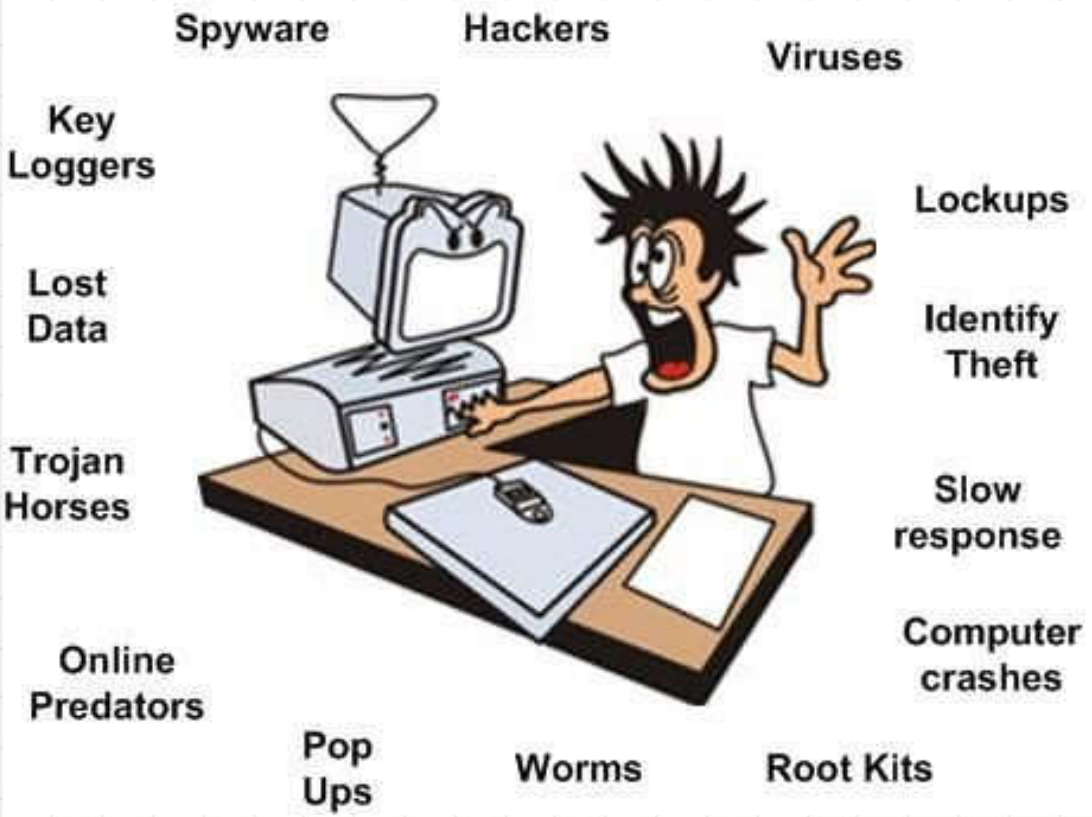
CHƯƠNG 2: CÁC MỐI ĐE DỌA VÀ CÁC LỖ HỔNG TRONG HỆ THỐNG MẠNG MÁY TÍNH

Mã HP: 841119

Khoa CNTT – ĐH Sài Gòn

What is:

– Vulnerability
– Threat
– Attack



Nội dung trình bày

- Vulnerability: A weakness that is inherent in every network and device (routers, switches, servers, and even security devices themselves)
- Threats: The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.
- Attacks: The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices (endpoints).

Nội dung trình bày

Security Threats:

- Sources of Security Threats
- Security Threat Motives
- Security Threat Management
- Security Threat Awareness

Nội dung trình bày

Security Threats:

- **Sources of Security Threats**
- Security Threat Motives
- Security Threat Management
- Security Threat Awareness

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - Rapid Growth of Cyberspace
  - The Growth of the Hacker Community
  - Vulnerability in Operating System Protocol
  - The Invisible Security Threat – The Insider Effect
  - Social Engineering
  - Physical Theft

Nội dung trình bày

- **Sources of Security Threats**
  - **Weaknesses in Network Infrastructure and Communication Protocols**
  - Rapid Growth of Cyberspace
  - The Growth of the Hacker Community
  - Vulnerability in Operating System Protocol
  - The Invisible Security Threat – The Insider Effect
  - Social Engineering
  - Physical Theft

