



Network Security: Introduction

Amir Rezapour
Institute of Information Security,
National Tsing Hua University

Introduction

- Interconnected Computers
 - Fitzroy, 1861
 - Telegraph Network
 - Weather Forecasting
- Multi-user Workstation
 - Unix



Introduction

- Distributed Systems facilitate data sharing and processing
 - Telecommunication networks (internet, wireless network)
 - www, online gaming, distributed database, network file system
 - Parallel Computing
 - cluster computing, cloud computing



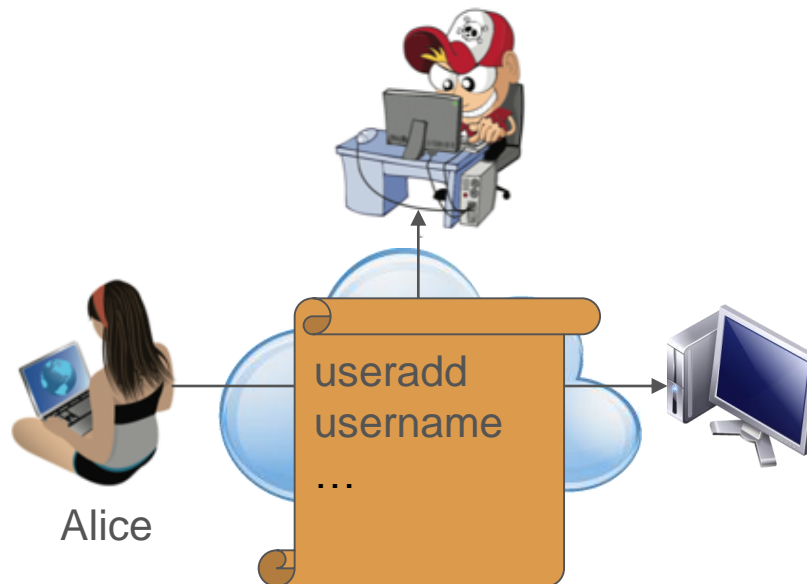
Problems?

- Alice transmits a file (contains sensitive info) to Bob.
 - Eve can monitor the transmission and see the content of the file.



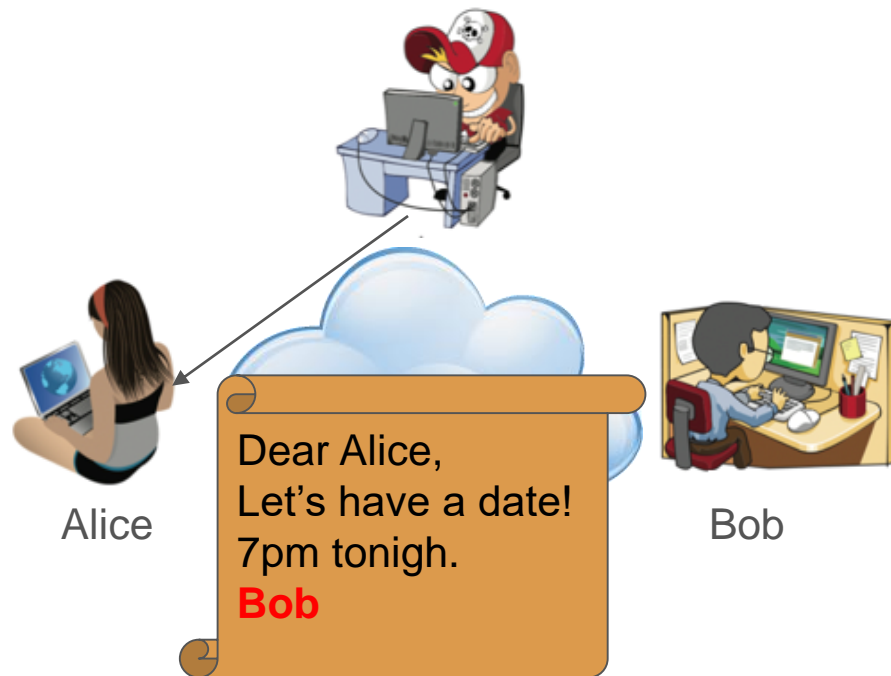
Problems?

- Alice aim to add/remove users on a computer
 - She sends a message (containing identity of new users) to the computer
 - Eve intercepts the message, modify it, and forwards it to the computer!



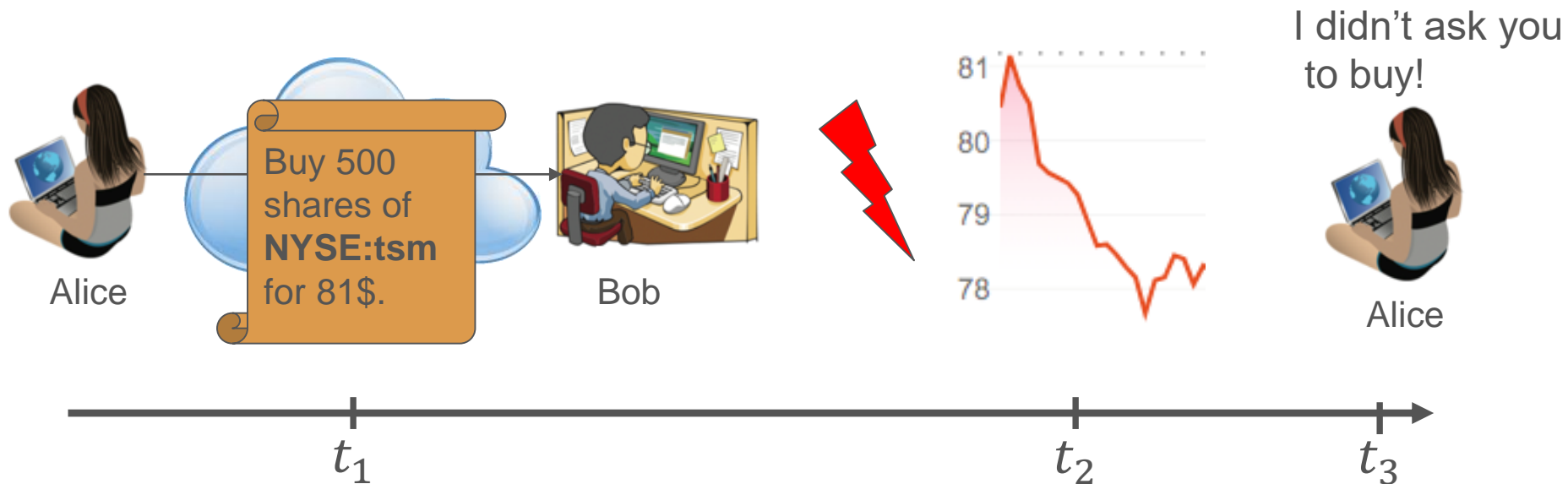
Problems?

