Module 2: Authentication and Access Control (6 hours)

Authentication and Access Control - Module 2 Summary

1. Authentication Authentication is the process of verifying the identity of a user. It ensures that an individual is who they claim to be. Authentication factors include:

- **Something You Know**: Passwords, PINs, security questions.
- **Something You Have**: Security tokens, smart cards.
- **Something You Are**: Biometrics like fingerprints, facial recognition.
- **Somewhere You Are**: Location-based authentication.
- **Something You Do**: Behavioral biometrics like typing patterns.

2. Key Management Schemes Key management is crucial for secure encryption and authentication. It involves:

- **Key Generation**: Creating cryptographic keys securely.
- **Key Distribution**: Ensuring only authorized entities receive keys.
- **Key Storage**: Protecting keys from unauthorized access.
- **Key Rotation**: Regularly updating keys to prevent breaches.
- **Key Revocation**: Disabling compromised keys.

3. Hierarchical Key Management Techniques This technique structures keys in a hierarchy:

- **Master Key**: Used to generate other keys.
- **Session Keys**: Temporary keys for secure transactions.
- **Sub-keys**: Assigned to specific systems or functions.

4. Security Standards Security standards provide best practices for ensuring data protection:

- **ISO 27001**: Information Security Management System (ISMS).
- **ISO 27002**: Security controls and guidelines.
- **GDPR**: Data protection regulations for EU citizens.
- **PCI DSS**: Standards for payment card security.
- **HIPAA**: Security rules for healthcare data.

5. User Authentication Protocols

- **Kerberos**: Uses tickets for secure authentication.
- **OAuth 2.0**: Authorization framework for API access.
- **SAML**: Security assertion for identity verification.
- **RADIUS**: Remote authentication for network access.
- **LDAP**: Directory-based authentication.

6. Implementing Access Controls Access control ensures users can only access resources they are authorized for. Methods include:

- **Discretionary Access Control (DAC)**: Users control access to their own resources.
- **Mandatory Access Control (MAC)**: Access is controlled by a central authority.
- **Role-Based Access Control (RBAC)**: Permissions are assigned based on user roles.
- **Attribute-Based Access Control (ABAC)**: Access is based on attributes like location or device type.

7. Access Control Models

- **RBAC (Role-Based Access Control)**: Users are assigned roles with predefined permissions.
- **ABAC (Attribute-Based Access Control)**: Decisions are based on multiple attributes.
- **Access Control Lists (ACLs)**: Lists of permissions assigned to users for each resource.

- **Capabilities List**: Specifies what actions a user can perform.

8. Role-Based Access Control (RBAC) RBAC assigns permissions based on roles rather than individuals, making it easier to manage access rights. It supports:

- **Hierarchical RBAC**: Roles inherit permissions from parent roles.
- **Static RBAC**: Users have fixed roles.
- **Dynamic RBAC**: Roles change based on user behavior.

9. Attribute-Based Access Control (ABAC) ABAC makes access decisions based on:

- **User Attributes**: Role, clearance level, group membership.
- **Resource Attributes**: File sensitivity, owner.
- **Environmental Attributes**: Time of access, location, device type.

10. Attribute-Based Encryption in Information Storage Encryption that ties decryption keys to specific attributes. It ensures:

- **Fine-grained access control**: Users can decrypt only the data they are authorized for.
- **Scalability**: Works well for cloud storage and large databases.

11. Physical Access Controls Ensuring physical security is as important as digital security. Methods include:

- **Biometric scanners**: Fingerprint, retina, facial recognition.
- **Security badges & smart cards**: Used for restricted area access.
- **Surveillance & alarms**: Monitoring physical access points.

12. Multi-Factor Authentication (MFA) Combines multiple authentication factors to enhance security, such as:

- Password (something you know) + Security token (something you have).
- Biometric scan (something you are) + Location-based verification.

13. Password Security & Brute Force Protection

- **Strong Password Policies**: Requires complex passwords.
- **Salted Hashing**: Adds random data to passwords before encryption.
- **Account Lockouts & CAPTCHA**: Prevents repeated login attempts.
- **Multi-Factor Authentication (MFA)**: Protects against credential theft.

14. Federated Identity Management (FIM) & Single Sign-On (SSO)

- **FIM**: Allows users to access multiple systems with one identity.
- **SSO**: Enables logging into multiple services using a single authentication.

15. Cryptography & Key Management

- **Symmetric Encryption**: Single key for encryption and decryption (e.g., AES).
- **Asymmetric Encryption**: Uses a public and private key (e.g., RSA, ECC).
- **Key Lifecycle Management**: Secure generation, distribution, and storage of cryptographic keys.

16. Reference Monitor & Access Control Enforcement A reference monitor enforces security policies by ensuring:

- **Complete Mediation**: Every access request is checked.
- **Tamperproof Protection**: It cannot be bypassed.
- **Verifiability**: Its correctness can be proven.

17. Access Control Directory & Lists

- **Access Control Lists (ACLs)**: Defines permissions for each object.
- **Privilege Lists**: Shows user-specific access rights.
- **Access Control Matrix**: Tabular representation of subject-object relationships.

18. Implementing Effective Access Policies

- **Least Privilege**: Users get only necessary permissions.
- **Separation of Duties**: Different users handle different security-sensitive tasks.
- **Audit Logging**: Records access attempts and modifications.

19. Summary Authentication and access control are critical for securing systems and data. Implementing robust authentication methods, using strong encryption, and enforcing access control policies help prevent unauthorized access and cyber threats.