Developed and Presented By Dr. Mehrdad S Sharbaf
CSUDH
Computer Science Department

http://csc.csudh.edu/

The some of the materials are excerpted from Ian Sommerville's Book, and Ross Anderson's Book

INFORMATION SECURITY GOAL

INTRODUCTION TO INFORMATION SECURITY

- What is Information Security?
- Information Security: To make sure that the information risks and controls are in balance
- Information security initiated with Rand Report R-609 (research paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization

INTRODUCTION TO INFORMATION SECURITY

- The protection of information and its critical elements, including systems, software, and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

SECURITY GOALS

- Confidentiality
  - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.

SECURITY GOALS

- Integrity
  - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.

SECURITY GOALS

- Availability
  - Availability means that people who are authorized to use information are not prevented from doing so

COMPONENTS OF INFORMATION SECURITY

- Computer Security(Hardware & Software)
- Data Security
- Network Security
- Physical Security
- Information Security Management
- Policy

NSTISSC

- The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established under National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems", dated 5 July 1990.
- On October 16, 2001, President George W. Bush signed Executive Order 13231, the Critical Infrastructure Protection in the Information Age, re-designating the **National Security Telecommunications and Information Systems Security Committee** (NSTISSC) as the **Committee on National Security Systems** (CNSS).
- The **CNSS** holds discussions of policy issues, sets national policy, directions, operational procedures, and guidance for the information systems operated by the U.S. Government, its contractors or agents that either contain classified information, involve intelligence activities, involve cryptographic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapons system(s), or are critical to the direct fulfillment of military or intelligence missions.

NSTISSC SECURITY MODEL

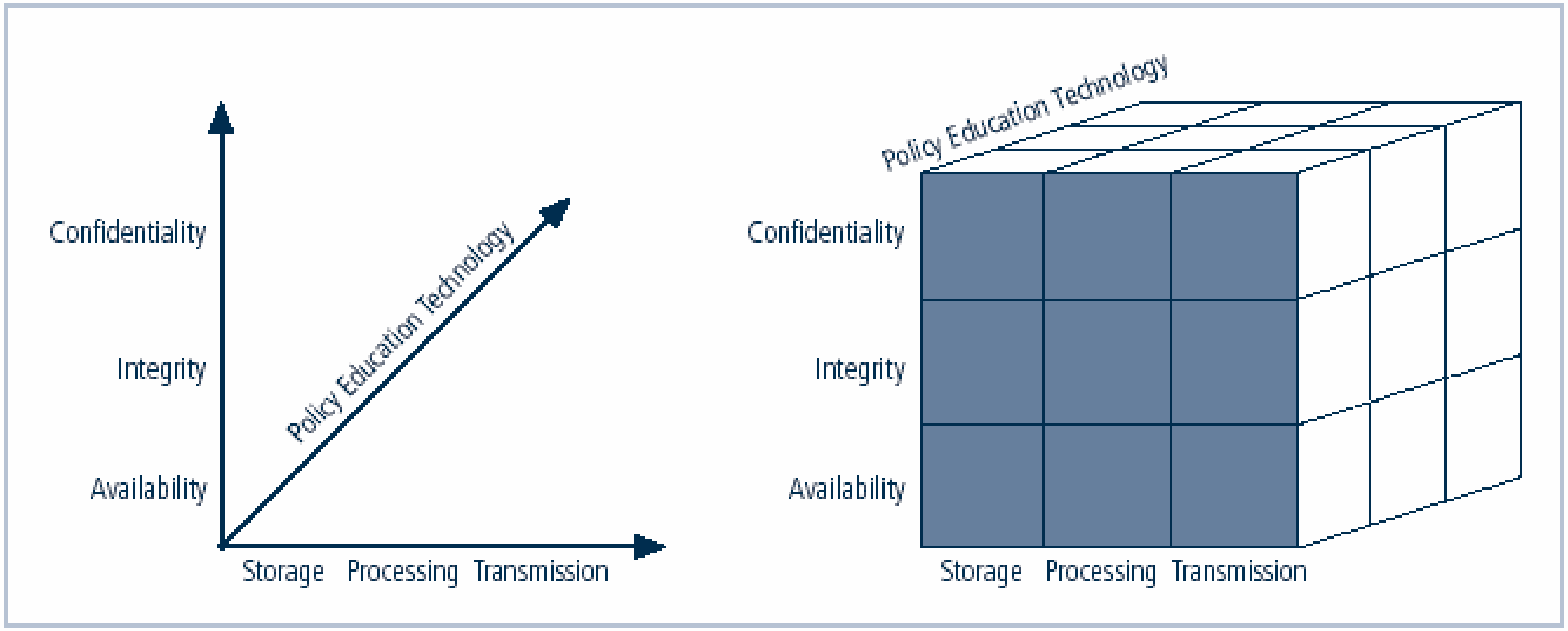

FIGURE 1-4 NSTISSC Security Model

THE THREAT ENVIRONMENT/COMPROMISES

- **The Threat Environment**
  - The threat environment consists of the types of attackers and attacks that companies face
- **Compromises**
  - Successful attacks
  - Also called incidents
  - Also called breaches

THE THREAT ENVIRONMENT/COMPROMISES

- **Employee Sabotage**
  - Destruction of hardware, software, or data
  - Plant time bomb or logic bomb on computer
- **Employee Hacking**
  - Hacking is intentionally accessing a computer resource without authorization or in excess of authorization
  - Authorization is the key

THE THREAT ENVIRONMENT/COMPROMISES

- **Malware**
  - A generic name for any “evil software”
- **Viruses**
  - Programs that attach themselves to legitimate programs on the victim’s machine
  - Spread today primarily by e-mail
  - Also by instant messaging, file transfers, etc.

