Introduction to Cybersecurity

David J. Malan
malan@harvard.edu
Securing Accounts
Authentication
Authorization
Usernames
Passwords
Dictionary Attacks
Brute-Force Attacks
4 digits
10 × 10 × 10 × 10 × 10
$10^4$
10,000
4 letters
26 × 26 × 26 × 26
$52 \times 52 \times 52 \times 52$
\[ 52^4 \]
4 characters
94 × 94 × 94 × 94
78,074,896
8 characters
94°
National Institute of Standards and Technology (NIST)
"Memorized secrets SHALL be at least 8 characters in length..."
"Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. All printing ASCII characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode characters SHOULD be accepted as well."
"... verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised...

- "Passwords obtained from previous breach corpuses.
- "Dictionary words.
- "Repetitive or sequential characters (e.g. 'aaaaaaa', '1234abcd').
- "Context-specific words, such as the name of the service, the username, and derivatives thereof."
"Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets."
"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)."
"Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account…"
iPhone is disabled
try again in 1 minute
Two-Factor Authentication (2FA)
Multi-Factor Authentication
Knowledge
Possession
Inherence
...
One-Time Password (OTP)
SIM Swapping
Keylogging
Credential Stuffing
Social Engineering
Phishing
Google

Sign in

to continue to Gmail

Email or phone

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more

Create account

Next
Google

2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

2-Step Verification

Get a verification code from the Google Authenticator app

Enter code

- Don't ask again on this device

Try another way  Next
Machine-in-the-Middle Attacks
Single Sign-On (SSO)
Password Managers
Apple iCloud Keychain
Google Password Manager
Microsoft Credential Manager
...
Passkeys