정보보호 개론

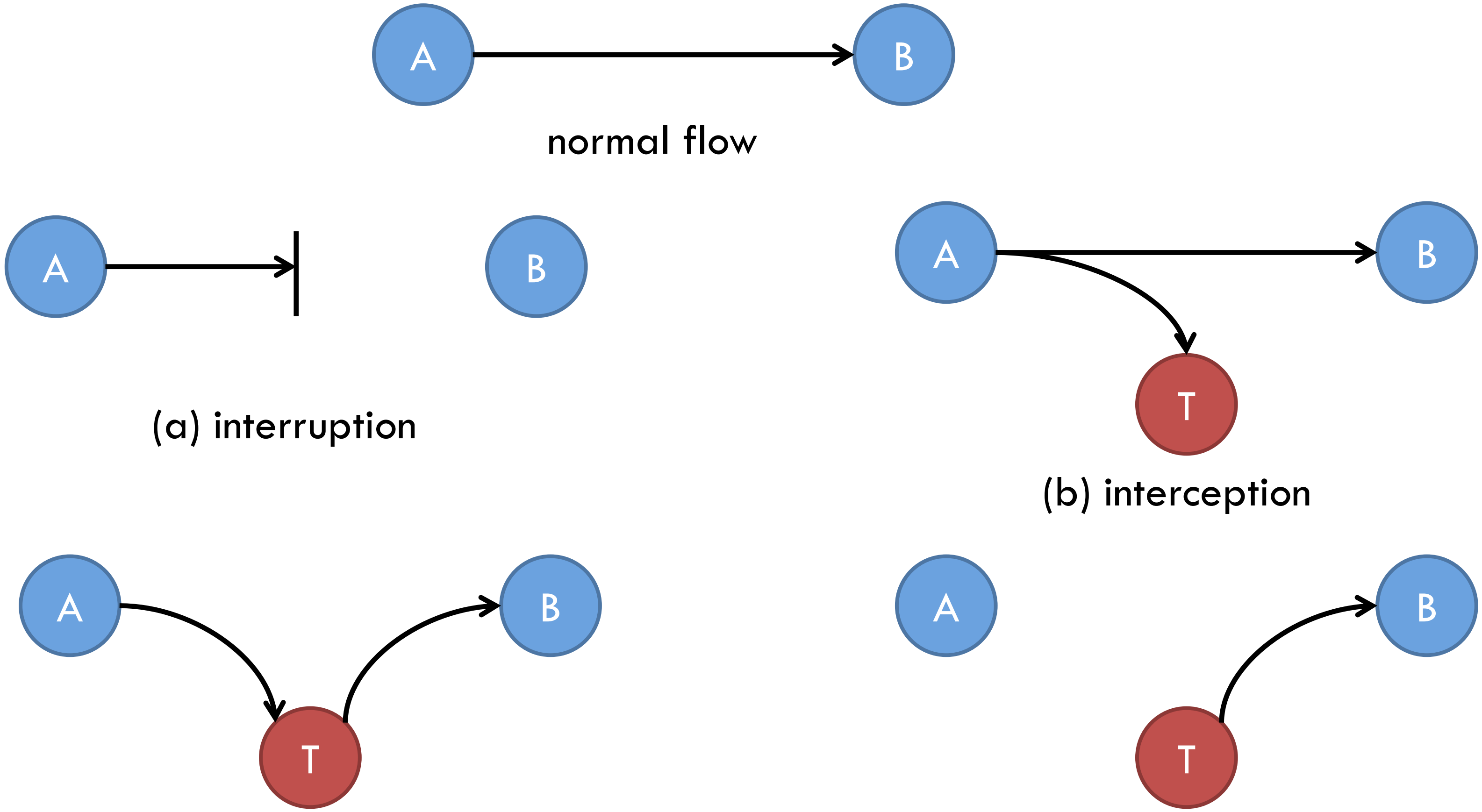
01. Introduction

Characters

- Alice & Bob
  - 선한 역할
- Trudy
  - 악당(공격자)
  - “intruder”

- AOB(Alice’s Online Bank)
  - 은행을 개설한 Alice의 역할(관심)과 이를 이용하는 Bob의 역할(관심) 차이
  - 이 상황을 이용하고자 하는 Trudy의 관심은 ?

