Operations Security

Ed Crowley, CISSP
'05

1

Topics

- Scope
- Function
- Controls and Control Categories
- Assurance
- Covert Channels
- Trusted Facility Management
- Concepts
- Configuration/Change Management
- Record retention
- Due Care and due diligence
- Operational Controls
- Monitoring and Auditing
- Threats and vulnerabilities

2

Operations Security Scope

- Involves secure computer facility controls as well as hardware, data media, and operator controls. Includes:
  - Controls and protections
  - Monitoring and Auditing
  - Threats and vulnerabilities

3

Operations Security Function

- Based upon operational threats and vulnerabilities
  - Supplies countermeasures.
- Controls can be:
  - Preventive
  - Detective
  - Corrective
  - Recovery
- Each control may have administrative, physical, or technical aspects.

4

Goals of Operational Controls

- Preventative
  - Lower amount and impact of errors
  - Prevent intruder access
- Detective
  - Detect error after occurrence.
- Corrective
  - Mitigate loss.

5

Additional Control Categories

- Deterrent
- Application
- Transaction
- Input, Processing, and Output
- Change
- Test

6

Orange Book on Controls

- Multiple defined secure computer operation assurance levels.
- Assurance is a level of confidence that ensures:
  - A Trusted Computer Base's (TCB) security policy has been correctly implemented
  - The system's security features have been accurately implemented

7

Orange Book Assurance

- Operational Assurance
  - Basic system features and architecture
- Lifecycle Assurance
  - Controls and standards necessary for building and maintaining a system

8

Operational Assurance Scope

- System architecture
- System integrity
- Covert channel analysis
- Trusted facility management
- Trusted recovery

9

Life Cycle Assurance

- Ensures that a TCB is designed, developed, and maintained with a process that enforces protections at each system life cycle stage. Includes:
  - Security testing
  - Design specification and testing
  - Configuration management
  - Trusted distribution

10

Covert Channel Analysis

- Covert channel
  - An information path not normally used for communication.
  - Likely, an unintentional channel.
- Can be considered a secret way to convey information.

11

Two Covert Channel Types

- Covert storage channels
  - Convey information by changing a system's stored data.
- Covert timing channels
  - Convey information by altering the performance of or modifying a system resource's timing in a measurable manner.

12

Orange Book on Covert Channels

- B2
  - Protects against convert storage channels.
- B3 and A1
  - Must protect against both:
    - Covert storage channels
    - Covert timing channels.

13

Trusted Facility Management

- Specific individual administrates a system's security related functions.
- Related to the concept of least privilege.
- B2 level
  - Supports separate operator and system administrator roles.
- B3 and A1
  - System security administrator's functions clearly identified.

14

Separation of Duties

- Assigns parts of tasks to different personnel.
  - Prevents any single person from compromising the system.
- Related to Least Privilege
  - System users should have the lowest level of rights and privileges necessary to perform their work.
  - Rights should be assigned for the shortest possible time.

15

Rotation of Duties

- Process limiting the time an operator is assigned to perform a specific security related task before being moved to a different task with a different security classification.

16

Trusted Recovery

- Ensures that a system crash or other system failure does not breach security.
- Failure preparation
  - Regular critical file back up.
- System recovery options
  - Rebooting system into a single user mode
  - Recovering all file systems that were active
  - Restoring any missing or damaged files and databases
  - Checking security critical files, such as the system password file.

17

Configuration/ Change Management

- Planful, documented, system change process.
  - Tracking
  - Change approval.
- Goal:
  - Ensure that system changes do not unintentionally diminish security.
- B2, B3, and A1, Requirement
- All systems, recommended

18

Administrative Controls

- Designed to reduce the threat and/or impact of computer security violations.
- Personnel security
  - Employment Screening
  - Background checks
  - Mandatory vacations

19

Concepts

- Separation of Duties and Responsibilities
  - "to ensure separation of duties, each user must be permitted to use only certain sets of programs (transactions)". *Clark and Wilson*
- Least Privilege
  - Access Change
  - Read/Write
  - Read Only
- Need to know
- Record retention and documentation

20

Operations Job Titles

- Computer Operator
- Operations Analyst
- Job Control Analyst
- Production Scheduler
- Production Control Analyst
- Tape Librarian

21

Record Retention

- Management or regulatory stipulation that may deal with legal, audit, or tax compliance requirements, including:
  - How long do transactions and other types of records need to be retained?

