Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

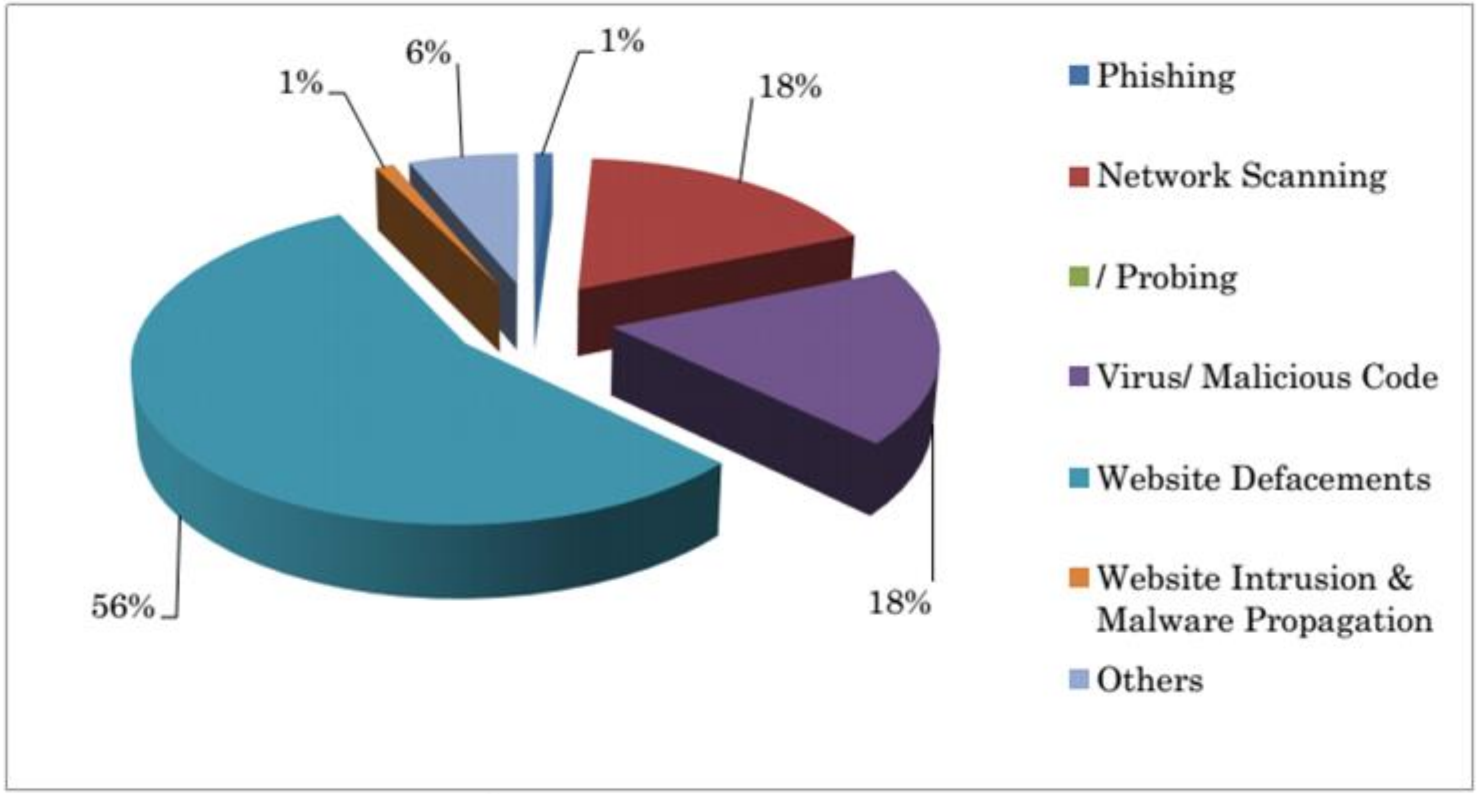
Lecture – 2: Security Basics

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

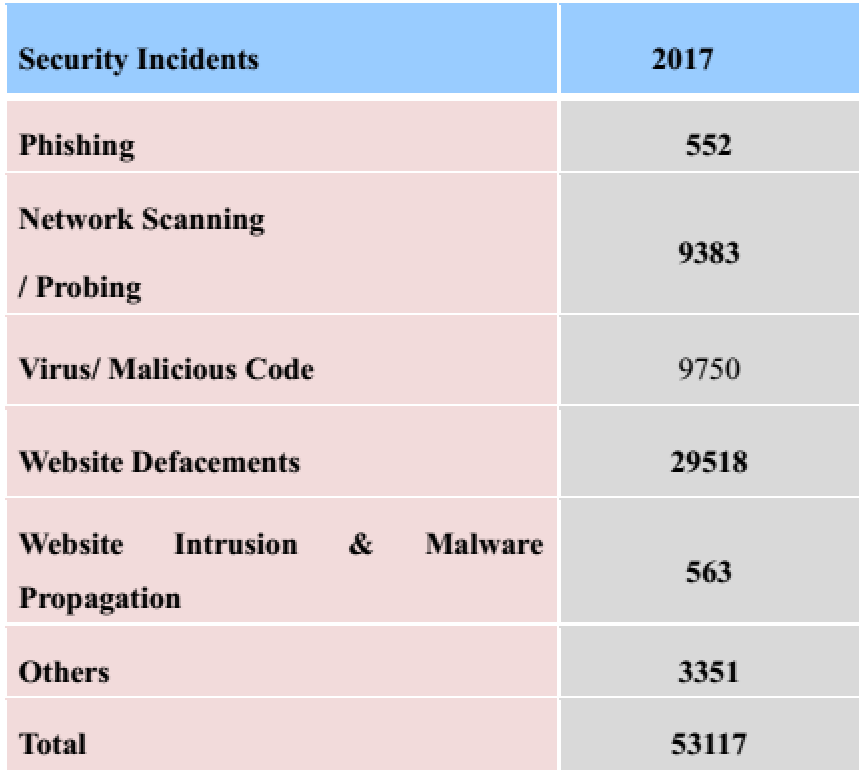
Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

Security Trends

