

# Network Security

---

PREPARED BY: DR. REEMA PATEL

# Course Content

---

- **UNIT I**
- Introduction to Security Threats: Threats to security: Viruses and Worms, Intruders, Insiders, Criminal organizations, Terrorists, Information warfare, Avenues of Attack, steps in attack, Security Basics – Confidentiality, Integrity, Availability; Types of attack: Denial of service (DOS), backdoors and trapdoors, sniffing, spoofing, man in the middle, replay, TCP/IP Hacking, Phishing attacks, Distributed DOS, SQL Injection.

# Course Content

---

- **UNIT II:**
- Organizational Security:
- Password selection, Piggybacking, Shoulder surfing, Dumpster diving, installing unauthorized software /hardware, Access by non-employees,
- Physical security: Access controls Biometrics: finger prints, hand prints, Retina, Patterns, voice patterns, signature and writing patterns, keystrokes, Physical barriers, Password Management, vulnerability of password, password protection, password selection strategies, components of a good password.

# Course Content

---

- **UNIT III**
- Cryptography and Public Key Infrastructure:
- Introduction to Symmetric encryption;
- Asymmetric encryption, Encryption algorithm / Cipher, Encryption and Decryption using: Caesar's cipher, play fair cipher, shift cipher, shift cipher, Vigenere cipher, one time pad (vermin cipher), hill cipher, Transposition techniques , Hashing function : SHA1 , Asymmetric encryption: Digital Signatures, Public key infrastructures : basics, digital signatures, digital certificates, certificate authorities, registration authorities, Trust Models: Hierarchical, peer to peer.

# Course Content

---

- **UNIT IV**
- Network Security: Firewalls: working, design principles, trusted systems, Kerberos, IP security: overview, architecture, IPSec configurations, IPSec security , Security topologies , Email security.
- Web Security: Intruders: Intrusion detection systems (IDS): host based IDS, network based IDS, logical components of IDS, signature based IDS, anomaly based IDS, Intrusion detection systems,
- Web security threats, web traffic security approaches, Introduction to Secure Socket Layer (SSL), Transport Layer Security(TLS)

# Reference Books

---

1. Principles Of Computer Security CompTIA Security And Beyond (Exam SY0-301), 3rd Edition,
2. Conklin, Wm. Arthur Gregory White, Dwayne Williams, Mc Graw Hill
3. **Cryptography and Network Security Principles and Practices, Williams Stallings, Pearson Education, Third Edition**
4. **Cryptography and Network Security , B A Forouzen , TMH**
5. **Cryptography and Network Security Principal and Practices , Atul Kahathe, TMH**
6. Computer Security , Dieter Gollman , Wiley India Education, Second Edition

# Introduction

---

- The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him/her; not on the chance of his/her not attacking, but rather on the fact that we have made our position unassailable.

**—The Art of War, Sun Tzu**

# Introduction

---

- We are living in the information age
- **Information: a meaningful data**
- We need to keep information about every aspect of our lives
  - Information is an asset that has a value like any other asset
- As an asset, information needs to be secured from attacks



# Introduction

---

- To be secured,
  - Information needs to be hidden from unauthorized access
  - Protected from unauthorized change
  - And available to an authorized entity when it is needed

# Introduction

---

- **Until a few decades ago,**
  - The information collected by an organization was stored on physical files
  - Confidentiality of files: achieved by restricting the access to a few authorized and trusted people in the organization
  - Integrity: Only a few authorized people were allowed to change the contents of the files
  - Availability: achieved by designating at least one person who would have access to the files at all times

# Introduction

---

- With the advent of computers,
  - Information storage became electronic
    - Instead of being stored on physical media, it was stored in computers
- The files stored in computers require confidentiality, integrity, and availability.
- The implementation of these requirements, however is different and more challenging

# Introduction

---

- During the last few decades, computer networks created a revolution in the use of information
  - Information is now distributed
- Authorize people can send and retrieve information from a distance using computer networks
- Three security requirements – confidentiality, integrity, and availability have not changed, they have new dimensions
- Not only should information be confidential when it is stored in a computer,
  - There should also be a way to maintain its confidentiality when it is transmitted from one computer to another

# Introduction

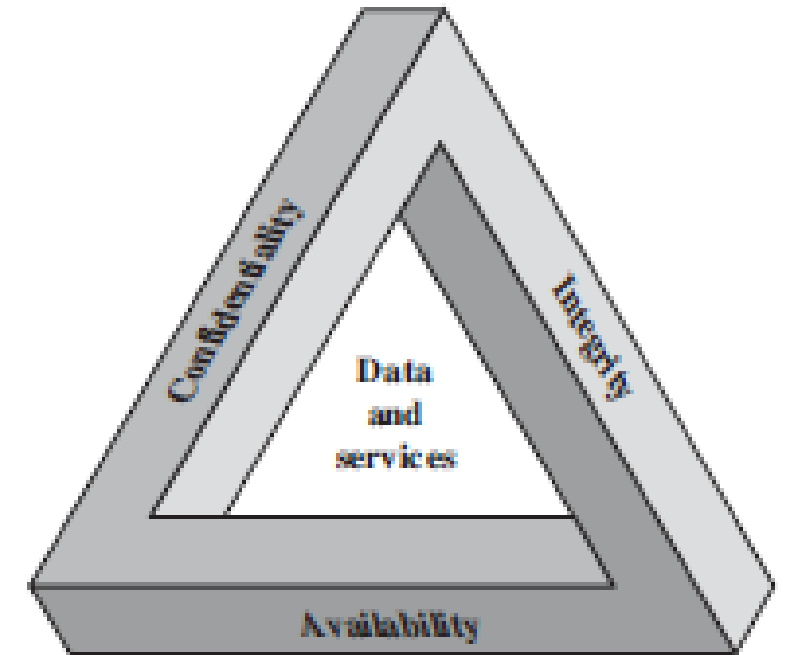
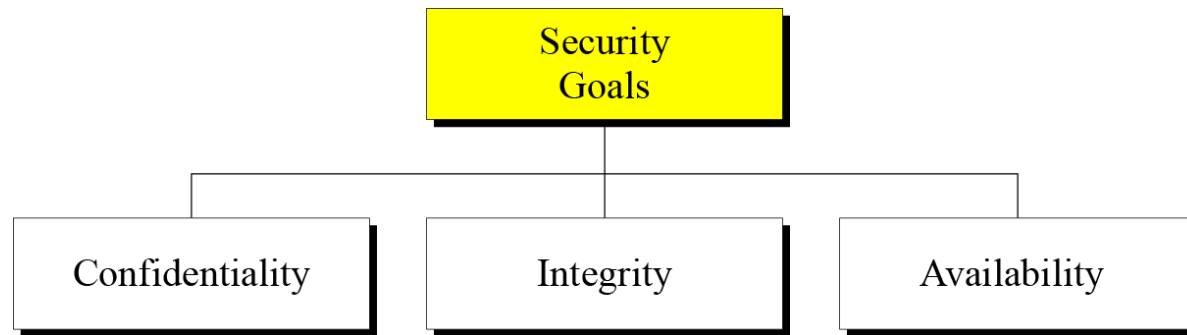


