FOUNDATIONS IN IT SECURITY: THE 5 FACTORS OF AUTHENTICATION

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)

TODAY ….

Today we will overview Multi-Factor Authentication, which includes:

- Defining the various factors.
- Out-of-Band Authentication

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: OVERVIEW

GORDON | REYNOLDS (2018)

OVERVIEW

- Today, the terms
  - "Multi-Factor Authentication",
  - "Two-Factor Authentication"
  - "Dual-Factor Authentication" are common place.
- Most people associate multi-factor authentication with entering a username or email, a password and a token which expires after 30 seconds.
- But there is a lot more to Multi-Factor Authentication.

GORDON | REYNOLDS (2018)

WHAT IS A FACTOR?

- A factor is a type of authentication.
- When you claim to be someone, you need to provide further information to prove that you are who you say you are.
  - For instance, suppose that you go to an ATM and use your credit or debit card. After the card is inserted into the machine, it will be used to claim an *identity*.
  - Now, how does the ATM know that whoever is in possession of the card is the owner of the card?
    - It knows by asking something that only the owner would be able to provide! That could be a password, a fingerprint or a 6–8 digit code which expires after a certain number of seconds.
    - These are all different types of information which are used for authentication purposes — they are factors of authentication.

GORDON | REYNOLDS (2018)

FACTOR #1 SOMETHING YOU KNOW

- Information is classified as *something you know* if you store it in your memory and can retrieve it when needed.
  - For instance, a password, an answer to a security question or a Personal Identification Number (PIN).
  - Memorising passwords nowadays is generally not advisable, a **Password Manager** should be used.

GORDON | REYNOLDS (2018)

FACTOR #1 SOMETHING YOU KNOW

- **Are usernames and email addresses a *something you know* factor?**

GORDON | REYNOLDS (2018)

FACTOR #1 SOMETHING YOU KNOW

- **Not really.**
- Usernames and email addresses are only used to *claim* an identity.
- A password or PIN (a type of authentication) is then used to prove the identity (i.e. to authenticate).

GORDON | REYNOLDS (2018)

FACTOR #2 SOMETHING YOU HAVE

- This factor refers to information that you can (physically) carry with you.
  - For example, before you send money to someone, many banks will ask you for a token (also referred to as one-time password and usually 6–8 digits long) that expires either after first use or after 30 seconds.
  - The token is usually generated by a device such as the **RSA SecurID.**
  - Depending on the bank, they might offer a mobile application which generates the token.

GORDON | REYNOLDS (2018)

FACTOR #2 SOMETHING YOU HAVE

- There are two open standards for generating these tokens:
  - HMAC-based One-Time Password (HOTP)
  - Time-based One-Time Password (TOTP).
- Essentially, HOTP generates a token which does not expire until the user uses it for the first time (after which a new token will need to be generated).
- TOTP generates a token every 30 seconds. If a user does not use it within 30 seconds, a new token will be automatically generated.
- Tokens are not classified as *something you know* because, well, you don't know the token until you actually see it!

GORDON | REYNOLDS (2018)

FACTOR #3 SOMETHING YOU ARE

- This factor generally refers to Biometrics.
- Simply put, *something you are* is an information that is in you.
- It's a characteristic that only you and no one else has it. These include,
  - Your fingerprint or thumbprint,
  - Palm or handprint,
  - Retina or iris scans,
  - Voice or facial recognition.

GORDON | REYNOLDS (2018)

FACTOR #4 SOMEWHERE YOU ARE

- This factor may not be as well known as the ones already mentioned.
- *Somewhere you are* is related to your location.
  - One of the most common methods of detecting a user's location is via Internet Protocol (IP) addresses.
- For instance, suppose that you use a service which has *Geolocation security checks*.
  - When you configure your account, you might say that you live in the Ireland.
  - If someone tries to log in to your account from an IP address located in Germany, the service will probably notify you saying that a login attempt was made from a location different than yours.
  - That is extremely useful to protect your account against hackers.

GORDON | REYNOLDS (2018)

FACTOR #4 SOMEWHERE YOU ARE

- As an example,
  - Monzo Bank Ltd., a mobile-only bank based in the United Kingdom, uses Geolocation to detect possible payment frauds.
  - If your last known location was, say, in France and then four minutes later your card is used in Japan, that could be an indication that you are not in the same location as your card.

GORDON | REYNOLDS (2018)

FACTOR #4 SOMEWHERE YOU ARE

- IP addresses, however, are not the only information that can be used for the *somewhere you are* factor.
- It is also possible to use Media Access Control (MAC) addresses.
- An organization might set up its network so only specific computers can be used to log in (based on MAC addresses).
- If an employee is trying to access the network from a different computer, the access will be denied.

