CRYPTOGRAPYHY AND NETWORK SECUIRTY

20CS6302

Mukesh Chinta

Asst Prof, Dept of CSE

VRSEC

Basic Building Blocks

- **Data:** raw facts {Alphanumeric, image, audio, and video}
- **Information:** result of processing, manipulating and organizing data in a way that adds to the knowledge of the receiver. *{Processed Data}*
- **Knowledge:** Knowledge is normally processed by means of structuring, grouping, filtering, organizing or pattern recognition. *{Highly structured information}*

An ***Information System*** is a set of interrelated components that collect or retrieve, process, store and distribute information to support decision making and control in an organization.

'Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected'

BS ISO 27002:2005

Need for Security!!!

- **Security is one of the oldest problem** that governments, commercial organizations and almost every person has to face. The need of security exists since information became a valuable resource.

- Introduction of computer systems to business has escalated the security problem even more.

- The advances in networking and specially in distributed systems made the need for security even greater.

- Any breach with the Information System will lead to **Loss of productivity, loss of revenue, legal liabilities, loss of reputation and other losses.**

- **Cyber crime** is defined as criminal activity involving the IT infrastructure, including illegal access, illegal interception, data interference, misuse of devices, ID theft and electronic fraud

What is Information Security ???

The U.S. Government's National Information Assurance Glossary defines **INFOSEC** as:

> *"Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats."*

Computer Security

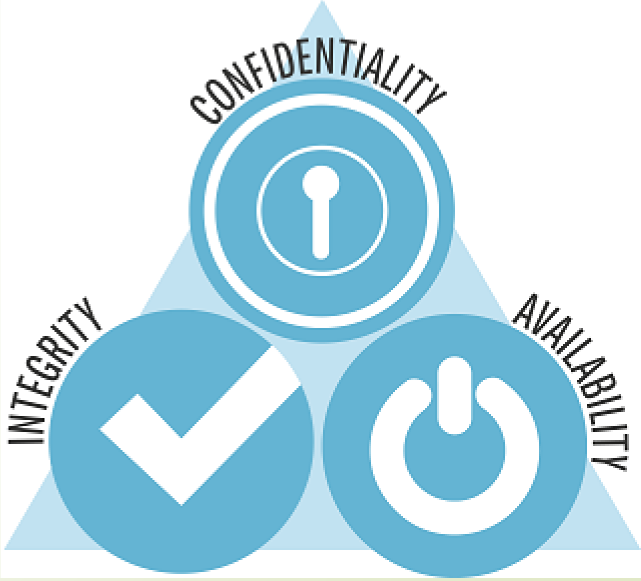
The NIST (National Institute of Standards & Technology} Computer Security Handbook [NIST95] (Available from: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf) defines the term computer security as

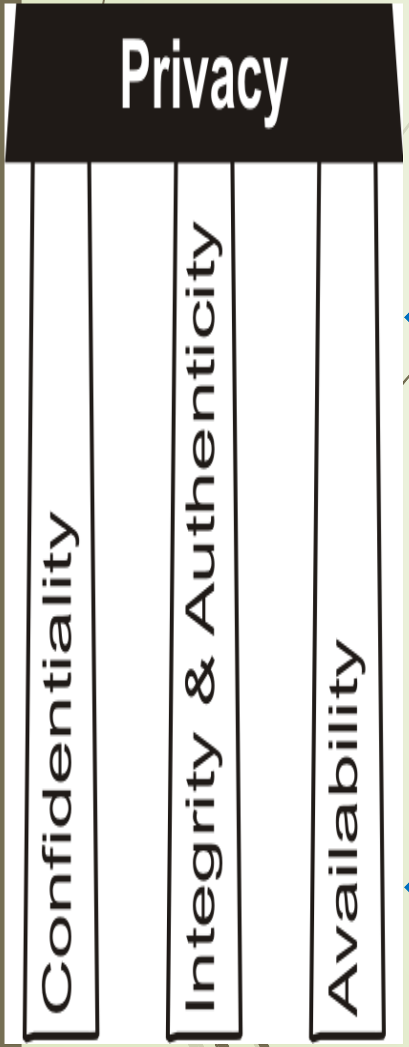
The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

The definition introduces three key objectives that are at the heart of the computer security:

- **Confidentiality**
  - Data Confidentiality
  - Privacy
- **Integrity**
  - Data Integrity
  - System Integrity
- **Availability**

CONFIDENTIALITY
AVAILABILITY
CIA TRIAD
INTEGRITY





- 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
  - **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.