Figure 1.1 The Security Requirements Triad

# Confidentiality

---

- Confidentiality is probably the most common aspect of information security.
- We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- Example:
  - In military, concealment of sensitive information is the major concern,
  - In industry, hiding some information from competitors is crucial to the operation of the organization
  - In banking, customers' accounts need to be kept secret

# Confidentiality

---

- **Example:** Confidentiality is the most important when the information is a record of people's personal activities, such as in cases involving personal and financial information of the customers of companies like Google, Amazon, Apple, and Walmart, etc.
- To guarantee confidentiality under the CIA triad, communication channels must be properly monitored and controlled to prevent unauthorized access.

# Confidentiality

---

- **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.



# Integrity

---

- Information needs to be changed constantly.
  - In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

# Integrity

---

- **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
- **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

# Integrity

---

- **Example:** Any change in financial records leads to issues in the accuracy, consistency, and value of the information.
- For example, banks are more concerned about the integrity of financial records, with confidentiality having only second priority.
- Some bank account holders or depositors leave ATM receipts unchecked and hanging around after withdrawing cash.
- This shows that confidentiality does not have the highest priority. Instead, the goal of integrity is the most important in information security in the banking system.
- To guarantee integrity under the CIA triad, information must be protected from unauthorized modification.

# Availability

---

- The information created and stored by an organization needs to be available to authorized entities.
- Information is useless if it is not available
- Information constantly changed, means it must be accessible to authorized entities
  - Imagine, what would happen to a bank, if customers could not access their accounts for transactions

# Availability

---

- **Availability:** Assures that systems work promptly and service is not denied to authorized users.
- Ensuring timely and reliable access to and use of information.
- A loss of availability is the disruption of access to or use of information or an information system.

# Availability

---

- **Example:** Press releases are generally for public consumption.
- For them to be effective, the information they contain should be available to the public.
- Thus, confidentiality is not of concern. Integrity has only second priority.
- In the CIA triad, to guarantee availability of information in press releases, governments ensure that their websites and systems have minimal or insignificant downtime.

# Security Attacks

---

# Security Attacks

---

- The three goals of security : confidentiality, integrity, and availability can be threatened by security attacks.
- Attacks Threatening Confidentiality
- Attacks Threatening Integrity
- Attacks Threatening Availability
- Passive versus Active Attacks