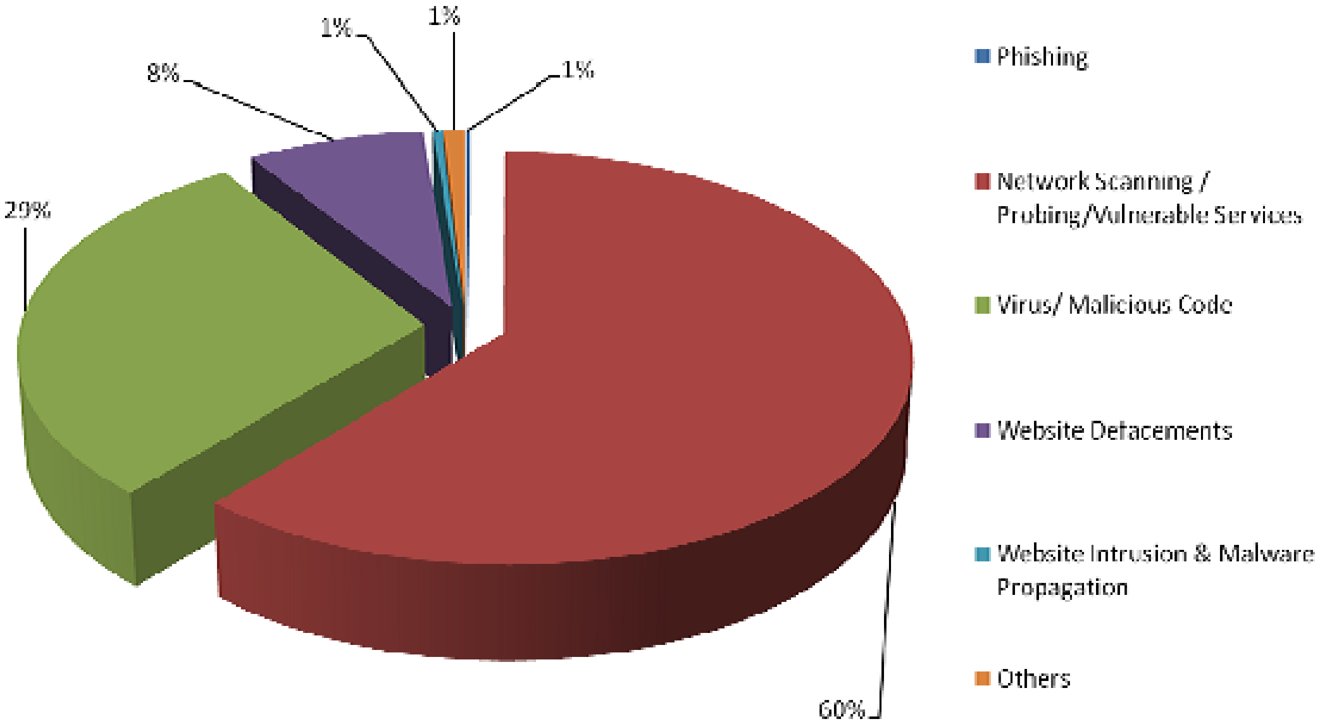


Summary of incidents handled by CERT-In during 2017



Security Incidents	2017
Phishing	552
Network Scanning / Probing	9383
Virus/ Malicious Code	9750
Website Defacements	29518
Website Intrusion & Malware Propagation	563
Others	3351
Total	53117

