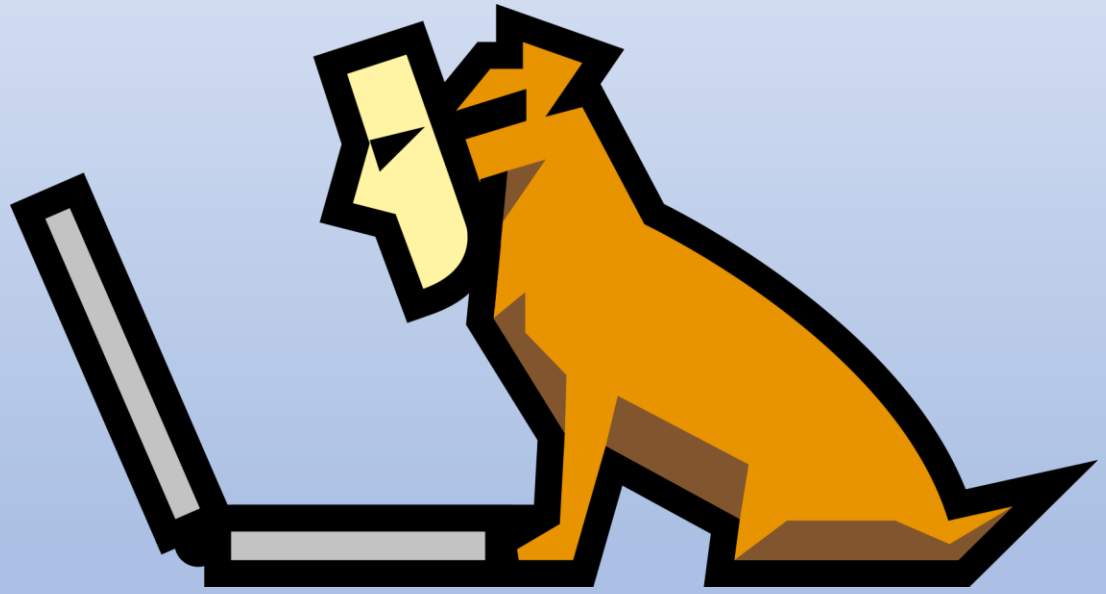
Two Factor Authentication: What You Need to Know

Christopher Birkbeck

Who should see this?

- Anybody who is unaware of …
  - … what Two Factor Authentication is.
  - … what their 2FA options are out there.
  - … what their pros and cons.
- Very basic overview; meant for those without much technical background.
- Generally aimed those in small to medium sized businesses, with a focus on the customer experience, but 2FA for employee is briefly considered.

Identity



- Any serious business on the Internet requires the people to have identities.
- **Authentication** is the process of confirming that identity.

Passwords

- Used in computing since 1961!
- Used everywhere.
- Recap:
    1. At user account creation: choose a username and password.
    2. At login: user enters username and password.
    3. If what they typed matches the recorded password, allow person to use the machine.

The Problem with Passwords

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

- Modern computers are fast enough that they simply can try *all* combination of characters to guess a password: **brute force attack**
- Any password less than 8-12 character is basically useless nowadays.

The Problem with Passwords

- But often hackers don’t need to guess – some passwords are *much* more common that others.
- Examples: ‘1234567’, ‘password’, ‘qwerty’
- Attackers can try those passwords before using others: **dictionary attack**.
- People will often use the same password on the different account, as they are easier to remember!
- If an attacker get one of the passwords, they can use it the get access other accounts.

Best Password Practices

- Passwords should be **long**.
- Passwords should be **unique**.
- Passwords should be **randomly generated**.
- Passwords should be stored in a **Password Manager**.
  - There are password managers made for both personal and enterprise use.
- Use **Two Factor Authentication**