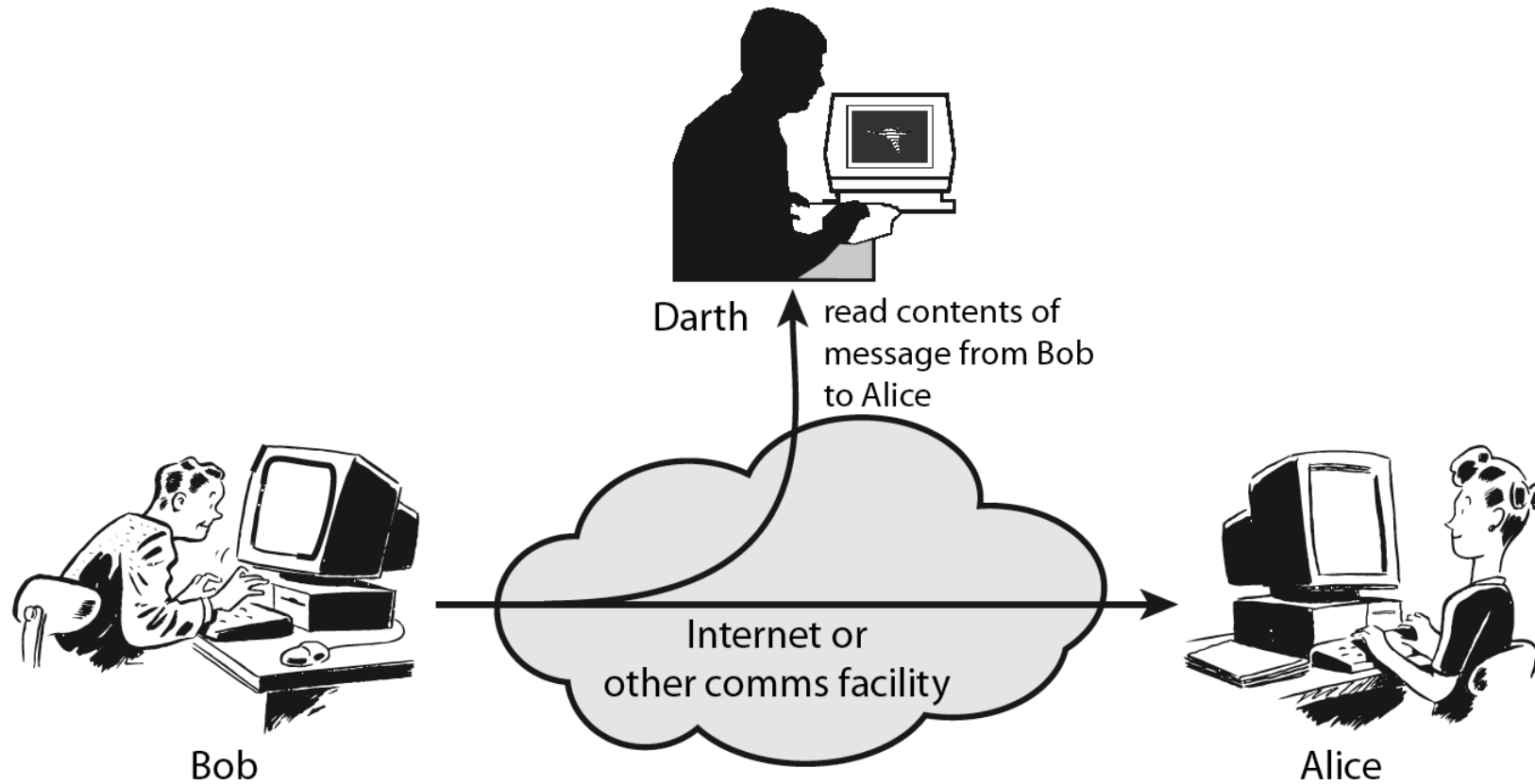


# Security Attacks

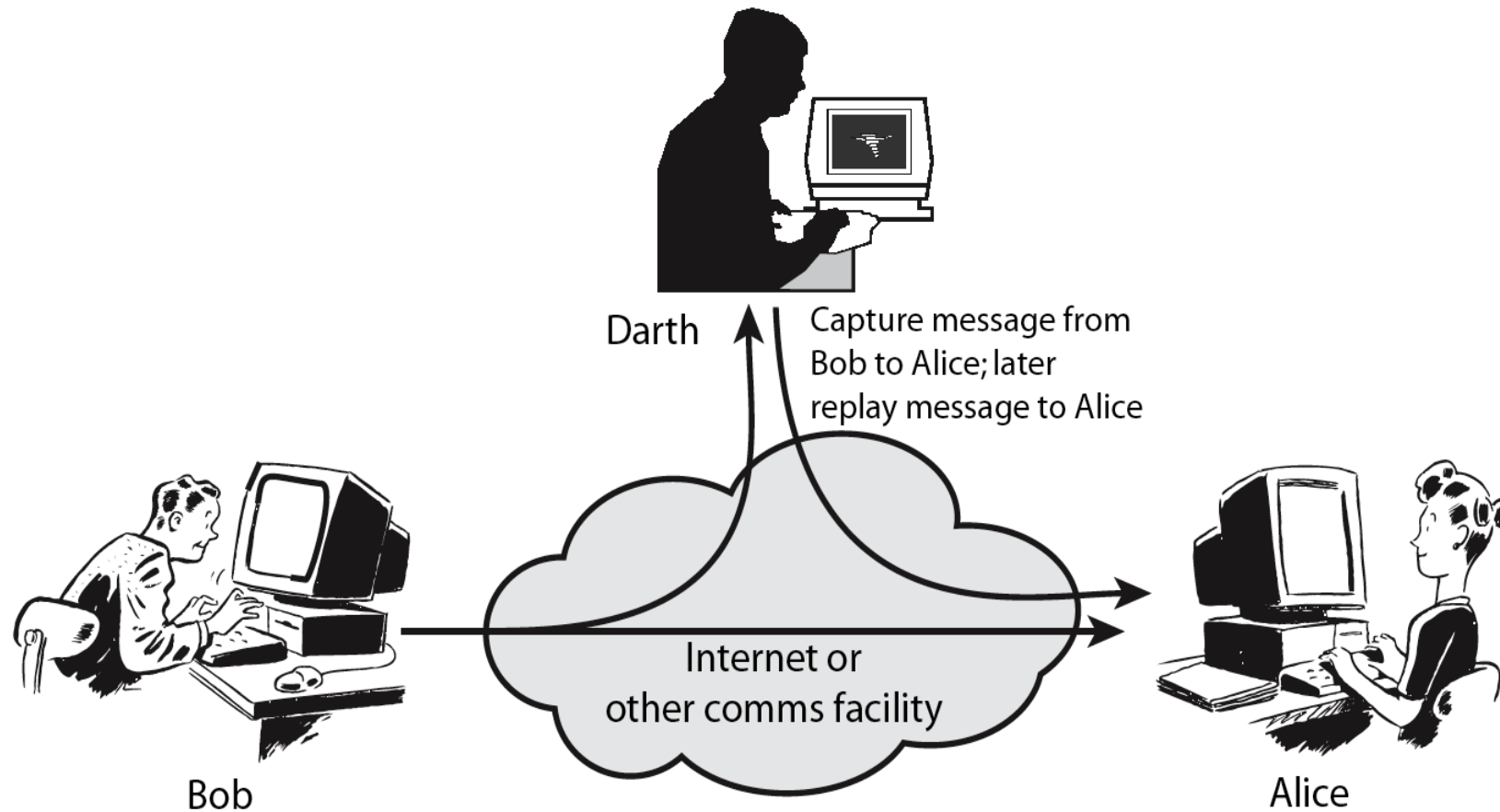
---

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attack
  - Passive
  - Active

