Contents

1 Usernames and Passwords

- Identification Who you are
- Authentication Verify that identity
- Authentication should expire. Remember my credentials turns this into something you have
- Time of check to time of use TOCTTOU
  - Repeated authentication
  - At the start and during a session

1.1 Problems With Passwords

- People forget them
- They can be guessed
- Spoofing and Phishing (pretend to be a different website)
- Compromised password files
- Keylogging
- Many of these are made many times worse by weak passwords

1.2 Problems with password policies

- This is not a great solution
- People attempt to make their life easier by re-using passwords
- When theyre forced to change to unique passwords, theyll simply increment a counter

1.3 Password shadow files

- Operating systems have taken steps to stop people reading hashes for offline attacks
- These files are now **read protected**
- Administrators or people booting another OS will often find a way in

2 Cracking passwords

- Cracking a password isnt always illegal, though obviously it sometimes is!
- Password cracking falls into two basic types:
- Offline: You have a copy of the password hash locally
- Online: You do not have the hash, and are instead attempting to gain access to an actual login terminal
- Online is usually attempted with phishing
- Offline password cracking quite simply a case of trying possible passwords, and seeing if we have a hash collision with a password list
- Might be a **brute force approach**

2.1 Dictionary Attacks

- Most password cracking is now achieved using dictionary attacks rather than brute force
- Using a dictionary of common words and passwords
- Apply small variations to this list, trying them all
- Combine words from two different lists

3 Password Salting

- We can improve security by prepending a random salt to a password before hashing
- The salt is stored unencrypted with the hash
- If we use a different random salt for each user, we get the following security benefits:
  - Cracking multiple passwords is slower a hit is for a single user, not all users with that password
  - Prevents rainbow table attacks we cant pre-compute that many password combinations
- Salting has no effect on the speed of cracking a single password so make your passwords good!

4 Hashing Speed

- When password cracking, the most important factor is hashing speed
- Newer algorithms take longer: partly because theyre more complex, but some have been specifically designed to take a while
- Iterate to increase complexity - PBKDF2
- bcrypt cant be used on easily GPUs

5 Pretexting

- Obtaining private details by offering some pretext as a reason for needing them
- We continue to rely on email addresses, DOB and Mothers maiden names as our last line of defense for security.
- What are alternatives?

6 Multi-factor authentication

- Combines something you know with something you have
- Common examples:
- Text codes to mobiles
- One time passwords, Google Authenticator, Microsoft Authenticator etc.
- USB devices e.g. Yubico
- New devices and TOCTTOU are a common uses for two-factor authentication

7 Biometrics

- Measurements of the human body, something you are
- Various forms, fingerprint recognition, iris / retina recognition, voice, gait, typing rhythm
- A password you always have with you, but you cant change
- Usually a trade off between false positives and negatives

Reference section

placeholder