Security Objectives

Federal Information Processing Standards Publications *(FIPS PUB 199)* provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

- **Confidentiality**: 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:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- **Availability:** 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.

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

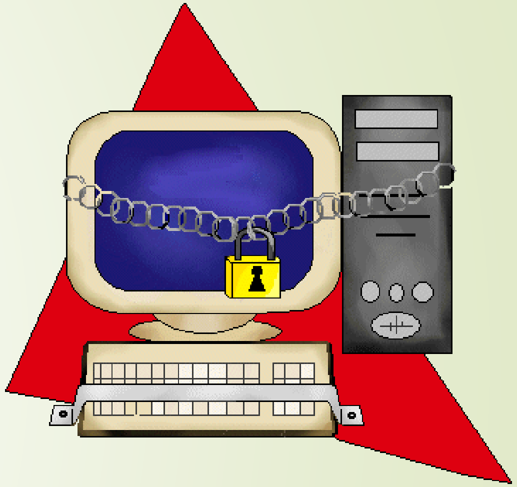
Levels of Security Breach

FIPS PUB 199 define three levels of impact on organizations or individuals should there be a breach of security : Low, Moderate and High

	LOW	MODERATE	HIGH
Effect on organizational operations, assets or individuals	Limited	Serious	Severe or even catastrophic
Primary functions of the organization and their effectiveness	Minor degradation	Significant degradation	Severe degradation
Damage to organizational assets	Minor	Significant	Major
Financial Loss	Minor	Significant	Major
Harm to individual	Minor	Significant	Severe (loss of life or life-threatening injuries)

Challenges of Computer Security

1. Not simple – seems to be straight forward but very complex
2. Must consider potential attacks on security features
3. Procedures used are often counter-intuitive
4. Involves multiple algorithms and secret information
5. Must decide where to deploy security mechanisms
6. Battle of wits between attacker / admin
7. Not perceived on benefit until a security failure happens
8. Requires regular/constant monitoring which is difficult
9. Often an after-thought rather than an integral part of the process
10. Strong security is regarded as impediment to free usage of a system



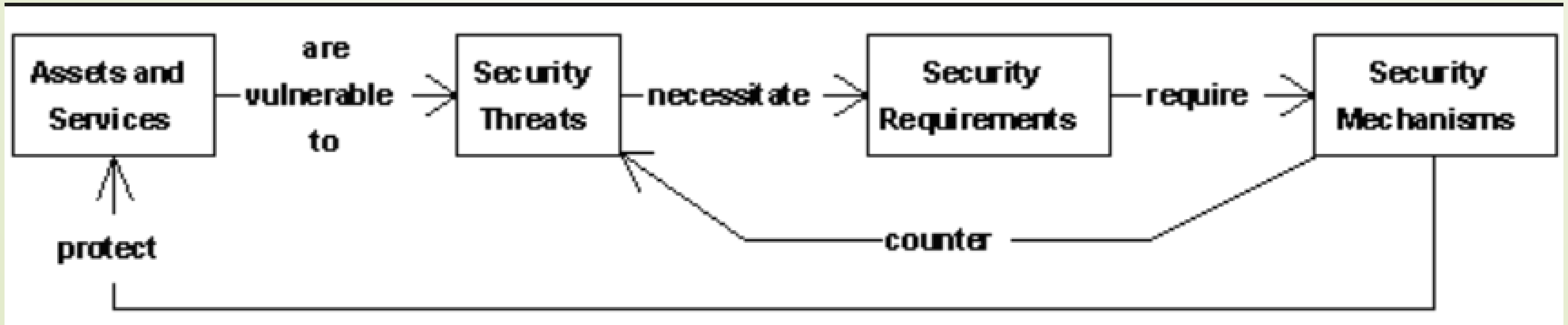
OSI Security Architecture

ITU-T X.800 “Security Architecture for OSI” defines a systematic way of defining and providing security requirements. Three important aspects of OSI security architecture are:

Security Attack: Any action that compromises the security of information owned by an organization.