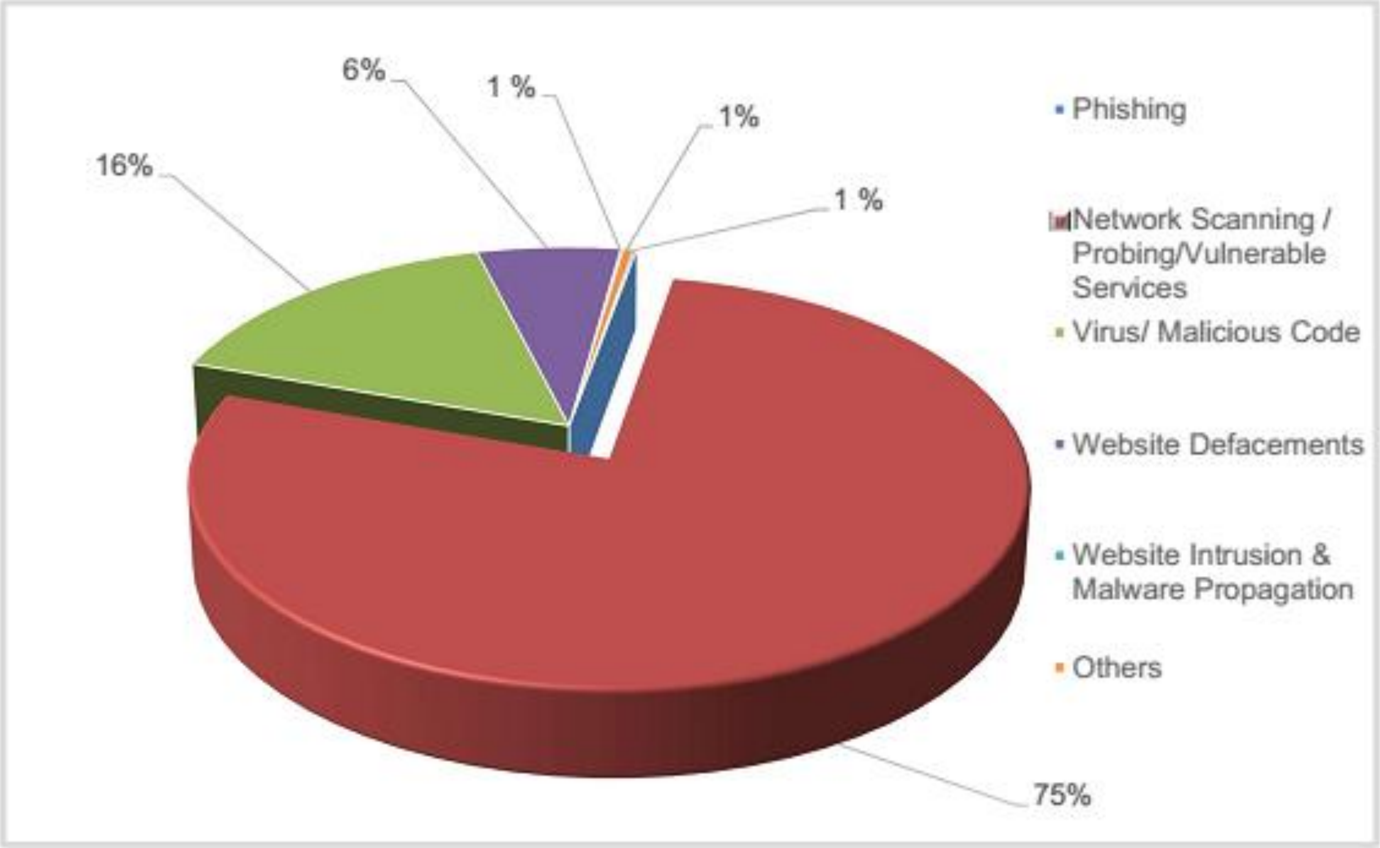
Security Trends



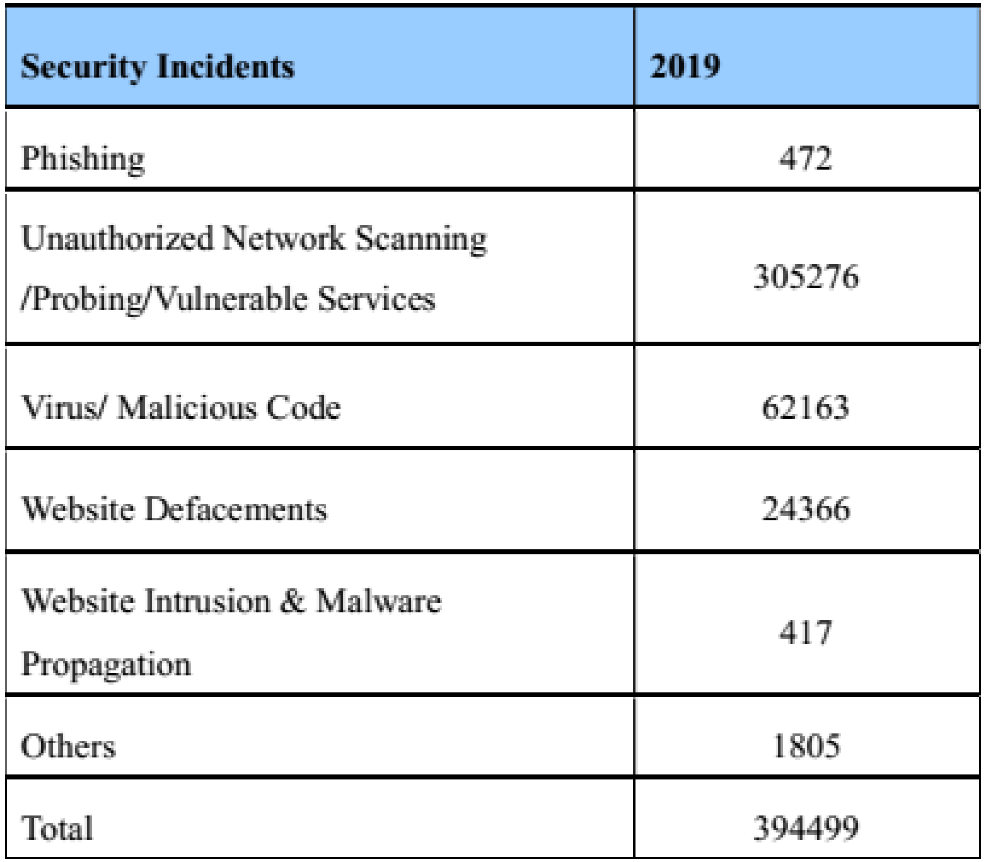
Summary of incidents handled by CERT-In during 2018