GORDON | REYNOLDS (2018)

FACTOR #4 SOMEWHERE YOU ARE

- Other examples include Revolute,
  - Revolute is a global online/mobile app based financial services organisation.
  - It is possible to link the usage of your bank card to the location of your mobile phone.
  - Hence, thieves can not use your bank card, or a clone of your bank card, unless it is in the vicinity of your mobile phone.

GORDON | REYNOLDS (2018)

FACTOR #5 SOMETHING THAT YOU DO

- This is possibly the factor that is the least utilised and less known.
- *Something you do* is a type of authentication which proves identities by observing actions.
- These actions could be things like gestures or touches.
  - Windows 8 users might recall a feature called **Picture Password** (similar to Android Pattern Lock)
  - This feature allows the user to set up gestures and touches on a picture as a way to authenticate themselves.

GORDON | REYNOLDS (2018)

VIDEO

- 34m

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: SFA, 2FA, MFA

GORDON | REYNOLDS (2018)

SFA , 2FA , MFA

- A system can use one or more factors for authentication.
- When only one factor is used, it is called **Single-factor authentication**.
- When two factors are used, it is called either
  - **Two-factor authentication** or **Dual-factor authentication**.
- Finally, when two or more factors are used, it is called **Multi-factor authentication**.
  - The word *multiple* usually refers to *more than one*, which means that when two factors are being used, it can be referred to as either Two-factor or Multi-factor authentication.

GORDON | REYNOLDS (2018)

MULTI-STEP AUTHENTICATION VS MULTI-FACTOR AUTHENTICATION

- Sometimes, instead of two-factor or multi-factor authentication, you will see two-step or multi-step authentication.
- **What's the difference between multi-step and multi-factor?**

GORDON | REYNOLDS (2018)

MULTI-STEP AUTHENTICATION VS MULTI-FACTOR AUTHENTICATION

- **What's the difference between multi-step and multi-factor?**
  - The difference is that multi-step authentication validates factors separately and multi-factor authentication validates them all at once.

GORDON | REYNOLDS (2018)

MULTI-STEP AUTHENTICATION VS MULTI-FACTOR AUTHENTICATION

- Think about a system which requires a username and a password, followed by a token.
- If the authentication is ***multi-factor***,
  - The system will not validate the username and password until the token is provided.
  - They will all be validated at once.
  - The advantage of this approach is that if the login fails, one cannot know whether the username, the password or the token was wrong.

GORDON | REYNOLDS (2018)

MULTI-STEP AUTHENTICATION VS MULTI-FACTOR AUTHENTICATION

- Think about a system which requires a username and a password, followed by a token.
  - However, if the authentication is ***multi-step***,
    - The system will first validate the username and password.
    - If both are correct, the token will be validated.
    - This approach is not ideal because if the username and password are correct, the process then becomes single-factor authentication — the only unknown factor now is the token.

GORDON | REYNOLDS (2018)

MULTI-STEP AUTHENTICATION VS MULTI-FACTOR AUTHENTICATION

- In some cases, multi-step and multi-factor authentication are used together, one after the other.
- You could, for instance, use multi-step to log into your computer and then use multi-factor to log into your company's Virtual Private Network (VPN).

GORDON | REYNOLDS (2018)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: OUT-OF-BAND AUTHENTICATION

GORDON | REYNOLDS (2018)

OUT-OF-BAND AUTHENTICATION

- Out-of-Band (OOB) means that authentication factors are transmitted via different channels or networks.
- This means that the device you use to enter a factor (e.g. *something you know*), is different than the device you use to receive or generate another factor (e.g. *something you have*).
  - For instance, if you are on a website in your computer and you enter your username and password and a token is required next, the token needs to be generated by a different *channel* — an application on a cell phone or a device such as the RSA SecurID.
  - An example of non-OOB authentication would be if the application used to generate tokens is located on the same device (e.g. computer or cell phone) as the one used to enter the username and password.

GORDON | REYNOLDS (2018)

OUT-OF-BAND AUTHENTICATION

- **Use of Short Message Service (SMS) for Out-of-Band Authentication**
- According to a special publication from the National Institute of Standards and Technology (NIST) about Digital Identity Guidelines (800–63B), SMS is not to be used for Out-of-Band authentication because an attacker, through Social Engineering, could potentially induce a mobile operator to redirect the victim's cell phone traffic to the attacker.

GORDON | REYNOLDS (2018)

SUMMARY ….

Today we overviewed Multi-Factor Authentication, which includes:

- Defining the various factors.
- Out-of-Band Authentication

GORDON | REYNOLDS (2019)