# Lecture 6 🛕

> **Class**: Implementing User authentication and access control
>
> **Date**: 13.14 AM , 11 Nov
>
> **Author**: Lasal Hettiarachchi

---

### Key learnings:

- How Encryption , Hash fucnctions, digital signatures are used together in actual security
- How internet works on a security standpoint

### User authentication vs message authentication

- Message authentication is how the receiver checks where the message originated from (Digital signatures)
- User authentication is accessing a system resouce. See whether who they claim to be.(Access control)

### Authentication

- Authentication is the way to determining who someone is so that you can make a decision about whether they're allowed to access a resource or not.
- Verifying a claimed identity
- Give a UN: claim to be someone
- Give PW : Prove that the someone is you

### Autherization

- You dont claim to be someone
- Identify and provide the privillages

### Types of Authentication

- User Authentication : Used to ensure that the user of the system is who them claim to be
- Message authentication: Used to ensure that messages have not been tampered with (typically referred to as Integrity)

### Purpose of Authentication

- Validate the identity of a person
- Decide to give the privillages

### Forms of Authentication

- Something you know
  - UN,PW/ PIN
- Something you are

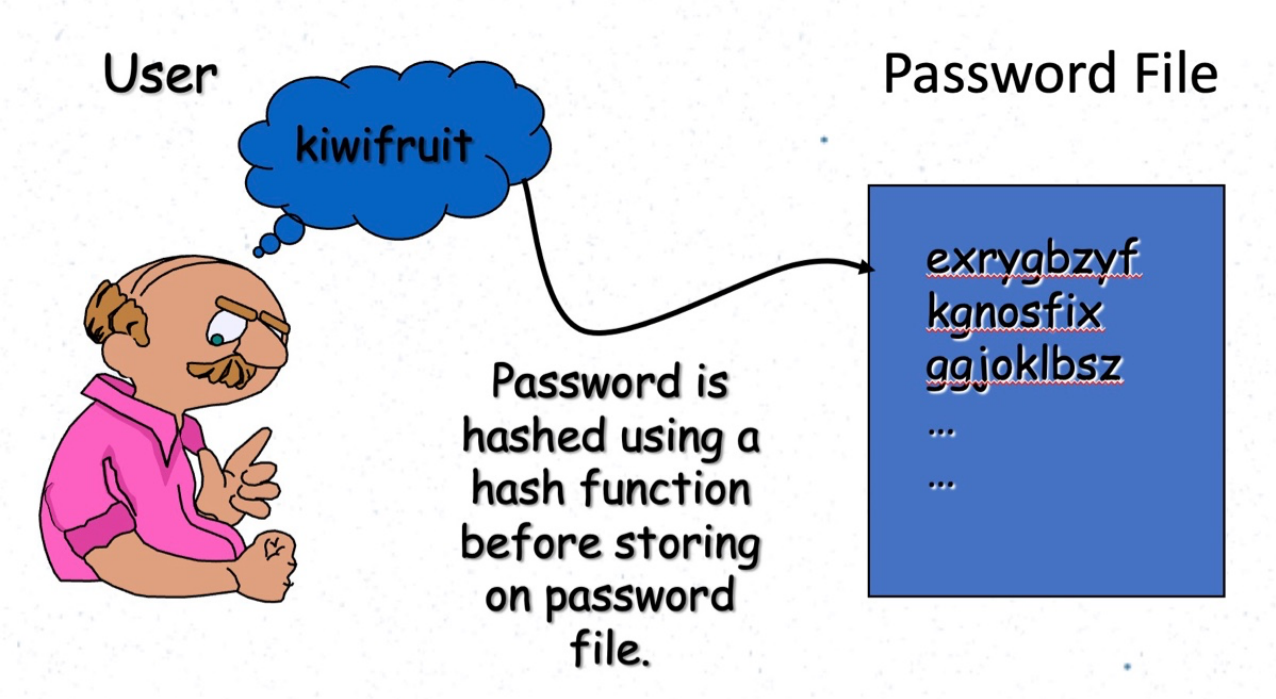
- Thumbprint, eye-print, face-print
- Something you have
  - Electronic keycards, smart cards(RFID cards ), physical keys

**Password**

- System checks the string that is authenticated against them
- Issues
  - How it is stored
  - How it is Communicated
  - How easy it is to guess