Security Incidents	**2018**
Phishing	**454**
Network Scanning / Probing/Vulnerable Services	**127481**
Virus/ Malicious Code	**61055**
Website Defacements	**16655**
Website Intrusion & Malware Propagation	**905**
Others	**1906**
Total	**208456**

Security Trends



Summary of incidents handled by CERT-In during 2019

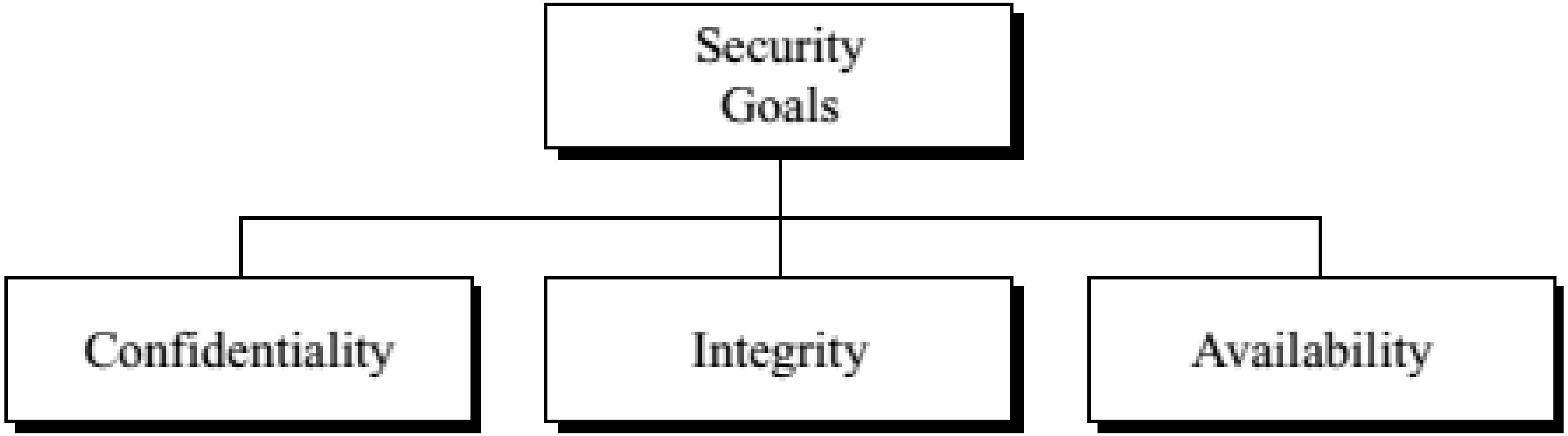


Security Incidents	**2019**
Phishing	472
Unauthorized Network Scanning /Probing/Vulnerable Services	305276
Virus/ Malicious Code	62163
Website Defacements	24366
Website Intrusion & Malware Propagation	417
Others	1805
Total	394499

Security Goals

- We are living in the information age.
- We need to keep information about every aspect of our lives.
- In other words, information is an asset that has a value like any other asset.
- As an asset, information needs to be secured from attacks.
- To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).

