Date _____ Day _____

CHAPTER # 07

→ User authentication is the basis for
↳ Access control & User accountability

→ User authentication encompasses two functions
(1) Identification — The user identifies itself to the system using credentials like user ID
(2) Verification — The system verifies the user by using credentials.

→ User authentication is different from message authentication.
↳ User auth. is to ensure that the entity trying to access the sys. is legitimate
↳ Message auth. is about verifying that a msg came from a legitimate source and has not been altered during transmission.

Date _____ Day _____

• Digital User Authentication Model

▷ The initial requirement for performing user authentication is that the user must be registered with the system

▷ An applicant applies to a registration authority (RA) to become a subscriber of a credential service provider (CSP) → organization that creates & issues digital signatures after approval from RA

▷ RA is a trusted entity that establishes & vouches for the identity of an applicant to a CSP

▷ The CSP then engages in an exchange with the subscriber. The CSP issues some sort of electronic credentials to the subscriber.

↳ The credentials (a data structure) binds an identity to a token possessed by the subscriber

▷ The party to be authenticated is called claimant

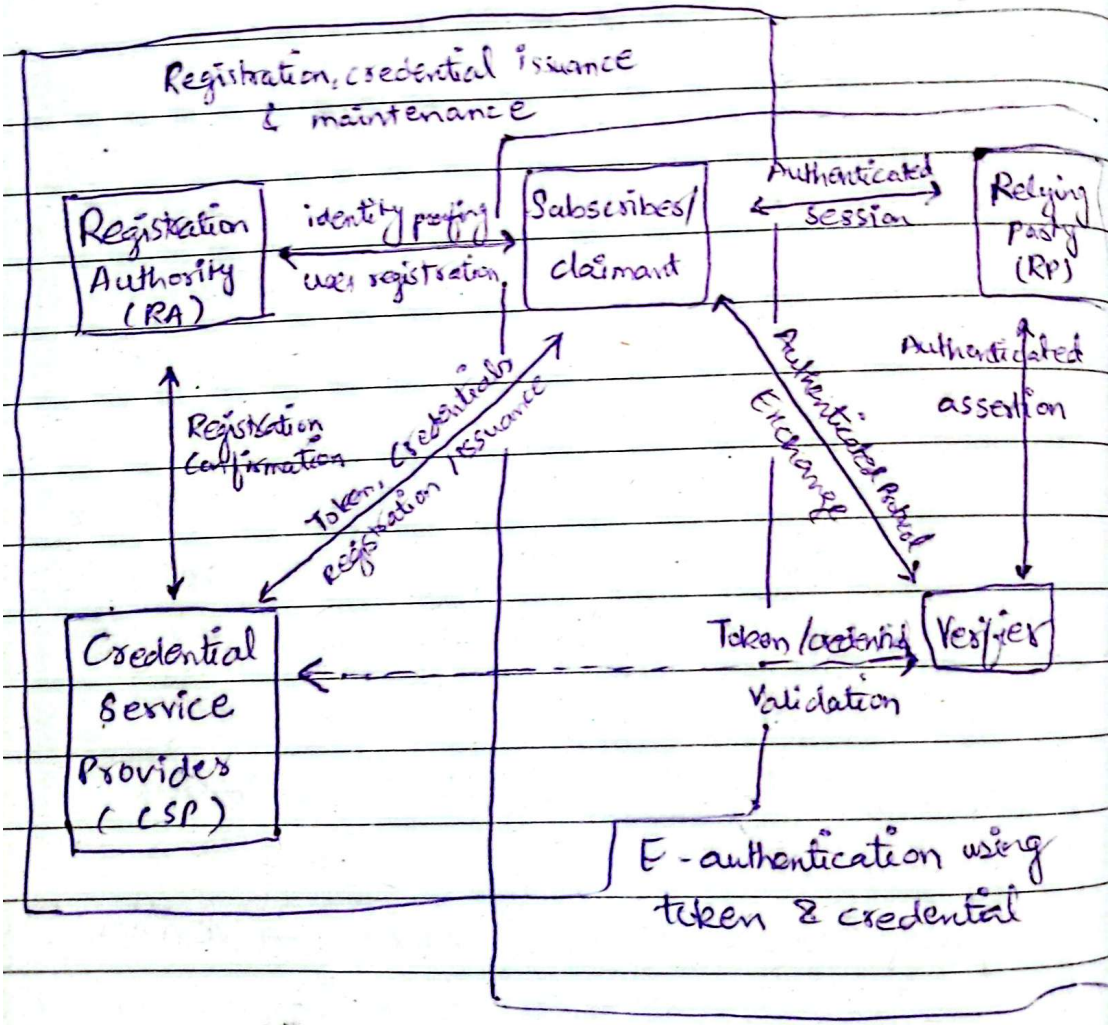
▷ The party verifying that identity → verifier

