

# *Information System Security (2)*

*Emergency Communications Group, Communications Research Laboratory, Japan*

独立行政法人 通信総合研究所 情報通信部門 非常時通信グループ

*Hiroyuki Ohno, Ph.D.*

大野 浩之 ([hohno@ohnolab.org](mailto:hohno@ohnolab.org))

# Information System Security (2)

# Today's lecture.

- Learn and understand more about ten important areas for improving information system security.

# Ten Important Areas on ISS

- 1. Security Management Practices
- 2. Access Control
- 3. Security Models and Architecture
- 4. Physical Security
- 5. Telecommunications and Networking Security

# Ten Important Areas on ISS

- 6. Cryptography
- 7. Business Continuity Planning
- 8. Law, Investigation, and Ethics
- 9. Application and System Development
- 10. Operations Security

# 1. Security Management Practices

## Topics:

- What's Security Management ?
- Fundamental Principles of Security
- Risk Management
- Policies, Standards, Baselines, Guidelines, and Procedures
- Type of Policies

# 1. Security Management Practices

What's Security Management ?

- Security management includes:
  - Risk management
  - Information Security policies
  - Policies, Procedures, Standards, guidelines, baselines
  - Information Classification
  - Security Organization
  - Security Education

# 1. Security Management Practices

## Fundamental Principles of Security

### □ Three Main Security Principles

- Availability
- Integrity
- Confidentiality

# 1. Security Management Practices

Policies, Standards, Baselines, Guidelines, and Procedures

- Security Policy
- Mandatory Standards
- Recommended Guidelines
- Detailed Procedures

# 1. Security Management Practices

## Security Roles Within an Organization

- Senior manager
- Security professional
- Data owner
- Data custodian
- User
- Auditor

# 1. Security Management Practices

## Risk management

- Physical damage
- Human error
- Equipment malfunction
- Inside and outside attacks
- Misuse of data
- Loss of data
- Application error

## 2. Access Control

Topics:

- Three Main Security Principles(again)
- Identification, Authentication, Authorization, and Accountability
- Biometrics and Password Approach
- Access Control Techniques
- Access Control Monitoring
- Threats to Access Control

## 2. Access Control

### Biometrics

□ Biometrics verifies an individual's identity by a unique personal attribute

- Fingerprint
- Palm Scan
- Hand Geometry
- Retina Scan
- Iris Scan
- Signature Dynamics
- Keyboard Dynamics
- Voice Print
- Facial Scan
- Hand Topology

## 2. Access Control

### Password

- Traditional Passwords
- Cognitive Password
- One-time Password
- Token Device
- Cryptographic Keys
- Passphrase

## 2. Access Control

### Access Control Techniques

- Rule-based
- Restricted interfaces
- Access control matrix
- Capability table
- ACL (Access Control List)
- Content-based access

## 2. Access Control

### Access Control Layers

- Administrative
  - Policy and procedures
  - Personnel controls
  - Supervisory structure
  - Security awareness training
  - Testing
- Physical Controls
  - Network segregation
  - Perimeter security

## 2. Access Control

### Access Control Layers

- **Technical Controls**
  - System access
  - Network architecture
  - Network access
  - Encryption and protocols
  - Auditing

## 3. Security Models and Architecture

### Topics:

- Computer Architecture
- CPU Modes and Protection Rings
- Process Activities
- Security Policy and Security Models
- The Common Criteria
- BS7799 and ISO17799

### 3. Security Models and Architecture

#### The Common Criteria (ISO15408)

- In 1990, ISO identified the need of international standard evaluation criteria to be used globally.
- The benefit of having a worldwide recognized and accepted criteria helps consumers by reducing the complexity of the ratings and eliminating the need to understand the definition and meaning of different ratings within various evaluation schemes.

### 3. Security Models and Architecture

#### BS7799 and ISO17799

- BS7799 is a risk-based method for assessing, evaluating, and managing risks. It takes holistic approach to security instead of just focusing on the technical issues. It is a standard and a framework for developing a security program.

### 3. Security Models and Architecture

10 areas in BS7799 and ISO17799

- Security Policy
- Security Organization
- Assets Classification and Control
- Personnel Security
- Physical and Environmental Security

### 3. Security Models and Architecture

10 areas in BS7799 and ISO17799

- Computer and Network Management
- System Access Control
- System Development and Maintenance
- Business Continuity Planning
- Compliance

## 4. Physical Security

### Topics:

- Physical Security Risks
- Administrative Controls

# 5. Telecom. and Networking Security

## Topics:

- OSI model
- TCP/IP and Many Protocols
- LAN, WAN, and MAN Technologies
- Wired and Wireless Technologies
- Devices and Equipment
- Remote Access

## 6. Cryptography

Topics:

- Methods of Encryption Algorithms
- Strength of the Cryptosystem
- Steganography, Digital Watermarking and Information Hiding

## 7. Business Continuity Planning

### Topics:

- Business Continuity and Disaster Recovery
- Make It Part of the Security Policy and Programs
- Business Continuity Planning Requirement
- Backup Alternatives
- Emergency Response

## 8. Ethics, Law, and Investigation

### Topics:

- Ethics
- Hackers and Crackers
- Well-Known Computers Crimes
- Types of Laws on Computer Crime
- Computer Crime Investigation
- Computer Forensics and Proper Collection of Evidence
- Incident Handling

# 9. Application and System Development

Topics:

- Various Types of Software Controls and Implementation

# 10. Operations Security

## Topics:

- Administrative Management
- Accountability
- Security Operations and Product Evaluation
- Countermeasures to Hacks and Attacks

# 10. Operations Security

## Countermeasures to Hacks and Attacks

### □ Countermeasures to Port Scanning and Network Mapping

- Disable unnecessary ports and services
- Block access at the perimeter network using firewalls, routers, and proxy servers
- Use an IDS to identify this type of activity
- Use TCP Wrappers on vulnerable services that had to be available

# 10. Operations Security

## Countermeasures to Hacks and Attacks

- Countermeasures to Port Scanning and Network Mapping
  - Remove as many banners as possible within operating systems and applications
  - Upgrade or update to more secure operating systems, applications, and protocols.

## FYI:

- This lecture mainly based on the following book:
  - CISSP Certification All-in-One Exam Guide, Second Edition
    - McGraw-Hill
    - ISBN 0-07-222966-7

Copyright (C) 2003 Communications Research Laboratory

Contact: [hohno-sec@ohnolab.org](mailto:hohno-sec@ohnolab.org)