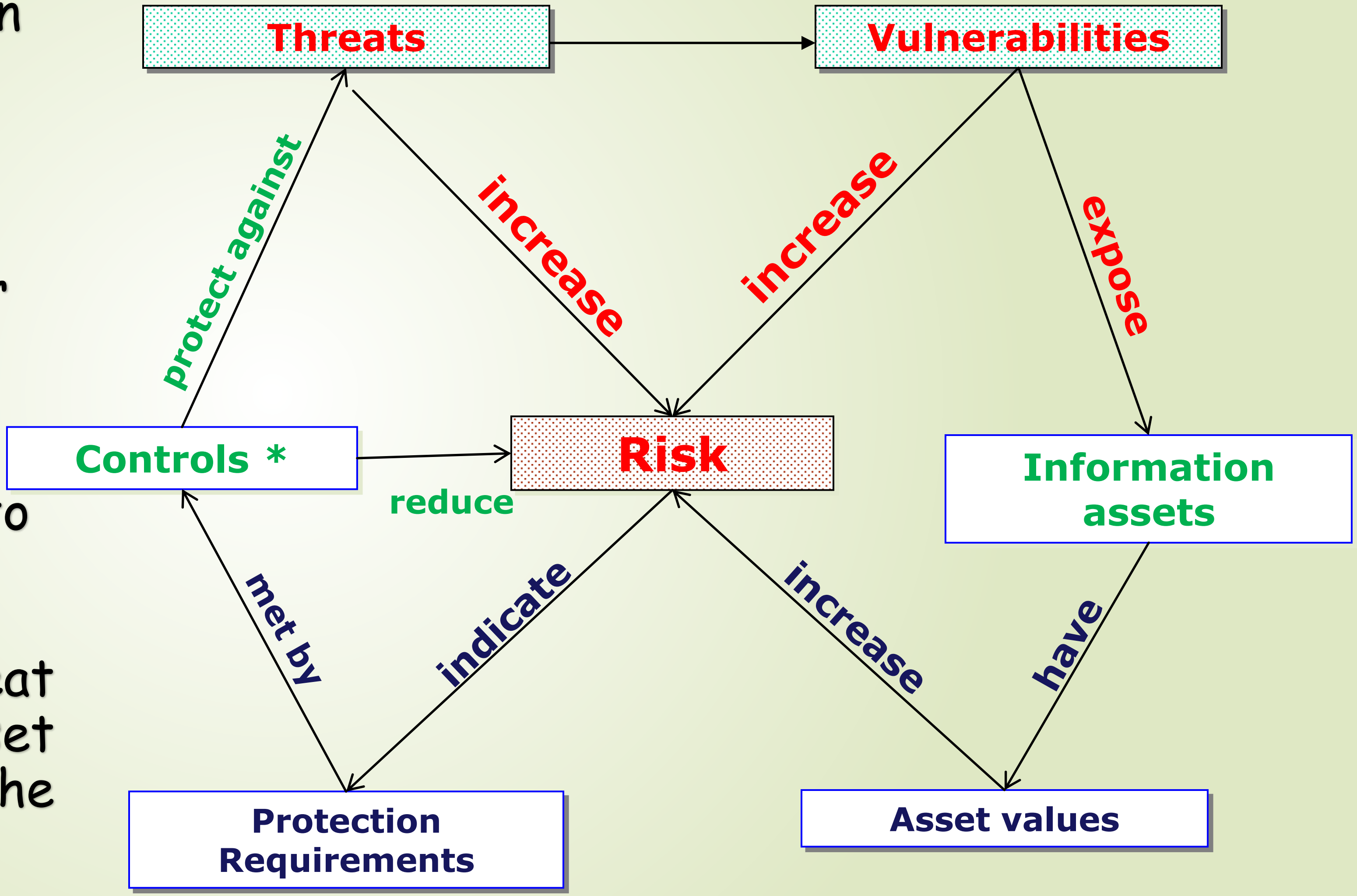
Security Mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security Service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

