



# Password Cracking

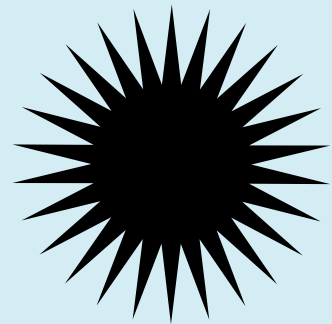


# Introduction

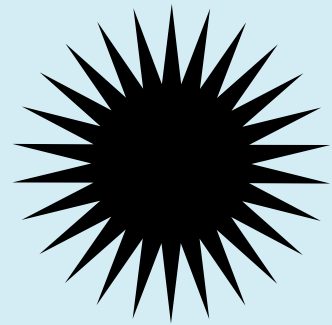
---

- Definition: Password cracking is the process of recovering passwords from data storage systems to gain unauthorized access.
- Importance: Passwords remain the most common form of authentication, and their security is crucial to protect sensitive data.
- Weak passwords can lead to breaches.

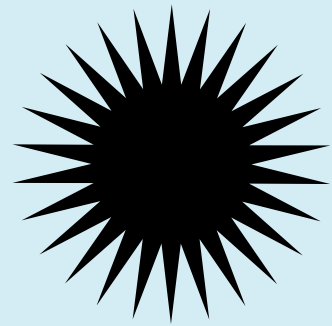
# Why Password Cracking is a Problem ?



**Why Target Passwords:** Passwords protect access to systems, accounts, and sensitive data. Once compromised, attackers can steal personal information, financial data, or intellectual property.



**Risks:** Weak or exposed passwords are the easiest way for attackers to penetrate systems.



**Statistics:** According to Verizon's 2021 Data Breach Investigations Report, 61% of breaches involved compromised credentials.

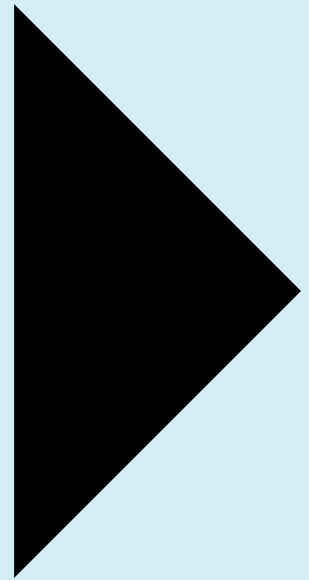
# Common Password Cracking Techniques:

- **Brute Force Attack:** Involves trying all possible combinations until the correct one is found. This attack is time-consuming, but with powerful hardware, it can crack weak passwords.
- **Dictionary Attack:** Uses a predefined list of words (like a dictionary) and common passwords to guess the correct password.

# Common Password Cracking Techniques:

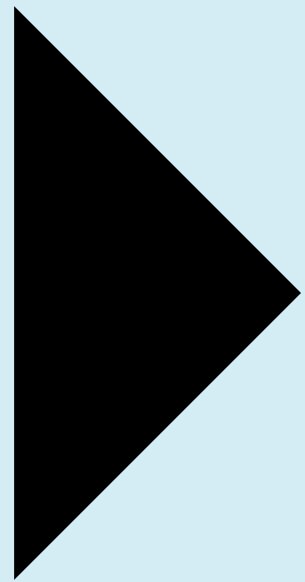
- **Phishing:** A social engineering tactic where attackers trick users into revealing their passwords, often via fake emails or websites.
- **Credential Stuffing:** Attackers use credentials obtained from one breach to try and log into other services (since many people reuse passwords)
- **Keylogger Attack:** Records keystrokes to capture the password when typed by the user.