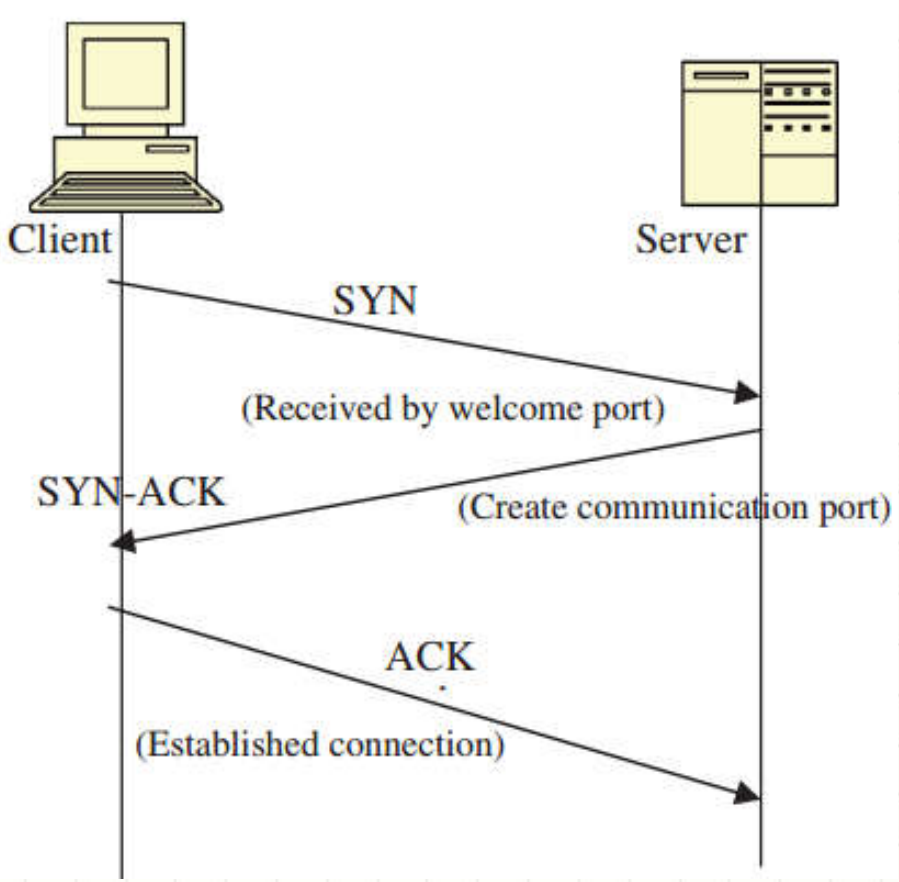
Sources of Security Threats

Weaknesses in Network Infrastructure and Communication Protocols: for ex 3 way handshake

- Two main communication protocols: TCP & UDP, use port numbers to identify higher layer services.
- Initial communication between a client and a server: the client addresses the server via a port number in a process called a **three-way handshake**

Sources of Security Threats

- The threeway handshake establishes a TCP virtual connection between server-client.
- half-opensocket problem



Sources of Security Threats

- Port scan.
- Initial sequence number attack

=> New vulnerabilities are being discovered almost everyday

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - **Rapid Growth of Cyberspace**
  - The Growth of the Hacker Community
  - Vulnerability in Operating System Protocol
  - The Invisible Security Threat – The Insider Effect
  - Social Engineering
  - Physical Theft

Sources of Security Threats

Rapid Growth of Cyberspace

- Security problem in numbers:
  - 1985: about 2000 computers – tens of thousands users
  - 2001: 109 million hosts.
  - current annual growth rate of 51% over the past 2 years

=> more services, more responsibilities.

Sources of Security Threats

Rapid Growth of Cyberspace

- Statistics from Symantec (2001):
  - Internet attack activity is currently growing by about 64% / year.
  - the first 6 months of 2002, companies connected to the Internet were attacked 32 times / week.
  - 400 and 500 new viruses every month and about 250 vulnerabilities in computer programs

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - Rapid Growth of Cyberspace
  - **The Growth of the Hacker Community**
  - Vulnerability in Operating System Protocol
  - The Invisible Security Threat – The Insider Effect
  - Social Engineering
  - Physical Theft