▷ The verifier passes on assertion about the identity of the subscribes to the relying party (RP) → The system that relies on verifier party

↳ RP uses the auth info to provide access control

Date _____ Day _____

- Purpose of this Model
  - → Establish trust in digital identities
  - → Seperate responsibilities among trusted parties (RA, CSP, Verifier, RP)
  - → Prevent fraud, impersonation or unauth. access
  - → Provide a foundation for secure login & access



Date _____ Day _____

- Means of Authentication

These are four general means of authenticating a user

(1) Something the individual knows – Password, PIN
(2) Something the individual possesses – Keycard, smart card
↳ This type is refered to as token
(3) Something the individual is (static biometrics) –
↳ Recognition by fingerprint, retina, face
(4) Something the individual does (dynamic biometrics)
↳ Recognition thru voice, typing rythm, handwriting characteristics

→ Multifactor Authentication refers to the use of more than one authentication means in the preceding list

- Risk Assessment for User Authentication

↳ It connects three key ideas.

(1) Assurance level – How confident we are in a user's identity
(2) Potential Impact – What would happen if authentication fails
(3) Areas of Risk – The points where authentication could be compromised

Date _____ Day _____

① Assurance Level (LOA - Level of Assurance)

↳ It defines how much confidence an organization has that:

↳ the person using a credential is really the person it was issued to

↳ the verification process was strong

#01 - Level [Little or No Confidence]

- Typical use : low-risk online activities
  ↳ Joining a discussion board or newsletter signup
- Authentication Method : Simple User ID + pswd
- Impact if Compromised : Minimal

#02 - Level [Some Confidence]

- Typical use : General online business or service
  ↳ Online Shopping acc, e-learning portal
- Authentication Method : Secure protocol (HTTP), password, PIN, OTP etc
- Impact if compromised : Could raise inconvinience but not critical harm

#03 - Level [High Confidence]

- Typical use : Sys handling confidential & sensitive info — Employee logging into company's internal financial reporting sys

Date • Authentication Method: Multi factor Authentication

- Impact if Compromised: loss of sensitive data or modeate financial loss

#04 – Level [Very High Confidence]

- Typical use: Systems with very high security requirements
  - ↳ Law enforcement officer accessing criminal records database
- Authentication Method: Multiple authentication factors
  - ↳ In-person identity verification req during registration
- Impact if Compromised = Severe – privacy violation national security risk, major financial loss

② Potential Impact

- LOW:
  - ▷ If authentication fails, the damage is minor – operations continue but slightly affected
  - ▷ Example
    - ↳ A user cannot post on a public discussion forum due to authentication error

Date

- MODERATE
  - If authentication fails damage is serious but not catastrophic - functions are reduced and losses are noticeable
  - Example
    - An unauth. person gains access to a company's internal HR system containing employee contact info & salaries

- HIGH IMPACT
  - Damage is catastrophic on authentication failure Critical funcs stops or life-threatening harm occurs
  - Example
    - A hackers gains access to a law enforcement or hospital database

(3) Areas of Risk

↳ Refers to different domains where authentication failure could cause harm, such as:

- Financial loss
- Damage to reputation
- Privacy breach
- Legal liability
- Operational Disruption

Date _____ Day _____

- LOW
  - Only minor financial loss or negible liability
  - Example
    - Aunauth access reveals small test data or demo transactions worth very little

- MODERATE
  - Serious but not catastrophic loss or liability

- HIGH
  - Severe or unrecoverable financial damage

- PASSWORD BASED AUTHENTICATION
  - Requires user to enter password + user ID
    - The system verifies it against the one stored in the system

- Role of User ID
  1. Determines who is allowed to log in (only registered users with valid IDs)
  2. Privilege Management — Define user roles and permissions (Admin, Superuser etc)
  3. Enables users to control who can access their private resources.
     - List ids with whom to share files

Date _____ Day _____

- Vulnerabilities of Password Based Authentication

① Offline Dictionary Attack
↳ Attackers steals the pswd hash file and compares hashes of common pswds to find matches
↳ Protect pswd file, use intrusion detection, reissue pswd quickly after breach.