# Brute Force Attack



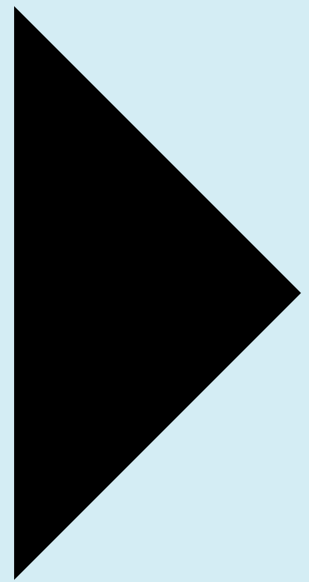
- Definition: The attacker systematically checks all possible passwords until the correct one is found.
- Process: Each combination of characters is tried until the password is guessed.
- Impact of Complexity: A simple password can be brute-forced in minutes, while a longer, more complex password can take years.
- Example: A 4-digit PIN can be cracked in seconds, while a 12-character alphanumeric password with symbols could take years without specialized hardware.

# Dictionary Attack :



- Definition: The attacker uses a pre-built list of common words and passwords (called a dictionary) to guess the password.
- Process: The attack assumes that users often choose passwords that are simple and easy to remember.
- Tools Used: Tools like John the Ripper and Hashcat can use these dictionaries to perform automated attacks.
- Mitigation: Using passwords that are not based on common words or combinations is key to preventing this attack.

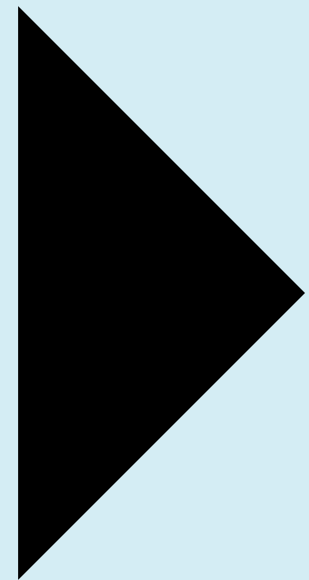
# Social Engineering and Phishing



- Social engineering uses manipulation and deception to trick individuals into giving up confidential information like passwords.
- Phishing: The most common form of social engineering where attackers send fake emails or messages to trick users into revealing credentials.
- Attackers often use fake websites or email addresses that mimic legitimate ones.
- Examples: Fake websites that look identical to login pages, phone calls pretending to be tech support, etc.
- Prevention: Awareness training, anti-phishing software, and scrutinizing all communications can reduce the success of these attacks.



# Rainbow Table Attacks



- Definition: A rainbow table is a precomputed table of hash values for passwords. Attackers use these tables to reverse cryptographic hash functions and recover passwords.
- How it Works: Instead of computing the hash of every possible password like in brute force, the attacker precomputes these values in a table.
- Example: A password's hash like 5f4dcc3b5aa765d61d8327deb882cf99 can be quickly matched to the word “password” in a rainbow table.
- Prevention: Salting (adding random data to the password before hashing) makes rainbow tables ineffective.

# Keylogger Attacks

Keylogging records every keystroke typed by the user, capturing passwords when they are typed.

Types:

- **Software Keyloggers:** Malicious software installed on a device to record keystrokes.
- **Hardware Keyloggers:** Physical devices connected to a keyboard that capture inputs.

**Prevention:** Using on-screen keyboards and anti-keylogging software can help protect against keyloggers.

# How Passwords are Stored

**Plain Text:** Storing passwords in plain text is highly insecure. Anyone who gains access to the storage medium can read them.

**Hashing:** Hashing converts passwords into fixed-length strings, making them harder to interpret if intercepted.

In Hashing, when you signup to a website and keep a password, the website hashes it and stores the password. When you again try to login and enter your password, the website again computes the hash of the password and checks if the new hash is equal to the old hash.

# Hashing & Salting

## Popular Hashing Algorithms:

- MD5: Older, now considered insecure.
- SHA-256: Commonly used and more secure.

Salting: A random string (salt) is added to the password before hashing. This ensures that even if two users have the same password, their hashes will differ.

