# Information Security
# (정보보안)

2024년 1학기

Myung Kyun Kim

(mkkim@ulsan.ac.kr)

# Course Mechanics

- Needs familiarities with
  - Internet protocol
  - Operating systems
- Course contents
  - Vulnerabilities in Internet
  - Cryptography and security mechanisms
  - Secure Internet protocols
- Textbook
  - Network Security Essentials

# Introduction

- Terminology
- Security goals
- Security attacks
- Security services
- Methods of defense
- A model for network security

# Terminology

- Vulnerability (취약점)
  - a weakness in hardware, software, personnel or procedures, which may be exploited by threat actors in order to achieve their goals
- Threat (위협)
  - any type of action or event, which can damage or steal data, create a disruption or cause a harm
  - (e.g.) malware, phishing, data breaches and even rogue employees

# Terminology

- Risk (위험)
  - the loss probability of a threat successfully exploiting a vulnerability
  - Risk management: A continuous process to identify all potential risks, analyze their impact and evaluate appropriate response

# Terminology

- Security attack
  - Any action that compromises the security of information
  - Attack to information system: system hacking, virus, DoS (Denial of Service) attacks
  - Illegal action on the cyberspace: cyber gambling, cyber stalking, on-line fraud, on-line phishing, invasion of privacy, etc.

# Terminology

- Security mechanism
  - A mechanism that is designed to detect, prevent, or recover from a security attack
- Security service
  - A service that enhances the security of data processing systems and information transfers
  - A security service makes use of one or more security mechanisms
- Assets to protect
  - hardware, software, data, or person

# Security Goals

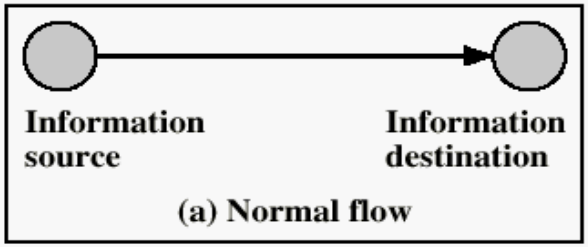
- Confidentiality
  - to assure that information is available and disclosed only to the authorized parties
  - privacy - assures that individuals control what information related to them may be collected and to whom that information may be disclosed
- Integrity
  - data integrity – assures that information can be modified only by authorized parties and only in authorized ways
  - system integrity – assures that a system performs its intended function in an authorized way, free from unauthorized manipulation of the system

# Security Goals

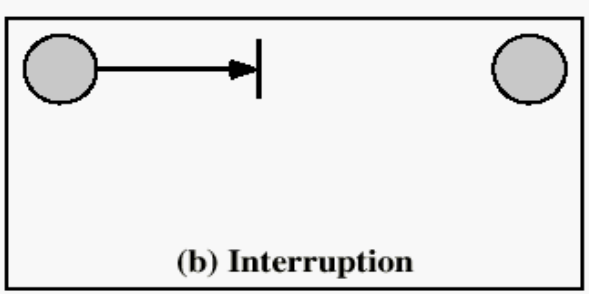
- Availability
  - assures that systems work promptly and service is not denied to authorized users
- Authenticity
  - user authenticity – individuals can assure the validity of the identity of peer
  - message authenticity – receivers can assure the originality of the message