SECURITY GOALS



Security Goals

Confidentiality

Integrity

Availability

SECURITY GOALS

- Confidentiality
  - Need to protect our confidential information.
  - An organization needs to guard against those malicious actions that endanger the confidentiality of its information
  - In the 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 not only applies to the storage of the information, it also applies to the transmission of information.
  - When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission

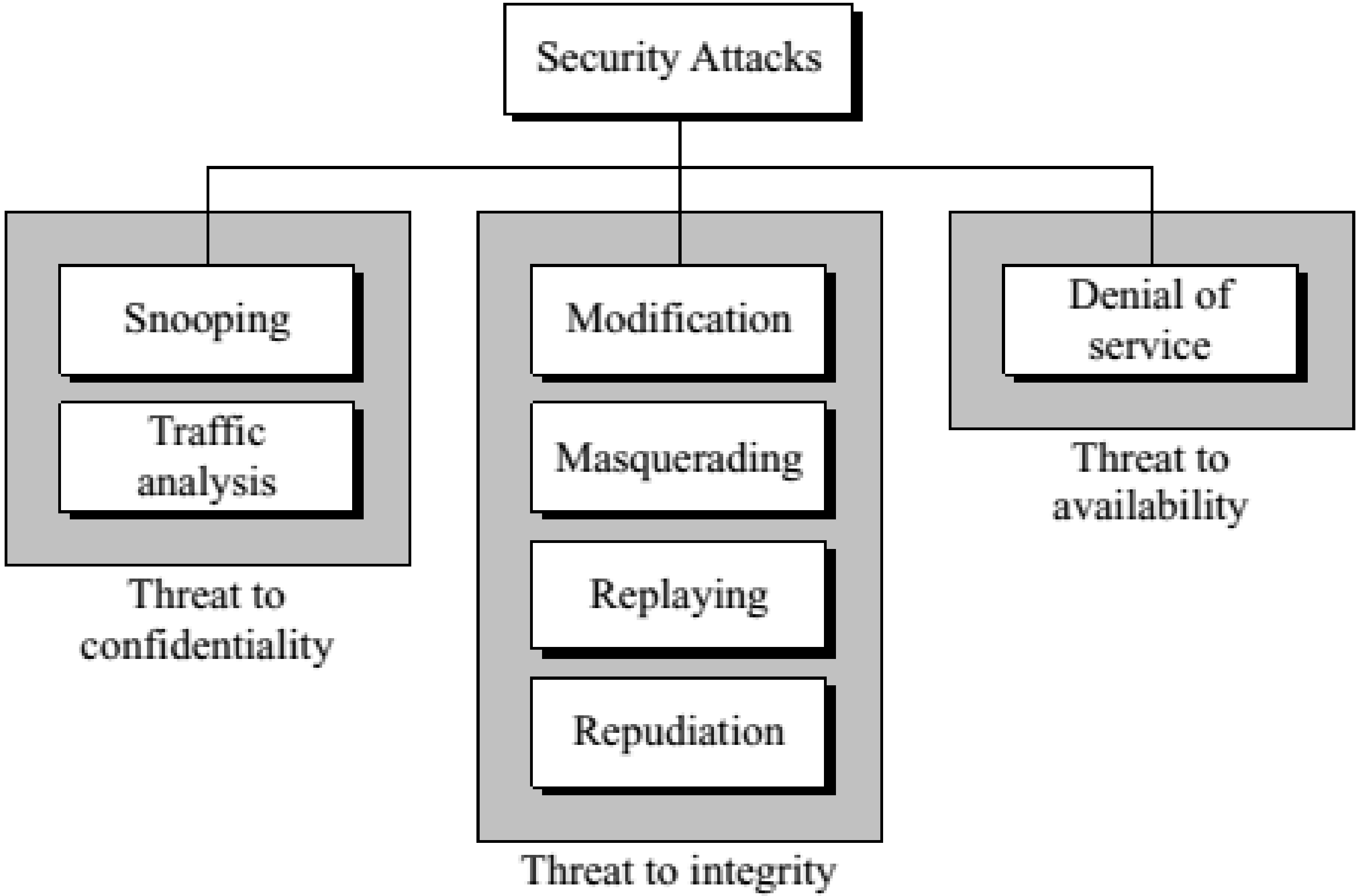
SECURITY GOALS

- 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 violation is not necessarily the result of a malicious act.
  - An interruption in the system, such as a power surge, may also create unwanted changes in some information.