- Eve create a new message and claims it is from Bob
 - Alice accepts the message as it comes from Bob!



Problems?

- A customer (Alice) sends a message to a stockbroker (Bob) to buy some stocks
 - Later, the Alice denies sending the message!



What does security mean?

- Email is secure. What does that mean?
- Computer Security (NIST):
 - Protecting an information system to preserve
 - Integrity
 - Confidentiality of resources including
 - HW, SW, firmware, data, and telecommunication
 - Availability



Computer Security Objectives

Confidentiality

- Data confidentiality
 - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
 - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

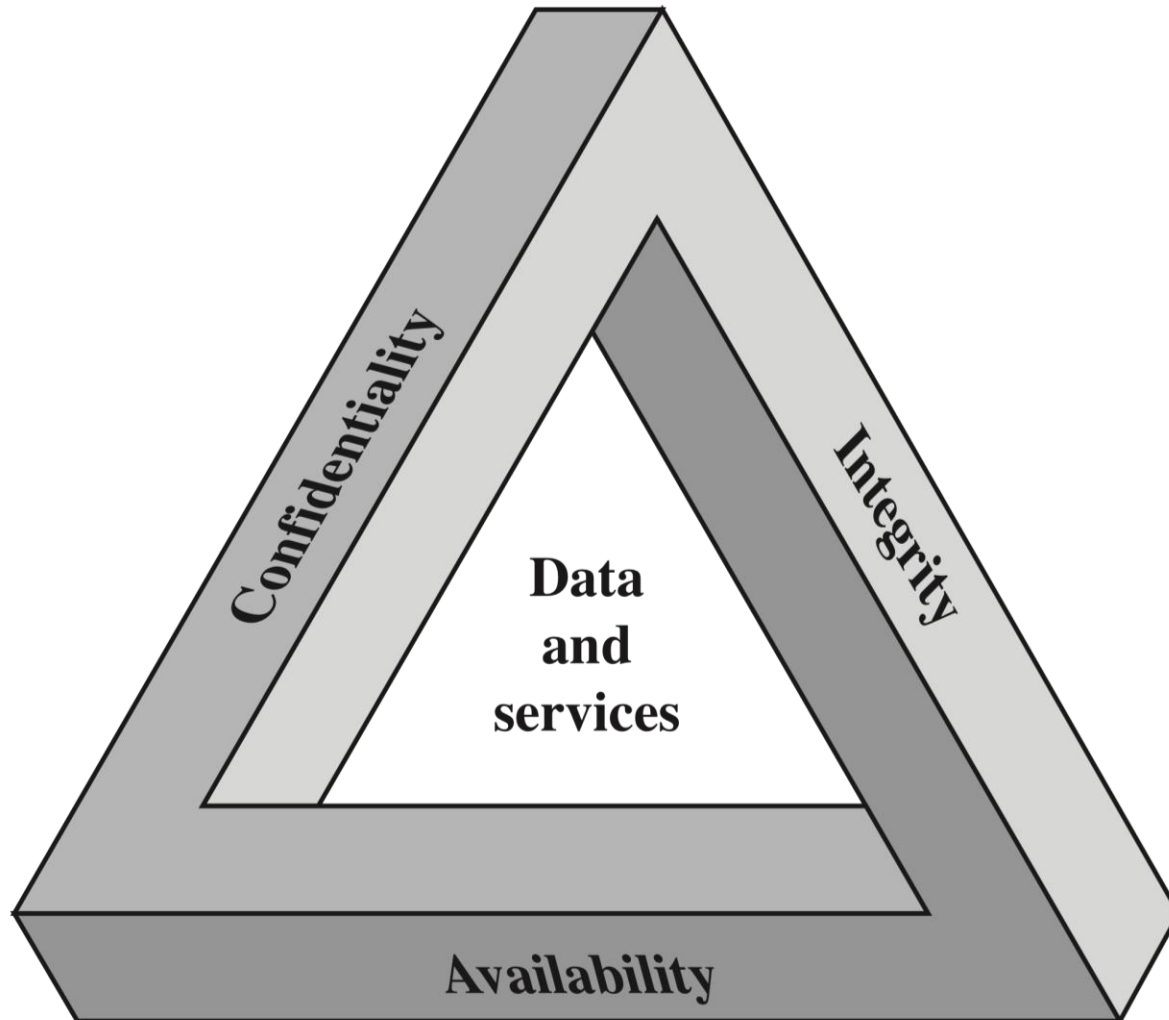
Integrity

- Data integrity
 - Assures that information and programs are changed only in a specified and authorized manner. E.g., database
- System integrity
 - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users. E.g., power backup, redundancy

