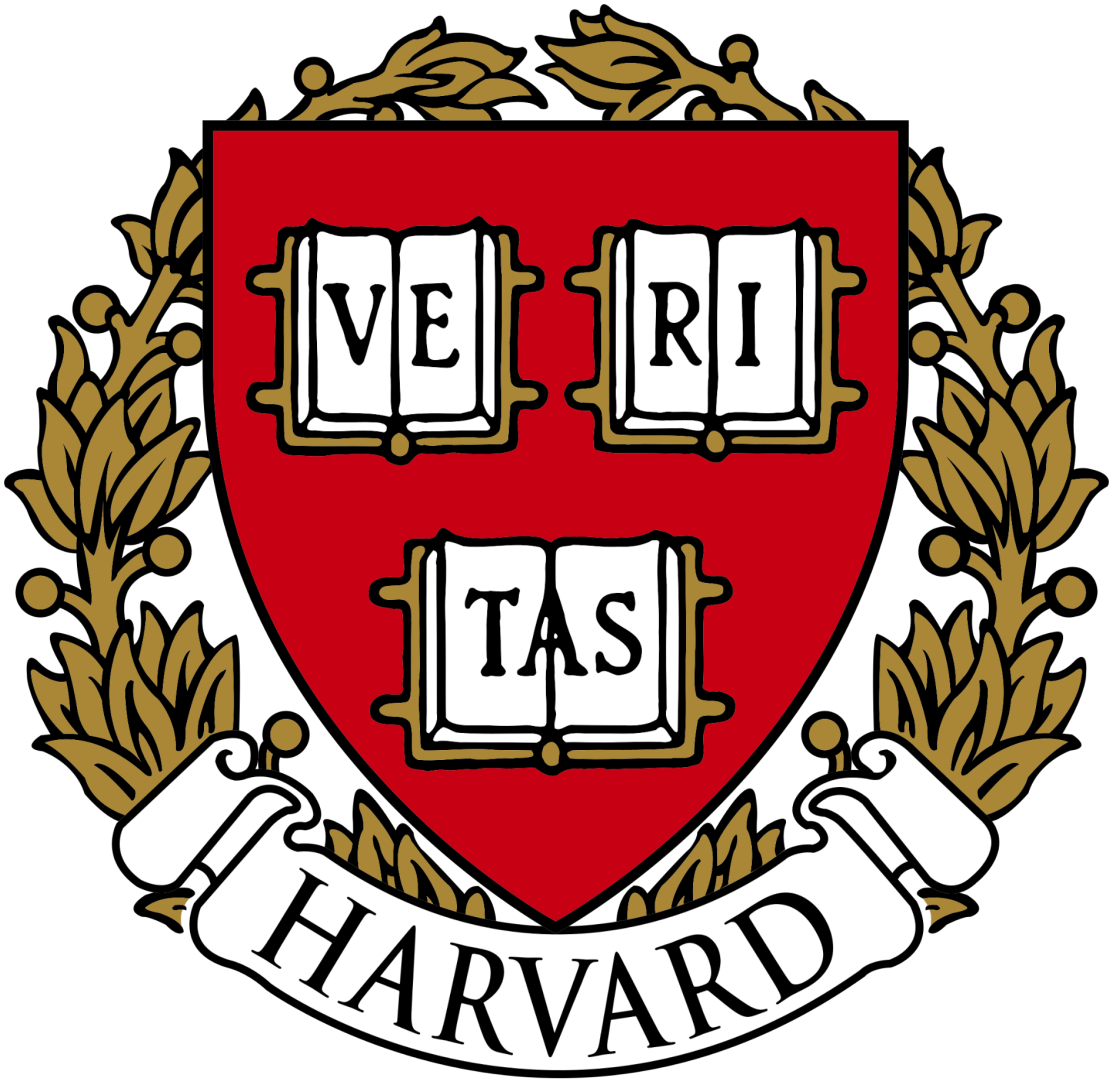
CS50

Cyber Security



2. Types of Password Attacks

2.1 Dictionary Attacks

Attackers employ curated lists containing common terms, phrases, and leaked credentials. These attacks are particularly effective against weak or predictable passwords and require minimal computational resources.

