Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

June 24-28, 2024

Murtuza Jadliwala

murtuza.jadliwala@utsa.edu

SPrITE LAB

UTSA

NSF

Introduction to Authentication and Password Cracking

Authentication

"The process of verifying an identity claimed by or for a system entity."

- Fundamental building block and primary line of defense
- Basis for access control and user accountability

Authentication Process

1. **Identification step**
   - Presenting an identifier to the security system.
   - Typically, identifier is unique for each user on the system

2. **Verification step**
   - Presenting or generating authentication information that corroborates the binding between the entity and the identifier
   - Depending on the scheme, authentication information may not be unique for each user on the system, however only the user has knowledge of this authentication information (or how to generate it)

Authentication Means

1. Something the individual **knows**
   - Password, PIN, answers to prearranged questions
2. Something the individual **possesses** (token)
   - Smartcard, electronic keycard, physical key
3. Something the individual **is** (static biometrics)
   - Fingerprint, retina, face
4. Something the individual **does** (dynamic biometrics)
   - Typing speed and characteristics

Password Authentication

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
  - If password matches, user authenticated, and access allowed. If password does not match, access not allowed!

- The user ID or login (identifier):
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control

- The password (authentication information):
  - Typically, composed of characters, numbers and symbols
  - Easier to remember passwords are less secure and easy to guess by adversary versus purely random passwords that are much more secure but less usable
  - Other forms of passwords: PINs (purely numeric) and Patterns (graphical)