Sources of Security Threats

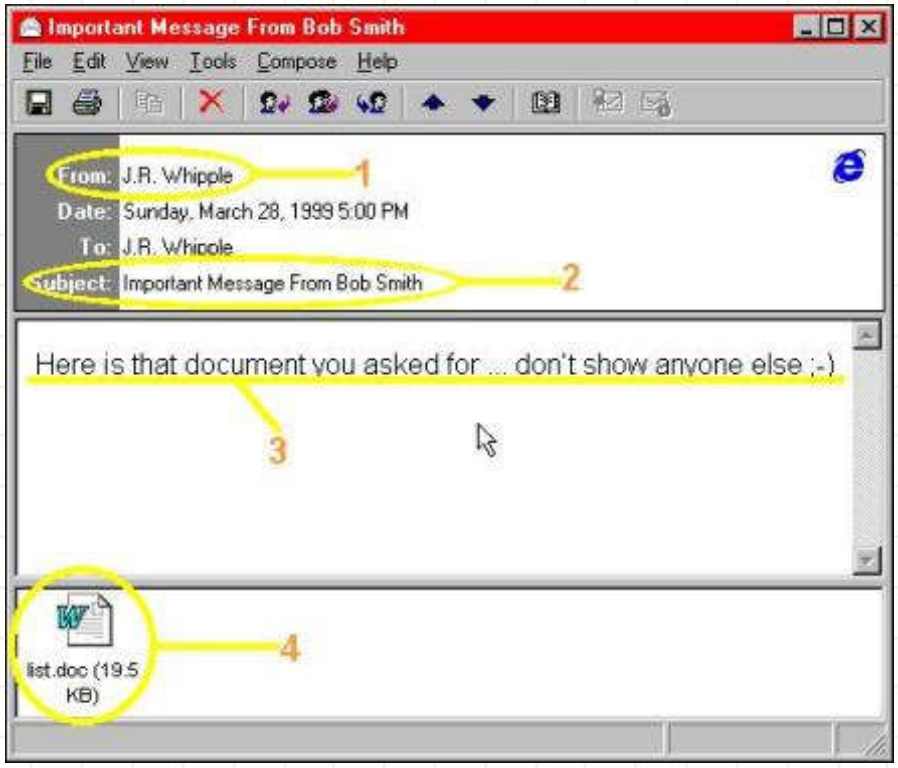
The Growth of the Hacker Community

- The Internet Worm (1988): Robert T. Morris – Morris Worm

Sources of Security Threats

The Growth of the Hacker Community

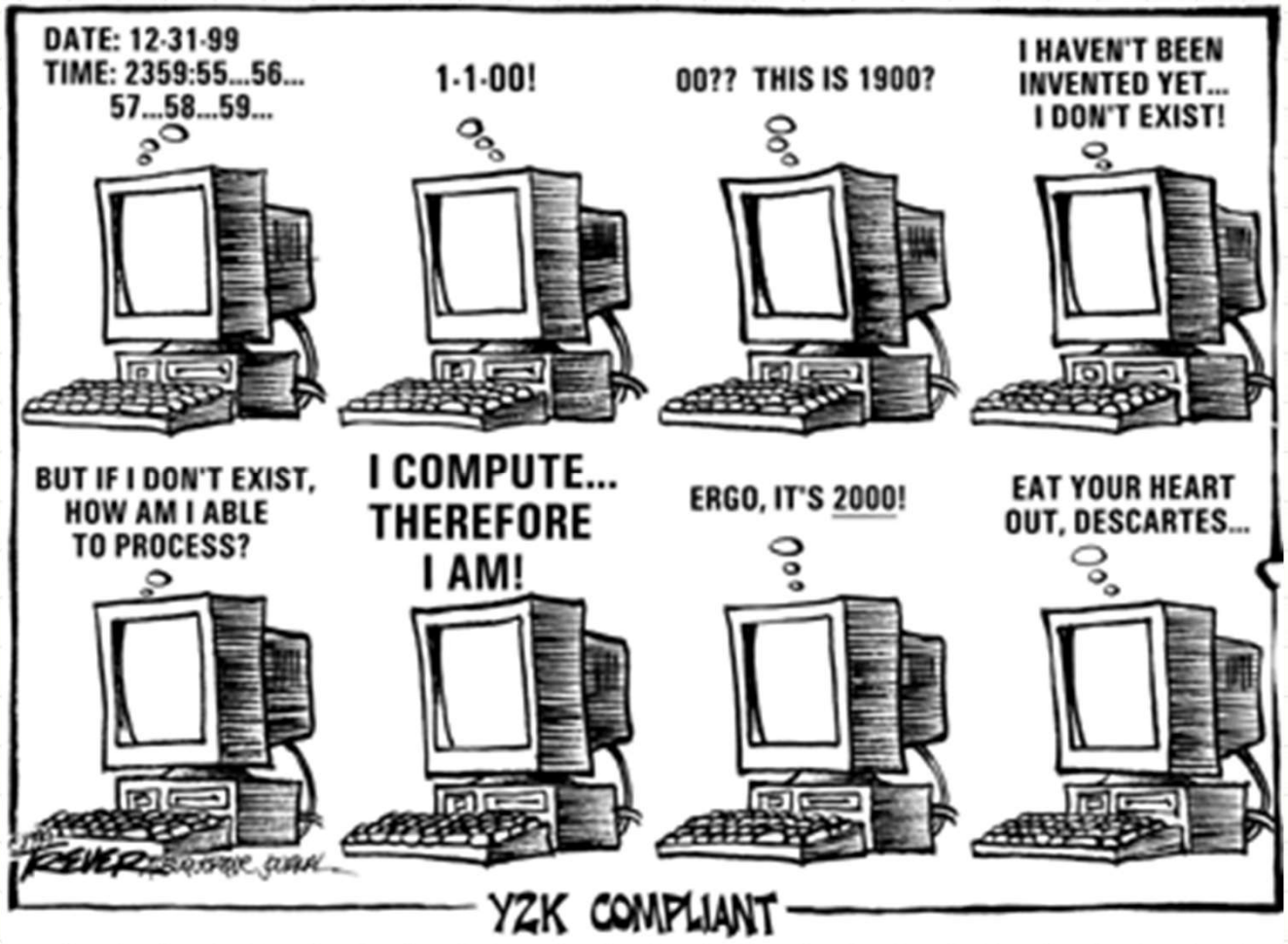
- Michelangelo Virus (1991): March – 06
- Melissa Virus (1999): David L. Smith