2.2 Brute Force Attacks

Brute force techniques systematically iterate through every possible combination until the correct password is discovered. The success rate depends on factors such as password complexity, system protections, and computational throughput.

3. Password Strength and Brute Force Analysis

Table 1 summarizes the correlation between character set size, total combinations, and estimated time to crack based on brute-force simulations.

Table 1: Password Complexity and Vulnerability

Password Type	Character Set Size	Total Combinations	Estimated Crack Time	Vulnerability Assessment
Numerical (4-digit PIN)	10	$$10^4 = 10,000$$	Milliseconds	Highly vulnerable; easily brute-forced
Alphabetic (4 letters)	52 (A-Z, a-z)	$$52^4 = 7,311,616$$	Seconds	More secure than digits alone, but still weak
Full Character Set (4 chars)	92 (A-Z, a-z, 0–9, symbols)	$$92^4 = 71,639,296$$	Minutes	Greater resistance; crackable if short in length

4. Complexity and Defense Strategy

4.1 Raising the Complexity Barrier

Expanding character variety and password length increases entropy and makes brute-force efforts computationally impractical. The primary goal is to either render the attack infeasible or disincentivize adversaries due to time and resource constraints.

5. Usability Considerations in Password Policy Design

Excessive complexity can impede user experience. Systems requiring high-character diversity often cause frequent password resets, leading to user dissatisfaction and potential abandonment. The balance must be struck between security enforcement and user accessibility.

6. NIST Guidelines for Secure Passwords

The National Institute of Standards and Technology (NIST) recommends the following best practices for password creation and management:

- Minimum of 8 characters
- Use of passphrases or full sentences
- Avoidance of:
    - Credentials from known breaches
    - Dictionary words
    - Repetitive characters (e.g., "aaaaaa")
    - Contextual keywords (e.g., username, service name)
- Periodic password changes under suspicion of compromise
- Implementation of multi-factor authentication

7. Multi-Factor Authentication (MFA)

MFA introduces multiple layers of identity verification. These mechanisms are broadly categorized as:

- **Knowledge:** Something the user knows (e.g., password)
- **Possession:** Something the user has (e.g., SMS or email verification)
- **Inherence:** Something the user is (e.g., biometrics)

7.1 One-Time Password (OTP)

Generated via applications or hardware keychains, OTPs synchronize authentication codes between client and server, thereby validating session integrity.

8. Common Attack Vectors

- **SIM Swapping:** Exploits mobile provider protocols to transfer victim's phone number to attacker-controlled SIM. Using apps over SMS is recommended.
- **Keylogging:** Records keystrokes and transmits credentials to remote servers. Adversaries may exploit captured data in real-time.
- **Credential Stuffing:** Utilizes large datasets of breached credentials across multiple platforms. Reusing passwords increases vulnerability.
- **Social Engineering:** Manipulates psychological factors to extract sensitive data (e.g., pet names for security questions). Advancements in AI-driven voice imitation pose additional risks.
- **Phishing:** Deceptive emails or sites trick users into divulging credentials. Verifying URLs and manually entering website addresses reduces exposure.
- **Machine-in-the-Middle Attacks:** Compromised intermediary systems intercept sensitive data during transmission. Use of encryption and trusted networks is advised.

9. Authentication Defenses

9.1 Single Sign-On (SSO)

Facilitates secure authentication using existing credentials from trusted providers. Cryptographic tokens ensure legitimacy without password reuse.

9.2 Password Managers

Password managers generate and securely store complex credentials for multiple services. Examples include:

- Apple iCloud Keychain
- Google Password Manager
- Microsoft Credential Manager

Users should protect password manager access with a master password of high entropy and uniqueness.

9.3 Passkeys

Passkeys are cryptographic credentials stored locally and synced across trusted devices. They enable secure login through challenge–response mechanisms without the need for plaintext passwords.