THE THREAT ENVIRONMENT/COMPROMISES

- **Worms**
  - Full programs that do not attach themselves to other programs
  - Like viruses, can spread by e-mail, instant messaging, and file transfers

THE THREAT ENVIRONMENT/COMPROMISES

- **Trojan Horses**
  - A program that replaces an existing system file, taking its name
- **Trojan Horses**
  - Remote Access Trojans (RATs)
    - Remotely control the victim’s PC
  - Downloaders
    - Small Trojan horses that download larger Trojan horses after the downloader is installed

THE THREAT ENVIRONMENT/COMPROMISES

- **Trojan Horses**
  - **Spyware**
    - Programs that gather information about you and make it available to the adversary
    - Cookies that store too much sensitive personal information
    - Keystroke loggers
    - Password-stealing spyware
    - Data mining spyware

THE THREAT ENVIRONMENT/COMPROMISES

- **Trojan Horses**
  - **Rootkits**
    - Take control of the super user account (root, administrator, etc.)
    - Can hide themselves from file system detection
    - Can hide malware from detection
    - Extremely difficult to detect (ordinary antivirus programs find few rootkits)

THE THREAT ENVIRONMENT/COMPROMISES

- **Mobile Code**
  - Executable code on a webpage
  - Code is executed automatically when the webpage is downloaded
  - Javascript, Microsoft Active-X controls, etc.
  - Can do damage if computer has vulnerability

THE THREAT ENVIRONMENT/COMPROMISES

- **Social Engineering in Malware**
  - Social engineering is attempting to trick users into doing something that goes against security policies
  - Several types of malware use social engineering
    - Spam
    - Phishing
    - Hoaxes

THE THREAT ENVIRONMENT/COMPROMISES

- **Professional Hackers**
  - Motivated by thrill, validation of skills, sense of power
  - Motivated to increase reputation among other hackers
  - Often do damage as a byproduct
  - Often engage in petty crime

COUNTERMEASURES

- **Countermeasures**
  - Tools used to thwart attacks
  - Also called safeguards, protections, and controls
  - Types of countermeasures
    - Preventative
    - Detective
    - Policy toward Correction

SECURITY TOOLS

- Most of security tools are listed in my blog
- http://msharbaf.wordpress.com
- Wireshark (known as Ethereal until a trademark dispute in Summer 2006) is a fantastic open source multi-platform network protocol analyzer. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, delving down into just the level of packet detail you need.
- http://www.wireshark.org/

SECURITY TOOLS

- Nmap (“Network Mapper”) is a free and open source (license) utility for network exploration or security auditing.
- http://www.nmap.org
- Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide.
- http://www.snort.org

SECURITY TOOLS

- Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic.
- http://www.kismetwireless.net
- Vistumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a, 802.11g, 802.11n,and 802.11ac WLAN standards.
- Vistumbler - Open Source WiFi scanner and channel scanner for windows

SECURITY POLICY

- One of the most important assets any organization possesses is its data
- Security policy is a very important component of information security
- Security policy
  - Series of documents that clearly defines the defense mechanisms an organization will employ
    - To keep information secure
  - Outlines how the organization will respond to attacks
    - Duties and responsibilities of its employees

SECURITY POLICY

- Proper development of a security policy
  - Accomplished through the security policy cycle
    - Never-ending process of identifying what needs to be protected, determining how to protect it, and evaluating the adequacy of the protection
    - Risk Identification
    - Security Policy development
    - Compliance monitoring and evaluation

Risk Identification

- Seeks to determine the risks that an organization faces against its information assets
  - Information then becomes the basis of developing the security policy itself
- Steps
  - Asset identification
  - Threat identification
  - Vulnerability appraisal
  - Risk assessment

Security Policy Development

- Policy creation
  - Consider a standard set of principles
- Policy must be implementable and enforceable
- Policy must be concise and easy to understand
- Policy must be balance protection with productivity

Compliance monitoring and evaluation

- Necessary to ensure that polices are consistently implemented and followed properly
- Involves the proactive validation that internal controls are in place and functioning as expected

COMPLIANCE MONITORING AND EVALUATION

- Change management
  - Manages the process of implementing changes
- Some of the most valuable analysis occurs when an attack penetrates the security defenses
- Incident response
  - Outlines the actions to be performed when a security breach occurs
  - Most incident responses include the composition of an incident response team (IRT)

COMPLIANCE MONITORING AND EVALUATION

- Code of ethics
  - Encourages members of professional groups to adhere to strict ethical behavior within their profession
  - Codes of ethics for IT professionals
    - Institute of Electrical and Electronics Engineers (IEEE)
    - Association for Computing Machinery (ACM)

NIST-COMPUTER SECURITY RESOURCE CENTER

- **Special Publications (800 Series)**
- Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
- http://csrc.nist.gov/publications/PubsSPs.html

ISO 27000 SERIES

- The ISO 27000 series standard was published in 2005, 2006, and 2009. The standard "established guidelines and general principles for initiating, implementing, maintaining, information security risk management, guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system and controls, and improving information security management within an organization
- http://www.27000.org/

THE NEW PERSPECTIVE IN CYBER SECURITY

- Total Quality Information Security Management(TQISM Model) introduced by **Dr. Mehrdad S Sharbaf**