Importance of Salting: Prevents attackers from using precomputed tables (like rainbow tables) to crack hashed passwords.

# Password Peppering

Peppering adds a “secret” key or value, known only to the system, to the password before hashing. It differs from salting because the pepper is constant across passwords but unknown to attackers.

## How It Works:

1. User enters their password.
2. System combines the password with a “pepper” (hidden string or key).
3. This combination is then hashed and stored.
4. During login, the system peppers and hashes the input to verify.

If attackers steal the hashed passwords, they still cannot crack them without knowing the pepper.

# Password Peppering

## Salting

Adds a unique, random value (salt) to each password before hashing.

The salt is stored alongside the hashed password in the database.

Visible in the database (to create unique hashes for each password).

Salting makes each password unique even if two users have the same password.

## Peppering

Adds a secret, fixed value (pepper) to all passwords before hashing.

The pepper is kept separate from the database, usually in the application code.

Hidden from attackers, as it's stored securely elsewhere.

Peppering adds an additional hidden layer, known only to the system, which makes cracking harder even if salts and hashes are stolen.

Using both salting and peppering together makes passwords exponentially harder to crack.

# Prevention: Strong Password Creation

## Methods:

- **Strong Password Policies:** Encourage users to create long, unique passwords.
- **Multi-Factor Authentication (MFA):** Adds a layer of security beyond passwords, like SMS or app-based codes.
- **Regular Password Changes:** Reduces the chance of long-term exposure if a password is compromised.

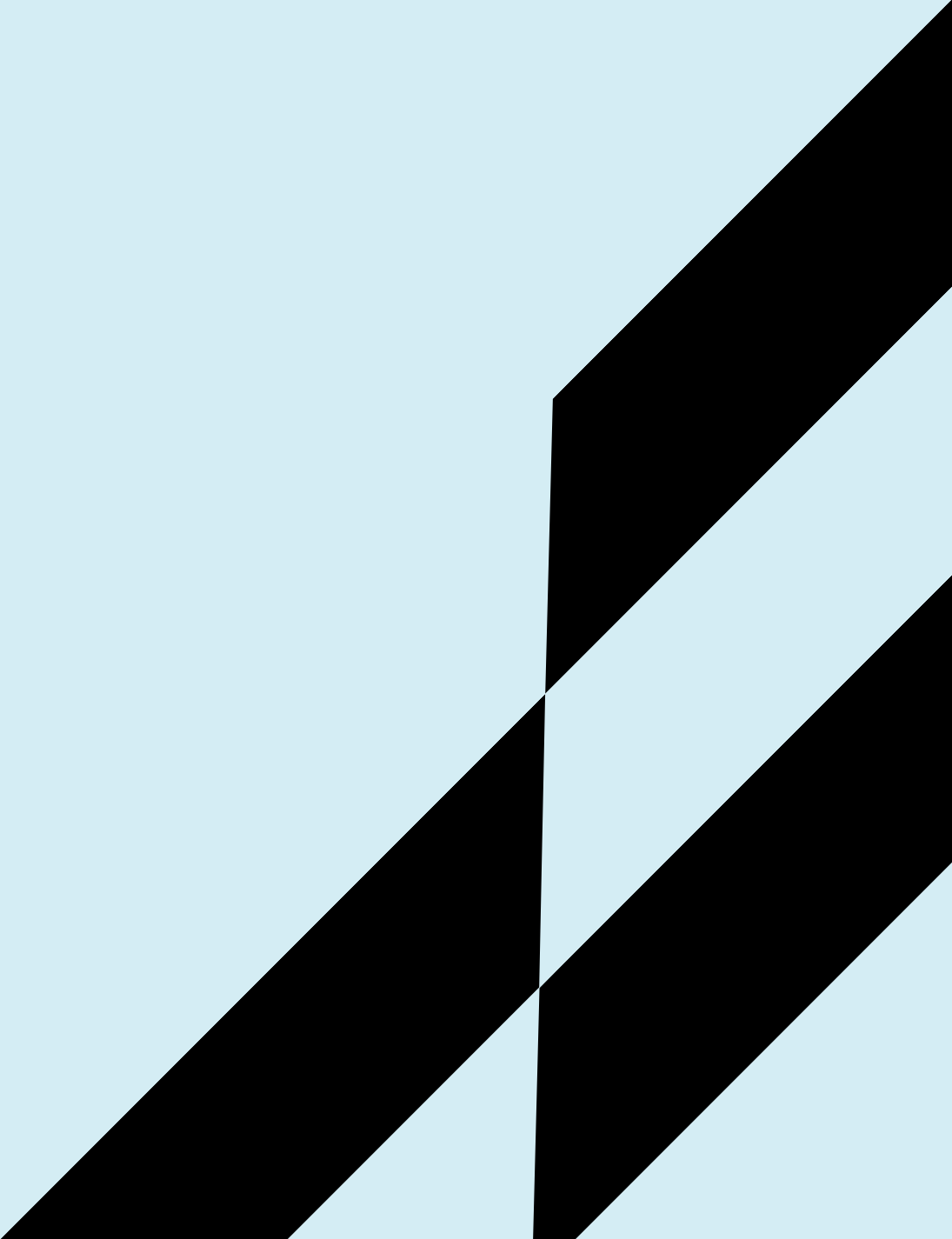
**User Education:** Regular training and reminders about cybersecurity best practices.

