Three-factor Authentication (3FA)

Knowledge factor	Something that is known by the user
Ownership factor	Something that the user possesses, like a key or a token.
Characteristic factor	A user characteristic, such as biometrics; fingerprints, face scan, signature.

Knowledge –Type/category 1 – something you know

Password authentication, Secret questions such as mother's maiden name, favorite food, date of birth, key combination / PIN.

Terminology and concepts

Salted hash	Random data added to a password before hashing and storing in a database on a server. Used instead of plaintext storage that can be verified without revealing password.
ComplEg. password	Alphanumeric, more than 10 characters. Includes a combination of upper and lower case letters, numbers and symbols.
One-time password (OTP)	Dynamically generated to be used for one session or transaction.
Static password	Password does not change. To be avoided.
Cognitive password	Something used to identify a person, i.e. pets name, favorite color, mother's maiden name etc, place of birth etc.
Password Hacking	Unauthorized access of a password file
Brute force attack	Multiple attempts using all possible password or pin combinations to guess the password.
Dictionary attack	Type of brute force attack that uses all the words from the dictionary.
Social engineering attack	Gain access by impersonating a user by establishing legitimate user credentials through social manipulation of trusted parties or authorities.
Rainbow Tables	Precomputed table for reversing cryptographic hash functions and cracking passwords.

Ownership –Type/category 2 – Something you have

Synchronous token	Create password at regular time intervals.
Asynchronous token	Generate a password based on the challenge-response technique.
Memory card	A swipe card containing user information.
Smart Cards or Integrated Circuit Card (ICC)	A card or dongle that includes a chip and memory, like bank cards or credit cards.
Contact Cards	Swiped against a hardware device.
Contactless Cards or Proximity Cards	Simply need to be within proximity to the reader device.
Hybrid Cards	Allows a card to be used in both contact and contactless systems.
USB drive	Bespoke USB with access credentials
Static password token	Simplest type of security token where the password is stored within the token.
Challenge/response token	A challenge has to be met by the correct user response.

Characteristic –Type/category 3 – Something you do / are

Biometric technology allows the user to be authenticated based on physiological behavior or characteristics.
• Physiological i.e. Iris, retina, and fingerprints.
• Behavioral i.e. Voice pattern

Physiological Characteristics

Fingerprint	Scans the thumb or edge of the finger.
Hand Geometry	Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken.
Hand Topography	Hand peaks and valleys pattern.
Palm or Hand Scan	Fingerprint and geometry combination of palm.
Facial Scan	Facial features such as bone, eye length, nose, chin shape etc.
Retina Scan	Retina blood vessel scan.
Retina blood vessel scan	Scans the colored part of the eye around the pupil.
Vascular Scans	Scans the pattern of the veins in the users hand or face.
Voice print	Verify speech sound patterns.

Scanning Behaviors

Signature Dynamics	Pen pressure and acceleration is measured.
Keystroke Dynamics	Scan the typing pattern.
Voice Pattern / Print	Measures the sound pattern of a user read particular word.
Biometric Considerations	Does not change throughout human life and unique. High accuracy rate.
Enrollment Time	Sample processing for use by the biometric system.
Feature Extraction	The process of obtaining the information from a collected sample.
Accuracy	Scan the most important elements for correctness.
Throughput Rate	The rate which the system can scan and analyze.
False Rejection Rate (FRR)	The percentage of valid users that will be falsely rejected. Type 1 error.
False Acceptance Rate (FAR)	The percentage invalid users that will be falsely accepted. Type 2 error.
Crossover Error Rate (CER)	The point at which FRR equals FAR. This is expressed as a percentage - lower CER is better.
Biometric scans	Order of effectiveness and accuracy: Iris Scan • Retina Scan • Fingerprint • Hand Geometry • Voice Pattern • Keystroke Pattern • Signature Dynamics.

Terminology

Access	Action required to allow information flow between objects.
Control	Security measures taken to restrict or allow access to systems.
Subject	An entity which requires access to an object or objects.
Object	Entity which consists information.