22

Data Remanence

- Without appropriate data removal procedures, sensitive information may be inadvertently disclosed.
  - Possibility if the storage media is released into an uncontrolled environment.
- Methods employed to safeguard against disclosure of sensitive information:
  - Degaussing
  - Overwriting
  - Data encryption
  - Media destruction.

23

Due Care and Due Diligence

- Requires an organization to engage in good (relative to the organization's industry) business practices.
- Documentation
  - Security plans
  - Contingency plans
  - Risk analysis
  - Security policies and procedures.

24

Operational Controls

- Day to day procedures that protect computer operations. Such as:
  - Resource protection
  - Hardware and Software controls
  - Privileged entity controls
  - Media controls
  - Physical access controls

25

Resource Protection

- Protect an organization's computing resources and assets from loss or compromise.

26

Hardware Control Issues

- Hardware Maintenance
  - Requires physical or logical system access.
- Maintenance accounts
- Diagnostic Port Control
- Hardware Physical Control

27

Software Control Issues

- Antivirus management
- Software testing
- Software Utilities
- Safe Software Storage
- Backup controls

28

Media Resource Protection

- Two areas:
  - Media security controls
  - Media viability controls
- Media Security Controls
  - Logging
  - Access Control
  - Proper Disposal

29

Media Viability Controls

- Protected by physical controls.
- Effective system recovery requires proper media marking and labeling.
- Proper handling and storage

30

Monitoring and Auditing

- Primary monitoring goals:
  - Problem:
    - Identification
    - Resolution
- Monitoring includes mechanisms, tools, and techniques which permit identification of security events that could impact computer operation.

31

Monitoring Techniques

- Intrusion detection
- Penetration testing
- Violation processing using clipping levels
  - Management by exception

32

Penetration Testing (White Hat)

- Attempts system access utilizing same techniques as an external intruder.
- Techniques can include:
  - Scanning and probing
  - Demon dialing
  - Sniffing
  - Dumpster Diving
  - Social Engineering

33

Violation Analysis

- Violation tracking, processing,and analysis
- For violation tracking to be effective, first clipping levels must be established.
  - A clipping level is a user activity baseline representing routine operations.

34

Auditing

- Monitoring is the foundation of operational security controls.
- Internal and External
  - Internal auditors usually have a broad mandate.
  - External auditors perform an independent audit of an organization's financial statements.

35

Audit Trails

- An audit (or transaction) trail enables a security practitioner to trace a transaction's history.
- Problem Management
  - Way to control the process of problem isolation and problem resolution.

36

Threats and Vulnerabilities

- Threat
  - Any event that, if realized, can cause damage to a system.
    - Potential loss of confidentiality, availability, or integrity.
- Vulnerability
  - A system weakness that can be exploited by a threat.

37

Types of Threats

- Accidental Loss
  - Incurred unintentionally, may be due to:
    - Lack of:
      - Operator training
      - Operator proficiency
    - Application malfunction.
- Inappropriate Activities
  - Behavior that while not at the criminal level, may be grounds for a job action or dismissal

38

Illegal Computer Operations/ Intentional Attacks

- Eavesdropping
- Fraud
- Theft
- Sabotage
- External Attack

39

Trend/Traffic Analysis

- Analysis of data characteristics (message length, message frequency, etc) and transmission patterns (rather than any knowledge of the actual information transmitted) to infer useful information.
  - For example, volume of Pentagon pizza deliveries increased immediately prior to the last invasion of Iraq.

40

IPL Vulnerabilities

- Initial program load (IPL) presents very specific system vulnerabilities whether the system is a centralized mainframe type or a distributed LAN type.
- Operator can put machine into single user mode (without security protections.).
- Note *IPL typically refers to mainframe operations*.

41

Questions?

42