Sources of Security Threats

The Growth of the Hacker Community

- The Y2K bug



Sources of Security Threats

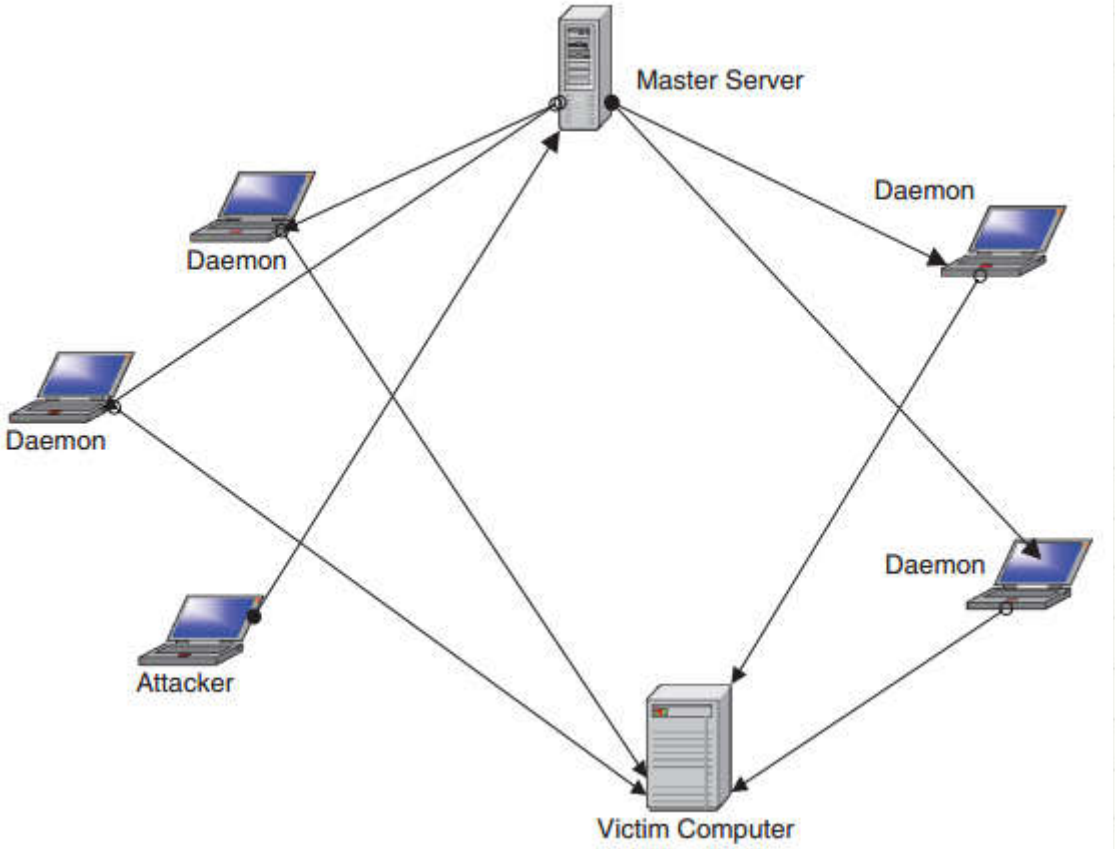
The Growth of the Hacker Community

- Distributed Denial-of-Service (DDoS):
  - Feb 7 – 2000, “mafia boy” (Michael Demon