Ron Shuck, CISSP, CISM, CISA, GCIA
Global Computing Security Manager
Spirit AeroSystems

ISC^2 CBK Roundtable: Application Security

November 5, 2010

ISSA™
Information Systems Security Association
CENTRAL PLAINS CHAPTER

Overview

- Databases & Data Warehousing
- Data / Information Storage
- Knowledge-based Systems
- System Development Controls
- Malicious Code
- Methods of Attack
- Attackers

Databases & Data Warehousing

- Security Issues
  - Aggregation
  - Data Mining
  - Inference
- Security Measures
  - Polyinstantiation
  - Cell suppression
  - Partitioning
  - Multi-Level Security

Databases & Data Warehousing

- DBMS Architecture
  - Relational
  - Hierarchical
  - Distributed

Data / Information Storage

- Primary
- Secondary
- Real
- Virtual
- Random
- Volatile
- Sequential

Knowledge-based Systems

- Expert Systems
  - Rule-based
  - Pattern Matching
  - Inference engine
- Neural Networks

System Development Controls

- Software Development Life Cycle (SDLC)
  - Conceptual Definition
  - Functional Requirements Determination
  - Protection Specifications Development
  - Design Review
  - Code Review or Walk-Through
  - System Test Review
  - Certification & Accreditation
  - Maintenance
    - Change & Configuration Management

System Development Controls

- Security Control Architecture
  - Separation of Privilege
  - Accountability
  - Process Isolation
  - Hardware Segmentation
  - Reference Monitor
  - System High
  - Security Kernel

System Development Controls

- **Security Control Architecture (cont.)**
  - Layering
  - Data Abstraction
  - Data Hiding

System Development Controls

- Modes of Operation
  - Supervisor
  - User
- Integrity Levels
  - Network
  - Operating System
  - Database
  - File

Malicious Code

- Viruses
- Myths/Hoaxes
- Malicious applets (Java & ActiveX)
- Logic Bombs
  - Trap Doors
- Hidden code
  - Alteration of authorized code
  - Trojan Horses
- Spoofing

Methods of Attacks

- **Denial of Service** (DoS/DDoS)
  - Flooding
- **Brute force or exhaustive**
- **Dictionary attacks**
- **Spam**
- **Social Engineering**
- **Maintenance hooks**
- **Sniffing & Eavesdropping**
- **Traffic analysis & Inference**

Attackers

- Hackers & Crackers
- Script kiddies
- Phreakers
- Bot herders
- Virus Writers
- Black hat & White hat

Application Security

Questions