CompTIA Security + 4.0 Identity and Access Management

Filename: comptia-secplussy0501-4-3-identity_and_access_management_controls
Title: Identity and Access Management Controls
Subtitle: CompTIA Security+ (SY0-501)

4.3 Identity and Access Management Controls

- 4.3 Given a scenario, implement identity and access management controls.
    - Access control models
        - MAC
            - Based classifications assigned to users and objects
            - Both classifications have to match for access to be granted
        - DAC
            - Users are given access based on their identity.
            - Identities are granted different levels of abilities on and object
        - Role-based access control
            - Logical grouping of identities with similiar affliations
            - Access is granted or denied based on the role each group has within an organization
        - ABAC
            - Based on a single or combination of attributes
            - Compared to RBAC which allows access to the Managers role, ABAC could combine additional attributes such as Managers group, east coast region, from their primary computer, with employee ID XYZ.
        - Rule-based access control
            - Access to a resources is based on predetermined and defined rules
            - Access to a Sales team, resource during business hours
            - While the Sale group is a role but the "during business hours is the rule
    - Physical access control
        - Proximity cards
        - Smart cards
            - RFID, proximity
            - Smartcard-access
                - http://bit.ly/2p8aH8S
    - Certificate-based authentication
        - PIV/CAC/smart card
            -
        - IEEE 802.1x
    - Biometric factors
        - Fingerprint scanner
        - Retinal scanner
        - Iris scanner
        - Voice recognition
        - Facial recognition
        - False rejection rate
            - Also known as FRR is the likelihood that a biometric authentication system will not ID an authorized person correctly and deny access
            - Called a Type I error
            - Scenario (mighted be increased)
                - Increased the confidence/sensitivity in the system
                - Increases the security
                - Lowers unauthorized access (FAR) events
                - Lowers convienence
        - False acceptance rate
            - Also known as FAR is the likelihood that a biometric authentication system will incorrectly ID an unauthorized person and allow access
            - Type II error
            - Worst between FAR and FRR
            - Scenario(how it can increase)
                - Lowering confidence/sensitivity
                - Lowers the false rejection instances(complaining users about being locked out)
                - Increases the likelihood of unauthorized access
        - Crossover error rate
            - The point a which the FAR and FRR are equal
            - Lower CER is desired
            - Lower the CER, the more accurate
        - FAR and FRR likelihood might be more or less for given scenarios
    - Tokens
        - Hardware
            - YubiKey - https://www.yubico.com/start/
        - Software

    - Google authenticator - http://bit.ly/2pkiFdL
  - HOTP/TOTP(Both governed by OATH)
    - Intiative for Open Authentication(OATH)
    - HOTP- Hashed OTP - HMAC-OTP
      - HOTP can have a long lifecycle
      - Allowing for attackers time to compromise the key
    - TOTP- Timed OTP - Time-stamped OTP
      - Generated a lot like the HOTP
      - Short lifecycle (time-based)
      - Less time to compromise
- File system security
  - Windows
    - NTFS, ReFS
  - Linux
    - Ext 3,4
  - MacOS
    - Mac OS Extended(Journaled), HFS+,
  - Permission Types
    - Unix/Linux
      - R,W,X
    - Windows
      - Read, Write, Read&Execute, Modify, Full Control
- Database security
  - Seperate the database from the web application servers
  - Input check validation
  - Data encryption
  - Data Normalization
    - Reducing duplication (integrity)
    - Converting data into expect/authorized values
    - Redundancy and backups