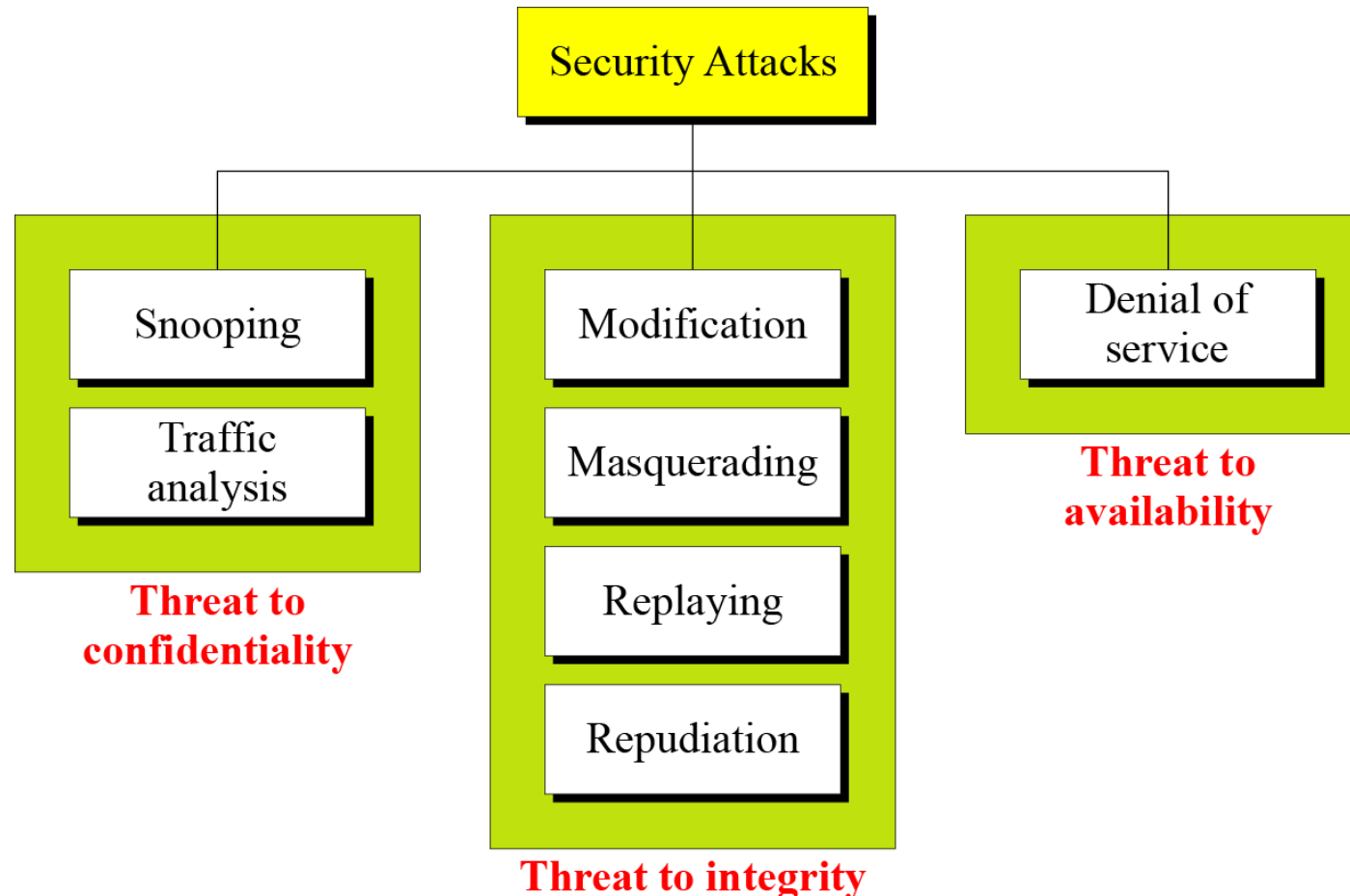
# Passive Attack



# Active Attack



# Taxonomy of attacks with relation to security goals



# Attacks Threatening Confidentiality

---

- **Snooping** refers to unauthorized access to or interception of data.
- **Traffic analysis** refers to obtaining some other type of information by monitoring online traffic.

# Attacks Threatening Integrity

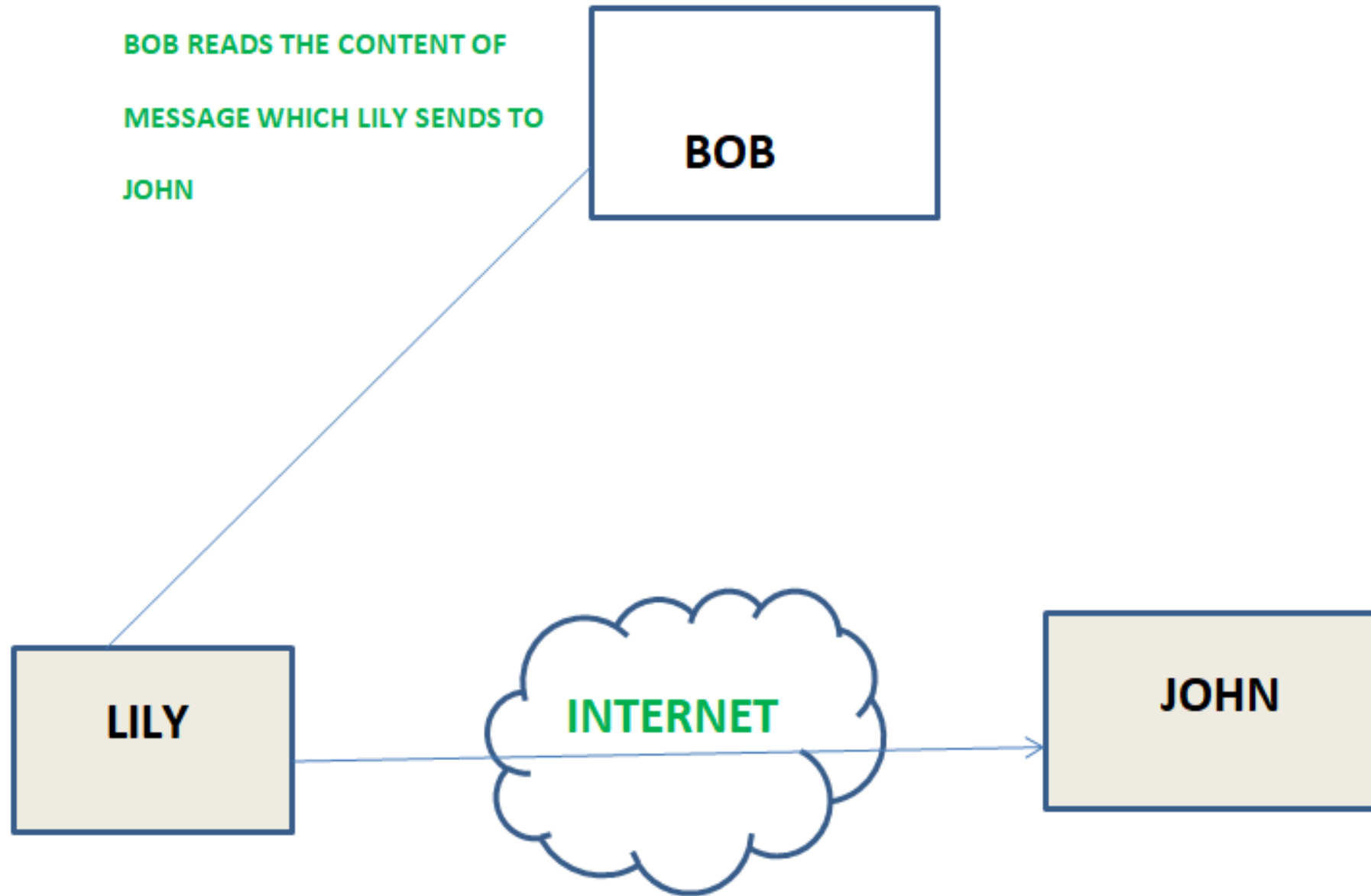
---

- **Modification** means that the attacker intercepts the message and changes it.
- **Masquerading** happens when the attacker impersonates somebody else.
- **Replaying** means the attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation** means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