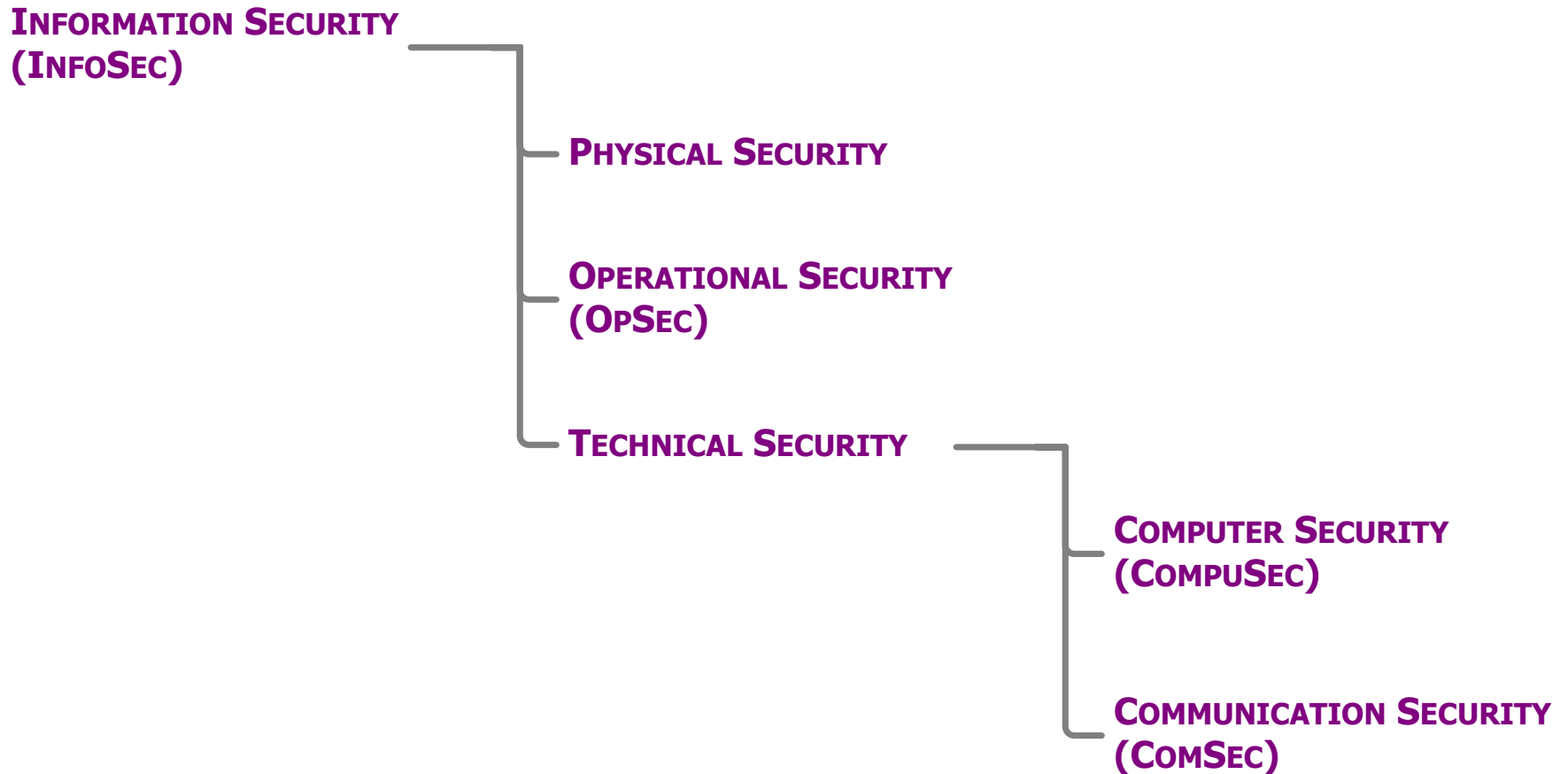
CIA Triad



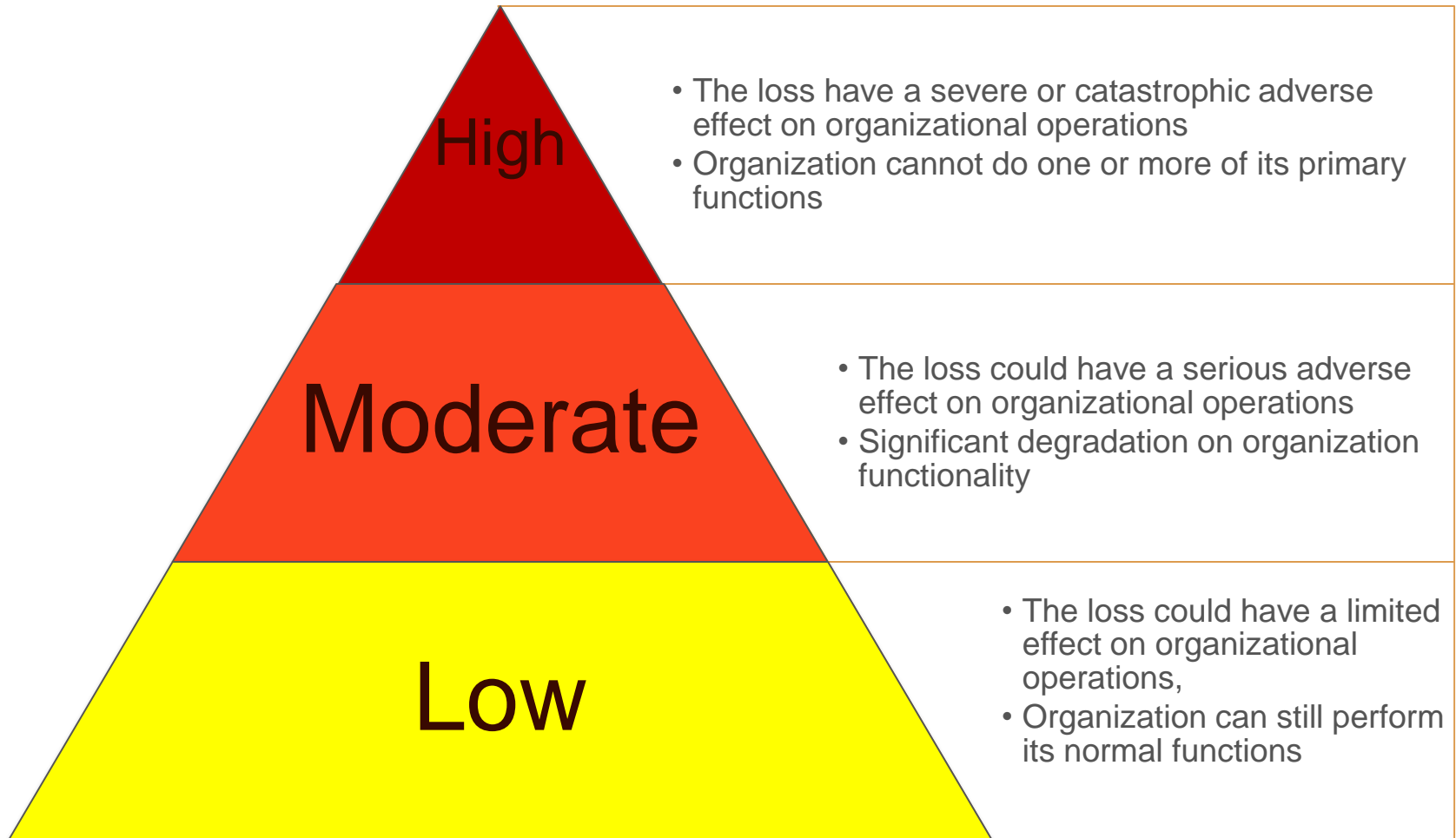
Possible Additional Concepts

- Authenticity
 - Verifying that users are who they say they are.
 - Gives confidence in the validity of a message or the sender of the message.
- Accountability
 - Log user actions for non-repudiation, deterrence
 - It helps to trace a security breach to a responsible user

Security Hierarchy




Breach of Security: Levels of Impact



Examples of Security Requirements


Confidentiality



Student grade should be available only to students, parents, and relevant employees




Students enrolment




Directory info (list of departments, faculties, and students)

Integrity



Patient information stored in a database – inaccurate information could result in serious harm or death to a patient



A entertainment Web site that offers a forum.
A user/hacker falsify some info.