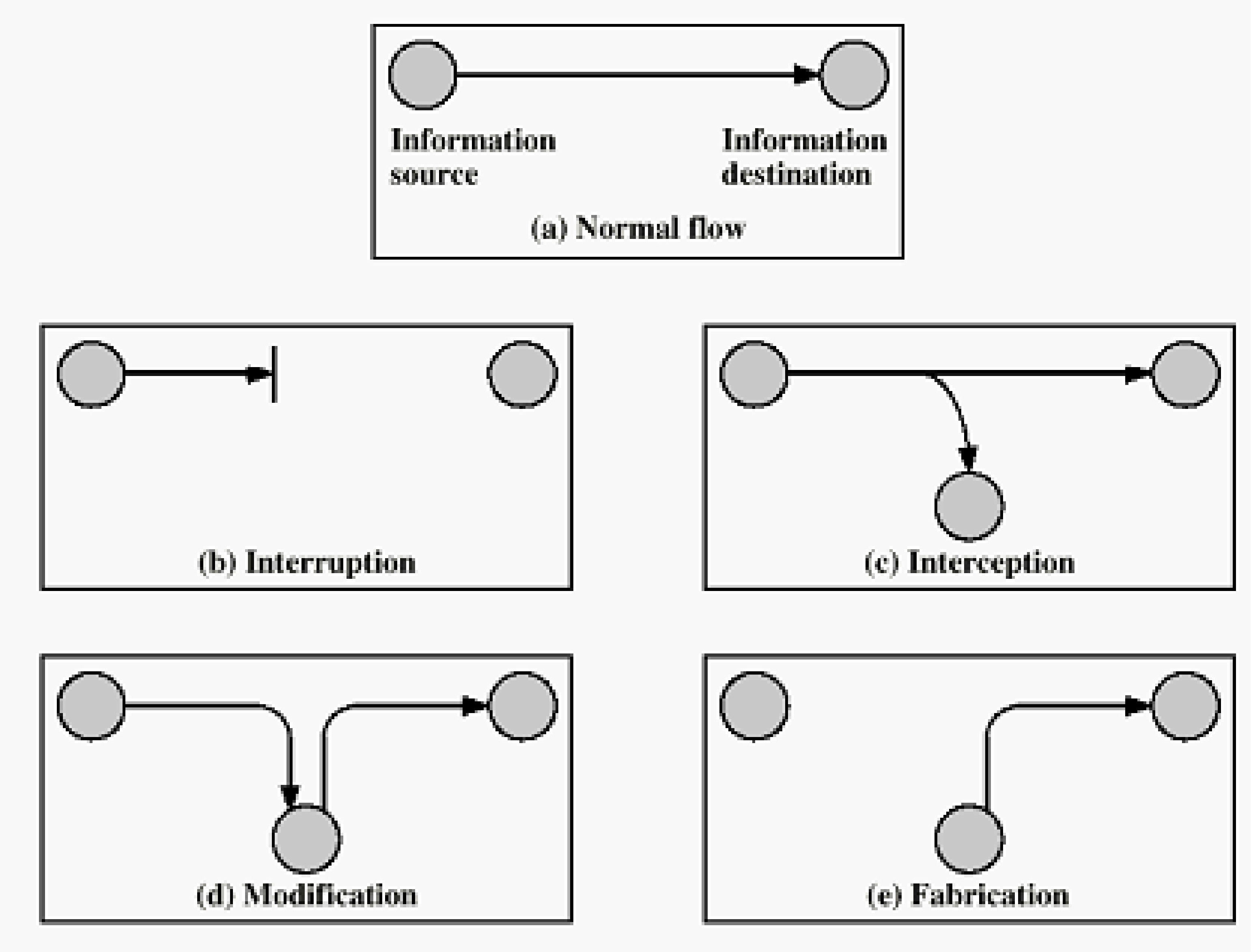
SECURITY GOALS

- 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 needs to be constantly changed, which means it must be accessible to authorized entities.
  - The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity.
  - Imagine what would happen to a bank if the customers could not access their accounts for transactions.

ATTACKS

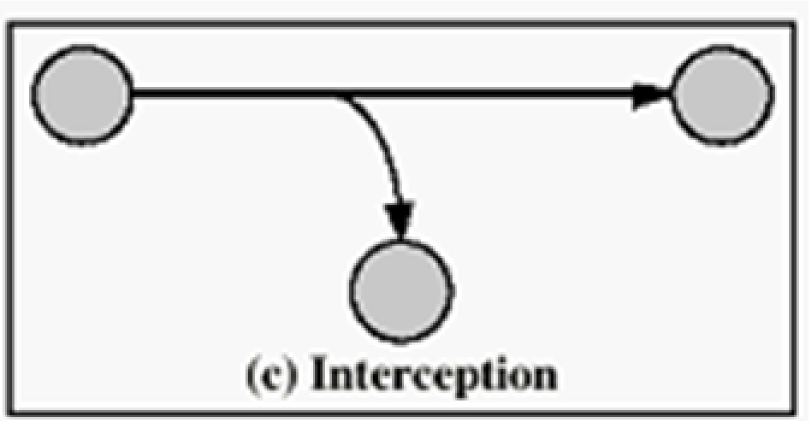

Security Attacks
Snooping
Traffic analysis
Threat to confidentiality
Modification
Masquerading
Replaying
Repudiation
Threat to integrity
Denial of service
Threat to availability

ATTACKS


Information source
Information destination
(a) Normal flow
(b) Interruption
(c) Interception
(d) Modification
(e) Fabrication

Attacks Threatening Confidentiality

- Snooping
  - Snooping refers to unauthorized access to or interception of data.
  - For example, a file transferred through the Internet may contain confidential information.
  - An unauthorized entity may intercept the transmission and use the contents for her own benefit.
  - To prevent snooping, the data can be made non-intelligible to the intercepter by using encipherment techniques