Levels of Access & Control

Centralized administration	Only one component can control access. Highly restricted level where control done centrally.
Decentralized administration	Access is controlled by information owners, Can be less consistent.
Hybrid	Combination of centralized and decentralized.

Access stances	**allow-by-default** or **deny-by-default**

Single Sign-On (SSO)	• A.K.A federated ID management • Pros – ComplEg. passwords, easy administration, faster authentication. • Cons – Risk of all systems comprised by unauthorized access of a key or keys.

Authorization

Access control policies: Level of access and controls granted for a user.

Separation of duties	Assigning different users different levels of access to protect privacy and security.
Dual Controls	Access to perform specific functions is granted to two or more users.
Split Knowledge	No single user can have full information to perform a task.
Principle of Least Privilege	User is given minimum access level needed to perform a task.
Need-to-Know	Minimum knowledge level to perform a task.
No Access	User is not assigned any access for any object.
Directory Service	Centrally managed database for user objects management. i.e. LDAP
Kerberos	Client /server model authentication protocol. • Symmetric Key Cryptography • Key Distribution Center (KDC) • Confidentiality and integrity and authentication, symmetric key cryptography
Realm	Authentication administrative domain. Uses symmetric-key cryptography
KDC (Key Distribution Center)	Issues tickets to client for server authentication • Stores secret keys of all clients and servers in the network • AS (Authentication Server) • TGS (Ticket Granting Server)
The Kerberos logon process	• User input username/password in client PC/Device. • Client system encrypts credentials using AES to submit for KDC. • KDC match input credentials against database. • KDC create a symmetric key and time-stamped TGT to be used by the client and the Kerberos server. • Key and TGT are encrypted using client password hash. • Client installs the TGT and decrypts the symmetric key using a hash.

Authorization Methods

Discretionary Access Control (DAC) • Mandatory Access Control (MAC) • Role-based Access Control (role-BAC) • Rule-based Access Control (Rule-BAC).

Discretionary Access Control (DAC)	Uses access control lists (ACLs - Access-control lists).
Mandatory Access Control (MAC)	Subject authorize according to security labels. Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects.
Role-BAC (RBAC)	Task-based access controls - subjects require access an object based on its role or assigned tasks.
Rule-BAC	Uses a set of rules or filters to define what can or cannot be done on a system.
Hybrid RBAC	Limited RBAC
Lattice based / Label	Objects are classified based on control level using a label.
Non-discretionary access / Mandatory-Access control	Based on policies defined by a central authority. Role based or task based.

Authorization Methods / Concepts

Constrained Interface Applications	Restrict actions which can be performed with given privileges.
Content-Dependent	Restrict access to data depends on the content of an object.
Context-Dependent	Granting users access after a specific condition. Eg. after specific date/time.
Work Hours	Context-dependent control
Least Privilege	Subjects are given access to object only to perform what they need to have. • No more or no less!
Separation of Duties and Responsibilities	Tasks split to be performed by two or more people.
User Accountability	Auditing and Reporting • Vulnerability Assessment • Penetration Testing • Threat Modeling
Auditing and Reporting	Users are responsible for what actions they have performed. Events to be monitored for reporting: Network Events • Application Events • System Events • User Events • Keystroke Activity

Access Control Types

Type	Scope / Purpose	Example
Administrative Controls	Administration of organization assets and personal.	Data classification, data labeling, security awareness training.
Logical / Technical Controls	Restrict access.	Firewalls, IDS's/ IPS's, encryption, biometrics, smart cards, and passwords.
Physical Controls	Protect organization's infrastructure and personnel.	Perimeter security, biometrics and cabling.

Procedure for user account management

Regular user account review and password changes, track access authorization using a procedure, regularly verify the accounts for active status.

Access Control Requirements

CIA Triad: **C**onfidentiality - **I**ntegrity - **A**vailability (See Domain 1 cheat sheet!!!!!)