Anonymous online poll with weak authentication.


Availability



Authentication provider services.



University's website



An online telephone directory

Breach of Security: Consequences

- Revenue loss
- Damage to brand reputation
- Loss of intellectual property
 - ideas, inventions, and creative methods
- Hidden Costs
 - legal fees
 - Investigations
 - Regulatory fines

OSI Security Architecture

- Security attack
 - Any action that compromises the security of information owned by an organization (or a person)
- Security mechanism
 - A mechanism that is designed to detect, prevent, or recover from a security attack. E.g., encryption
- Security service
 - A service that enhances the security of the systems and the information transfers of an organization
 - The services make use of one or more security mechanisms to provide the service

OSI: Passive Security Attack

- Passive Attacks
 - eavesdropping on, or monitoring of, transmissions
 - Goal of the opponent is to obtain information that is being transmitted
- Two types of passive attacks are:
 - The release of message contents
 - Traffic analysis
 - Location
 - IP
 - Frequency and length of messages
- These attacks are very hard to detect.



OSI: Active Security Attack

- Active Attack
 - Involve some modification of the data or the creation of a false data
 - Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
 - Goal is to detect attacks and to recover from any disruption or delays caused by them

Run this command in your terminal in the directory the iso was downloaded to verify the SHA256 checksum:

```
echo "b45165ed3cd437b9ffad02a2aad22a4ddc69162470e2622982889ce5826f6e3d
*ubuntu-20.04.1-desktop-amd64.iso" | shasum -a 256 --check
```

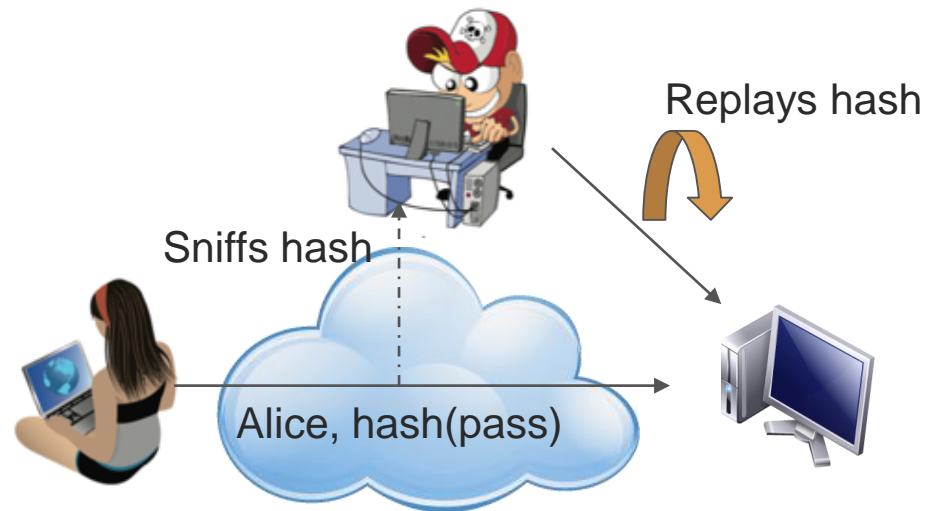
You should get the following output:

```
ubuntu-20.04.1-desktop-amd64.iso: OK
```

Or follow this tutorial to learn [how to verify downloads](#) 

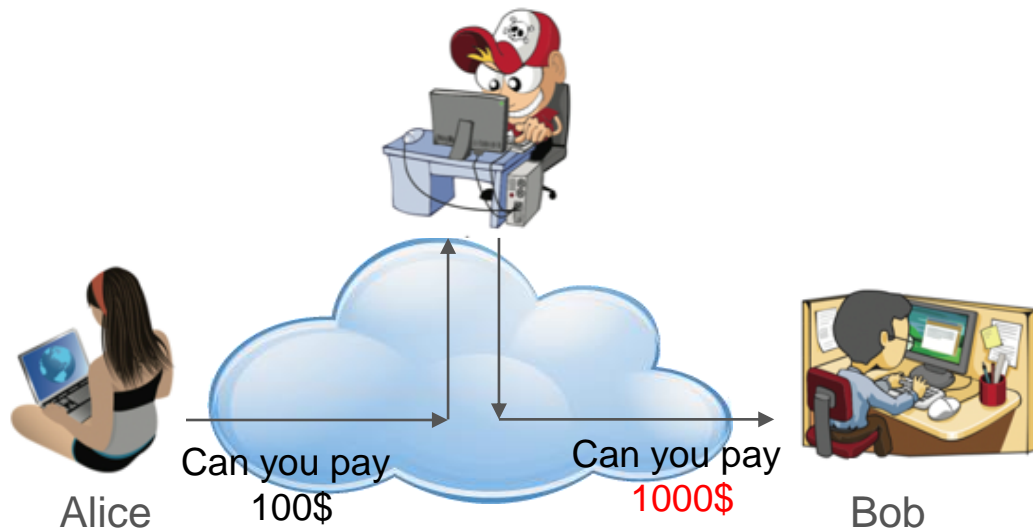
OSI: Active Security Attack

- Masquerade
 - Happens when one user pretends to be a different user
 - Use stolen passwords to login as victim.
 - Capture a valid authentication sequence and replay them to login as victim.
 - Phishing attacks on on-line bank accounts
- Replay
 - Replay of messages