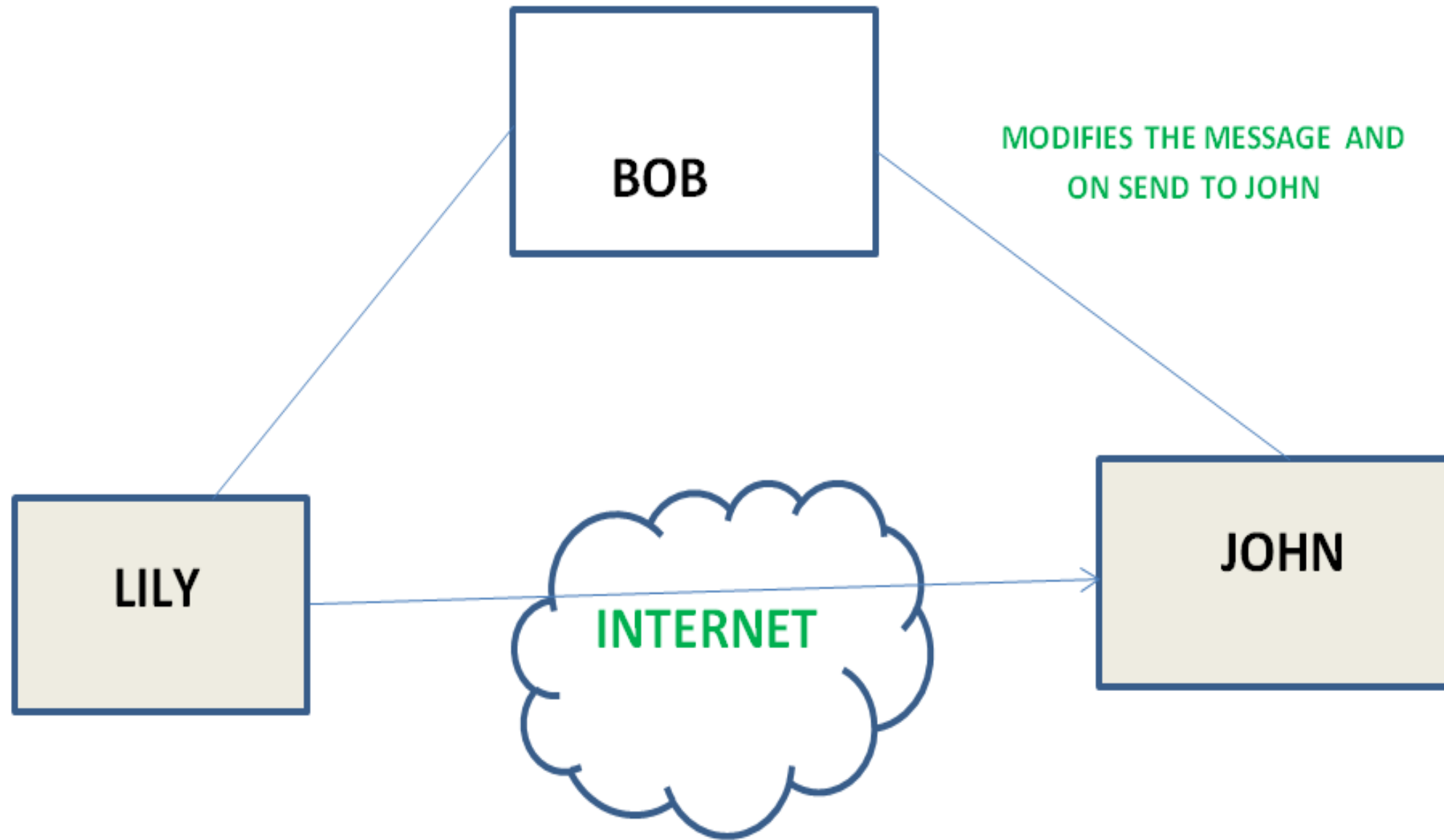
# Attacks Threatening Availability

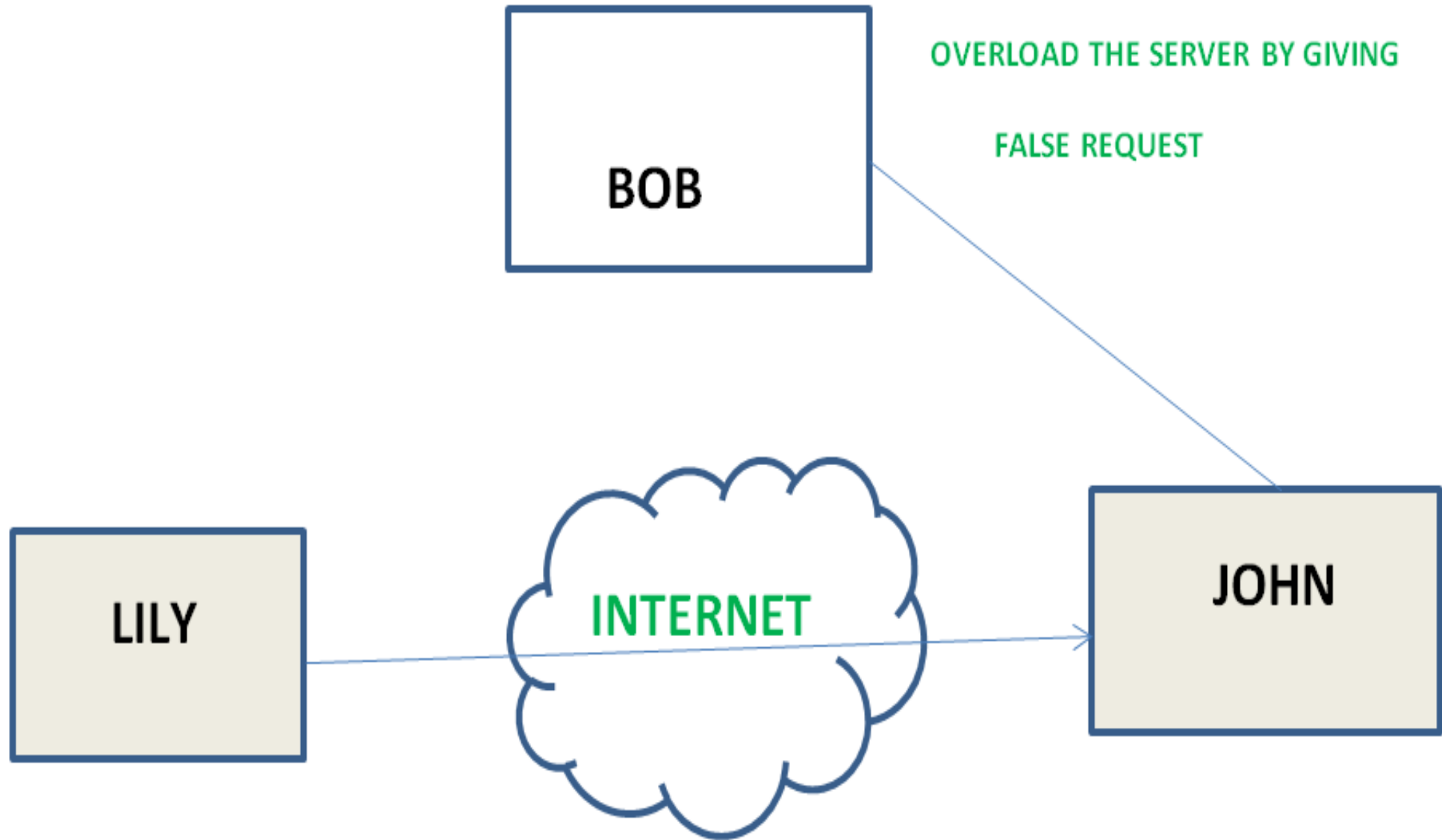
---