Identity Management

IAAA – **I**dentification - **A**uthentication - **A**uthorization - **A**ccountability.

Identification	• Registration verification of user identity and add an identifier to system. • Assign user the proper controls • Commonly use user ID or username.
Authentication	• User verification process • Commonly used passwords
Authorization	• Defining resources for user access
Accountability	• Person responsible for the controls, uses logs.

SESAME (Secure European System for Applications in a Multi-vendor Environment)

Public Key cryptology only authenticates initial segment without authenticating full message. Two separate tickets are in use one for authentication and other one defines the access privileges for user. Both symmetric and asymmetric encryptions are used.

SAML - (SOAP/XML)	Exchange authentication and authorization information between security domains and systems. • Components: Principal User • Identity provider • Service provider. • Use in directory federation SSO.

Authorization Concepts

Security domain	Set of resources having the same security policies.
Federated Identity	Organization having a common set of policies and standards within the federation.

Federation Models

Cross-Certification Model	Every organization is certified and trusted by the other organizations within the standards defined internally by said organizations.
Trusted Third-Party / Bridge Model	Every organization adheres to the standards set by a third party.
IDaaS (Identity as a Service)	Identity and access management is provided by a third party organization.
SSO (Single sign-on)	Access management for multiple similar, yet independant systems. Primarily used for the cloud and SaaS based system access.
Cloud Identity	User account management (Office 365)
Directory Synchronization	On-premises identity provider (Microsoft Active directory)
Federated Identity	On-premises identity provider for managing login request. (MS AD)

Access Control Models

Implicit Deny	By default access to an object is denied unless explicitly granted.
Access Control Matrix	Table which included subjects, objects, and access controls / privileges.
Capability Tables	List access controls and privileges assigned to a subject. • ACLs focus on objects whereas capability lists focus on subjects.
Permissions	Access granted for an object.
Rights	Ability/access to perform an action on an object.
Privileges	Combination of rights and permissions.

Access Control Categories

Category	Scope / Purpose	Example
Compensative	Risk mitigation action.	Two keys or key and combination to open a safety locker.
Corrective	Reduce attack impact.	Having fire extinguishers, having offsite data backups.
Detective	Detect an attack before happens.	CCTV, intrusion detection systems (IDS).
Deterrent	Discourages an attacker.	User identification and authentication, fences
Directive	Define and document acceptable practices within an organization.	Acceptable Use Policy (AUP)
Preventative	Stop an attack.	Locks, biometric systems, encryption, IPS, passwords.
Recovery	Recovery of a system after an attack.	Disaster recovery plans, data backups etc.

Vulnerability Assessment

Personnel Testing • Physical Testing • System and Network Testing

Penetration Testing and Threat Modeling

Simulate an attack to determine the probability of the attack to the application systems

Steps	1. Record information about the system
	2. Collect information about attack against the system
	3. Discover known system vulnerabilities
	4. Perform attacks against the system attempting to gain access
	5. Document the outcome of the penetration test

Penetration Test Types

Blind Test	Organization knows about possible attack but very limited knowledge.
Double-Blind Test	Organization doesn't know about incoming attack except for very few people in the organization who do not exchange information.
Target Test	Organization has prior knowledge of the attack, including key details

Penetration Strategies

Zero-Knowledge Test	Test team doesn't know any information about the target network A.K.A. black box testing.
Partial Knowledge Test	The testing team knows public knowledge about the organization's network.
Full Knowledge Test	The testing team knows all available information regarding the organization's network.

Password types

Simple Passwords	Single word usually a mixture of upper and lowercase letters.
Combination / Composition Passwords	Combination of two unmatching dictionary words.
Passphrase Passwords	Requires that a long phrase be used.
One-Time or Dynamic Passwords	Passwords that are valid for a single session login.
Graphical Passwords (CAPCHA)	Uses of character images or graphics as a part of the authentication.
Numeric Passwords	A password that only uses numbers.