# Security Attacks

- Normal information flow

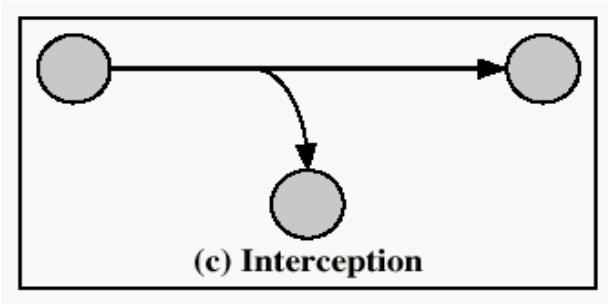



- Interruption: attack on availability

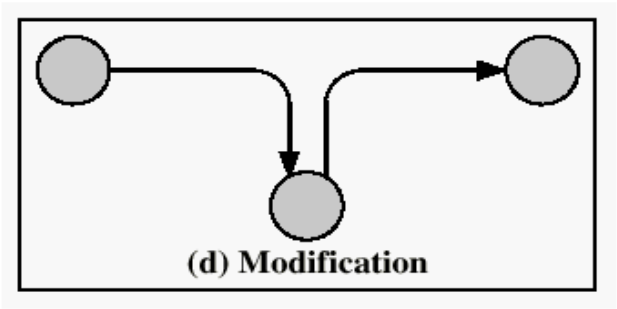


# Security Attacks

- Interception: attack on confidentiality

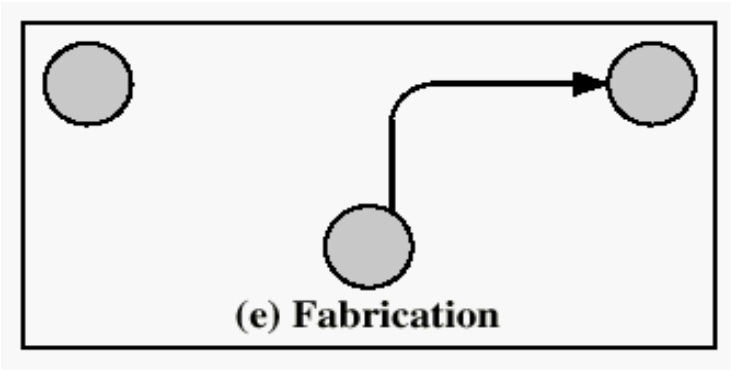



- Modification: attack on integrity



# Security Attacks

- Fabrication: attack on authenticity



# Security Attacks

Passive attacks:

- Interception
  - attacks confidentiality a.k.a., eavesdropping (or sniffing)
  - Encryption is an effective means to protect interception
- Traffic Analysis
  - attacks confidentiality, or anonymity
- Difficult to detect
  - the emphasis is on prevention

# Security Attacks

Active attacks:

- Interruption: attacks availability
  - e.g., DoS (denial-of-service) attacks
- Modification: attacks integrity
  - e.g., man-in-the-middle attacks, masquerading
- Fabrication: attacks authenticity
  - e.g., replay attacks

# Security Services (ITU X.800)

- Confidentiality
  - Ensuring information is accessible only by authorized persons
  - Encryption is a good way to provide confidentiality
  - Anonymity : concealing the origin of the information
- Data integrity
  - ensuring information is altered only by authorized person and in authorized means
  - Digital signature, hash functions

# Security Services (ITU X.800)

- Authentication
  - Peer entity authentication : provide the confidence of the identity of an entity
  - Data origin authentication : provide the assurance of the source of data
  - (e.g.) Password, Kerberos, digital signature
- Authorization (Access control)
  - Allows only entities that have been authenticated to utilize a service
  - Access control list or access control matrix

# Security Services (ITU X.800)

- Non-repudiation
  - preventing the denial of previous commitments or actions
  - Sender repudiation: your signature on a document
  - Receiver repudiation
- Availability
  - ensures that a service or information is available to an (authorized) user upon demand and without delay
  - DoS attacks seek to interrupt a service or make some information unavailable to legitimate users

# Security Services (ITU X.800)

- Certification
  - endorsement of information by a trusted entity
  - (e.g.) public-key certificate
  - needs a certification authority (CA)
- Revocation
  - Retraction of certification or authorization because of compromise, a change in security policy
  - CRL (certification revocation list)

# Security Services (ITU X.800)

- Security services vs. security mechanisms

| SERVICE \ MECHANISM | Encipherment | Digital signature | Access control | Data integrity | Authentication exchange | Traffic padding | Routing control | Notarization |
|---|---|---|---|---|---|---|---|---|
| Peer entity authentication | Y | Y | | | Y | | | |
| Data origin authentication | Y | Y | | | | | | |
| Access control | | | Y | | | | | |
| Confidentiality | Y | | | | | | Y | |
| Traffic flow confidentiality | Y | | | | | Y | Y | |
| Data integrity | Y | Y | | Y | | | | |
| Nonrepudiation | | Y | | Y | | | | Y |
| Availability | | | | Y | Y | | | |