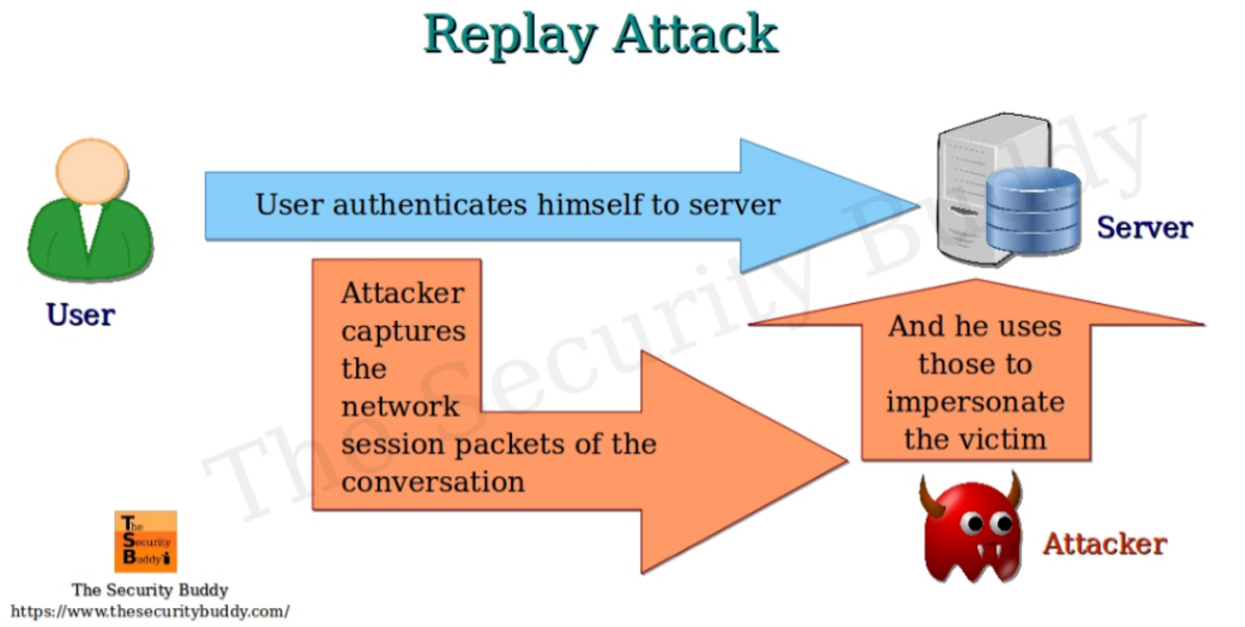
(1) How it is stored

- Hashed format in hard drives (One way function)



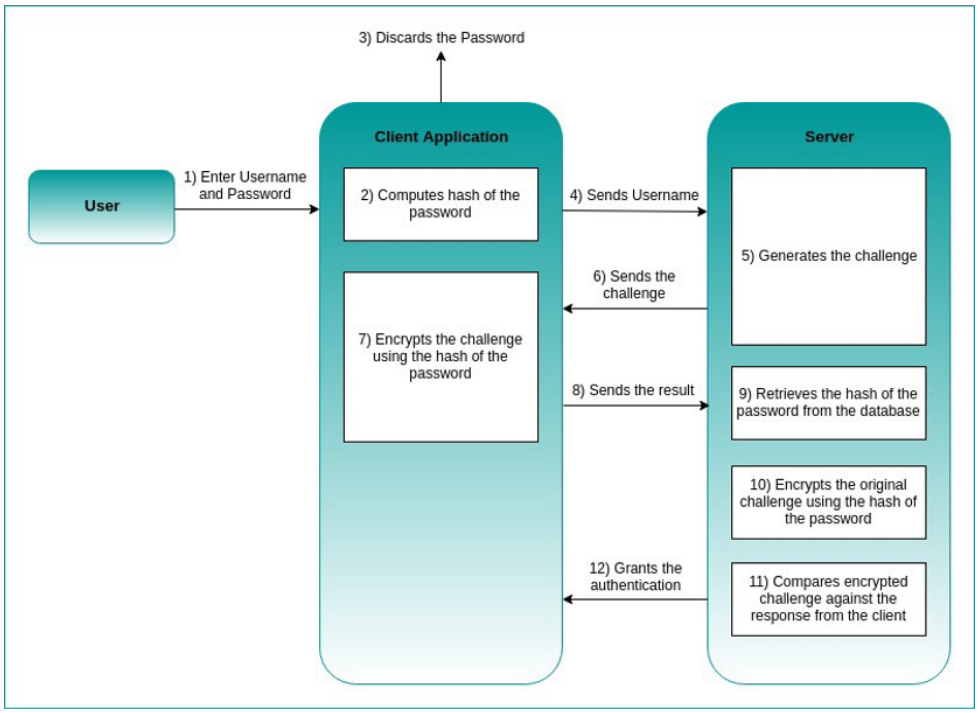

(2) Password communication

- Encrypt the password and send over the network
- Replay attack: Someone on the network can intercept and takes the encrypted pw adn sends it later




**Challenge response Authentication**

- Here the person/service doing the authentication sends a challenge to the person/service being authenticated
- This is appended/added/combined to the password in some way before being hashed
- Results in a one-time password being generated
- Client app takes both UN and PW and send the UN to the server
- The server responds with a challenge
- Server generates a nonce and send to the client and the server remembers the nonce
- Client combines the nonce and the pw together
- the pw + challenge is hashed and sent to the sever




(3) Password security

- How it is secured when stored in the head
- Brute force attacks: attempts all possible combinations
  - Max attempts can stop external entities from attacking
- Dictionary attacks: Uses preset common words blanks to try and generate the password
  - Most used letter is e
- Social engineering : Tricking people to reveal the pw.
  - Phishing
- Shoulder Surfing: Watching people while people enter credentials
- Hacking software: Worms, Trojans,XSS (Keyloggers). (Screen loggers: record the screen).
- Password policy:
  - Passphrase
  - Best practices
    - Cannot use actual words.