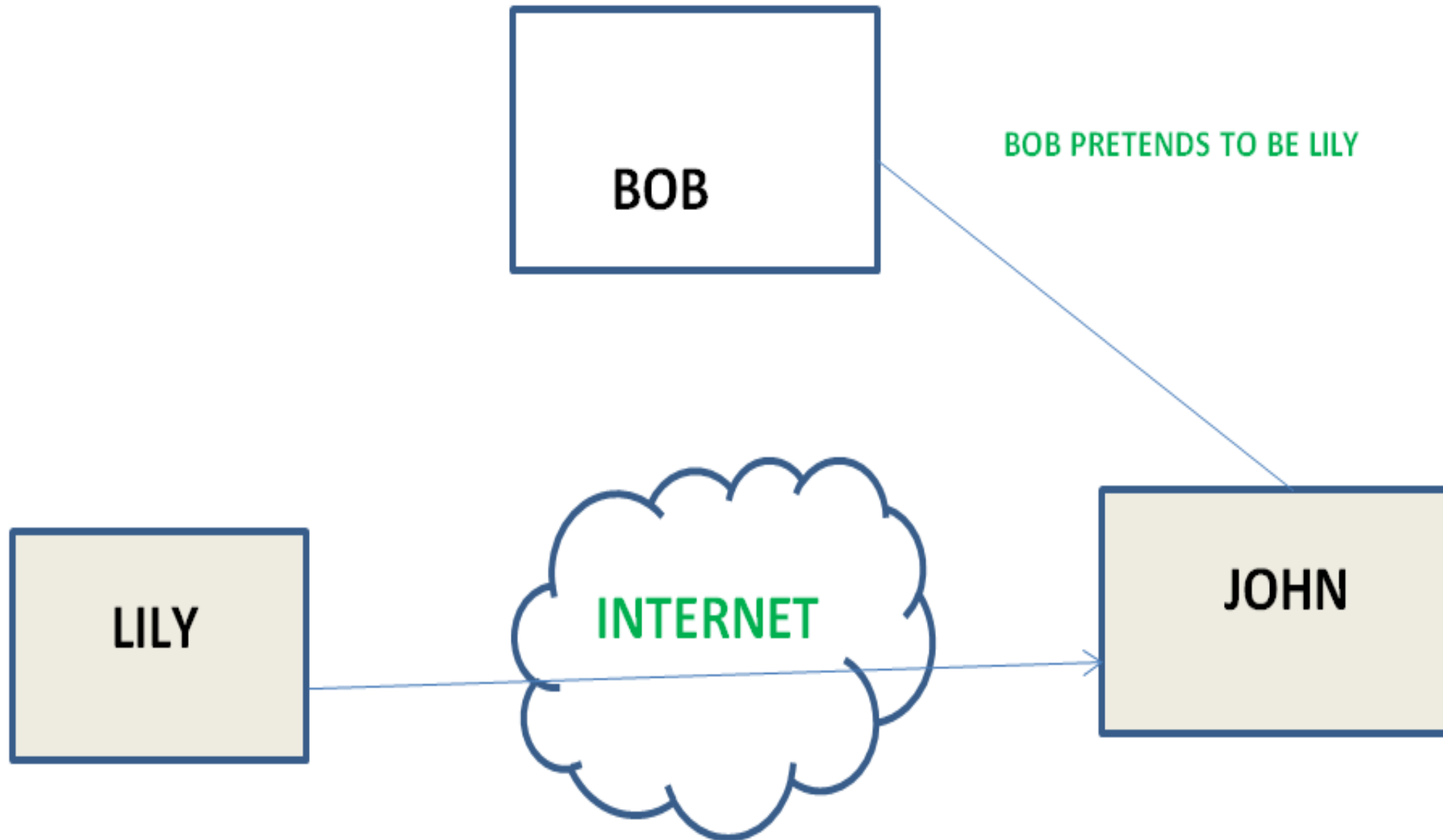
- **Denial of service (DoS)** is a very common attack. It may slow down or totally interrupt the service of a system.