# Security Manager

Security manager should consider

- Prevention
  - taking measures that prevent damage from possible attacks
  - (e.g.) strong passwords, one-time passwords
- Detection
  - measures that allow detection of when an asset has been damaged, altered, or copied
  - E.g., access logging, intrusion detection system

# Security Manager

Security manager should consider

- Recovery
  - restoring systems that were compromised
  - (e.g.) periodic backup
- Assets
  - should know the assets to protect and the value of the assets
  - Assets: hardware, software, data, and person

# Security Manager

Security manager should have to understand

- Operating systems
- Communication network and protocols
- Implementation: secure programming
- Sever system management
- Cryptographic system
- Enterprise business processes
- Security systems
  - Network management systems, network security systems, anti-virus systems, etc.

# Secure or Not?

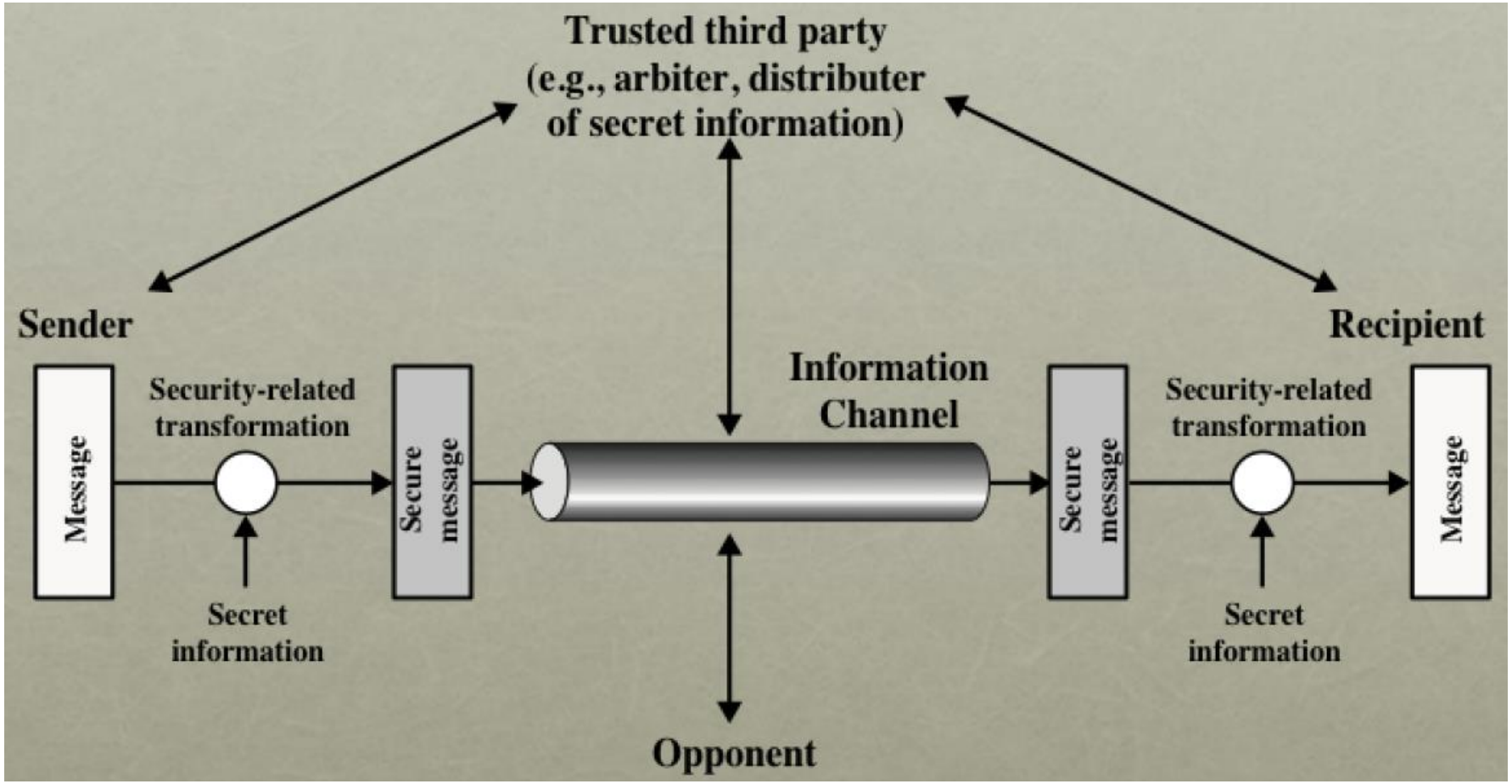
What does it mean for information to be secure?

