

Introduction to  
**Cybersecurity**

David J. Malan  
malan@harvard.edu

# Securing Accounts



# Authentication

# Authorization

Username

Passwords

# Dictionary Attacks



# Brute-Force Attacks

4 digits

$$10 \times 10 \times 10 \times 10$$

$10^4$

10,000

4 letters

26 × 26 × 26 × 26

52 × 52 × 52 × 52



52<sup>4</sup>

7,311,616

4 characters

94 × 94 × 94 × 94

$94^4$

78,074,896

8 characters

94<sup>8</sup>



6,095,689,385,410,816

# 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..."

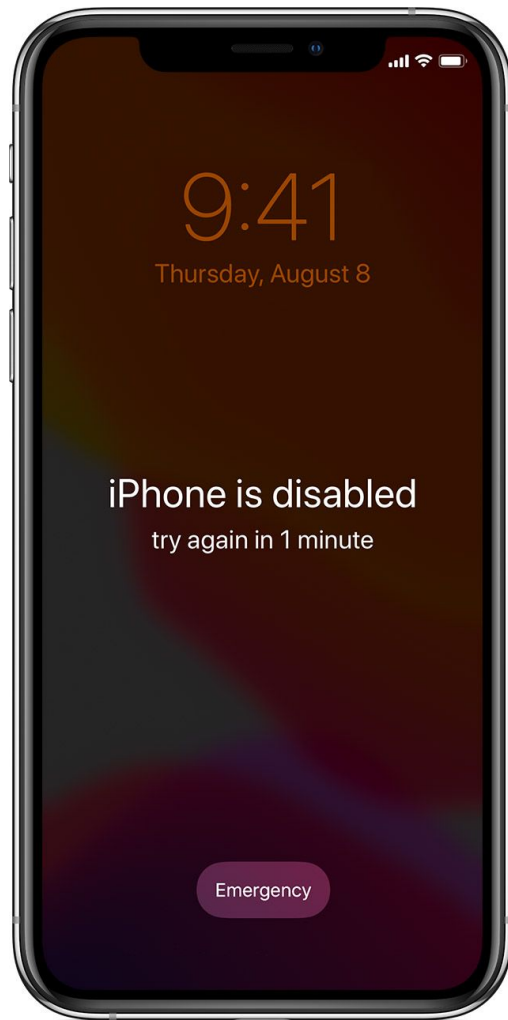
- "Passwords obtained from previous breach corpuses.
- "Dictionary words.
- "Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').
- "Context-specific words, such as the name of the service, the username, and derivatives thereof."

"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..."





9:41

Thursday, August 8

iPhone is disabled

try again in 1 minute

Emergency

# Two-Factor Authentication (2FA)

# Multi-Factor Authentication

Knowledge

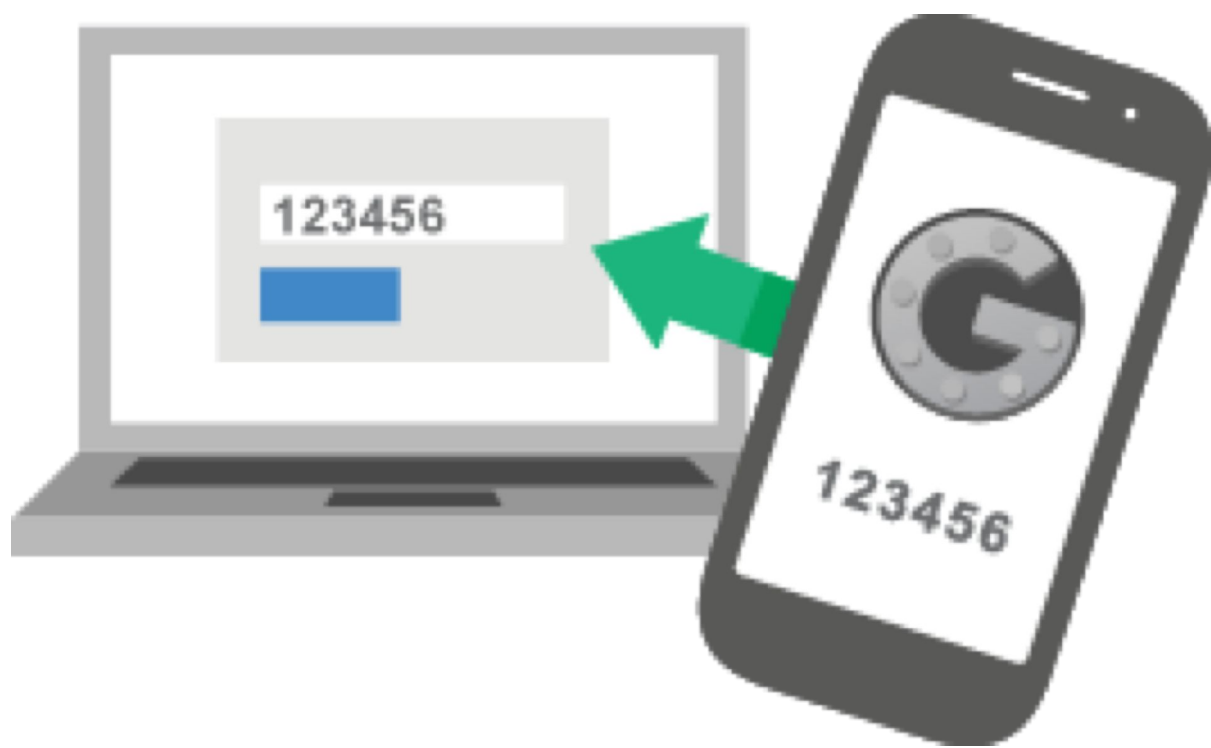
Possession

Inherence

...

One-Time Password (OTP)





# SIM Swapping



Keylogging

# Credential Stuffing

# Social Engineering

Phishing



## Sign in

to continue to Gmail

[Forgot email?](#)

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

[Learn more](#)

[Create account](#)

Next



## 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

Don't ask again on this device

[Try another way](#)


Next

# Machine-in-the-Middle Attacks





Single Sign-On (SSO)

 Log in with Google

 Log in with Facebook

**Email**

**Password**

[Forgot password?](#)

Log in

# Password Managers

Apple iCloud Keychain  
Google Password Manager  
Microsoft Credential Manager

...

Passkeys

Introduction to  
**Cybersecurity**

David J. Malan  
malan@harvard.edu