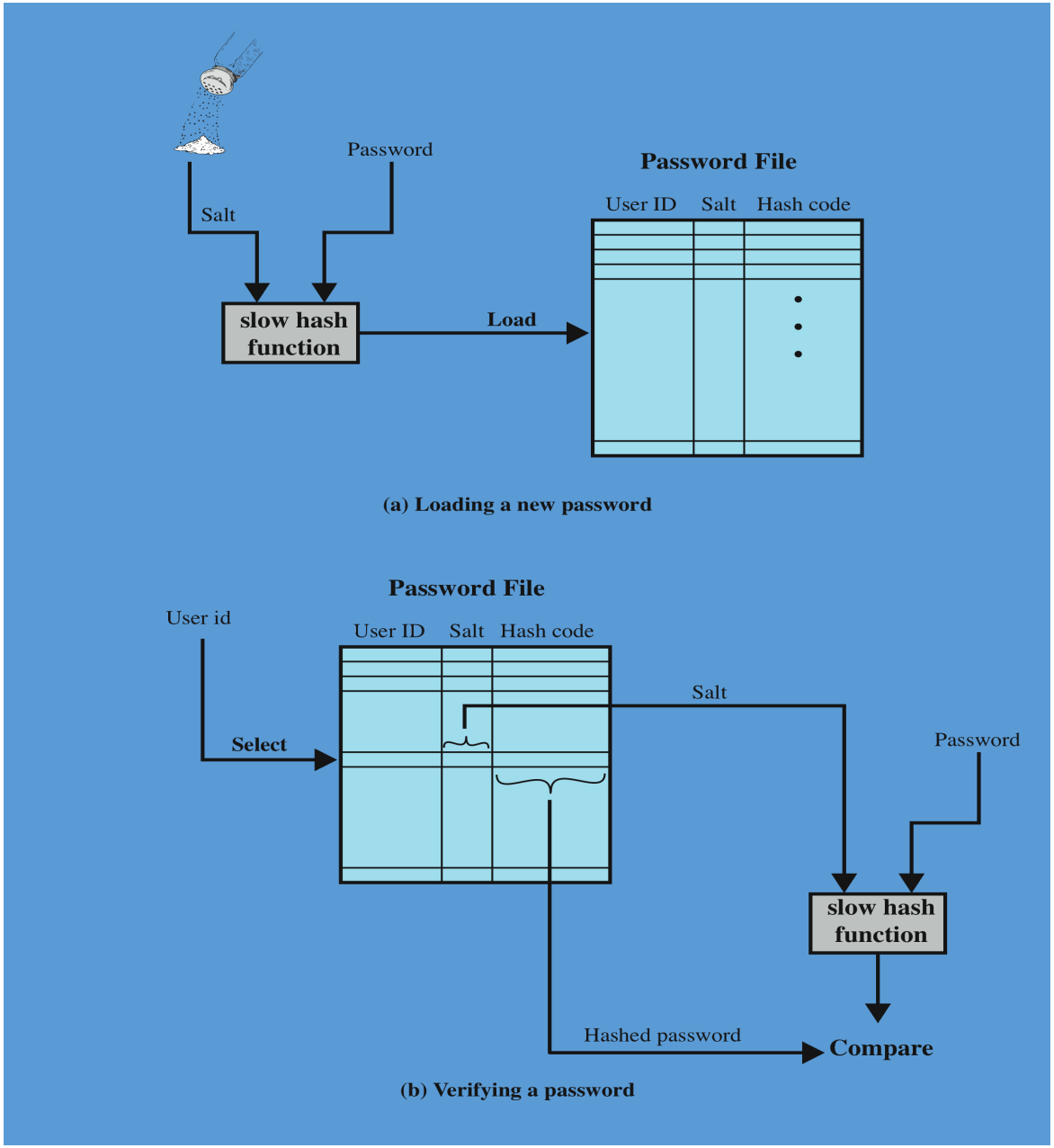
Password Storage

- On most operating/software systems passwords are stored in special files (called password files).
  - In UNIX/Linux systems, password information was stored in the *\etc\passwd* file.

- Problems of storing passwords in plaintext?
  - Stolen or compromised password file compromises the accounts of all users on the system!
  - System administrators can easily read user passwords.

- Solution?
  - Rather than storing plaintext passwords, store them as hash values!

Use of Hashed Passwords



Password Cracking

1. **Online Password Cracking:**
   - Adversary only has access to the authentication service as a blackbox
   - Does not have access to the password file
   - Easier to protect against online attacks – e.g., account lockout mechanism
2. **Offline Password Cracking**
   - Adversary not only has access to the authentication service, but also has access to the password file!
   - Much more stronger adversarial assumption
   - Much more difficult to protect against offline attacks – change password on a service, if it announces it has been compromised

Offline Password Cracking

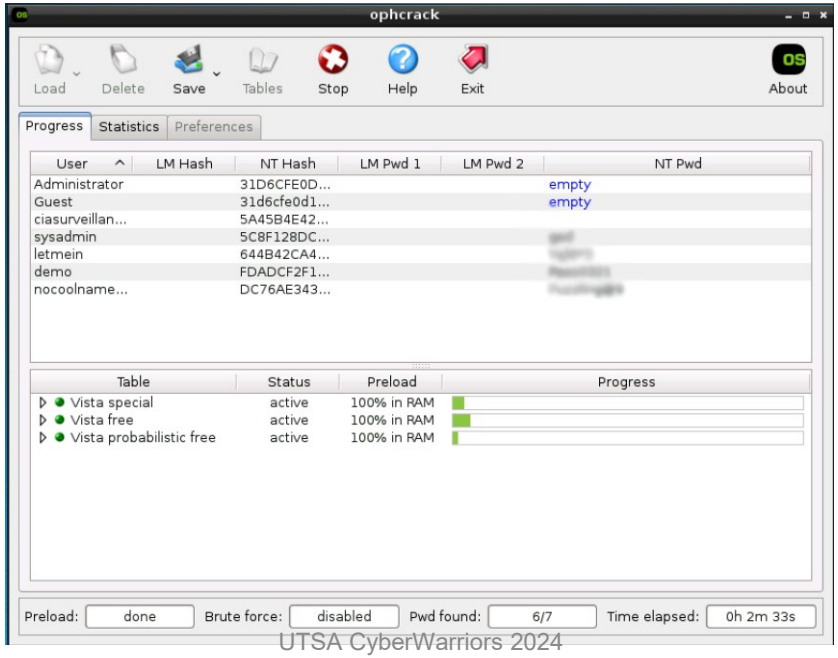
1. **Dictionary attacks**
   - Develop a large dictionary of possible passwords and try each against the password file
   - Each password must be hashed using each salt value and then compared to stored hash values
2. **Rainbow table attacks**
   - Pre-compute tables of hash values for all salts
   - A mammoth table of hash values
   - Can be countered by using a sufficiently large salt value and a sufficiently large hash length

