beyond cost for a cellphone and network access)
- Deployment is easy and cheap.

Disadvantages:

- Some users may not want to give their cell phone number.
- If the number of messages sent is large enough, it becomes expensive.
- Dependent on cellular networks for their reliability and security.
- Text messages are vulnerable to hackers changing the message during transmission (man-in-the-middle attack).
- Cellphones numbers are vulnerable to thief by hackers with phishing and SIM swapping.

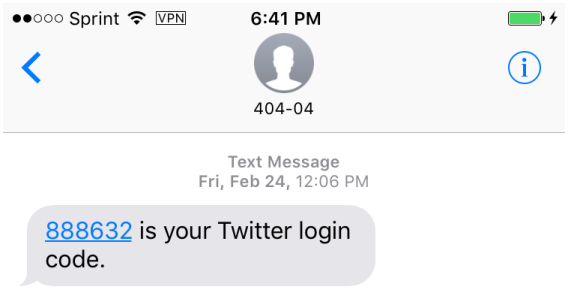


Figure 4. Password sent over text messaging.

Recommendation

Because of their security flaws, SMS passwords are **not** recommended as a 2FA authentication method. At best, they should only be limited as a fall-back measure.

Time-based One Time Password (TOTP)

What is it?

Like with the SMS password, TOTP uses a temporary password to verify a login, but it does not send the password through cellular networks. Instead, it uses authenticator apps on a smartphone, as follows:

1. The user installs an authenticator app onto their smartphone. Some common authenticator apps include Google Authenticator and Microsoft Authenticator.
2. During the 2FA setup process, the website will show a QR code. Users scan the code into the authenticator app. The code contains information about the site along with a secret key that only the server and the app have.
3. During the login process, the apps and server combine the secret key with the time to create the temporary password. The apps will show the password along with a time limit. Users have to enter the password before the time limit expires. Otherwise, the password expires and is not long valid, and the user will have input the new password to authenticate.

Advantages:

- There is no communication between the app and the server, so the app does not need Internet or cellular network access.
- No extra cost to users (beyond cost of smartphones) as most authenticator apps are free.
- Deployment is easy and cheap.

Disadvantages:

- Hackers comprise the system if they steal the secret key.
- Requires a smartphone that is both turned on and in easy reach during login.
- The 30 second time limit can be inconvenient. Logins might require multiple attempts.

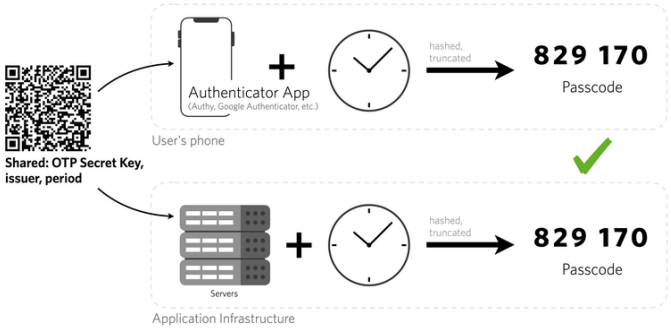


Figure 5. How TOTP work

Recommendation

TOTP fixes many of the security flaws of SMS Passwords while maintaining the same cost and usability. Thus, the TOTP is preferable as a primary 2FA factor over SMS Passwords.

Universal 2nd Factor (U2F) keys

What is it?

Unlike the pervious two methods, U2F does not rely on any user input for authentication. This method uses a special USB key for its authentication. It works as follows:

1. The user purchases a U2F key. Some common keys include the YubiKey and the NitroKey.
2. During U2F setup, the user inserts their key into a USB slot on their computer. When prompted, they press a button on the key to confirm their possession.
3. During U2F authentication, the user inserts their key and press on the button, just as they did during setup.

Advantages:

- U2F is resistant to phishing.
- There are no secrets shared between server and the user's machine, so an attacker cannot defeat the system.
- There is no timed password entry, which reduces errors and user frustration.