Security Threats



normal flow

(a) interruption

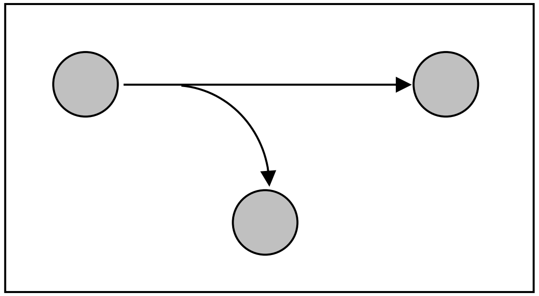
(b) interception

(c) modification

(d) fabrication

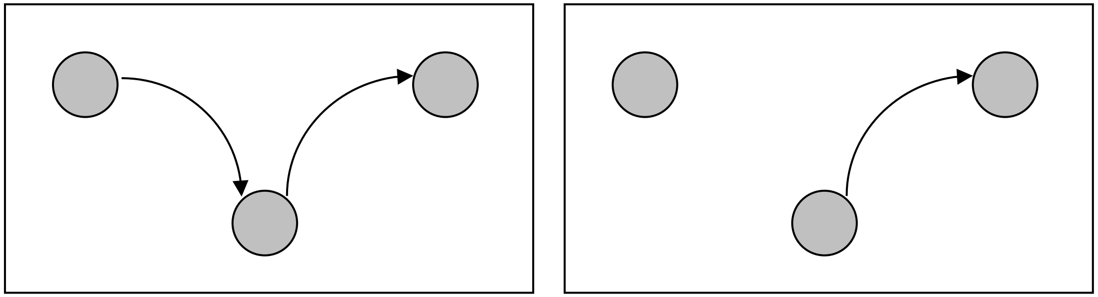
CIA (1)

- CIA: Confidentiality, Integrity, and Availability
- Confidentiality (기밀성)
  - AOB must prevent Trudy from learning Bob's account balance
  - **Confidentiality**: prevent unauthorized reading of information



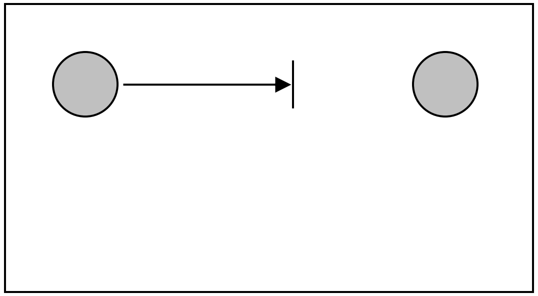
CIA (2)

- Integrity (일관성, 무결성)
  - Trudy must not be able to change Bob's account balance
  - Bob must not be able to improperly change his own account balance
  - **Integrity**: prevent unauthorized writing of information



CIA (3)

- Availability(가용성)
  - AOB’s information must be available when needed
  - Alice must be able to make transaction
    - If not, Bob’ll take his business elsewhere
  - **Availability**: Data is available in a timely manner when needed
  - Availability is a “new” security concern
  - In response to DOS
    (denial of service: 서비스 거부)



Beyond CIA (1)

- CIA are only beginning of the Inf Sec.
- Case 1: when Bob logs on his computer
  - How does Bob's computer know that "Bob" is really Bob and not Trudy?
- Bob's password must be verified
  - This **may** require some clever **cryptography**
- What are security concerns of passwords?
- Are there alternatives to passwords?

