Authentication

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

The beginning of the end of the password

- ► This might be the last time I have to talk about passwords in the present tense.
 - Matt Kijowski, Sep 12, 2023
 - Matt Kijowski, Jan 16, 2024

What is Authentication

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

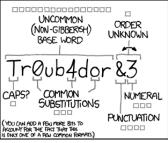
In cybersecurity this usually means

Verifying the identity of a user or process

Passwords

- Most common form of authentication
- ► "Something you know"
- ▶ Different ideas of strong versus weak passwords
- **12345**

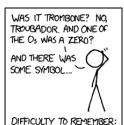
CorrectHorseBatteryStaple



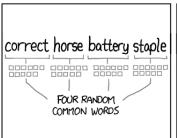


1000 GUESSES/SEC
PLAUSIBLE ATTACK ON A WEAK REMOTE.
WEB SERVICE, YES, CRACKING A STOLEN
HACH IS FASTER, BUT IT'S NOT WHAT THE
AVERAGE USER SHOULD WORKY ABOUT.

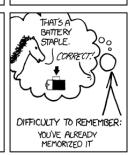
DIFFICULTY TO GUESS:



HARD



DIFFICULTY TO GUESS: HARD



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 weaknesses

- People
- Weak passwords
- Phishing
- Shoulder surfing
- Leaks (raw or hashed!)
- Dictionaries
- ► Rainbow Tables
- ► Brute force
- Side channel attacks!!!
 - Password resets
 - Removal of MFA devices
 - Account recovery
- Bypass attacks
- People

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)
- Bypass (steal / access an already authenticated system)

This slide is bad...

But is a good example of an online password attack that does NOT require the internet.

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

2 2 1 5 1 2 2 1 7 1 2 2 1 0 1 2 2 2 2 1 2 2 2 5 1 2 2 2

Offline Password Attacks

We will perform one of these in our next lab.

- Frequently much faster (attack speed can scale with attacker resources)
- Can be invisible to defenders (you dont know if/when your password is compromised)
- Many of the same attacks as online (brute force, dictionary, rainbow tables, etc.)
- Requires an offline source to attack
 - File containing stolen password hashes
 - Phishing the user themselves
 - Key logging software that captures the password

Authentication defenses

- ► Password managers
- ► Multi-Factor Authentication (MFA / 2FA)
- Keys/tokens (PKI)
- Biometrics
- ► Policies and procedures

Password Managers

- Allow for much stronger passwords
- Convenient for users
 - Until they are very inconvenient...
- Helps prevent easily guessable passwords
- ► Helps prevent re-used passwords

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.

Policies and Procedures

- ▶ How the people and processes handle all parts of authentication
- ► How many password attempts?
- How long do you wait for MFA?
- How do you verify a user during account recovery?
- etc.

Incident Response

You (will) get hacked. Then what?

Mat Honan - A case study

- circa 2012
- ▶ Wired.com tech blogger
- twitter @mat
- Apple fanboy (joking, but does use apple products)
 m******@me.com
- ▶ Enjoys amazon.com delivery of goods to his home address

The incident

- ► August 2012
- ▶ 5pm iphone resets
- phone power on and iphone is at setup screen
 - (backups etc were done nightly so no fear yet)
- plug phone in to laptop to restore/recover
 - notification on macbook of incorrect gmail credentials
 - macbook has new (unknown) 4 digit pin protection

What would you do?

The hack

These are the steps the attacker went through:

- ► First all, the reason behind it, they (attacker) wanted @mat Twitter handle
 - Yes I chose not to update this slide to the new name of X, they are all still tweets in my mind...
 - backround research revealed @mat is Matthew Honan
 - find physical address from various online lookups
 - find email address from various online lookups
- try to sign into twitter with that gmail address
 - this confirmed that the gmail address is @mat
- try to sign into that gmail address
 - ▶ no 2fa!!!! :(:(!!!!
 - account recovery is m*****@me.com

The hackening continued

- me.com allows for account recovery with two simple things
 - last 4 of your credit card
 - billing address

Lets go shopping!!

- There is a way to trick amazon into giving up the last 4 digits of your CC
 - Attacker orders an item through Amazon.com as the victim by adding a new CC!!!!
 - Attacker then resets the amazon.com password by using the above malicious CC as an account recovery proof of identity
 - Attacker can now see last 4 of all CC in Amazon as well as billing addresses

Scorched earth

- This lets people into me.com (AppleID)
- which gave them his gmail
- which gave them his twitter
- which was really his entire digital life. . .
- Hacker resets twitter account info, password, and recovery email
- Hacker initiates google account removal, deleting ALL google data and account (no twitter recovery email anymore)
- Hacker initiates me.com account removal, deleting ALL apple data, purchased songs, movies, stored pictures, and removes access to phone and laptop
- ► Hacker tweets about his victory

Incident response plan

- Know what ALL forms of authentication are for critical services
- Setup MFA for critical/all accounts
- Know how to disable/re-enable the MFA
- ▶ Be prepared to provide necessary information
- Be aware of chained accounts / vulnerabilities