Disadvantages:

- U2F keys are expensive. For example, at the time of writing, a YubiKey can cost between 45-80 USD.
- The hardware keys can be lost, thus locking the user out of an account.
- The USB standard has changed over time, so a there are different keys for Type A and Type C connectors.

Figure 6. A Yubikey.

Recommendation

The extra phishing protection U2F comes with the increased cost of buying hardware tokens, either by users or for an organization for its employees. For user applications, they should be available as an option alongside TOTP. For employees, IT must determine if the sensitivity of the work justifies the additional costs.

Push Notifications

What is it?
Push methods uses a smartphone app to send a push notification. Google has built this feature into the Android OS, and some authenticator apps use this as an alterative authentication method.

Advantages:

- No password entry like SMS or TOTP.
- No physical hardware token to buy or lose like U2F.
- Push notification will include the location of the current login request, allowing users to determine if a login is legitimate or not.

Disadvantages:

- Unlike TOTP or U2F, there are no open standards. Thus, users have no choice in choosing their authentication.
- Requires an active Internet connection.

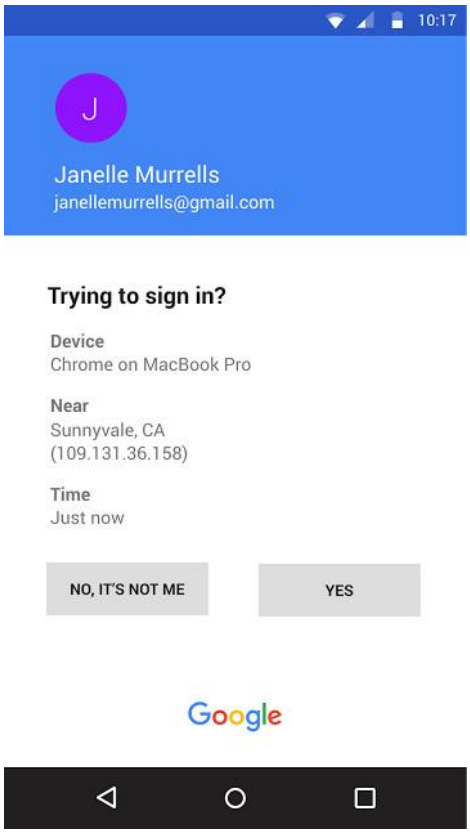


Figure 7. Push notification for a Google account.

Recommendation
Because of the lack of open standards, push notification should be used if it is provided with some other software used by the organization.

Inheritance Factors (Biometrics)

What is it?

Biometrics factors confirms identity based on a unique biological characteristic of an individual. Different biometrics authentication systems include:

- Fingerprint detection
- Retinal scans
- Voice recognition

Advantages:

- There are no passwords that can be intercepted and no keys or smartphones to lose.

Disadvantages:

- If hackers compromise the biometric data, it is impossible to reset, as biological data cannot be changed.
- Many users might be reluctant to use biometric 2FA on privacy grounds, and it is possible that future government regulation will restrict the usage of this data.
- Some forms of biometric authentication require special hardware, like fingerprint readers, increasing the costs.

