# Chương 1: tổng quan về an ninh mạng máy tính

Mã HP: 841119

Khoa CNTT – ĐH Sài Gòn

# Nội dung trình bày

- Introduction
- Securing the computer network
- Forms of protection
- Security standards

# Nội dung trình bày

- Introduction
- Securing the computer network
- Forms of protection
- Security standards

# Introduction

- What is security?
  - Security is a continuous process of protecting an object from unauthorized access. It is as state of being or feeling protected from harm. Object can be:
    - a person
    - an organization such as a business
    - property such as a computer system or a file

# Introduction

- What is security?
  - An object can be in a physical state of security or a theoretical state of security.
    - Physical stace: four protection mechanisms: deterrence, prevention, detection, and response.
      - The areas outside the protected system: secured by wire and wall fencing, vibration sensors,…
      - Inside the system: electronic barriers (firewalls and passwords)
    - Theoretical state: based solely on a philosophy, a person is not dangerous as long as that person doesn't have knowledge that could affect the security of the system. Ex: Coca-Cola, KFC.

# Introduction

- Computer security
  - –a branch of Computer Science
  - –focusing on creating a secure environment for the use of computers
  - –complex field of study involving detailed mathematical designs of cryptographic protocols.

# Introduction

- Network security
  - –a branch of Computer Science
  - –computer network security is a broader study of computer security.
  - –*creating an environment in which a computer network, including all its resources, which are many; all the data in it both in storage and in transit; and all its users are secure.*
  - –involving more detailed mathematical designs of cryptographic, communication, transport, and exchange protocols.

# Introduction

- Information security
  - –is even a bigger field of study including computer and computer network security.
  - –variety of disciplines, including computer science, business management, information studies, and engineering
  - –involves the creation of a state in which information and data are secure.

# Nội dung trình bày

- Introduction
- Securing the computer network
- Forms of protection
- Security standards

# Securing the computer network

- Security in the computer network: *creating secure environments for a variety of resources.*
- A resource is secure if that resource is protected from both internal and external unauthorized access.
- Resources are objects: tangible (hardware) or intangible (information, data).

# Securing the computer network

- Protecting hardware resources include:
  - –End user objects that include the user interface hardware components: keyboard, mouse, touch screen, light pens, and others.
  - –Network objects like firewalls, hubs, switches, routers and gateways which are vulnerable to hackers.
  - –Network communication channels to prevent eavesdroppers from intercepting network communications.

# Securing the computer network

- Protecting software:
  - protecting hardware-based software, operating systems, server protocols, browsers, application software, and intellectual property stored on network storage disks and databases.
  - protecting client software such as investment portfolios, financial data, real estate records, images, and other personal files commonly stored on home and business computers

# Nội dung trình bày

- Introduction
- Securing the computer network
- Forms of protection
- Security standards

# Forms of protection

- Access Control
  - Hardware Access Control Systems
  - Software Access Control Systems
- Authentication: username, password, fingerprints, physical location, identity cards
- Confidentiality (bảo mật): encryption algorithms

# Forms of protection

- Integrity (toàn vẹn): encryption and hashing algorithms
- Nonrepudiation (không từ chối): a service that provides proof of the integrity and origin of data, both in a forgery-proof relationship, which can be verified by any third party at any time

# Nội dung

- Introduction
- An ninh mạng
- Forms of protection
- Security standards

# Security standards

- Security Standards Based on Type of Service/Industry
- Security Standards Based on Size/Implementation

# Security standards

- Security Standards Based on Type of Service/Industry:
  - Public-Key Cryptography Standards (PKCS)
  - The Standards For Interoperable Secure MIME (S/MIME)
  - Federal Information Processing Standards (FIPS)
  - Secure Sockets Layer (SSL)
  - Web Services Security Standards

# Security standards

- Security Standards Based on Type of Service/Industry

**Table 2.1** Organizations and their standards

| Organization | Standards |
|---|---|
| IETF | IPSec, XML-Signature XPath Filter2, X.509, Kerberos, S/MIME, |
| ISO | ISO 7498–2:1989 Information processing systems – Open Systems Interconnection, ISO/IEC 979x, ISO/IEC 997, ISO/IEC 1011x, ISO/IEC 11xx, ISO/IEC DTR 13xxx, ISO/IEC DTR 14xxx |
| ITU | X.2xx, X.5xx, X.7xx, X.80x, |
| ECBS | TR-40x |
| ECMA | ECMA-13x, ECMA-20x |
| NIST | X3 Information Processing, X9.xx Financial, X12.xx Electronic Data Exchange |
| IEEE | P1363 Standard Specifications, For Public-Key Cryptography, IEEE 802.xx, IEEE P802.11g, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications |
| RSA | PKCS #x – Public Key Cryptographic Standard |
| W3C | XML Encryption, XML Signature, exXensible Key Management Specification (XKMS) |

# Security standards

- Security Standards Based on Type of Service/Industry

**Table 2.2** Security standards based on services

| Area of Application | Service | Security Standard |
|---|---|---|
| Internet security | Network authentication | Kerberos |
| | Secure TCP/IP communications over the Internet | IPSec |
| | Privacy-enhanced electronic mail | S/MIME, PGP |
| | Public-key cryptography standards | 3-DES, DSA, RSA, MD-5, SHA-1, PKCS |
| | Secure hypertext transfer protocol | S-HTTP |
| | Authentication of directory users | X.509/ISO/IEC 9594–8:2000: |
| | Security protocol for privacy on Internet/transport security | SSL, TLS, SET |
| Digital signature and encryption | Advanced encryption standard/PKI/ digital certificates, XML digital signatures | X509, RSA BSAFE SecurXML-C, DES, AES, DSS/DSA, EESSI, ISO 9xxx, ISO, SHA/ SHS, XML Digital Signatures (XMLD-SIG), XML Encryption (XMLENC), XML Key Management Specifica-tion (XKMS) |
| Login and authentication | Authentication of user's right to use system or network resources. | SAML, Liberty Alliance, FIPS 112 |
| Firewall and system security | Security of local, wide, and metropolitan area networks | Secure Data Exchange (SDE) protocol for IEEE 802, ISO/IEC 10164 |

# Security standards

- Security Standards Based on Size/Implementation:

**Table 2.3** Best security practices for a small organization

| Application area | Security standards |
|---|---|
| Operating systems | Unix, Linux, Windows, etc. |
| Virus protection | Norton |
| Email | PGP, S/MIME |
| Firewalls | |
| Telnet and FTP terminal applications | SSH (secure shell) |

**Table** 2.4 Interest-based security standards

| Area of application | Service | Security standard |
|---|---|---|
| Banking | Security within banking IT systems | ISO 8730, ISO 8732, ISO/TR 17944 |
| Financial | Security of financial services | ANSI X9.x, ANSI X9.xx |

# Questions?

Tham khảo:

- UNDERSTANDING COMPUTER NETWORK SERCURITY – Chapter 2 (page 43-57)