Beyond CIA (2)

- Case2: when Bob logs into AOB
  - how does AOB know that “Bob” is really Bob?
- As before, Bob’s password is verified
- Unlike standalone computer case, network security issues arise
- What are network security concerns?
  - **Protocols** are critically important
  - **Cryptography** also important in protocols

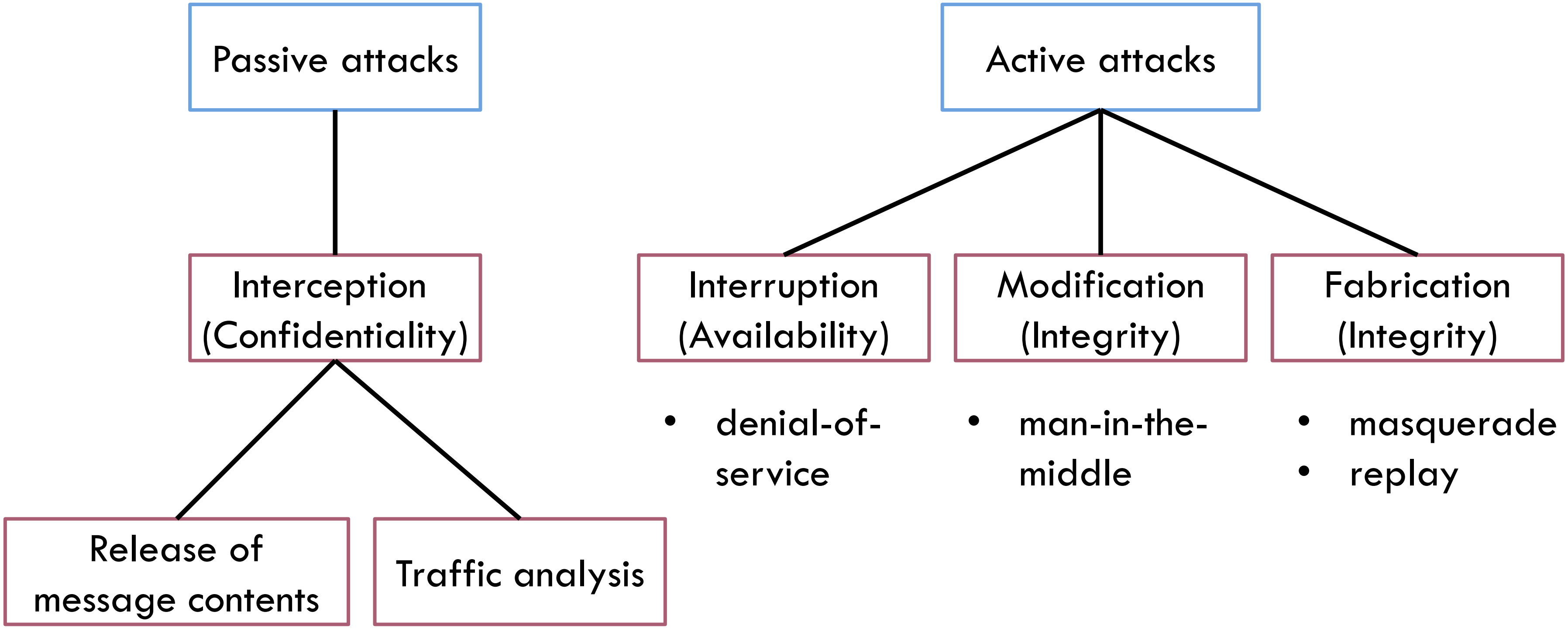
Beyond CIA (3)

- Once Bob is **authenticated** by AOB, then AOB must restrict actions of Bob
  - Bob can’t view Charlie’s account info
  - Bob can’t install new software, etc.
- Enforcing these restrictions is known as **authorization**(인증)
- Access control(접근제어) includes both **authentication** and **authorization**

Beyond CIA (4)

- Non-repudiation
  - Prevents either sender or receiver from denying a transmitted message
  - **Digital signature** (디지털 서명)
  - **Protocols** / **log** system

Active & Passive Network Threats



Passive attacks

Interception (Confidentiality)

Release of message contents

Traffic analysis

Active attacks

Interruption (Availability)

- denial-of-service

Modification (Integrity)

- man-in-the-middle

Fabrication (Integrity)

- masquerade
- replay

Think Like Trudy

- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice and Bob's stupidity
- But, we **cannot act** like Trudy