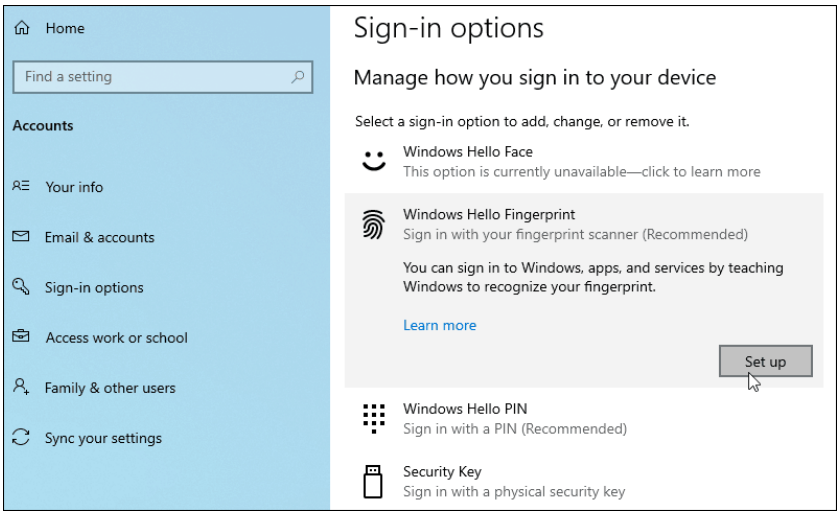


Figure 8. Windows sign-in with fingerprints or face recognition

Summary

For medium to small organization, the increase security does not justify the extra costs. Like with push notifications, only consider it comes with some other software the organization is using.

Summary of Recommendations

- Practice good password security:
  - Use long, random and unique passwords.
  - No mandatory password changes.
  - Use password managers.
- Avoid:
  - SMS passwords
- Consider instead:
  - TTOP
  - U2F
- Consider only if convenient:
  - Push notification
  - Biometrics

Image Credits

Figure 1. https://dialogictelecom.com/2019/02/password-security-keeping-eggs-one-basket/

Figure 2. https://www.intego.com/mac-security-blog/how-to-choose-and-answer-security-questions/

Figure 3. https://support.huntress.io/hc/en-us/articles/4404004941459-Generating-New-2FA-Backup-Codes

Figure 4. https://mshelton.medium.com/two-factor-authentication-for-beginners-b29b0eec07d7

Figure 5. https://www.twilio.com/docs/glossary/totp

Figure 6. https://privacyaustralia.net/yubikey-review/

Figure 7. https://www.neowin.net/news/google-to-push-those-still-using-sms-two-factor-login-towards-google-prompt-from-next-week/

Figure 8. https://www.intego.com/mac-security-blog/how-to-choose-and-answer-security-questions/

References

Anderson, M. (2020, April 19). TOTP Two-Factor Authentication (2FA)—Pros and Cons. *JumpCloud*. https://jumpcloud.com/blog/totp-2fa-pros-cons

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). "It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–11. https://doi.org/10.1145/3173574.3174030

Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A.-R. (2014). On the (In)Security of Mobile Two-Factor Authentication. In N. Christin & R. Safavi-Naini (Eds.), *Financial Cryptography and Data Security* (Vol. 8437, pp. 365–383). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-45472-5_24

Edelstein, H. (2019, February 25). *The Problem with Your Password? Everything.* Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/

Gebhart, J. H.-A. and G. (2017, September 22). *A Guide to Common Types of Two-Factor Authentication on the Web*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2017/09/guide-common-types-two-factor-authentication-web

Gunson, N., Marshall, D., Morton, H., & Jack, M. (2011). User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, *30*(4), 208–220. https://doi.org/10.1016/j.cose.2010.12.001

Hasley, M. (2012, April 7). *How Secure is Your Password? - GHacks Tech News*. GHacks Technology News. https://www.ghacks.net/2012/04/07/how-secure-is-your-password/

Olynyk, M. (2019, July 18). *SMS Authentication: All Pros and Cons Explained - Protectimus Solutions*. Protectimus. https://www.protectimus.com/blog/sms-authentication/

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Orrok, K. (2016, August 18). *Are Security Questions Considered Two-Factor Authentication?* https://www.eci.com/blog/15875-should-answering-security-questions-really-be-considered-two-factor-authentication-.html

Pomputius, A. F. (2018). A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory. *Medical Reference Services Quarterly*, *37*(4), 397–402. https://doi.org/10.1080/02763869.2018.1514912

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (n.d.). *A Usability Study of Five Two-Factor Authentication Methods*. 15.

Shaklett, M. (2021, September). *What is Authentication?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/authentication

Sumo Logic. (2021). *What is an Authentication Factor?* Sumo Logic. https://www.sumologic.com/glossary/authentication-factor/

Twilio. (2021). *What is a Time-based One-time Password (TOTP)?* https://www.twilio.com/docs/glossary/totp?utm_source=docs&utm_medium=social&utm_campaign=guides_tags