- The cost of breaking the security exceeds the value of the secured service or information
- The time required to break the security exceeds the useful lifetime of the information

# Steganography

- Security by obscurity
- Practice of hiding messages in other messages
- (e.g.) invisible ink, minute differences between handwritten characters, hiding a message in an audio, image or video

# Network Security Model



# Network Security Model

- Security techniques has two components:
  - A security-related transformation on the information to be sent
  - Some secret information shared by the principals
- Trusted third party:
  - responsible for distributing the secret information to the principals
  - Arbitrate disputes among the principals

# Network Security Model

Designing a security service includes

- Design an algorithm to perform the security-related transformation
- Generate the secret information to be used with the algorithm
- Develop methods for the distribution of the secret information
- Design a protocol used by the two principals that make use of the algorithm and the secret information to achieve the security service

# Network Access Security Model

- Opponents: human, software (viruses, worms)
- Threats
  - Information access threats: intercept or modify data illegally
  - Service threats: inhibits use by legitimate users
- Security mechanisms
  - Gatekeeper function: authentication function, screening logic to detect and reject attacks or viruses
  - Internal security controls: monitoring activity and analyzing security-related logs (IDS)

# ISMS-P 인증

- ISMS-P 인증

정보보호 및 개인정보보호 관리체계 (ISMS-P: Information Security Management System-Personal)는 과학기술정보통신부가 공시한 "정보보호관리체계 인증 등에 관한 고시" 와 방송통신위원회와 행정안전부가 공동 고시한 "개인정보보호관리체계 인증 등에 관한 고시"의 내용을 통합하여 "정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시"로 공동으로 개정하여 고시하였다