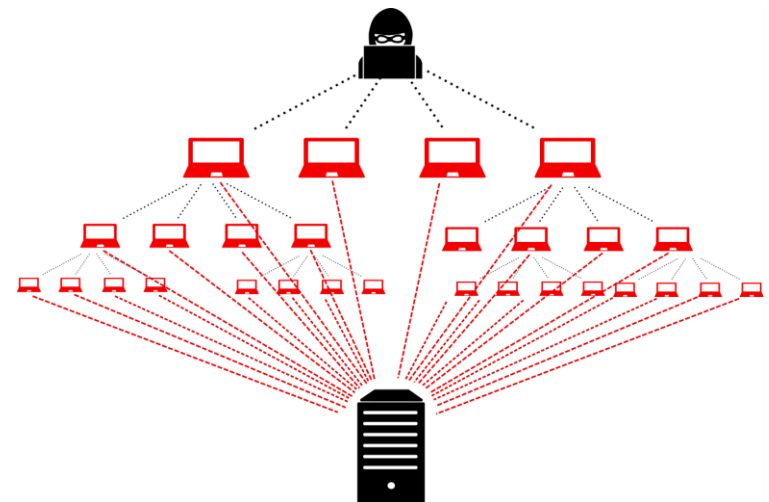
OSI: Active Security Attack

- Modification of messages
 - An attacker intercepts messages and modifies them

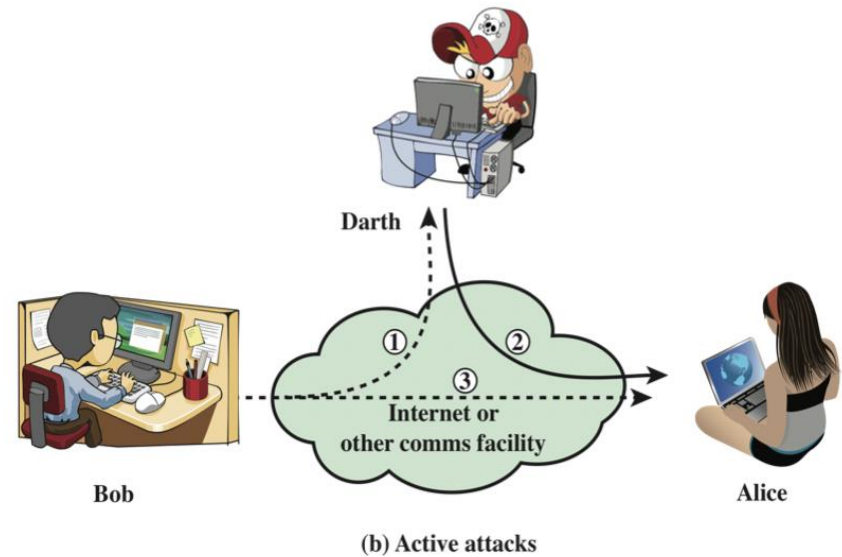
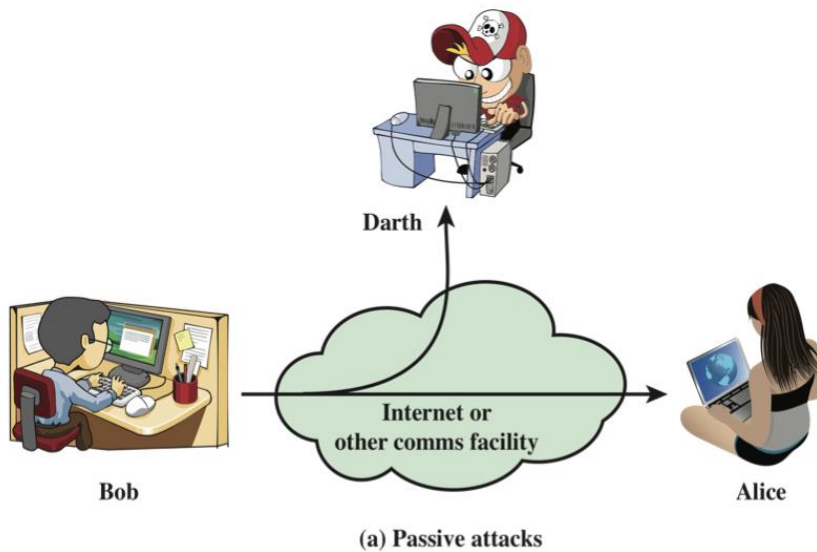


OSI: Active Security Attack

- Denial of service
 - Prevents or inhibits the normal use or management of communication facilities.
 - Disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.
 - Mirai, 2016
 - GitHub, Netflix, Twitter, Airbnb, etc.



OSI: Active vs Passive Attack

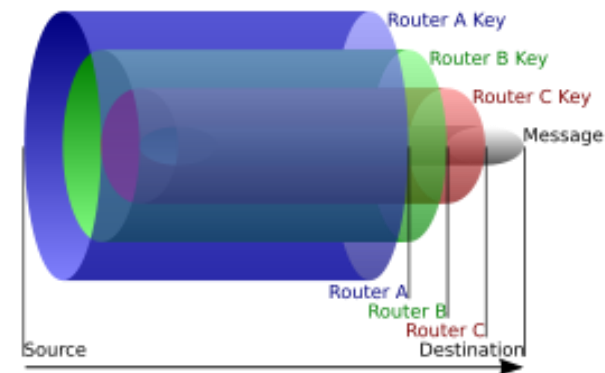


OSI: Security Services

- Authentication
 - Data Origin Authentication
 - This service assures that the data is from the source it claims to be from.
 - E.g., Sign a bank cheque, X.509 certificates
 - Peer entity authentication
 - It provides mutual confidence in the identities of the parties involved in a connection.
 - Typically used at start of a connection.
 - Addresses masquerade and replay threats.

OSI: Security Services

- Confidentiality: Protect data from passive attack.
 - Connection Confidentiality
 - Protects all the data transmitted between two users over a period of time.
 - E.g, TCP connection
 - Connectionless Confidentiality
 - Protection of a single message/data block
 - E.g., UDP
 - Selective Field Confidentiality
 - Protection of a selected field within a message
 - E.g., “Please meet me at XXXXXX tomorrow.”
 - Traffic Flow Confidentiality
 - Protection of traffic flow from analysis.
 - E.g., padding, onion networks



OSI: Security Services

- Integrity
 - Connection Integrity
 - Integrity of a stream of messages
 - E.g., hash of an IOS file on a website with HTTPS connection
 - Connectionless Integrity
 - Integrity of a single message
 - E.g., protect a sensor's measurement
 - Selective Field Integrity
 - A single field in data cannot be modified, deleted, inserted
- Non-Repudiation
 - Data Origin
 - It is the proof that the message was sent by the specified party.
 - Data Reception
 - It is the proof that the message was received by the specified party.

