Ron Shuck, CISSP, CISM, CISA, GCIA
Infrastructure Security Architect
Spirit AeroSystems

ISC² CBK Roundtable: Access Control

March 5, 2010

Overview

- Control Types
- Control Models
- Identification & Authentication
- Authentication Methodologies
- Monitoring
- NIST 800-53 Access Control Family

Control Types

- **Preventative**
  - Administrative – policies, etc
  - Technical – logic controls, encryption, passwords, biometrics
  - Physical – badges, man-traps
- **Detective**
  - Administrative – job rotation, audits, reviews
  - Technical – IDS
  - Physical – cameras, etc

Control Models

- **Access Control Lists (ACL)**
- **Mandatory –** rule based, need-to-know
  - Lattice Based (LBAC) – upper/lower bound pairs
  - Role Based (RBAC) – user's job function
  - Bell-La Padula – focuses on data confidentiality
  - Biba Integrity – focuses on data integrity
  - Clark-Wilson – formalizing information integrity
- **Discretionary** – user can modify ACL

Identification & Authentication

- **Authentication Factors**
  - Type 1 – something you know - PIN
  - Type 2 – something you have - securid
  - Type 3 – something you are – biometrics
  - Geodetic – somewhere you are
- **Authentication Types**
  - Passwords
  - Biometrics
  - Single Sign On (SSO)

Authentication Methodologies

- **Centralized**
  - **RADIUS** - Remote Authentication Dial In User Service
  - **CHAP** - Challenge-handshake authentication protocol
  - **TACACS** - Terminal Access Controller Access-Control System
- **Decentralized**

Monitoring

- **Intrusion Detection Systems (IDS)**
  - Methods
    - *Signature based*
    - *Statistical anomaly based*
  - Network Based
  - Host Based
- **Penetration Tests**
- **Vulnerability Scans**

NIST 800-53

- Access Control Policy And Procedures
- Account Management
- Access Enforcement
- Information Flow Enforcement
- Separation Of Duties
- Least Privilege
- Unsuccessful Login Attempts
- System Use Notification

NIST 800-53

- Previous Logon Notification
- Concurrent Session Control
- Session Lock
- Supervision And Review
- Permitted Actions Without Identification Or Authentication
- Automated Marking
- Automated Labeling

NIST 800-53

- Remote Access
- Wireless Access Restrictions
- Access Control For Portable And Mobile Devices
- Use Of External Information Systems

Access Control

Questions

ISSA™ Information Systems Security Association
CENTRAL PLAINS CHAPTER