② Specific Account Attack
↳ Attacker repeatedly guesses pswd for a single user account
↳ Account lockout after a few failed attempts

③ Popular Password Attack
↳ Attackers tries common pswd
↳ Enforce strong pswd pdicies

④ Password Guessing (Social-based)
↳ Attacker uses knowledge about the user (eg: birthday date) to guess pswd

Date _____ Day _____

⑤ Workstation Hijacking

↳ Attacker uses an "un-attended" logged in system.

↳ Auto logout after certain period of inactivity

⑥ Exploiting User Mistakes

↳ Users write down, share, or reveal pswd or uses default admin credentials

⑦ Multiple Password Use

↳ Same pswd used accross multiple systems — one breach compromises all

⑧ Electronic Monitoring

↳ Password sent over the network can be intercepted

↳ Use encrypted channels like TLS.

• Hashed Passwords

↳ The use of hashed passwords and a salt value

↳ To load a new pswd into the sys, pswd is either assigned or entered by user

↳ Pswd is combined with a fixed length salt value (a random number)

Date Day

↳ The password is hashed using the salt.
↳ (user id, salt, hash code) stored in the system.
↳ When user logs in, his attempted pswd is hashed & than compared with the stored one. If matches than user is given access

- Why salt?
  ↳ Prevents duplicate pswd from being visible in password file
    ↳ Bcz each pswd will get different ~~hash~~ salt value
  ↳ Increases difficulty of offline dictionary attack
  ↳ Nearly impossible to tell if a person used the same pswd on multiple systems.

- Password Cracking Approaches

(1) Traditional Offline Dictionary Attack:
→ Attacker builds a list ("dictionary") of likely passwords and tries each one
→ For an online attack the attacker submits guesses to the login interface

Date _____ Day _____

→ For an offline attack (attacker has stolen the pswd hashfile) the attacker computes the hash of each dictionary pswd and compares to stored hashes

→ Cost : Time to compute hash for each guess × no. of guesses

(2) Rainbow Tables

→ An alternative is to trade off space for time by precomputing potential hash values.

→ Attacker generates a large dictionary of possible pswds

→ For each pswd, the attacker generates the hash value associated with each possible salt value.

→ The result is a mamoth table of hash values known as rainbow table.

→ Takes less computes processing time & more storage than a brute-force attack

→ Countermeasure : Use sufficiently large salt value & large hash value

Day

• TOKEN BASED AUTHENTICATION

→ Objects that a user possess for the purpose of user authentication are called "tokens"

▷ Memory Cards

→ Memory cards can store but not process data

→ Example:

↳ Bank Card with a magnetic strip, that stores a simple security code

→ Memory cards when combined with PIN offers more security like in ATM (we have to insert card as well as PIN)

→ Drawbacks:

① Requires special readers — increases the cost and to maintain the security of the readers

② Loss of Token (card)

③ User dissatisfaction

▷ Smart Cards

→ Physical Characteristics

↳ Smart tokens contain an embedded microproc and memory

↳ They can take various physical forms

- Smart Card: looks like a credit / bank card
- Other forms: USB tokens, or small devices resembling calculators or keys

Date _____ Day _____

→ User Interface

↳ Some smart tokens include manual interface

↳ Keypad — allows user input

↳ Display — shows generated codes or status information

↳ Enables ~~token to~~ human to token interaction

→ Electronic Interface

↳ Smart cards need an electronic interface to communicate with a reader/writer.

