# 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

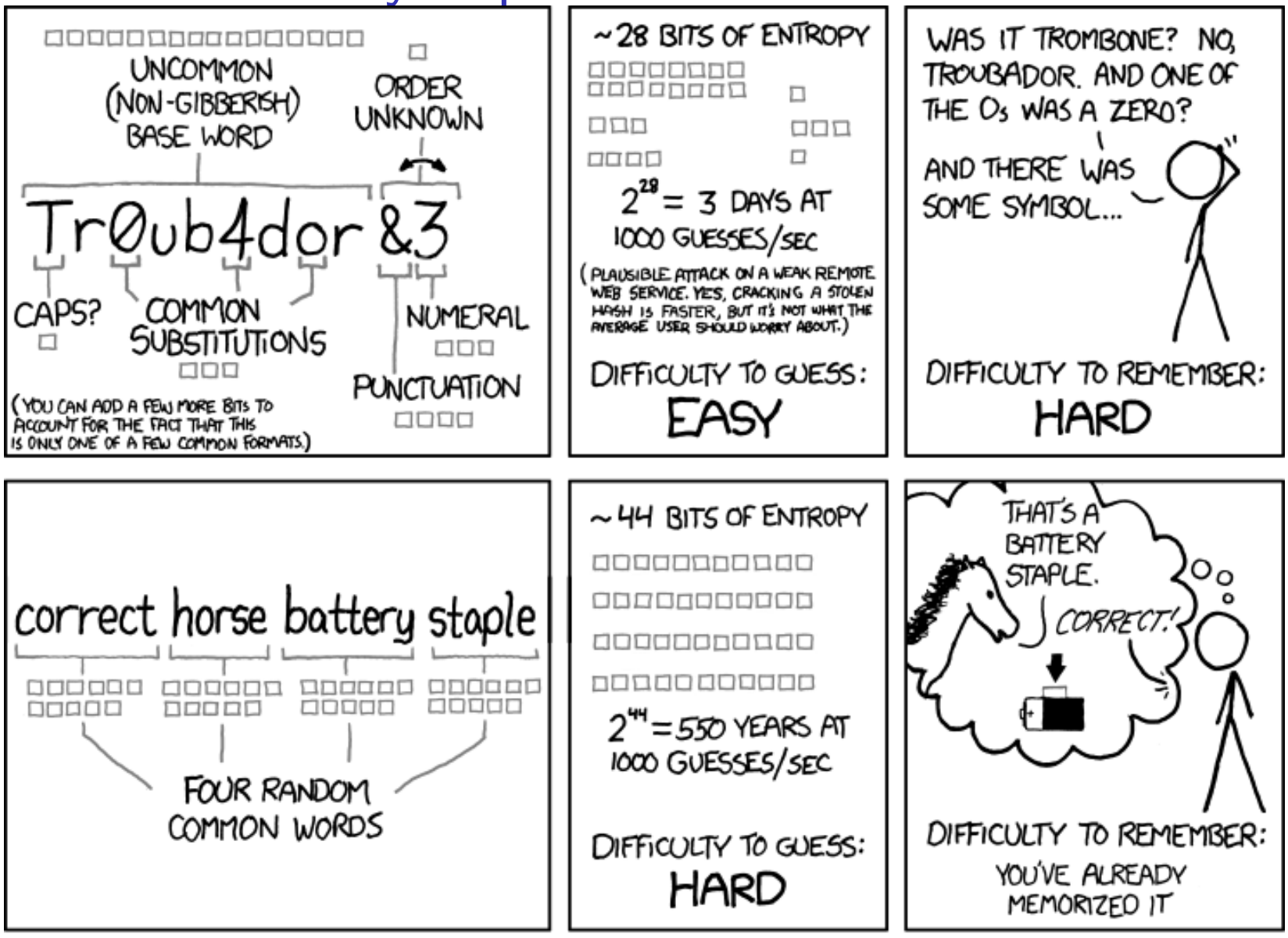
# Password weaknesses

- 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




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?

# 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

- First all, the reason behind it: @mat...
  - 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`

# 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