CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

User Authentication, Access Control, and Operating System

Introduction to User Authentication

Video Summary

- What is User Authentication (UA)
- Password Based Authentication
- Vulnerability of Passwords

NIST SP 800-63-3 (Digital Authentication Guideline, October 2016) defines digital user authentication as:

> “The process of establishing confidence in user identities that are presented electronically to an information system.”

Two Steps of Authentication

1. Identification step: presenting an identifier to the security system
   - E.g. user ID
   - Generally unique but not secret
2. Verification step: presenting or generating authentication information that acts as evidence to prove the binding between the attribute and that for which it is claimed.
   - E.g. password, PIN, biometric information
   - Often secret or cannot be generated by others

Means of Authentication

Something the individual . . .

Knows

- E.g. password, PIN, question answers

Possesses

- Token, e.g. keycards, smart card, physical key

Is

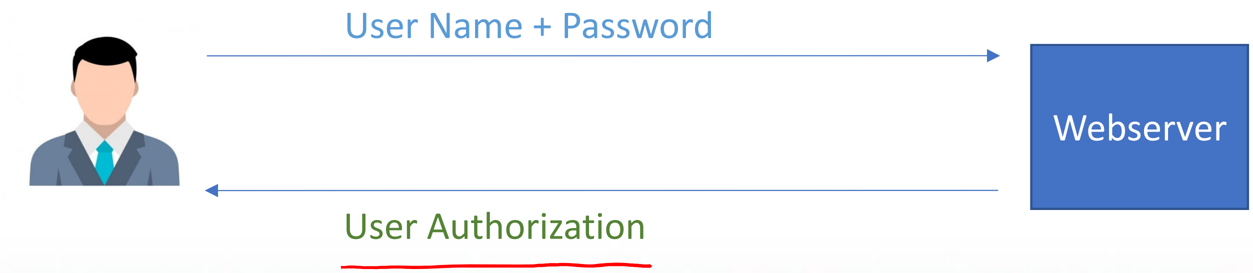
- Static biometrics, e.g. fingerprint, retina, face

Does

- Dynamic biometrics, e.g. voice pattern, handwriting, typing rhythm

Password-Based Authentication

- Many multiuser computer systems used combination of ID and password for user authentication
- System initially stores username and password
- User submits username/password to system; compared against stored values; if match, user is authenticated



Password-Based Authentication

- Identity (ID):
  - Determines whether user is authorised to gain access to system
  - Determines privileges of user, e.g. normal or superuser
  - Used in access control to grant permissions to resources for user
- Password:
  - What is a good password?
  - How to store the passwords?
  - How to submit the passwords?
  - How to respond (if no match)?

Vulnerability of Passwords

Offline Dictionary Attack Attacker obtains access to ID/password (hash) database; use dictionary to find passwords

- Countermeasures: control access to database; reissue passwords if compromised; strong hashes and salts

Specific Account Attack Attacker submits password guesses on specific account

- Countermeasure: lock account after too many failed attempts

Popular Password Attack Try popular password with many IDs

- Countermeasures: control password selection; block computers that make multiple attempts

Data Base

Vulnerability of Passwords

Password Guessing Against Single User Gain knowledge about user and use that to guess password

- Countermeasures: control password selection; train users in password selection

Computer Hijacking Attackers gains access to computer that user currently logged in to

- Countermeasure: auto-logout

Exploiting User Mistakes Users write down password, share with friends, tricked into revealing passwords, use pre-configured passwords

- Countermeasures: user training, passwords plus other authentication

Vulnerability of Passwords

Exploiting Multiple Password Use Passwords re-used across different systems/accounts, make easier for attacker to access resources once one password discovered

- Countermeasure: control selection of passwords on multiple account/devices

Electronic Monitoring Attacker intercepts passwords sent across network

- Countermeasure: encrypt communications that send passwords

Video Summary

- What is User Authentication (UA)
- Password Based Authentication
- Vulnerability of Passwords