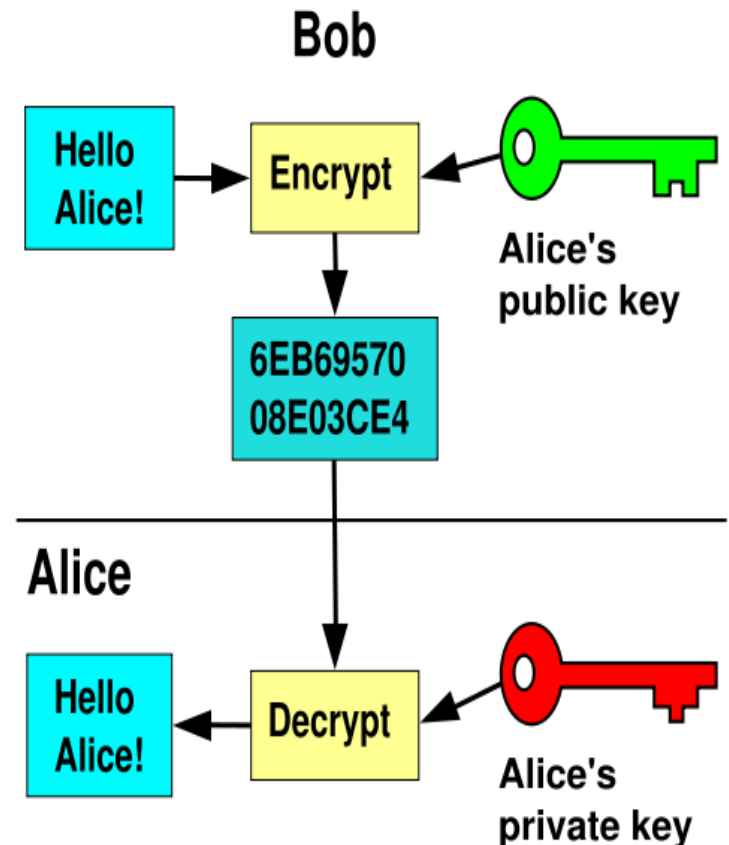
OSI: Security Services

- Access Control
 - Provides protection against an unauthorized use of resources.
 - Use communication network
 - Read, write, delete data from information sources
 - Execution of a processing resource
 - E.g., File permissions in Unix file system, databases
 - E.g., Who can use the printer.



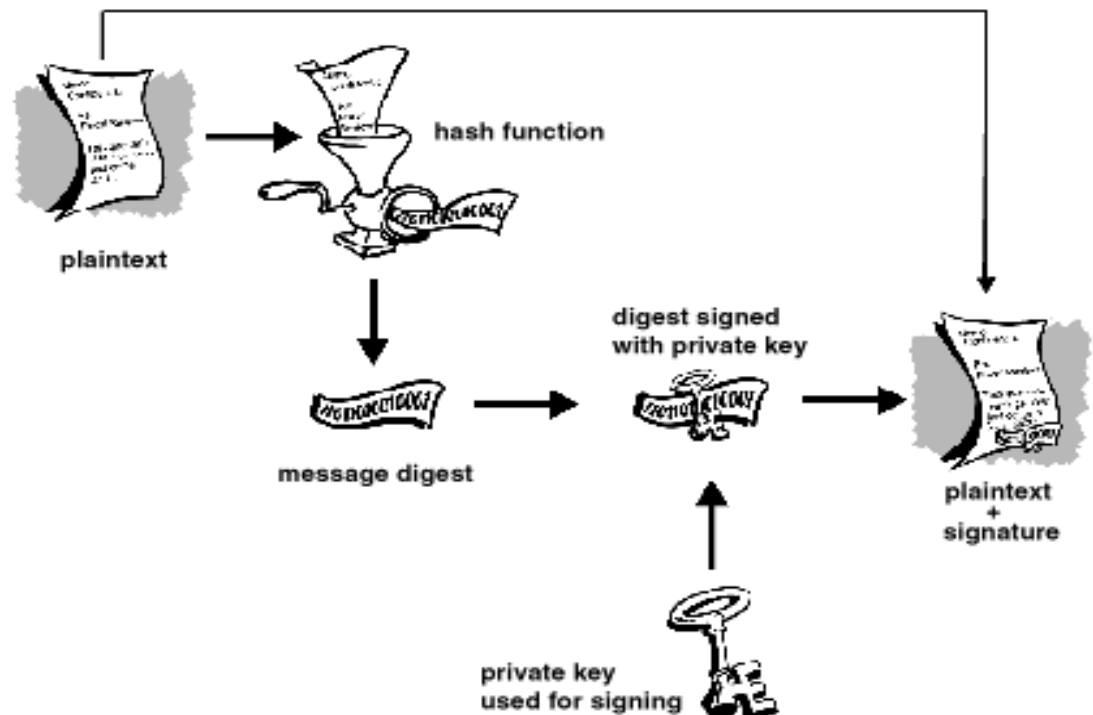
OSI: Security Mechanisms

- Encryption (Encipherment)
 - Asymmetric encryption
 - Public and private pair of keys
 - Symmetric encryption
 - Single key



OSI: Security Mechanisms

- Digital Signature
 - Proves the source and integrity of the data.



OSI: Security Services & Mechanisms

- Security Services

- Authentication
 - Data Origin Authentication
 - Peer Entity Authentication
- Confidentiality
 - Connectionless Confidentiality
 - Connection Confidentiality
 - Selective Field Confidentiality
 - Traffic Flow Confidentiality
- Integrity
 - Connectionless Integrity
 - Connection Integrity
 - Selective Field Integrity
- Non-Repudiation
 - Data Origin
 - Data Reception
- Access Control