Offline Password Cracking using Kali Linux

- Kali provides several tools for password cracking:
  - John the Ripper –

```
labuser@CRC011:~$ john --wordlist=/lab/lower.txt
        --format=Raw-SHA1-Linkedin --fork=4
        /lab/linkedin2012.txt
```

  - Ophcrack -



Protection Techniques

- **User education**
  - Importance of using hard to guess passwords and guidelines for selecting strong passwords
- **Computer generated passwords**
  - Users have trouble remembering them
- **Reactive password checking**
  - System periodically runs its own password cracker to find guessable passwords
- **Proactive password checking**
  - User allowed to select own password; however system checks to see if it is allowable, and if not, rejects it
  - Goal: Eliminate guessable passwords while allowing the user to select a password that is memorable

Other Password-related Vulnerabilities

1. Offline dictionary attack
2. Specific account attack
3. Popular password attack
4. Password guessing against single user
5. Workstation hijacking
6. Exploiting user mistakes
7. Exploiting multiple password use
8. Electronic monitoring

Countermeasures

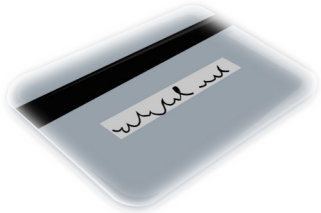
1. **Controls to prevent unauthorized access to password file**
2. Intrusion detection measures
3. Rapid re-issuance of compromised passwords
4. **Account lockout mechanisms**
5. Policies to inhibit users from selecting common passwords
6. Training in and enforcement of password policies
7. Automatic workstation logout
8. **Policies against similar passwords on network devices**
9. **2nd Factor Authentication**

Authentication Means

1. Something the individual **knows**
   - Password, PIN, answers to prearranged questions
2. Something the individual **possesses** (token)
   - Smartcard, electronic keycard, physical key
3. Something the individual **is** (static biometrics)
   - Fingerprint, retina, face
4. Something the individual **does** (dynamic biometrics)
   - Typing speed and characteristics

Types of Cards Used as Tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card



2nd Factor or Two-step Authentication

What is 2nd Factor Authentication?

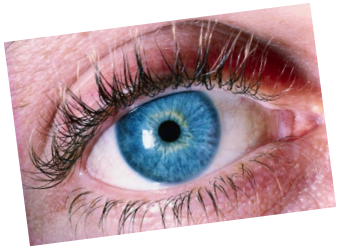
- Supplement traditional authentication using one factor (say, password) with an additional factor (say, a token) for additional security!
- Most modern Internet applications (e.g., financial, educational and email services) already support, or even require, it!
- The following two are the most commonly found (used):
  1. Time-Based One-Time Passwords (TOTP)
  2. Tokens (e.g., YubiKeys)

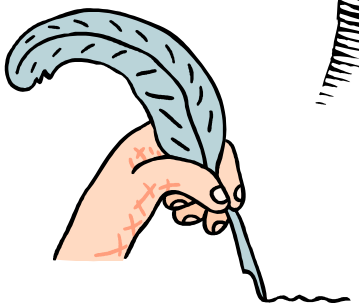
Authentication Means

1. Something the individual **knows**
   - Password, PIN, answers to prearranged questions
2. Something the individual possesses (token)
   - Smartcard, electronic keycard, physical key
3. Something the individual **is** (static biometrics)
   - Fingerprint, retina, face
4. Something the individual **does** (dynamic biometrics)
   - Typing speed and characteristics

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice





- Authentication scheme based on pattern recognition
- Technically complex and expensive compared to passwords and tokens

Operation of a Biometric System