Calce) knocked out Yahoo servers for a period of about 3 hours (2 days later: eBay, Amazon, Buy.com, ZDNet, CNN and MSN)

Sources of Security Threats

The Growth of the Hacker Community

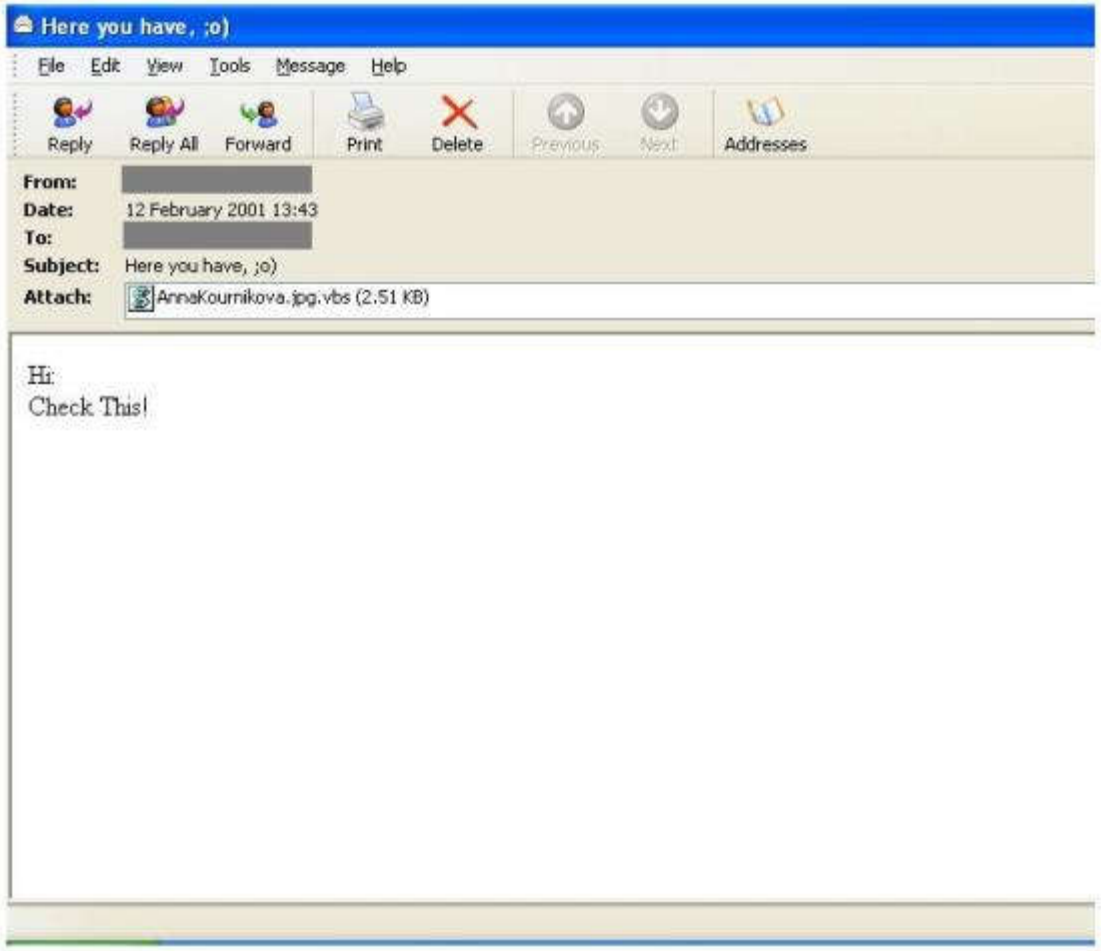
- Distributed Denial-of-Service (DDoS):