**Something you have**

Tokens:

- RFID tags
- Security token
- Credit cards

- Hardware tokens: Has an internal clock, serial number.
- OTP : Something u have

**Something you are**

- Biometrics
- Advantages: Cannot be disclosed lost
- Disadvantages:
  - Cost, Installation, maintenance
  - Reliability of compression
  - Needs AI
  - If forged, cannot revoke

**Authentication Models**

- One factor
  - using only one authentication credential
- Two factor
  - Requires 2 types of authetication credentials
  - 2 factor using biometrics are becoming the norm
- Three factor
  - Requires 3 types of authetication credentials

**Human authentication**

- Determining whether u are a human
- CAPTCHA

---

**Access contol and Authorisation**

- Access control : Different users allowed to do different functions
- Authorization: Once authenticated, determine whether the user is permited to perform the requested task
- Identification: Review of credentials
- Authentication: Validating the credentials
- Authorization: Granting permission
- Access: Right given to access the resource

**Principle of least privilege**

When user of a system is allowed access to functionality they should be given the minimum functionality in the system

- Giving users only read access to shared files if that's what they need, and making sure write access is disabled
- Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password
- Not allowing software developers to move software from development servers to production servers

**Elements of Access control**

- Obect:

An object is a specific resource which access needs to be controlled,

  - Example: records, files, mailbox, program, messages
- Subject:

A subject is an entity that attempts to access an object.

  - Example: Users, Groups, Roles
- Operation/ acess right

The action that is taken by the subject over the object is called an operation.

  - Example: read, write, execute, delete, create, search

Owner : System admin who has all the access in the system

Groups: Has specific rights on the ibject

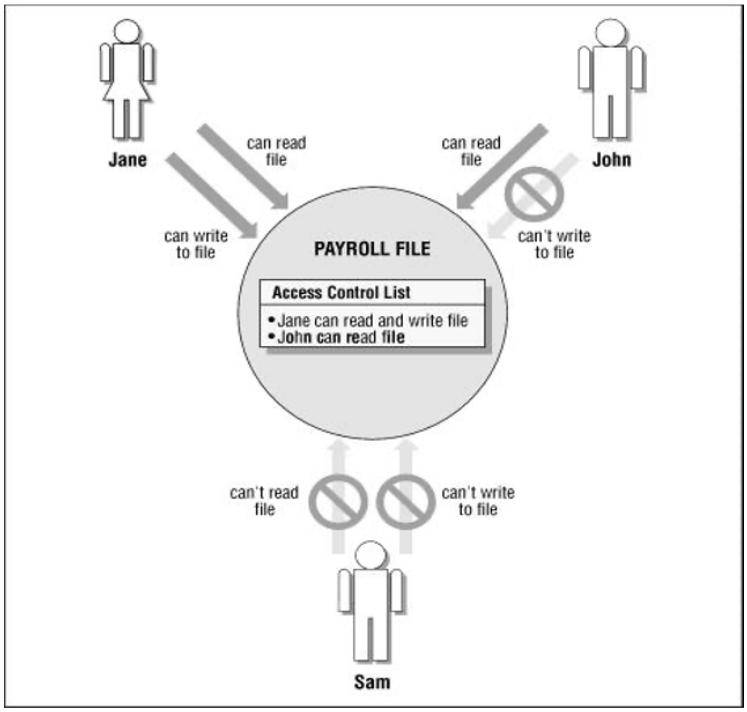
World: Everyone who can access the system that doesnt have the rights

**Access control methods**

- Security levels and asset classification:
  - DAC: Discretionary Access Control (least secure)
  - RBAC: Role-Based Access Control
  - MAC: Mandatory Access Control (Most secure)

**DAC**

- Owner decides how resources can be shared and choose access




Access control matric

- rows : List of subjects in one dimension
- columns: List of objects in the other direction

---

| | | OBJECTS | | | |
|---|---|---|---|---|---|
| | | File 1 | File 2 | File 3 | File 4 |
| SUBJECTS | User A | Own Read Write | | Own Read Write | |
| | User B | Read | Own Read Write | Write | Read |
| | User C | Read Write | Read | | Own Read Write |

(a) Access matrix

---

Role based access control is where ratherthan access is provided to individuaks access is provided to roles.

---

MSFTGuest Login

https://msftguestap.partners.extranet.microsoft.com/guest/msftguest_launcher_c.php?switch_url=https://msftguest-virtual....

https://msftguestap.partners.extranet.microsoft.com/guest/msftguest_launcher_c.php?switch_url=https://msftguest-virtual....