Security Engineering: Passwords and their limitations

Password

- a secret word or phrase or code that you need to know in order to have access to a place or system

- it is a series of letters or numbers that you must type into a computer or computer system in order to be able to use it

- A password is a real-life implementation of challenge-response authentication (a set of protocols to protect digital assets and data).

Password

- Definition:

- A string of characters i.e letters, numbers, special characters, used to verify the identity of a user during the authentication process is known as password

Password Management

- Since passwords are meant
  - to keep the files and data secret and safe
  - so it is prevented the unauthorized access,

- Password management refers to
  - the practices and
  - set of rules or principles or standards

- that out must follow or at least try to seek help from in order to be a good/strong password and along with its storage and management for the future requirements.

Issues Related to Managing Passwords

- It is not safe to use the same password for multiple sites, therefore having different passwords for different sites and on top of that remembering them is quite difficult

- As per the statistics, more than 65% of people reuse passwords across accounts and the majority do not change them, even after a known breach

- Meanwhile, 25% reset their passwords once a month or more because they forgot them

Password Manager

- To escape from this situation people often tend to use password managers

- A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services

- Password managers to a certain extent reduce the problem by having to remember only one “master password” instead of having to remember multiple passwords

Password Manager

- The only problem with having a master password is that once it is out or known to an attacker, the rest of all the passwords become available

- The main issues related to managing passwords are as follows:
- Login spoofing - fake login page created
- Sniffing attack - captures data packets
- Brute force attack - try out multiple passwords
- Shoulder surfing attack - observe entering passwords(Happens in ATM,pass on comp etc)
- Data breach - hacking, malicious attacks

Methods to Manage Password

- There are a lot of good practices that we can follow to generate a strong password and also the ways to manage them

- **Strong and long passwords:**
- A minimum length of 8 to 12 characters long,
- also it should contain at least three different character sets (e.g., uppercase characters, lowercase characters, numbers, or symbols)

Methods to Manage Password

- **Password Encryption:**
- Using irreversible end-to-end encryption is recommended
- In this way, the password remains safe even if it ends up in the hands of cybercriminals.

- **Multi-factor Authentication (MFA):**
- Adding some security questions and
- a phone number that would be used to confirm that it is indeed you who is trying to log in will enhance the security of your password.

Methods to Manage Password

- **Make the password pass the test:**
- Yes, put your password through some testing tools that you might find online in order to ensure that it falls under the strong and safe password category

- **Avoid updating passwords frequently:**
- Though it is advised or even made mandatory to update or change your password as frequently as in 60 or 90 days.

Attacks on Passwords

- Password attacks are one of the most common forms of corporate and personal data breach
- A password attack is simply when a hacker try to steal your password
- 81% of data breaches were due to compromised credentials

Attacks on Passwords

- Because passwords can only contain so many letters and numbers, passwords are becoming less safe

- Hackers know that many passwords are poorly designed, so password attacks will remain a method of attack as long as passwords are being used

Phishing

- Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email,
- hoping you will reveal your personal information voluntarily
- Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device
- Here are a few examples of phishing

Phishing

- **Regular phishing**

- You get an email from what looks like goodwebsite.com asking you to reset your password,

- but you didn't read closely and it's actually goodwobsite.com

- You "reset your password" and the hacker steals your credentials

Phishing

- **Spear phishing**

- A hacker targets you specifically with an email that appears to be from a friend, colleague, or associate

- It has a brief, generic blurb ("Check out the invoice I attached and let me know if it makes sense.") and hopes you click on the malicious attachment

Phishing

- **Smishing and vishing**
- You receive a text message (SMS phishing, or smishing) or phone call (voice phishing, or vishing) from a hacker who informs you that your account has been frozen or that fraud has been detected

- You enter your account information and the hacker steals it

To avoid phishing attacks

- **Check who sent the email:**
- look at the From: line in every email to ensure that the person they claim to be matches the email address you're expecting
- **Double check with the source:**
- when in doubt, contact the person who the email is from and ensure that they were the sender.
- **Check in with your IT team:**
- your organization's IT department can often tell you if the email you received is legitimate.

Man-in-the-Middle Attack

- Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords

- If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle.

Man-in-the-Middle Attack

- Similarly, in 2017, Equifax removed its apps from the App Store and Google Play store because they were passing sensitive data over insecure channels where hackers could have stolen customer information

prevent man-in-the-middle attacks

- **Enable encryption on your router**
- If your modem and router can be accessed by anyone off the street, they can use "sniffer" technology to see the information that is passed through it.

- **Use strong credentials and two-factor authentication**
- Many router credentials are never changed from the default username and password.
- If a hacker gets access to your router administration, they can redirect all your traffic to their hacked servers.

prevent man-in-the-middle attacks

- **Use a VPN**
- A secure virtual private network (VPN) will help prevent man-in-the-middle attacks by ensuring that all the servers you send data to are trusted.

Brute Force Attack

- If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram

- A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs

prevent brute force attacks

- **Use a complex password**

- The difference between an all-lowercase, all-alphabetic, six-digit password and a mixed case, mixed-character, ten-digit password is enormous

- As your password's complexity increases, the chance of a successful brute force attack decreases

prevent brute force attacks

- **Enable and configure remote access**
- Ask your IT department if your company uses remote access management

- An access management tool like OneLogin will mitigate the risk of a brute-force attack.

prevent brute force attacks

- **Require multi-factor authentication**

- If multi-factor authentication (MFA) is enabled on your account, a potential hacker can only send a request to your second factor for access to your account

- Hackers likely won't have access to your mobile device or thumbprint, which means they'll be locked out of your account

prevent brute force attacks

- **Require multi-factor authentication**

- If multi-factor authentication (MFA) is enabled on your account, a potential hacker can only send a request to your second factor for access to your account

- Hackers likely won't have access to your mobile device or thumbprint, which means they'll be locked out of your account

Dictionary Attack

- A type of brute force attack, dictionary attacks

- rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries"

- More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name

prevent a dictionary attack

- **Never use a dictionary word as a password**

- If you've read it in a book, it should never be part of your password.

- If you must use a password instead of an access management tool, consider using a password management system

prevent a dictionary attack

- **Lock accounts after too many password failures.**

- It can be frustrating to be locked out of your account when you briefly forget a password, but the alternative is often account insecurity.

- Give yourself five or fewer tries before your application tells you to cool down.

prevent a dictionary attack

- **Consider investing in a password manager**

- Password managers automatically generate complex passwords that help prevent dictionary attacks.

Credential Stuffing

- If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website

- Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in

- Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them