# ISMS-P 인증

## ISMS-P 의무 인증 대상

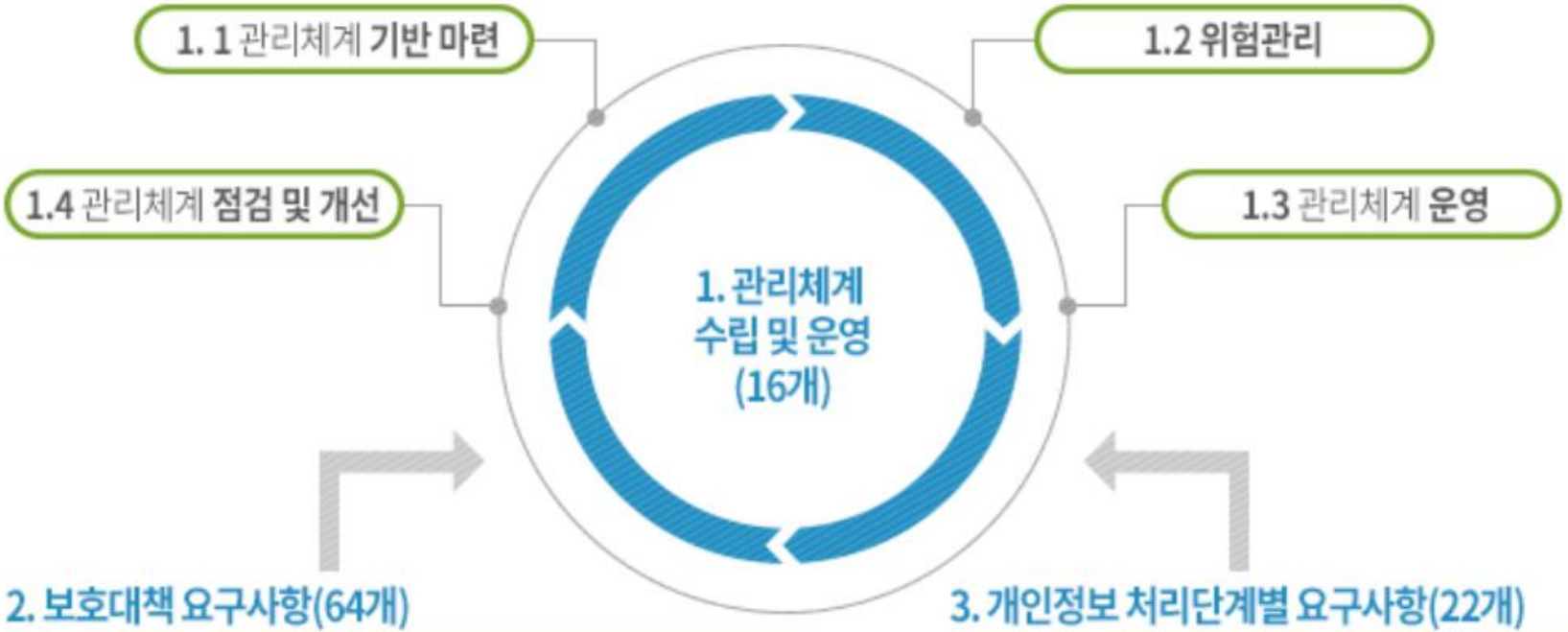
| 대상자 기준 | 정보통신서비스 제공자 |
| --- | --- |
| (ISP) 전기통신사업법의 전기통신사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자 | 인터넷 접속 서비스, 인터넷 전화 서비스 등 |
| (IDC)타인의 정보통신 서비스 제공을 위하여 집적된 정보통신시설을 운영, 관리하는 사업자 | 서버 호스팅, 코로케이션 서비스 등 |
| (정보통신서비스 제공자)정보통신서비스 매출액 100억 또는 이용자 수 100만명 이상인 사업자 | 인터넷 쇼핑몰, 포털, 게임, 예약, Cable 방송국 등 |
| 연간 매출액 및 세입 등이 1500억 이상인 기업 중 상급종합병원, 1만명 이상 재학생이 있는 학교 | - 정보통신제공자가 아니여도 매출액이 1500억 이상인 상급종합병원<br>- 매출액이 1500억 이상이면서 재학생이 1만명 이상인 학교 |

# ISMS-P 인증

## ISMS-P 인증 체계

# ISMS-P 인증

## ISMS-P 인증 기준




**2. 보호대책 요구사항(64개)**

| | |
|---|---|
| 2.1 정책, 조직, 자산관리 | 2.7 암호화 적용 |
| 2.2 인적보안 | 2.8 정보시스템 도입 및 개발보안 |
| 2.3 외부자 보안 | 2.9 시스템 및 서비스 운영관리 |
| 2.4 물리 보안 | 2.10 시스템 및 서비스 보안관리 |
| 2.5 인증 및 권한관리 | 2.11 사고 예방 및 대응 |
| 2.6 접근통제 | 2.12 재해복구 |

**3. 개인정보 처리단계별 요구사항(22개)**

- 3.1 개인정보 수집 시 보호 조치
- 3.2 개인정보 보유 및 이용 시 보호조치
- 3.3 개인정보 제공 시 보호조치
- 3.4 개인정보 파기 시 보호조치
- 3.5 정보주체 권리보호