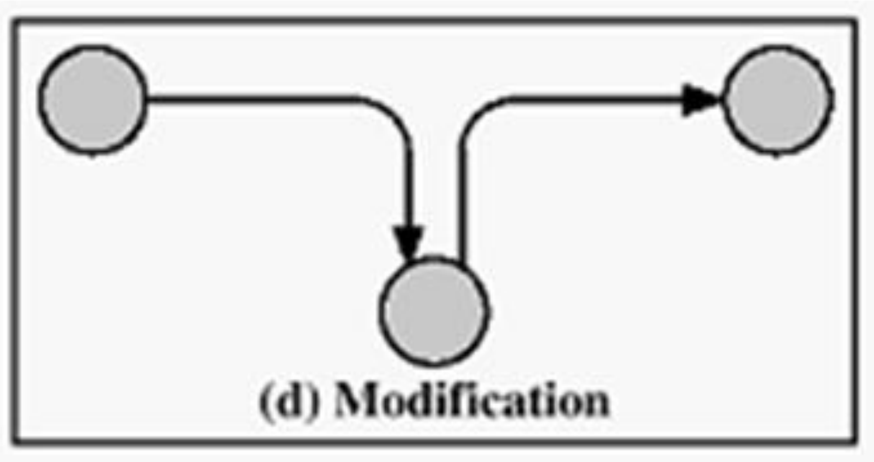
Attacks Threatening Confidentiality

- Traffic Analysis
  - Although encipherment of data may make it nonintelligible for the intercepter, one can obtain some other type information by monitoring online traffic.
  - For example, he/she can find the electronic address (such as the e-mail address) of the sender or the receiver.
  - He/She can collect pairs of requests and responses to help him/her guess the nature of transaction.

Traffic analysis
H

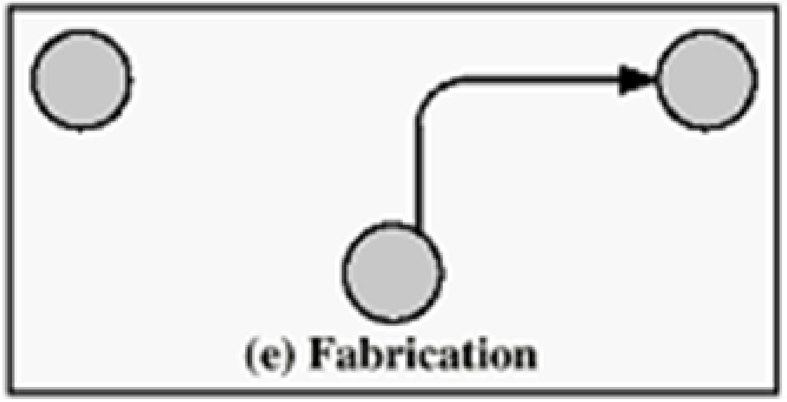
Attacks Threatening Integrity

- Modification
  - After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.
  - For example, a customer sends a message to a bank to do some transaction.
  - The attacker intercepts the message and changes the type of transaction to benefit herself.
  - Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.



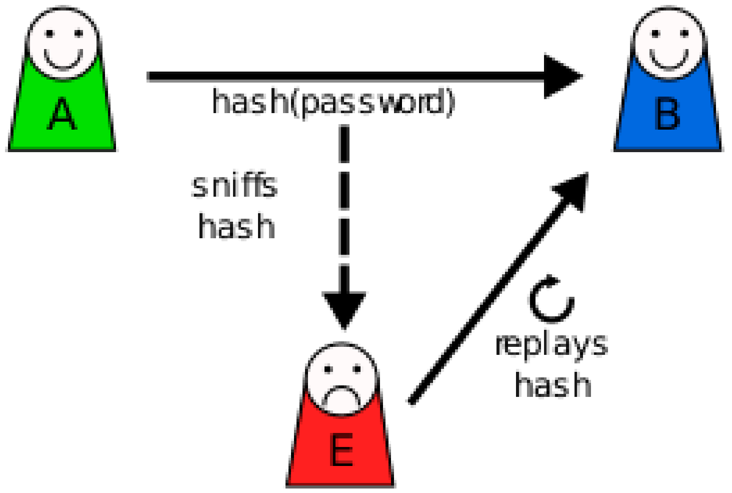
Attacks Threatening Integrity

- Masquerading
  - Masquerading, or spoofing, happens when the attacker impersonates somebody else.
  - For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer.
  - Sometimes the attacker pretends instead to be the receiver entity.
  - For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.



Attacks Threatening Integrity

- Replaying
  - Replaying is another attack.
  - The attacker obtains a copy of a message sent by a user and later tries to replay it.
  - For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her.
  - The attacker intercepts the message and sends it again to receive another payment from the bank.