# Prevention: Strong Password Creation

- Characteristics of Strong Passwords:
- At least 12 characters long
- Contains uppercase and lowercase letters, numbers, and special characters
- Does not use easily guessable information like birthdays or names
- Password Length and Complexity: Longer, more complex passwords are exponentially harder to crack with brute force or dictionary attacks.
- Example: Password like P@ssword123 is weak, while Tj\$%7xQmN!9Q@7cA is much stronger.



# Password Management Best Practices

- **Use of Password Managers:** Tools like Google Passwords, LastPass or Bitwarden can securely store and generate strong, unique passwords for every account.
  - **Multi-Factor Authentication (MFA):** Adds an extra layer of security by requiring a second form of authentication, such as a code from a mobile app.
  - **Avoiding Password Reuse:** Reusing passwords across multiple accounts increases the risk of credential stuffing attacks.
- 

# Emerging Technologies in Password Security

- Passwordless Authentication: Biometric authentication, such as fingerprint or facial recognition.
- Hardware Tokens: Physical devices that generate or store secure codes, used in two-factor authentication.
- Behavioral Biometrics: Analyzes unique behaviors like typing speed and mouse movement.

Advantages: Offers enhanced security with better convenience, reducing reliance on password-based systems.

# Rate Limiting

Rate limiting restricts the number of attempts a user or IP address can make to log in within a set time frame.

How It Works:

1. System allows a limited number of failed attempts (e.g., 5 attempts within 10 minutes).
2. If this limit is reached, the system enforces a lockout period or requires additional verification like CAPTCHA.
3. Alternatively, an exponential backoff can be applied, increasing the time between allowed attempts.

# Rate Limiting

## Benefits:

- Prevents brute-force attacks by slowing down or stopping repeated login attempts.
- Protects against credential stuffing (reusing stolen credentials from one site to access others).
- Exponential Delay: Increases delay time for each failed attempt.
- CAPTCHAs and MFA (Multi-Factor Authentication): Requires additional verification after failed attempts, especially helpful for bots.

# Recent High-Profile Password Breaches

- Yahoo Breach (2013): 3 billion accounts were compromised due to weak encryption of passwords.
- LinkedIn Breach (2012): 117 million credentials leaked, which were stored using an inadequate hashing method (SHA-1).

Passwords were easy to unscramble because of LinkedIn's failure to use a salt when hashing them  
It allowed attackers to quickly reverse the scrambling process using existing standard rainbow tables

THANK YOU