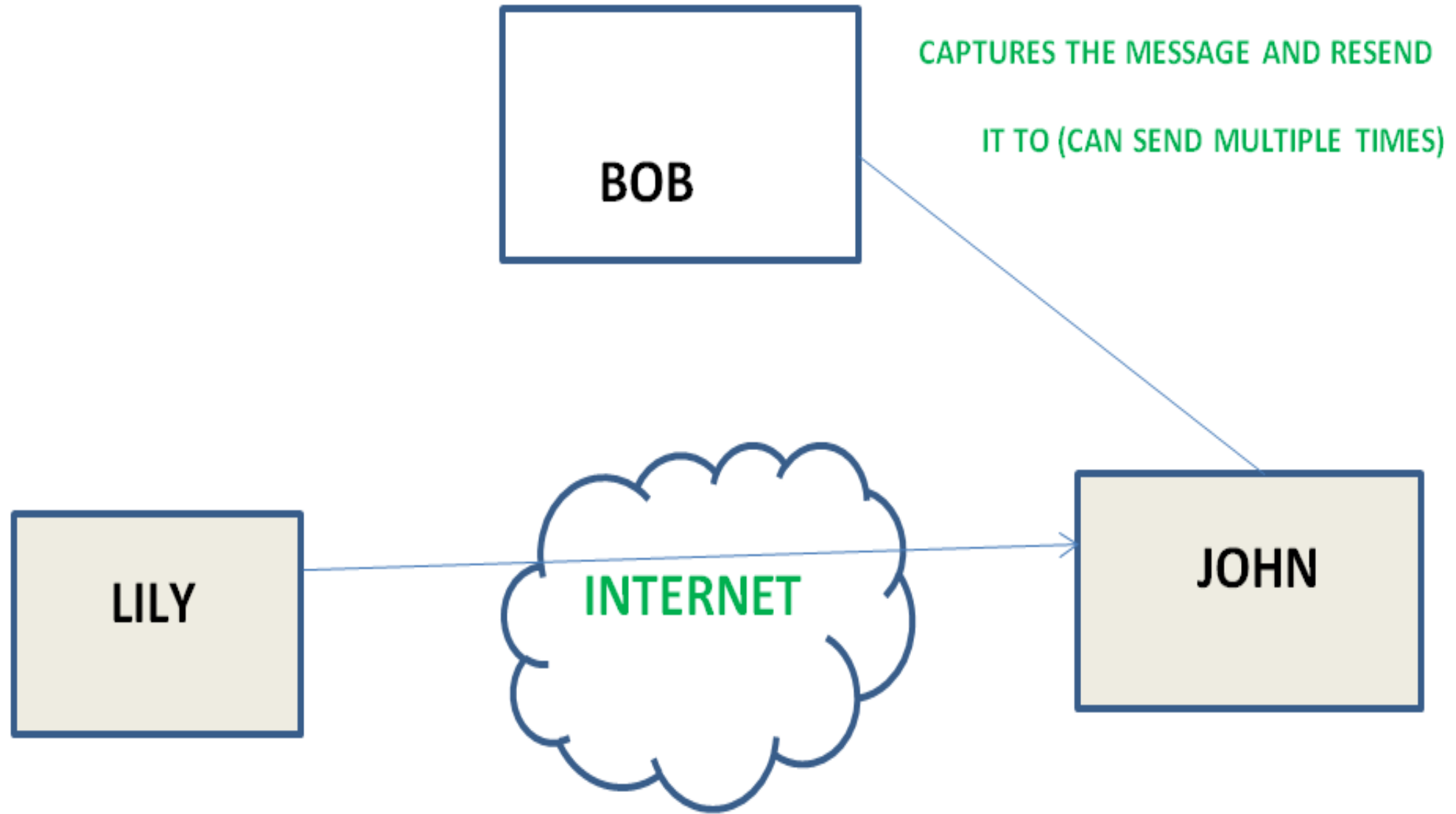


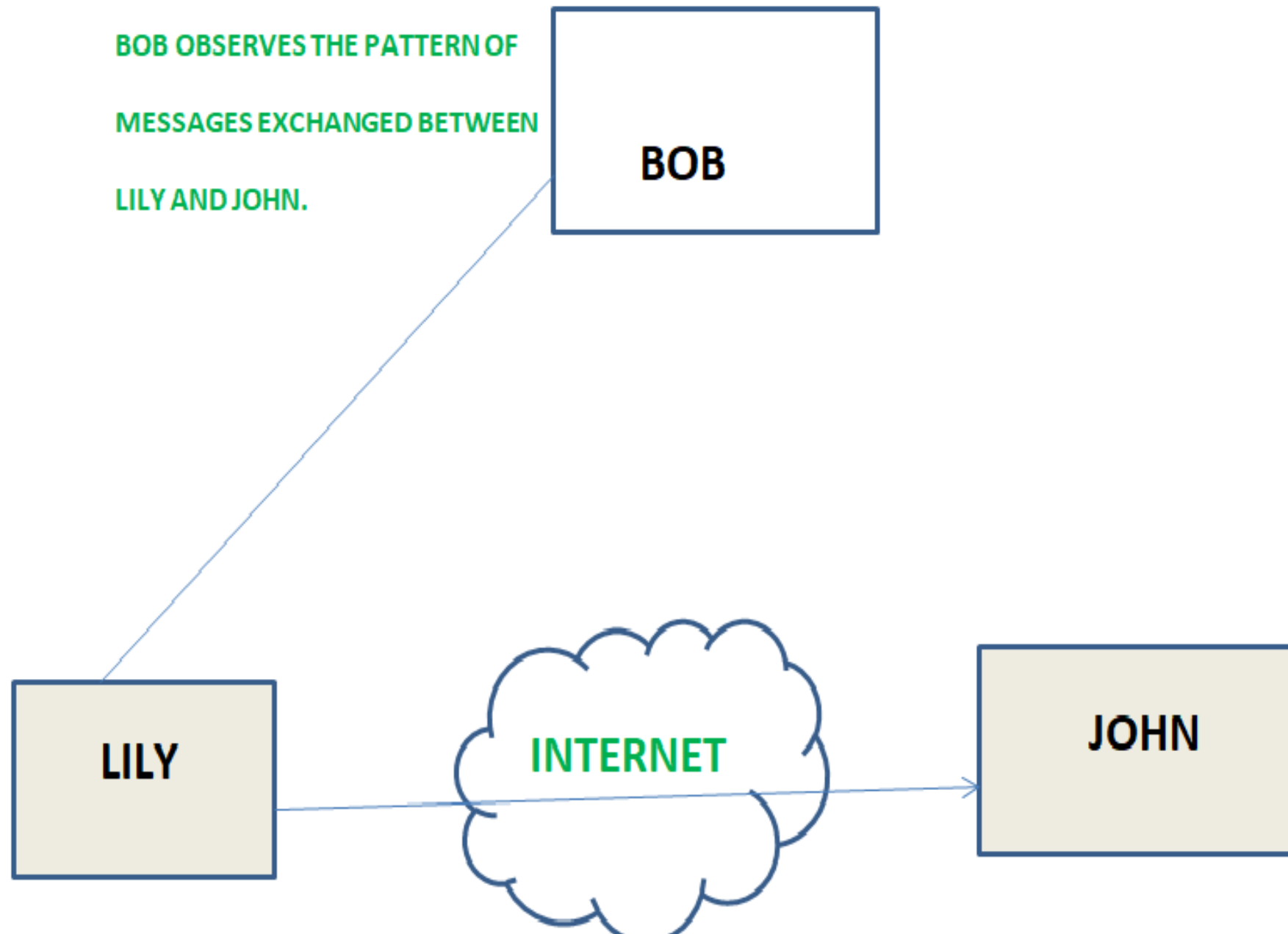




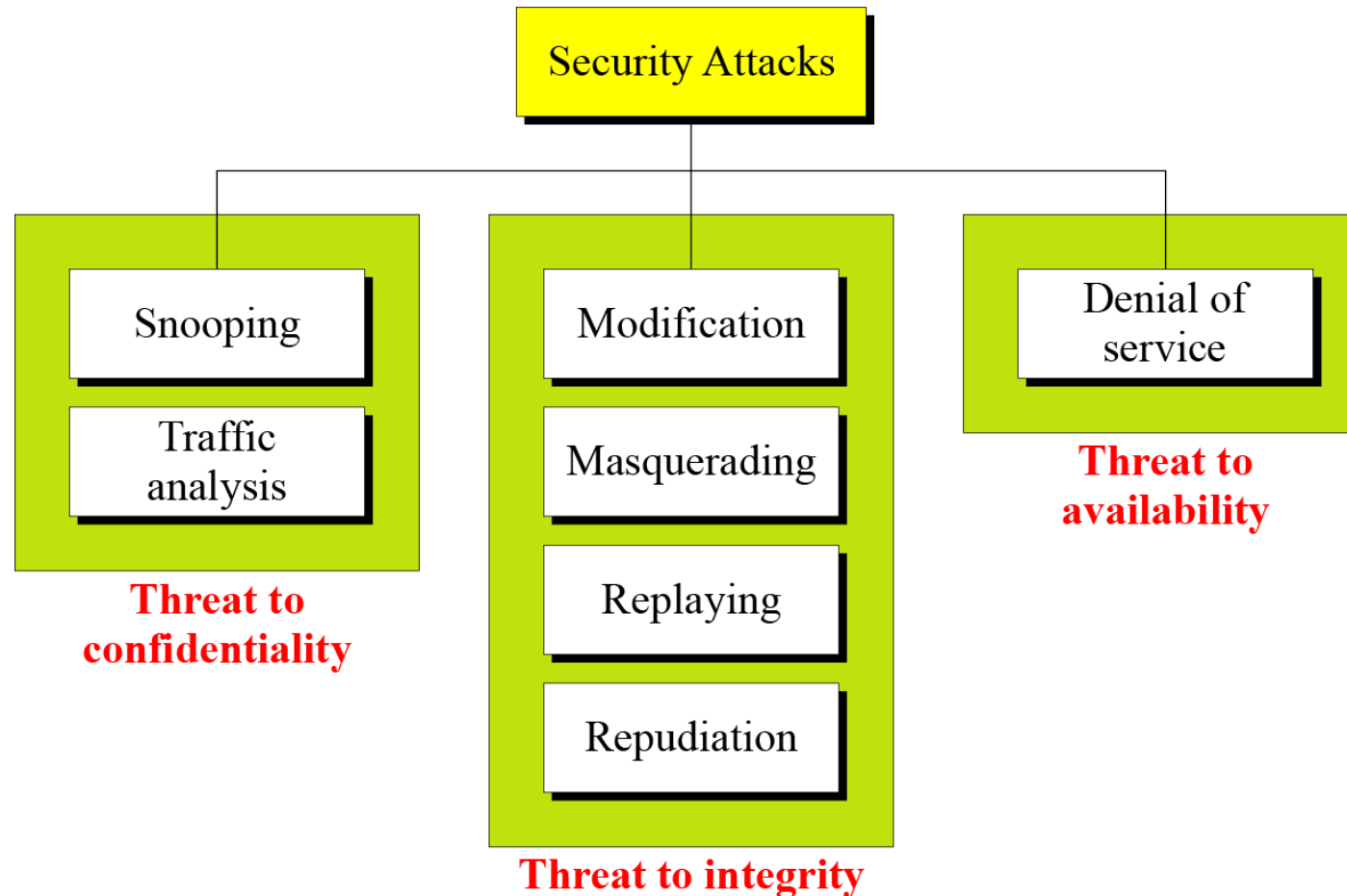








# Taxonomy of attacks with relation to security goals



# Passive Versus Active Attacks

---

<i>Attacks</i>	<i>Passive/Active</i>	<i>Threatening</i>
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

# Difference between Active Attack and Passive Attack

---

Sr. No	ACTIVE ATTACK	PASSIVE ATTACK
1	In Active Attack, information is modified.	In Passive Attack, information remain unchanged.
2	Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
3	Attention is to be paid on detection.	Attention is to be paid on prevention.
4	In Active Attack, system is damaged.	In Passive Attack, system has no impact.
5	Victim gets informed in active attack.	Victim does not get informed in passive attack.
6	System Resources can be changed in active attack.	System Resources are not changed in passive attack.
7	Active attack influence the services of the system.	While in passive attack, information and messages in the system or network are acquired



# Difference between Active Attack and Passive Attack

---

Sr. No	ACTIVE ATTACK	PASSIVE ATTACK
8	In active attack, information collected through passive attacks are used during executing.	While passive attack are performed by collecting the information such as passwords, messages by itself.
9	Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.

# Policy and Mechanism

---

- A *security policy* is a statement of what is, and what is not allowed.
- A *security mechanism* is a method, tool, or procedure for enforcing a security policy
- Mechanisms can be nontechnical, such as requiring proof of identity before changing a password;
- Policies often require some procedural mechanisms that technology cannot enforce.

# Policy and Mechanism

---

- Example:
- Suppose a university's computer science laboratory has a policy that **prohibits any student from copying another student's assignment files**.
- The computer system provides mechanisms for preventing others from reading a user's files.
- Anna fails to use these mechanisms to protect her assignment files, and Bill copies them.
- A breach of security has occurred, because Bill has violated the security policy.
- Anna's failure to protect her files does not authorize Bill to copy them.

# Policy and Mechanism

---

- Policies may be presented mathematically, as a list of allowed (secure) and disallowed (nonsecure) states.
- For our purposes, we will assume that any given policy provides an axiomatic description of secure states and nonsecure states.
- In practice, policies are rarely so precise; they normally describe in English, or some other natural language, what users and staff are allowed to do.