Authentication

- Passwords
- Hopelessness
- Password Managers
- Password attacks
- Password defenses
- Incident response plan!

What is Authentication

- The act of showing something to be true, genuine, or valid.

In cybersecurity this usually means

Verifying the identity of a user or process

Passwords

- Most common form of authentication
- Different ideas of strong versus weak passwords
- `12345`

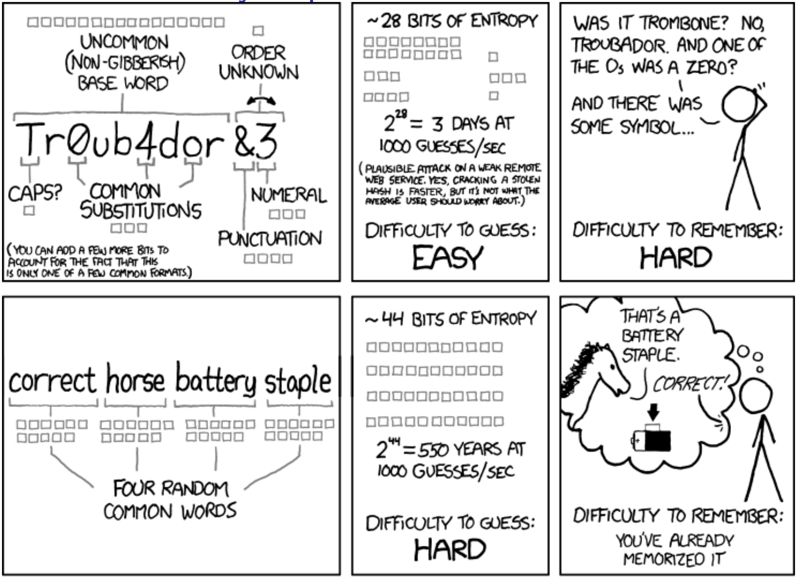
Password weaknesses

- Phishing
- Shoulder surfing
- Leaks (raw or hashed!)
- Weak passwords
- Rainbow Tables

Password Managers

- Allow for much stronger passwords
- Convenient for users
- Until they aren't

CorrectHorseBatteryStaple


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password Attacks

Generally can be classified into two types:

- Online Password attacks
- Offline Password attacks

Online Password Attacks

Attacks the login interface directly, frequently limited by speed (of network / response from authenticator / input).

- Brute force
- Smarter brute force (dictionary / rainbow tables)
- Shoulder surfing (watching someone enter password)
- Pass the hash (application accepts hashes or passwords)

This slide is bad. . .

```
9 9 9 9 1 1 1 1 1 3 1 1 1 1 5 1 1 1 1 7 1 1 1 1 9 1 1 1 3
```

Offline Password Attacks

We will perform one of these in our next lab.

- Much faster (attack speed scales with attacker resources)
- Invisible to defenders (you dont know if/when your password is compromised)
- Many of the same attacks as online (brute force)
- Requires an offline source to attack (stolen password hashes)

Authentication defenses

- Multi-Factor Authentication (MFA / 2FA)
- Keys/tokens (PKI)
- Biometrics

Multi-factor Authentication (MFA)

- If passwords are so weak, then we will use another form of authentication alongside them.
- Hopefully a second form of authentication is chosen that is both secure and easy to remember.
- Processes introduced to deal with lost or forgotten MFA can provide attackers avenues of entry or data gathering.

Key based authentication

- Public/Private Key pairs
  - User provides ***public key*** securely upon account setup
  - User authenticates with ***private key***
- Digital Certificates build upon key based authentication
  - Includes digital signature of a certification authority
  - Server verifies credibility of the certificate authority

Biometric authentication

Relies on unique biological characteristics of the user such as:

- fingerprints
- facial recognition
- speech recognition
- retinal scan
- etc.

Token based authentication

User authenticates and receives a unique encrypted string to use for authentication against other related servers.

Typically used with APIs with multiple frameworks and clients.

Incident Response

You (will) get hacked. Then what?

To be continued. . .