↳ Two main types:

① Contact Smart Cards (ATM Card, Sim Card)

↳ Must be inserted into a card reader

↳ Has metallic contacts

↳ Data, cmds & power are transmitted thru physical contact point

② Contactless Smart cards

↳ Works via radio frequency — only needs proximity to reader

↳ Both card & reader have same antennas

→ Authentication Protocol

• Static Protocol

↳ User first authenticates to the token (eg: by PIN)

↳ Token then authenticates the user to the system

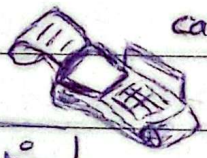
↳ Similar to memory token

Date _____ Day _____

↳ Smart ID cards used in office

- Dynamic Password Generator
  - ↳ The token generates a new, unique pswd periodically (eg every 60 sec) → Multifactor Auth
  - ↳ The pswd is enter manually or sent electronically to the system
  - ↳ Token & system must be time-synchronized

- Challenge-Response Protocol
  - ↳ The computer system sends a challenge (eg: a random no.)
  - ↳ The smart card computes a response using a cryptographic algo (eg: encryption with a pvt key)
  - ↳ System verifies the response using pub key
  - ↳ Provides strong two-way authentication
  - ↳ Military grade smart cards



| Smart Card Activation |

← ATR — ATR = Answer to Reset

— Protocol Negotiation PTS → PTS = Protocol Type

← Negotiation Answer PTS — Selection

↗ — Command APDU → APDU = Application

↙ ← Response APDU — Protocol Data Unit

| End of Session |

Date _____ Day _____

① When the smart card is inserted, the reader initiates a reset, to set parameters (eg: clock value)

② The card sends an Answer To Rest (ATR) message showing supported protocols & functions

③ The reader may send a Protocol Type Selection (PTS) command to modify protocols or parameters

④ The card replies with a PTS response, confirming the chosen settings

⑤ Both the card & reader then communicate using the agreed protocol to perform the desired application

▷ Electronic ID Cards

→ eID card – A gov. issued smart card that provides verified identity for access to public & pvt services

→ Printed Data on Card

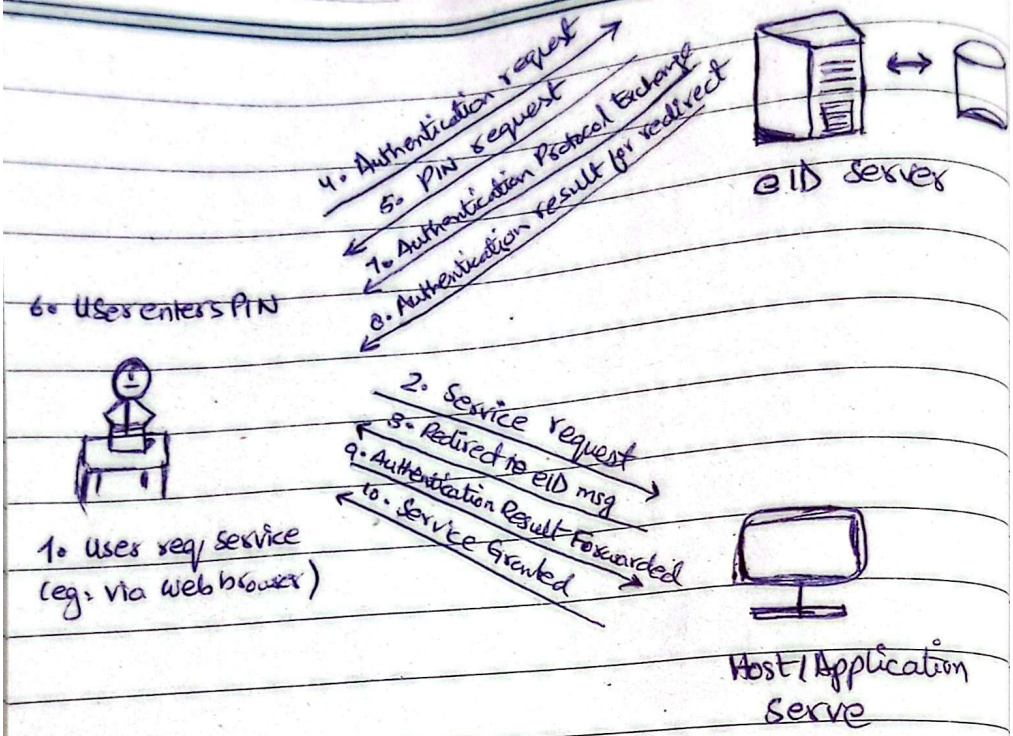
↳ Personal Data

↳ Document number – An alphanumeric nine character unique id of each card

↳ Card access number (CAN) – A six digit decimal random no. Used as a password

↳ Machine Readable Zone (MRZ) – three lines of human- and machine readable text on back of card. Also used as pswd.