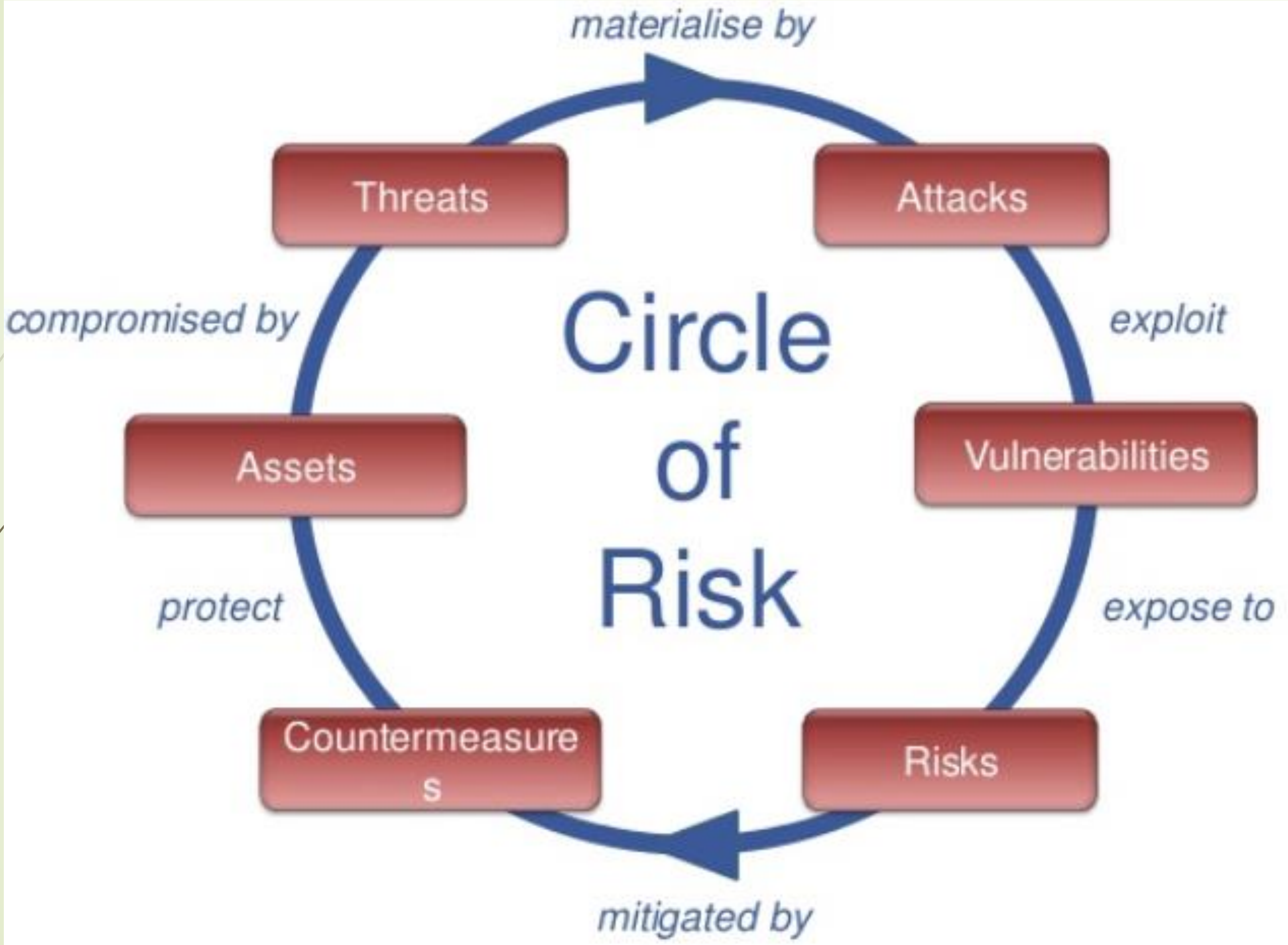


Threat, Vulnerability, Attack & Risk

- *Threat* – a potential for violation of security
- *Vulnerability* – Something that can potentially cause damage to the organization, IT Systems or network
- *Attack* – an assault on system security, a deliberate attempt to evade security services
- Risk: A possibility that a threat exploits a vulnerability in an asset and causes damage or loss to the asset.