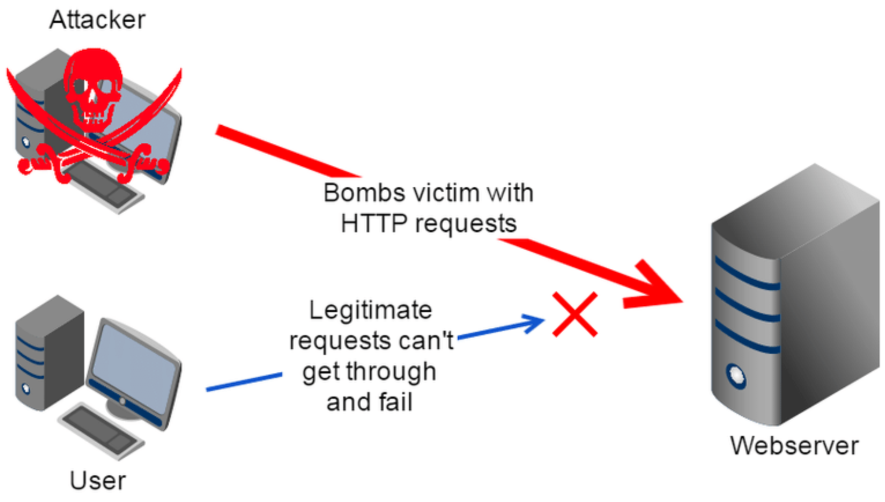


Attacks Threatening Integrity

- Repudiation
  - This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.
  - The 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.
  - An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request.
  - An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

Attacks Threatening Availability

- Denial of Service
  - Denial of service (DoS) is a very common attack.
  - It may slow down or totally interrupt the service of a system.
  - The attacker can use several strategies to achieve this.
  - He/She might send so many bogus requests to a server that the server crashes because of the heavy load.
  - The attacker might intercept and delete a server’s response to a client, making the client to believe that the server is not responding.
  - The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

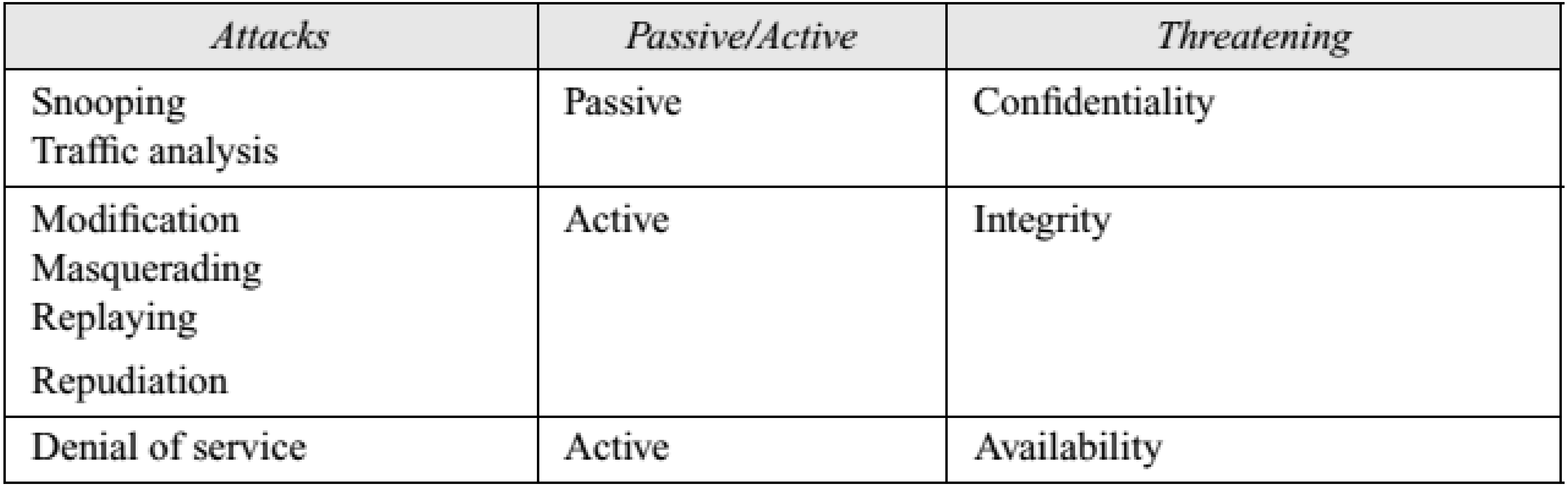
Passive Versus Active Attacks

- Passive Attacks
  - In a passive attack, the attacker’s goal is just to obtain information.
  - This means that the attack does not modify data or harm the system.
  - However, the attack may harm the sender or the receiver of the message.
  - Attacks that threaten confidentiality, snooping and traffic analysis, are passive attacks.
  - The revealing of the information may harm the sender or receiver of the message, but the system is not affected.
  - For this reason, it is difficult to detect this type of attack until the sender or receiver finds out about the leaking of confidential information.
  - Passive attacks, however, can be prevented by encipherment of the data.

Passive Versus Active Attacks

- Active Attacks
  - An active attack may change the data or harm the system.
  - Attacks that threaten the integrity and availability are active attacks.
  - Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

Passive Versus Active Attacks



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