Date _____ Day _____



△ User Authentication with eID

▷ Password Authenticated Connection Establishment (PACE)

↳ Ensures that the contactless RF chip in the eID card cannot be read without explicit access control.

• BIOMETRIC AUTHENTICATION SYSTEM

↳ Attempts to authenticate by means of unique physical characteristics – finger prints, hand geometry, facial characteristics, retinal & iris patterns.

↳ Dynamic characteristics such as voiceprint

Date _____ Day _____

- Operation of Biometric Authentication System

① Enrollment
- ↳ User provides name/ID and PIN/Pswd
- ↳ System then captures biometric trait
- ↳ The biometric input is digitized & features one extracted & stored in DB linked with user ID

② Verification (1:1 Matching)
- ↳ User provides ID / Pswd & biometric
- ↳ System compares the biometric with the stored one.
- ↳ If matched → User verified ; else → Access denied

③ Identification (1:N Matching)
- ↳ User provides only biometric input
- ↳ Sys compares biometric with all stored biometric
- ↳ If a match is found → User identified ; else → rejected.

- REMOTE USER AUTHENTICATION
- ↳ An authentication over a network, the internet, or a communications link is more ~~more~~ complex
- ↳ Additional security threats such as:
  - Eavesdropping, capturing a pswd, replaying an auth sequence that has been observed.

Date _____ Day _____

→ Generally use challenge-response protocol

- Password Protocol

→ A challenge-response protocol is used for secu
psud-based auth.

→ Process

① User → Host : Sends ID

② Host → User : Sends a challenge, which include
- A random number (nonce) "γ".
- Two functions : A hash function h() &
a combining function f()

③ User, computes $f(\gamma', h(P'))$
the response

where,
- $\gamma' = \gamma$ (nonce recvd)
- P' = user's pswd

④ User → Host : Sends the computed response

⑤ Host : Compares user's response with
$f(\gamma, h(P(U)))$
- If they match → User authenticated

- Use of "γ" :

↳ Without "γ" an attacker could record the user's
login msg & replay (resend) it later to gain acc
↳ Since "γ" is new each time, even if an att

→ Even the hash of psswd is not directly send the function f() is sent in which psswd is one of it args

Date _____ Day _____

replays an old response, it will not match the new challenge.

↳ Ensures freshness of authentication

↳ Since "r" changes each time, the output of f() also changes — meaning if same psswd is used, the transmitted value is always different so cryptanalysis also not possible

Client

Host

U, User —— U ——→

r, random no.

←— (r, h(), f()) —— h(), f(), functions

p'

r', return of r

—— f(r', h(p')) ——→

if f(r', h(p')) == f(r, h(p(U)))

then yes else no

←—— yes / no ——

▲ Protocol for a password

Date _____ Day _____

• Security Issues For User Authentication

① Client Attacks

- Goal: Attacker tries to impersonate a legitimate user
- Ex: Guessing or brute-forcing pswd
- Countermeasure:
  - ↳ Use strong, lengthy, unpredictable pswd (high entropy)
  - ↳ Limit login attempts / user

② Host Attacks

- Goal: Attack pswd / token / biometric file stored at the host
- Ex:
  - ↳ Stealing pswd files
  - ↳ Extracting biometric templates
- Countermeasures:
  - ↳ Store hashed pswd (not plain txt)
  - ↳ Use one time passcodes (not stored)
  - ↳ Use device authentication for biometric sys

Date _____ Day _____

③ Eavesdropping Attack

- Goal: Capture psswd or tokens via observation or logging
- Ex:
  - ↳ Watching user type
  - ↳ Keylogging malware
- Countermeasure
  - ↳ MFA
  - ↳ Dynamic biometrics (voice, signature)
  - ↳

④ Replay Attacks

- Goal: Capture & resend a legitimate authenticatic message
- Countermeasures:
  - ↳ Use challenge-response protocols

⑤ Trojan Horse Attacks

- Goal: Fake applications or device capture use credentials
- Ex: Fake ATM, stealing PINS
- Countermeasure
  - ↳ Verify authenticity of device & software
  - ↳ Use secure hardware tokens

Date _____ Day _____

⑥ Denial of Service Attack

- Goal : Disable or block authentication service
  - ↳ Flood the sys with fake logins
  - ↳ Lockout legit users via repeated failed attempts
- Countermeasures
  - ↳ Rate limiting & intrusion detection
  - ↳ Token based or MFA protocols