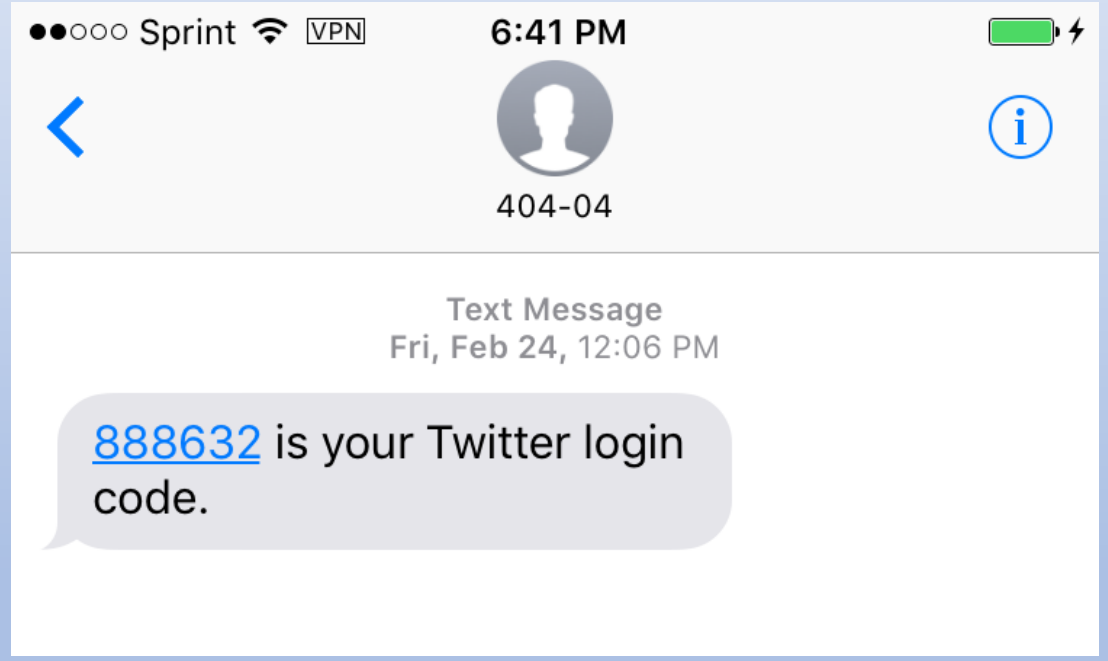
What is Two Factor Authentication?

- Instead of proving identify by one method, use two methods.
- If any fail, do not allow use.
- Currently uses passwords as one of the factor, but does not have to use it.

Factor		Examples
Knowledge	What you know.	Passwords, PIN, secret questions
Possession	What you have.	SMS passwords, Temporary One-Time Passwords (TOTP), Universal 2nd Factor (UTF), Push notifications
Inherence	What you are.	Biometrics (fingerprint, voice recognition)

SMS Password

1. At account creation: add a cell number.
2. At login, service sends to the cell phone a temporary password of 6-8 digits.
3. User then types in the password at the prompt.



SMS Passwords

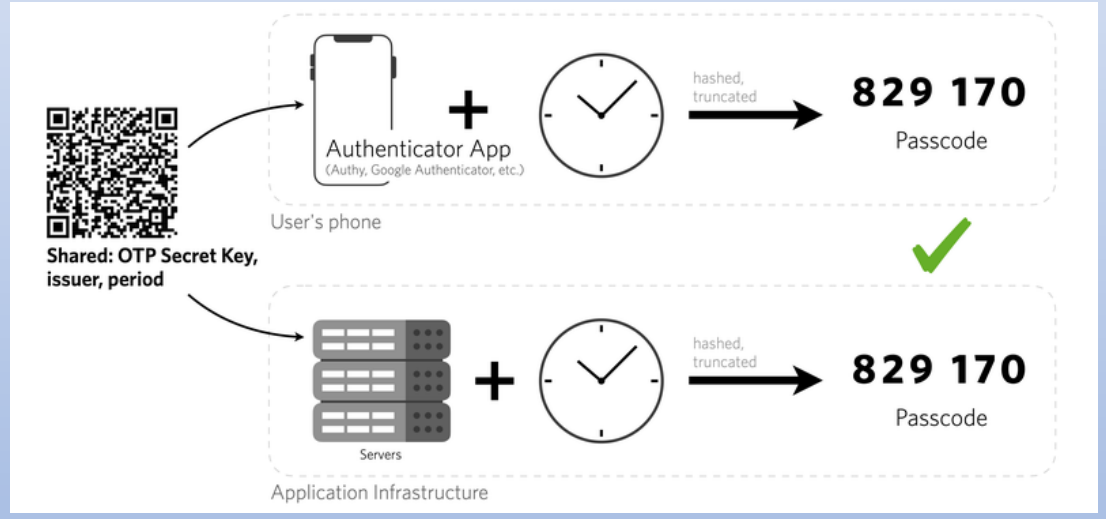
Advantages

- 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.

Time-based One Time Passwords (TOTP)



1. Install an authenticator app (e.g., MS Authenticator, Authy)
2. At 2FA setup, scan in a QR code into the app.
3. At login, type in the temporary password before the time limit (It will change in 30 seconds!).

Time-based One Time Passwords (TOTP)

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 compremise 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.

Universal 2nd Factor (U2F)

1. Buy a U2F key.
2. At 2FA setup, plugin the key into a USB port. Press the button the key when prompted.
3. At login, when prompted, plugin the key and press the button when prompted.

Universal 2nd Factor (U2F)

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.

