Authentication

Madiba Hudson-Quansah

Contents

Chapter 1

Introduction

Controlling threats and vulnerabilities to a computer system involves a policy that specifies, who can access what and how, i.e. which subjects, can access which objects, and by which means. There are three key tools to achieve this:

- Authentication
- Access Control
- Cryptography

Definition 1.0.1: Authentication

The property of accurate identification.

Definition 1.0.2: Access Control

The selective restriction of access to a place or other resource.

Definition 1.0.3: Cryptography

Converting data into a form unreadable to unauthorized users.

Determining an entity's identity consists of two phases:

Identification - The act of asserting who an entity is, involving presenting a credential

Authentication - The act of proving that the entity is who it claims to be, involving exchanging authentication information.

1.1 Means of Authentication

There are three primary means of authentication:

Something the users knows / Credentials - A piece of private information

Something the user is / Biometrics - A physical characteristic of the user.

Something the user has / Tokens - A physical item possessed by the user.

1.1.1 Credentials

Definition 1.1.1: Credentials

Pieces of information presented by a user to prove their identity during initial authentication.

Credentials are data structures that binds an identity and additional attributes to a token.

1.1.2 Token

Definition 1.1.2: Token

A digital artefact issued after successful authentication to maintain as session or delegate access without resubmitting credentials.

Tokens can either be hardware or software possessed by a subscriber.

1.2 Multi-Factor Authentication (MFA)

Definition 1.2.1: Multi-Factor Authentication (MFA)

An authentication process where a user presents two or more independent pieces of evidence (factors) to verify their identity.

For example, using a password (something you know) and a fingerprint (something you are) to access a secure system.

1.3 NIST (National Institute of Standards and Technology) Assurance Levels for User Authentication

These levels indicate the degree of confidence in the identity proofing and authentication processes. It also provides options for organization to choose between depending on the security risk assessment.

It defines three separate levels for Identity Assurance Level (IAL) and Authenticator Assurance Level (AAL).

1.3.1 Identity Assurance Level (IAL)

Focuses on verifying who the user is.

IAL1 - No need to link the applicant to a specific real-life identity. Example anonymous discussion forums.

IAL2 - Provides evidence for the claimed identity using either remote of physically present identity proofing. Example requiring a National ID card or passport.

IAL3 - Requires physical presence (in-person) for identity proofing. Example applying for a security clearance.

1.3.2 Authenticator Assurance Level (AAL)

Focuses on verifying how securely the user authenticates.

AAL1 - Provides some assurance (low confidence) / Single Factor Authentication. Example password-based authentication.

AAL2 - Provides high confidence / Multi-Factor Authentication with proof of possession and control of two factors.

AAL3 - Provides very high confidence / MFA using hardware-based cryptographic tokens resistant to phishing and replay attacks. Example using a smart card with a PIN.

1.4 Password Based Authentication

Definition 1.4.1: Discretionary Access Control (DAC)

An access control model where the owner of the resource determines who can access it and what privileges they have, i.e. a user may grant permission to other users to access their files.

Uses a user ID and password pair to authenticate users, where the user ID identifies the account and links the account to the user's privileges and access permissions under Discretionary Access Control (DAC).

A system using this method maintains a password file indexed by user ID, with a one-way has of the password stored in it rather than the password itself. This ensures that even if the password file is compromised the actual passwords are not immediately exposed.

1.4.1 Attacks and Countermeasures

1.4.1.1 Offline Dictionary Attack

An attack who gains access to the password file and systematically compares password hashes against hashes of commonly used passwords. If a match is found the attacker can gain access with the corresponding user ID.

1.4.1.1.1 Countermeasures

- Prevent unauthorized access to the password file
- Intrusion detection systems to monitor for suspicious activity
- Re-issuance of passwords if compromise is suspected

1.4.1.2 Specific Account Attack

The attacker targets a specific account and submits password guesses until the correct password is found.

1.4.1.2.1 Countermeasures

- Account lockout after a certain number of failed attempts.

1.5 UNIX Password Scheme

Definition 1.5.1: Salt

A random value added to the password before applying the one-way hash function. The salt:

- Prevents duplicate passwords from having the same hash value.
- Increases the complexity of dictionary attacks by requiring attackers to compute hashes for each possible salt value.
- Almost impossible to find whether a person with passwords on two or more systems has used the same password on those systems.

1.5.1 Attacks

1.5.1.1 Dictionary Attacks

An attacker pre-computes hash values for a large number of commonly used passwords and their variations. When the password file is compromised, the attacker compares the stored hash values against the pre-computed hashes to find matches.

1.5.1.2 Rainbow Table Attacks

Definition 1.5.2: Rainbow Table

A pre-computed hash table used to reverse weakly hashed passwords.

An attacker uses a rainbow table to look up the hash values from the compromised password file to find the corresponding plaintext passwords.

1.5.1.3 Brute-Force Attacks

An attack uses a tool like John the Ripper to systematically generate and hash all possible password combinations until a match is found.

1.6 Biometric Authentication

Definition 1.6.1: Biometric

A measurable physical or behavioural characteristic used to uniquely identify individuals.

Authenticates an individual based on their unique physical or behavioural characteristics. Harder to implement and more expense than password-based or token-based identification. Once compromised, biometric data cannot be changed like passwords or tokens. Some common biometric modalities include:

- Facial characteristics
- Fingerprints
- Hand geometry
- Retinal patterns
- Iris patterns
- Signature dynamics
- Voice patterns