**Module 4 Identity & Access Management**

**4.3 Identity & Access Management**

**Access Control Models**

* Terms

1. *Subject* is an active entity (Generally an individual/process/device)
2. *Object* is some resource that subject is attempting to access

* MAC (Mandatory Access Control)
* DAC (Discretionary Access Control)
* ABAC (Attribute-Based Access Control)
* RBAC (Role-Based Access Control)
* RBAC (Rule-Based Access Control)

**MAC (Mandatory Access Control)**

* Assigning labels to resources & accounts (objects)
* Users & system accounts (subjects) assigned a classification level
* Eg. SECRET, CONFIDENTIAL, PROPRIETARY & PUBLIC
* Subjects access rights must be above object’s classification
* Access is nondiscretionary
* Used In government/military
* Right & most secure

**DAC (Discretionary Access Control)**

* Access rights at discretion of system/information owner/security principal
* Owner assigns security access/has flexibility in accessing information/systems
* Allows dynamic sharing
* Increased risk of unauthorised disclosure/access

**ABAC (Attribute-Based Access Control)**

* Denied in NIST 800-162, Attribute-Based Control Definition & Considerations
* Attributes are characteristics that define specific aspects of subject, object, environment conditions &/or requested actions predefined & pre-assigned by authority
* Considers all various attributes associated with subject & object in making access control decision
* Dynamic access control method
* Based on Extensible Access Control Mark-up Language (XACML)

**RBACs**

* Role-based access control (RBAC)

1. Access control based on established roles/job functions in organisation
2. Group-based permissions
3. Reduces effect of permissions creep

* Rule-based access control (RBAC)

1. Uses settings in preconfigured security policies to make all access decisions
2. Includes controls such as time of day, day of week, specific terminal access & GPS coordinates of requester
3. Implemented with Access Control Lists (ACLs)

**Biometrics**

* Metrics related to human characteristics/body measurement
* Fingerprint scanner
* Retinal scanner
* Iris scanner
* Voice recognition
* Facial recognition
* Signature
* Gait

**Biometrics Factors**

* False acceptance rate
* False rejection rate
* Crossover error rate

**Tokens**

* Physical device used for access
* Software/hardware based
* One-time passwords (OTP)

1. HOTP – HMAC (Hash Message Authentication Code) OTP – uses a hash
2. TOPT – Time-based – limited time availability

* Eg. Wireless key card, key fob, any physical device
* Contains *digital certificate* &/or *static password token*

**Physical Access Controls**

* Both use embedded microchips
* Also see PIV (Personal Identification Verification) & CAC (Common Access Card) – using certificates
* Proximity cards

1. Hold little information
2. Determines access by matching card identification number to access database information

* Smart cards

1. Provides authenticating cryptographic key to its reader
2. May include other information on programmable chip (biometrics, certificates)

**Certificate-Based Authentication**

* PIV (Personal Identity Verification) cards – contactless smart card used by US Federal Workers
* CAC (Common Access Card)

1. Credit card-sized “smart” card used by US DoD (Department of Defence) workers
2. Inserted into smart card reader authenticated with PIN

* IEEE 802.1x

1. Certificate based network authentication
2. Allows only authorised devices to connect to network

**Fire System Security**

* AKA flat files
* Leverage access controls, encryption & RAID
* Microsoft NTFS (New Technology File System) allows file-level access control where FAT (File Allocation Table) allows only share-level access
* Consider using encryption for sensitive directories/media

**Database Security**

* Store organisations most sensitive/critical data
* Leverage network security & access, controls within the Database Management System (DBMS)
* Transparent Data Encryption (TDE) for data
* Crypto key management