

# *Information System Security*

*Emergency Communications Group, Communications Research Laboratory(CRL)*

*National Incident Response Team (NIRT), Cabinet Secretariat, Japan*

*Hiroyuki Ohno, Ph.D. ([hohno@ohnolab.org](mailto:hohno@ohnolab.org))*

# Information System Security (ISS)

# Contents of the day

- Introduction
- Cyber Attacks in these days.
- CSIRT, CERT, and ISAC
- Ten Important Areas of Information System Security
- International Collaboration and Partnership

# Introduction

## □ Speaker of the day:

○ Hiroyuki Ohno, Ph.D.

○ Group Leader of the Emergency Communications Group,  
Communications Research Laboratory(CRL)

○ Leader of the National Incident Response Team (NIRT),  
Cabinet Secretariat, Japan

○ Rapporteur of Question 10 / SG17 / ITU-T

# Security problems caused by someone

- Players
  - Student, Cracker/Attacker, Sales rep, Businessman, Ex-employee, Accountant, Stockbroker, Con man, Spy, Terrorist

# Security problems caused by someone

- Student
  - To have fun snooping on people's e-mail
  
- Cracker/Attacker
  - To test out someone's security system, steal data

# Security problems caused by someone

- Sales rep.
  - To claim to represent all of Europe, not just Andorra
  
- Businessman
  - To discover competitor's strategic marketing plan

# Security problems caused by someone

- Ex-employee
  - To get revenge for being fired
  
- Accountant
  - To embezzle money from a company

# Security problems caused by someone

- Stockbroker
  - To deny a promise made to a customer by e-mail
  
- Con man
  - To steal credit card numbers for sale

# Security problems caused by someone

- **Spy**
  - To learn an enemy's military or industrial secrets
  
- **Terrorist**
  - To steal germ warfare secrets

# Cyber Attacks in these days.

- Number of attacks towards "our" information systems are increasing and increasing...
- In these two months (July-Aug/03), we hit:
  - Blaster A/B/C - Worm
  - Welchia (Nachi) - Worm
  - Sobig.F - Virus
- They made huge damage to many information systems all over the world.

## Open question

- What did you do against the attacks ?
- What do you do against the attacks ?
- What will you do against the attacks ?

## Four levels of cyber attacks.

- Script Kiddies
- Cyber Crimes
- Cyber Terrorism
- Cyber Warfare
  
- Where are we now ?

# CSIRT, CERT, and ISAC

- CSIRT
  - Computer Security Incident Response Team
- CERT
  - Computer Emergency Response Team
- ISAC
  - Information Sharing and Analysis Center

# Important CSIRTs and Related

- **CERT/CC**
  - Center of the ISS world
  - <http://www.cert.org/>
  
- **FIRST**
  - Forum for Incident Response Security Teams
  - <http://www.first.org/>

# Important CSIRTs and Related

- AusCERT
  - Australia CERT
  - <http://www.auscert.org/>
  
- JPCERT/CC
  - CERT/CC in Japan
  - <http://www.jpert.or.jp/>

# Important CSIRTs and Related in Japan

- **CSIRT/CERT**
  - JPCERT/CC
  - NIRT (National Incident Response Team, Cabinet Secretariat, Japan)
  - Several CSIRTs in private companies are active now.
  
- **ISAC**
  - Telecom ISAC Japan
  
- **Others**
  - IPA (Information Technology Promotion Agency, Japan)

# 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

# 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.

# Important!

- Discussion on "network security" is a part of "information systems security"(ISS).

# 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

# Ten Important Areas on ISS (1)

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

# Ten Important Areas on ISS (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

# Ten Important Areas on ISS (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

# Ten Important Areas on ISS (4)

- Physical Security
- Topics:
  - Physical Security Risks
  - Administrative Controls

# Ten Important Areas on ISS (5)

- Telecommunications 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

# Ten Important Areas on ISS (6)

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

# Ten Important Areas on ISS (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

# Ten Important Areas on ISS (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

# Ten Important Areas on ISS (9)

- Application and System Development
- Topics:
  - Various Types of Software Controls and Implementation

# Ten Important Areas on ISS (10)

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

# 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.

## BS7799 and ISO17799

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

# 10 areas in BS7799 and ISO17799

- 1. Security Policy
- 2. Security Organization
- 3. Assets Classification and Control
- 4. Personnel Security
- 5. Physical and Environmental Security

# 10 areas in BS7799 and ISO17799

- 6. Computer and Network Management
- 7. System Access Control
- 8. System Development and Maintenance
- 9. Business Continuity Planning
- 10. Compliance

# International Collaboration and Partnership

- ISS is "Think Globally and Act Locally"
- CSIRT must be organized in every countries.
  - It need not to be government CSIRT
- Asia Pacific CSIRT Collaboration and Partnership is very important

# FYI

- URLs
  - Communications Research Laboratory, Japan
    - <http://www.crl.go.jp/>
  - CERT/CC
    - <http://www.cert.org/>
  - FIRST
    - <http://www.first.org/>
  - AusCERT
    - <http://www.auscert.org/>
  - JPCERT/CC
    - <http://www.jpCERT.or.jp/>

Copyright (C) 2003 Communications Research Laboratory

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

