**Module 4 Identity & Access Management**

**4.1 Identity Access & Management Concepts**

**Logical & Access Management Concepts**

* Logical access controls
* Identification, authentication, authorization & accounting (IAAA)
* Multifactor authentication
* Federation/federated identity
* Single sign-on (SSO)
* Transitive trust

**Identification & Authentication**

* Identification

1. 1st step
2. Subject provides identification information – unique to subject
3. Username, User ID, account number

* Authentication

1. Verifying identification information
2. Proving identity
3. Password/phrase, PIN, fingerprint, smart card

**Authorising & Auditing**

* Authorisation

1. What subject allowed to see/do
2. Determining operations subject mat perform on object
3. Permissions

* Auditing/accounting – record of events, logs

**Authentication Factors**

* Something you know Eg. Password, PIN
* Something you have Eg. Smart card, token, identification device
* Something you are Eg. Fingerprints, retinal pattern (biometrics)
* Something you do Eg. Action you must take to complete authentication
* Somewhere you are (based on geo-location)

**Authentication**

* Single Factor (SFA)

1. 1 type
2. Traditionally password

* Multi-Factor Authentication (MFA)

1. Uses 2 or more access methods
2. Factors should not be in same category

* Mutual authentication – each party validates other’s identity

**Biometrics**

* Type 3 – something you are
* Metrics related to human characteristics/body measurements

**Biometric Errors**

* False Acceptance Rate (FAR) – system accepts intruder who should be rejected
* False Rejection Rate (FRR) – system rejects authorised user
* Cross-Over Error Rate (CER)

1. Metric for comparing biometric systems
2. Point where FAR & FRR are equal

**Federation/Federated Identity**

* Means of linking person’s electronic identity & attributes, stored across multiple distinct identity management systems
* Means of linking user’s identity with their privileges in manner that can be used across business boundaries
* Allows user to have single identity they can use across different businesses
* Eg. Google, Facebook, Microsoft

**Single Sign-On (SSO)**

* Allows user to authenticate 1 time & then access resources in environment w/o needing to re-authenticate
* Different from *password synchronisation*
* Vulnerability – if attacker uncovers user’s credentials, they will have access to all user’s resources
* May also be single point of failure

**Transitive Access/Trust**

* If Domain A trusts Domain B & Domain B trusts Domain C, Domain A also trusts Domain C