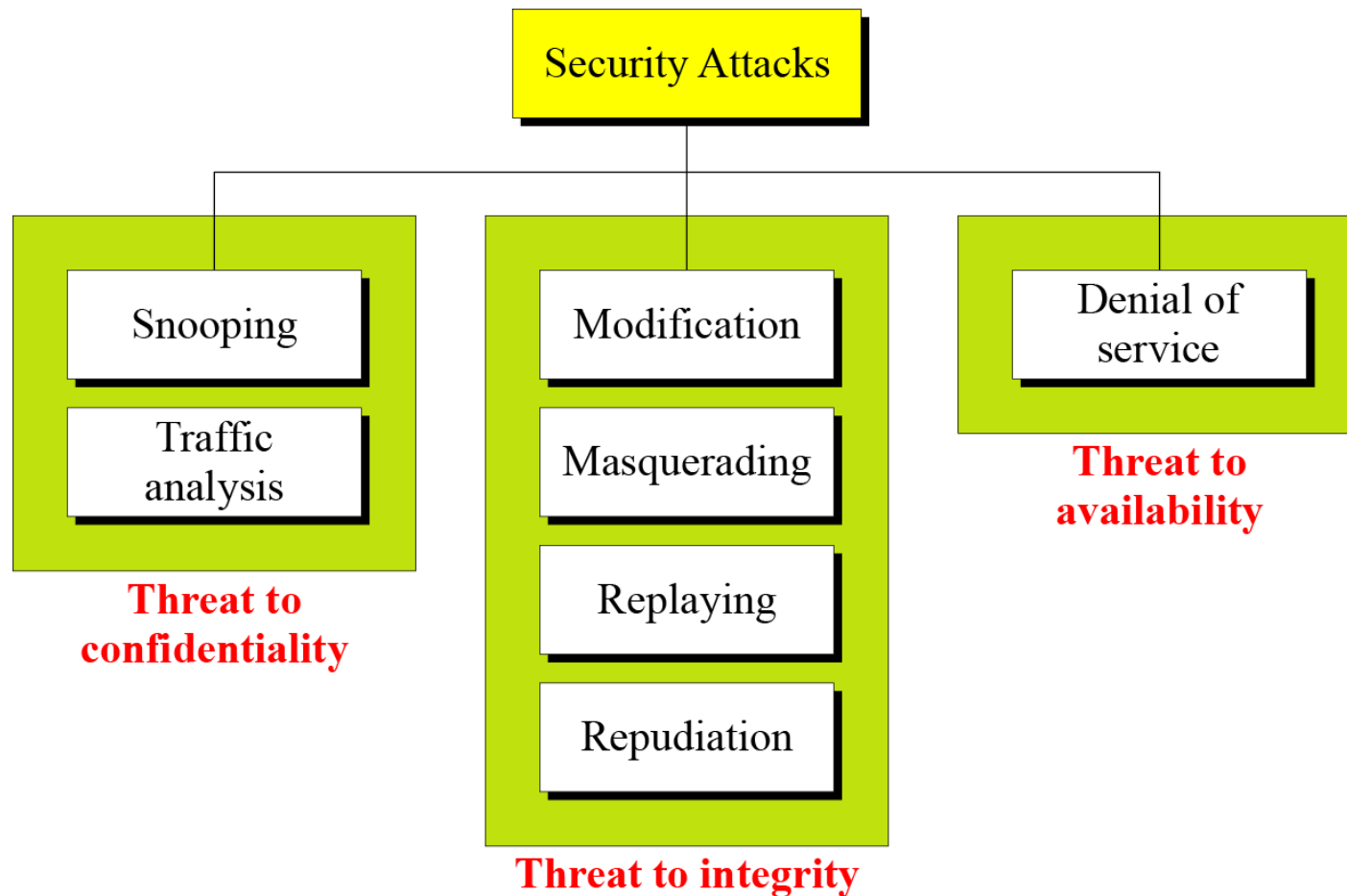
- Security Mechanisms

- Encipherment
 - Secret Key Ciphers
 - Public Key Ciphers
- Integrity Checks
- Digital Signature
- Access Control
- Traffic Padding
- Notarization
- Audit

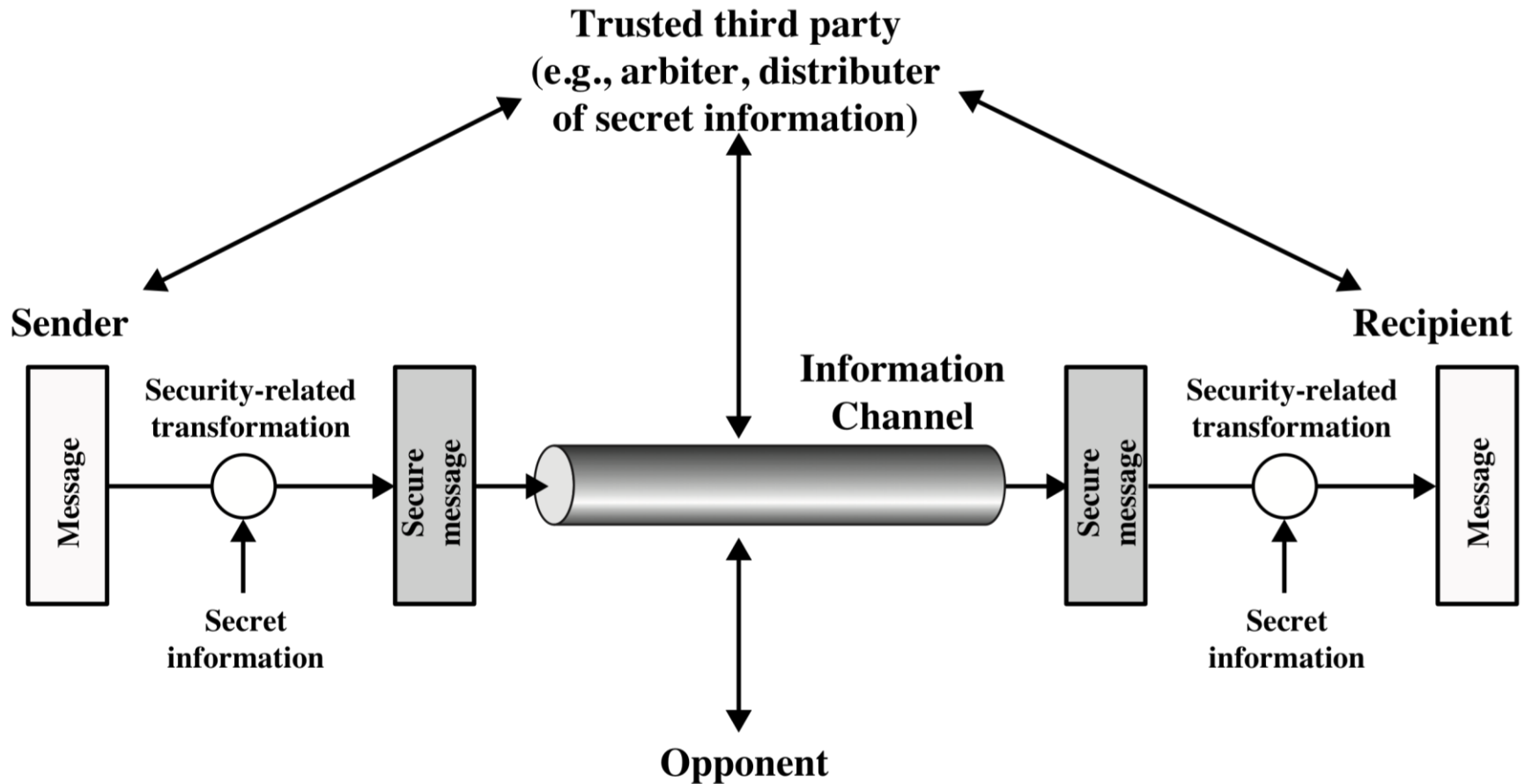
Relationship Between Security Service and Mechanisms