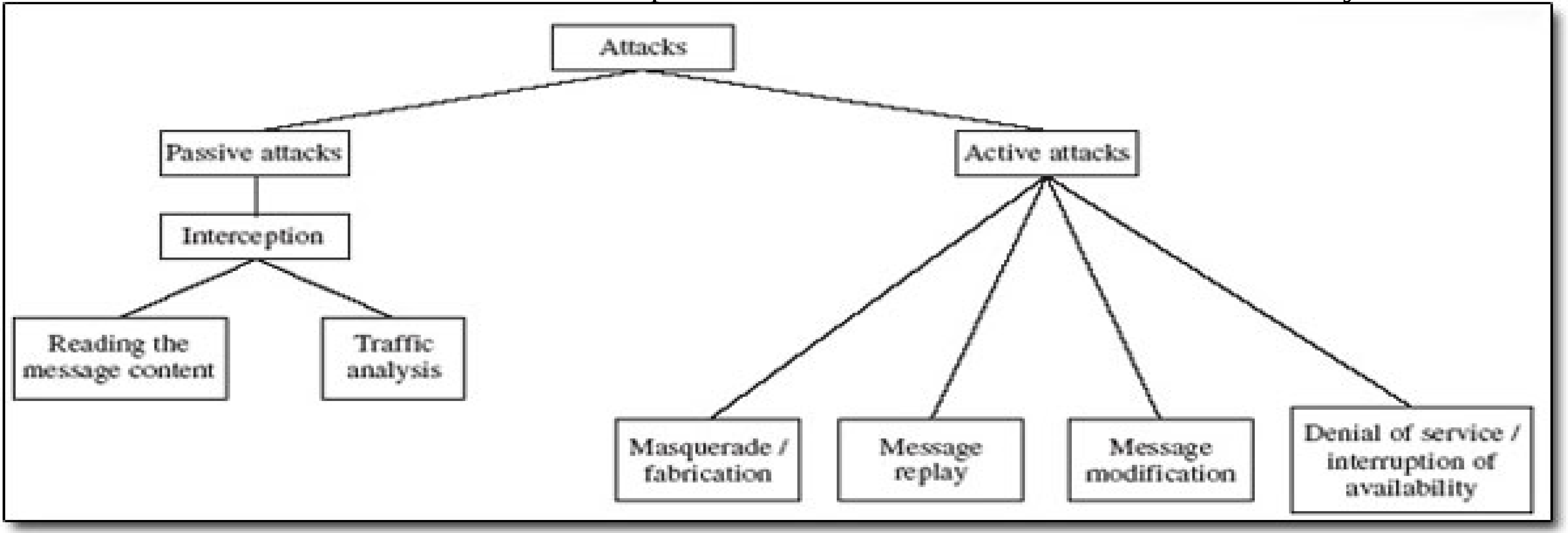
Relationship between Risk, Threats, and Vulnerabilities


materialise by
Threats
Attacks
compromised by
Circle of Risk
exploit
Assets
Vulnerabilities
protect
expose to
Countermeasure
s
Risks
mitigated by

Security Attacks

The security attacks are classified into **passive attacks** and **active attacks**