Sources of Security Threats

The Growth of the Hacker Community

- Anna Kournikova virus: Feb 2001



Sources of Security Threats

The Growth of the Hacker Community

- Hackers View 8 Million Visa/MasterCard, Discover, and American Express Accounts: Feb - 2003

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - Rapid Growth of Cyberspace
  - The Growth of the Hacker Community
  - **Vulnerability in Operating System Protocol**
  - The Invisible Security Threat – The Insider Effect
  - Social Engineering
  - Physical Theft

Sources of Security Threats

Vulnerability in Operating System Protocol

- The greatest security threat to global computer systems is the area of software errors, especially network OS errors
- A vulnerable OS can allow an attacker to take over a computer system and do anything that any authorized super user can do, such as changing files, installing and running software, or reformatting the hard drive

Sources of Security Threats

Vulnerability in Operating System Protocol

- Every OS comes with some security vulnerabilities -> Hacker look for OS-identifying information like file extensions for exploits

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - Rapid Growth of Cyberspace
  - The Growth of the Hacker Community
  - Vulnerability in Operating System Protocol
  - **The Invisible Security Threat – The Insider Effect**
  - Social Engineering
  - Physical Theft

Sources of Security Threats

The Invisible Security Threat – The Insider Effect

- The greatest threat to security in any enterprise is “the guy down the hall”
- In 1997, Ernst & Young interviewed 4,226 IT managers and professionals about the security of their networks:
  - 75 % (managers) belived that authorized users and employees represent a threat to the security of their systems.
  - 43 % reported malicious acts from employees

Sources of Security Threats

The Invisible Security Threat – The Insider Effect

- The Information Security Breaches Survey 2002:
  - in small companies, 32 percent of the worst incidents were caused by insiders
  - In large companies, 48 percent

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - Rapid Growth of Cyberspace
  - The Growth of the Hacker Community
  - Vulnerability in Operating System Protocol
  - The Invisible Security Threat – The Insider Effect
  - **Social Engineering**
  - Physical Theft

Sources of Security Threats

Social Engineering

- Social engineering can be carried out using a variety of methods, including physically impersonating an individual known to have access to the system, online, telephone, and even by writing.

Sources of Security Threats

Social Engineering

- “Hackers find the hole in the human firewall“, "What's the biggest hole? It's the illusion of invulnerability” - Kevin Mitnick

Nội dung trình bày

- **Sources of Security Threats**
  - Weaknesses in Network Infrastructure and Communication Protocols
  - Rapid Growth of Cyberspace
  - The Growth of the Hacker Community
  - Vulnerability in Operating System Protocol
  - The Invisible Security Threat – The Insider Effect
  - Social Engineering
  - **Physical Theft**

Sources of Security Threats

Physical Theft

- Thousands of company executive laptops and PDA disappear every year with years of company secrets.

Nội dung trình bày

Security Threats:

- Sources of Security Threats
- **Security Threat Motives**
- Security Threat Management
- Security Threat Awareness

Security Threat Motives

- Terrorism
- Military Espionage
- Economic Espionage
- Targeting the National Information Infrastructure (denial or disruption of computer, cable, satellite, or telecommunications)
- Vendetta/Revenge
- Hate (National Origin, Gender, and Race)
- Notoriety
- Greed
- Ignorance

Nội dung trình bày

Security Threats:

- Sources of Security Threats
- Security Threat Motives
- **Security Threat Management**
- Security Threat Awareness

Security Threat Management

- Security threat management is a technique used to monitor an organization's critical security systems in real-time to review reports from the monitoring sensors such as the intrusion detection systems, firewall, and other scanning sensors.
- Security managers have to do real-time management, response time between a threat and a real attack is down to 20 minutes or less.

Security Threat Management

- Techniques used for security threat management are
  - risk assessment
  - forensic analysis

Nội dung trình bày

Security Threats:

- Sources of Security Threats
- Security Threat Motives
- Security Threat Management
- **Security Threat Awareness**

Security Threat Awareness

- Security threat awareness is meant to bring widespread and massive attention of the population to the security threat.
- Once people come to know of the threat, it is hoped that they will become more careful, more alert, and more responsible in what they do

QUESTIONS?

Tham khảo:

- UNDERSTANDING COMPUTER NETWORK SERCURITY – Chapter 3 (page 63-85)