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			

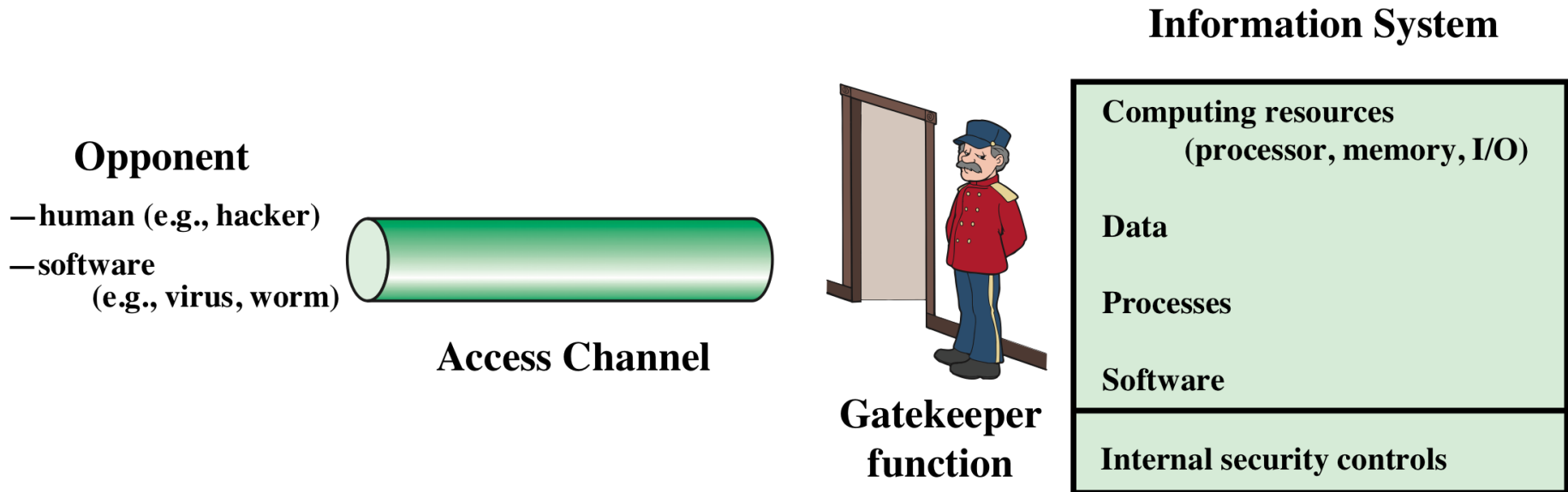
Security Services vs. Attacks



Model for Network Security

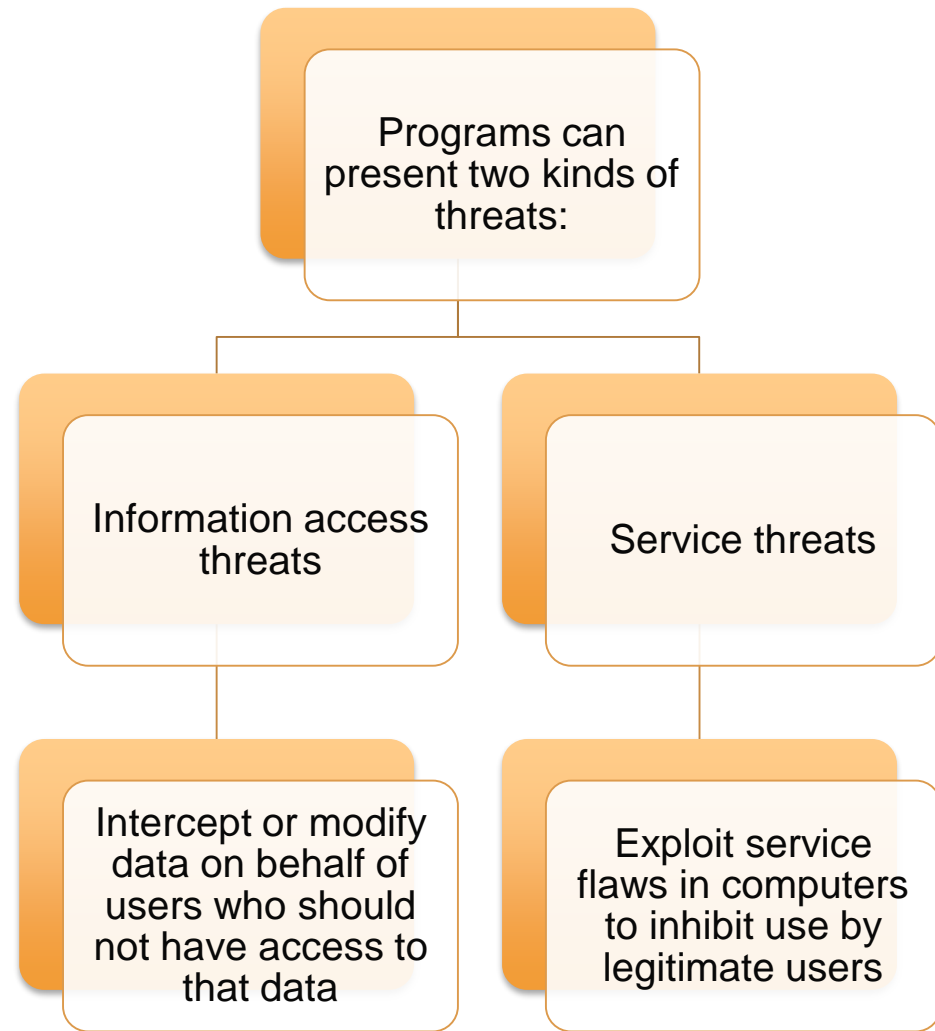


Network Access Security Model



Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect
 - Application programs (editor)
 - Utility programs (compilers)



Summary

- Computer security concepts
 - Definition
 - Examples
 - Challenges
- The OSI security architecture
- Security attacks
 - Passive attacks
 - Active attacks
- Security services
 - Authentication
 - Access control
 - Data confidentiality
 - Data integrity
 - Nonrepudiation
 - Availability service
- Security mechanisms
- Model for network security