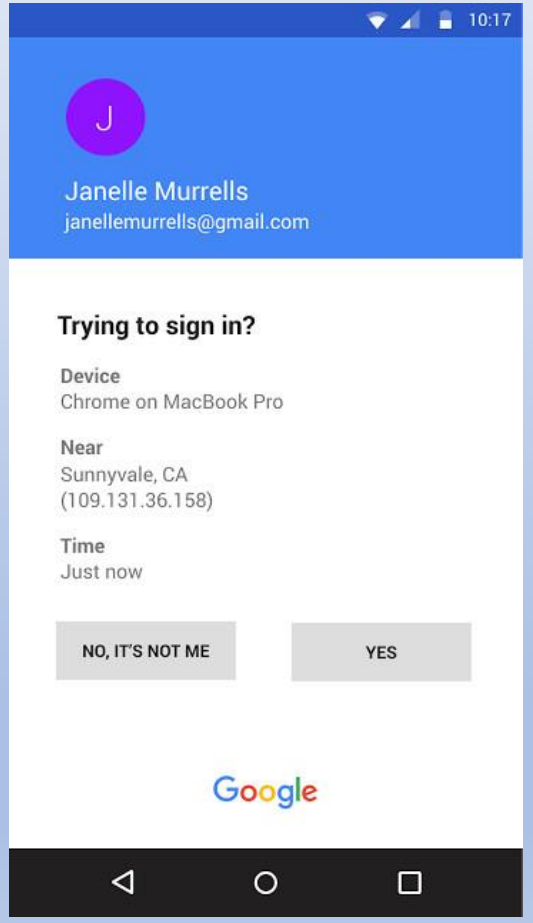
Disadvantages

- 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.

Push Notification

- Built into some apps.
- Google has built into the Android OS for Google Accounts.

- Uses the push notification system on smartphones for authentication.



Push Notification

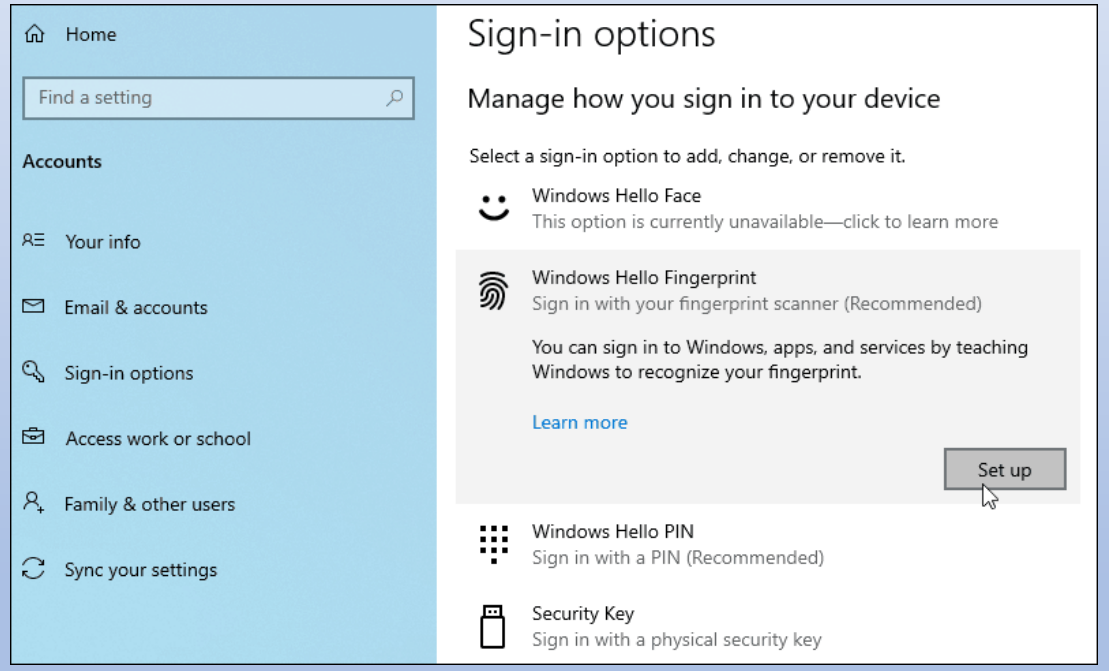
Advantages

- 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.

Biometrics



- Use a physical identities of a person to verify their identity.
- Examples:
  - Face Recognition
  - Fingerprint Detection
  - Voice Identification

Biometrics

Advantages

- There are no passwords that can be intercepted and no keys or smartphones to lose.
- Very easy, person just has provide the physical characteristic to the speaker.

Disadvantages

- Impossible to reset
- Could raise privacy concerns among users and governments.
- May require special hardware
- Deployment is hard for small and medium companies at the moment

Recommendations

- Practice good password security (long, random and unique passwords, use a password manager)
- Avoid SMS Passwords
- Consider using: TOTP or U2F
- Consider if convenient: Push Notifications or Biometrics