Access Controls

Mike Smith

26/04/10 - Rev.27

Threats

- Identity Theft
- Phishing
- Spoofing at logon
- Brute force attacks
  - Wardialing
- Dictionary Attack

Intrusion Detection Systems

- Signature Based
  - Pattern Matching
  - Requires continual update
  - Pattern & Stateful
- Anomaly Based
  - Can detect new attacks
  - Statistical, Protocol and Traffic
- Rule Based
  - Uses an Expert System
  - Cannot detect new attacks
- Network-Based - NIDS
  - NIC in promiscuous mode
- Host-Based - HIDS

Controls

- Administrative
  - Personnel Controls
  - Supervisory Structure
  - Security-Awareness Training
  - Testing
- Physical
  - Network Segregation
  - Perimeter Security
  - Computer Controls
  - Work Area Separation
  - Cabling
  - Control Zone
- Technical or Logical
  - System Access
  - Network Architecture
  - Network Access
  - Encryption and Protocols
  - Auditing
- Deterrent - Intended to discourage
- Preventative - prevent harmful occurrence
- Corrective - restore after harmful occurrence
- Recovery - Intended to bring controls back
- Detective - detect after harmful occurrence
- Compensating - Controls that provide for an alternative
- Directive - Mandatory controls, regulations or environment

Biometrics

- Acceptance
  - False Rejection Rate - FRR = Type I error
  - False Acceptance Rate - FAR = Type II error
  - Crossover Error Rate - CER = % when FRR = FAR
  - Privacy, Physical, Psychological
  - Time to authenticate is the main factor
- Fingerprints
- Retina Scans
- Iris Scans
- Facial Scans
- Palm Scans
- Hand Geometry
- Signature Dynamics
- Keyboard Dynamics
- Hand Topology

Three Factor Authentication

- 1 Something you know (password)
- 2 Something you have (token)
- 3 Something you are (biometric)
- Passwords
  - Static
  - Dynamic
- Tokens Smartcards
  - Static Password
  - Owner authenticates to token
  - Token authenticates to system
  - Dynamic Password
  - Synchronous
  - Asynchronous
  - Side-channel attacks

Accountability

- System-level events
- Application-level events
- User-level events

Access Control Models

- DAC - Data owners decide who has access to resources and ACLs are used to enforce security policy
- MAC - Operating systems enforce the system's security policy through the use of security or sensitivity labels
- RBAC - Access decisions are based on role
- Lattice based - provides least access privileges of the access pair - Greatest lower bound and Lowest upper bound

SSO

- Kerberos
  - Symmetric Key Encryption
  - KDC - Kerberos-trusted Key Distribution Center
  - TGS - Ticket Granting Service
  - AS - Authentication Server
  - KDC knows secret keys of client and server
  - KDC exchanges info with the client and server using symmetric keys
  - Using TGS grants temporary symmetric key
  - Client and server use temporary session key
  - Weaknesses
    - Replay is possible with time frame
    - TGS and Auth server are vulnerable as they know all
    - Initial exchange passed on password authentication
    - Keys are vulnerable
- SESAME
  - Needham-Schroeder Protocol
  - Supports MD5 and CRC32 Hashing

Access Control

- Centralized
  - RADIUS - incorporates an AS and dynamic password
  - TACACS - Terminal Access Controller Access Control System - for network applications - static password
  - TACACS+ - supports tokens
- CHAP - supports encryption
- Operate and maintain
- Monitor and evaluate