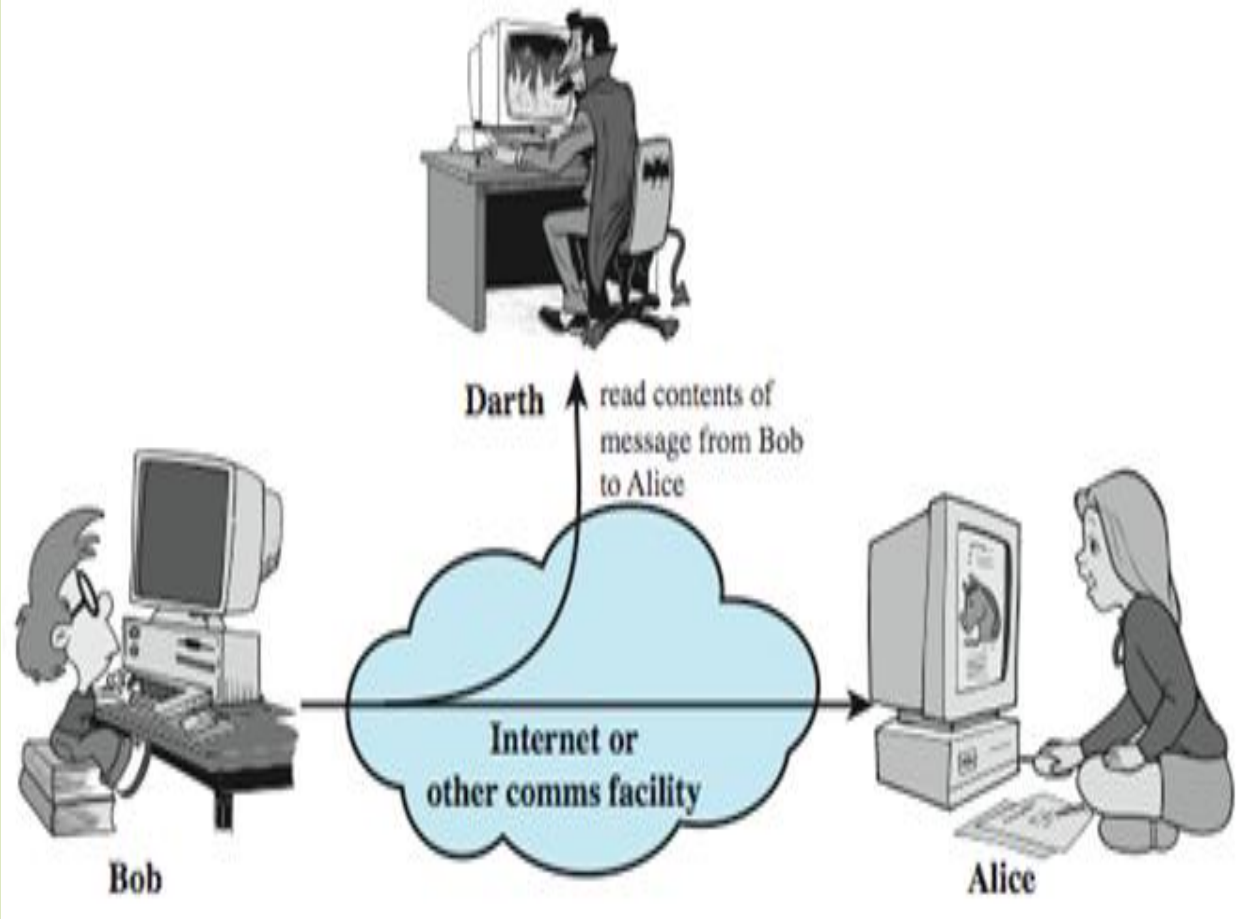
- A passive attack attempts to learn or make use of information from the system but does not affect system resources. These are difficult to detect and focus will be on prevention.
- Active attacks involve some modification of the data stream or the creation of a false stream. These are difficult to prevent and focus is on detection and recovery.



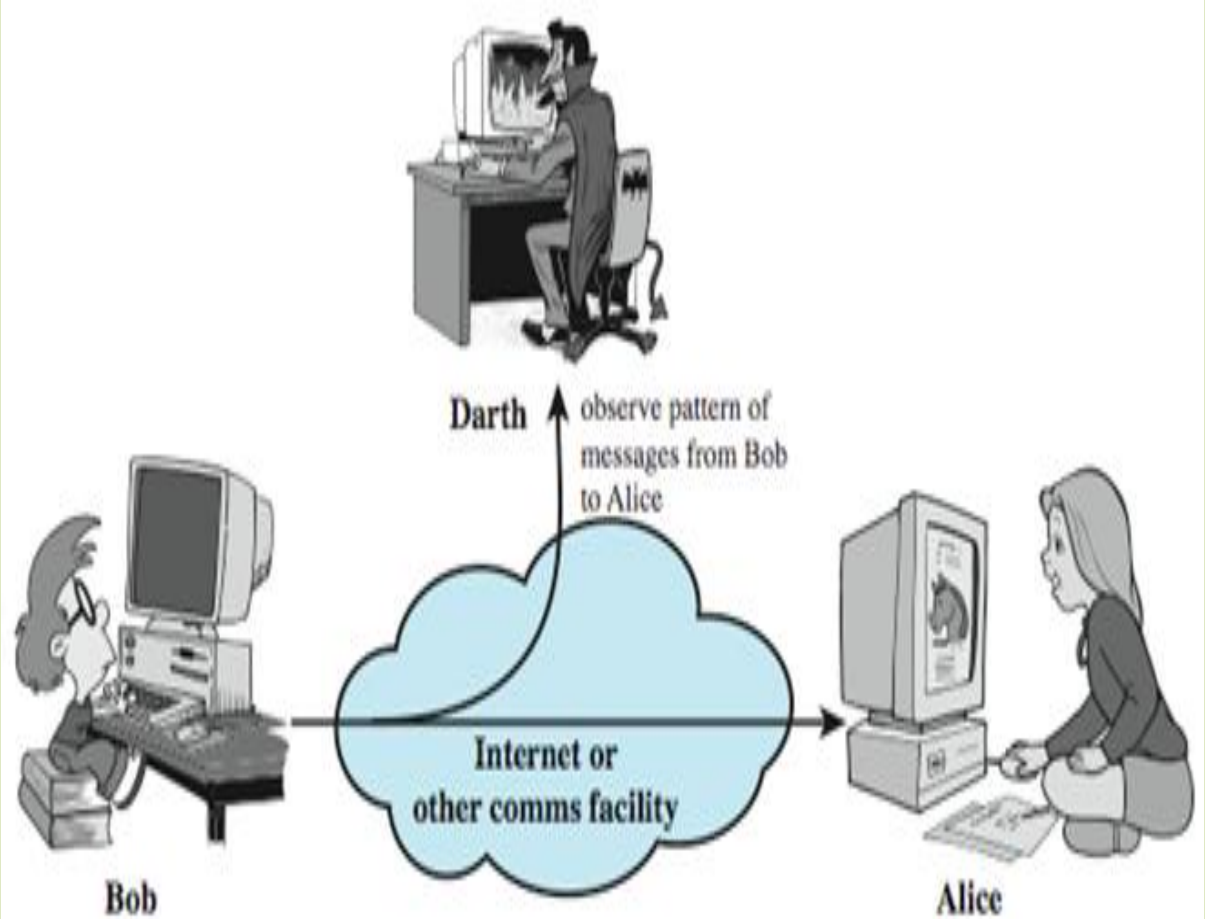
Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are:

- Release of message contents – Any transferred message could be intercepted or listened to
- Traffic analysis - monitor traffic flow to determine location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.



Release of Message Contents



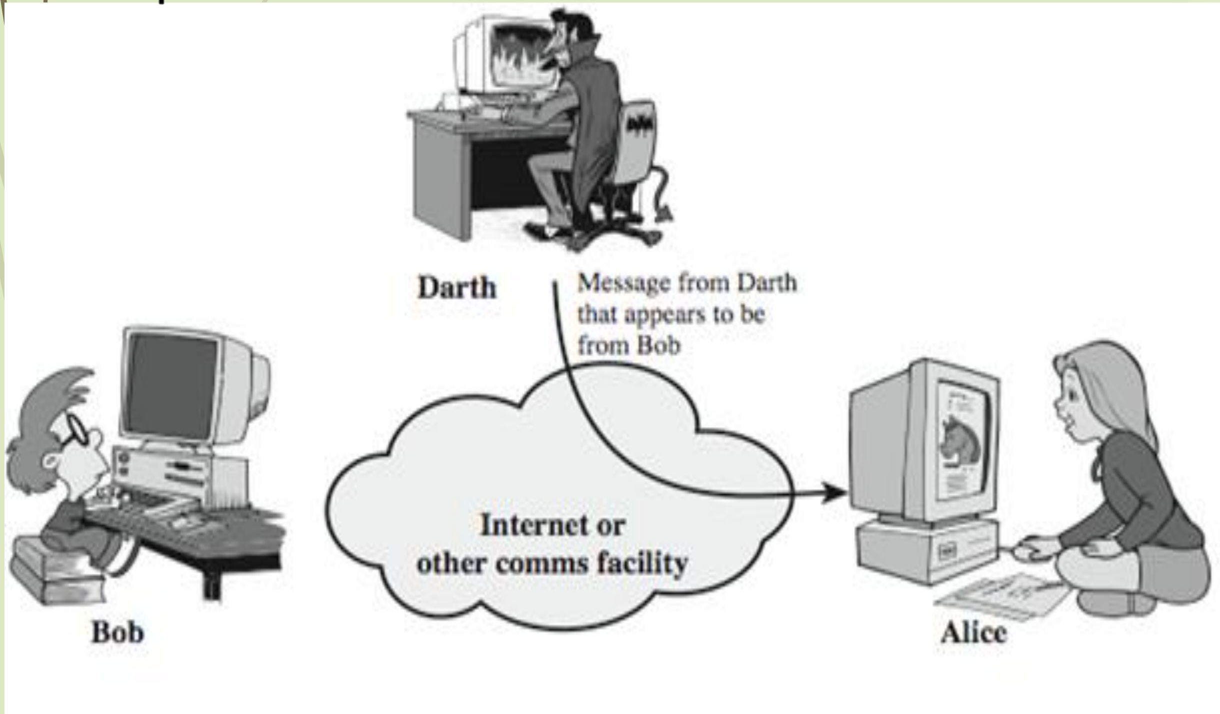
Traffic Analysis

Active Attacks

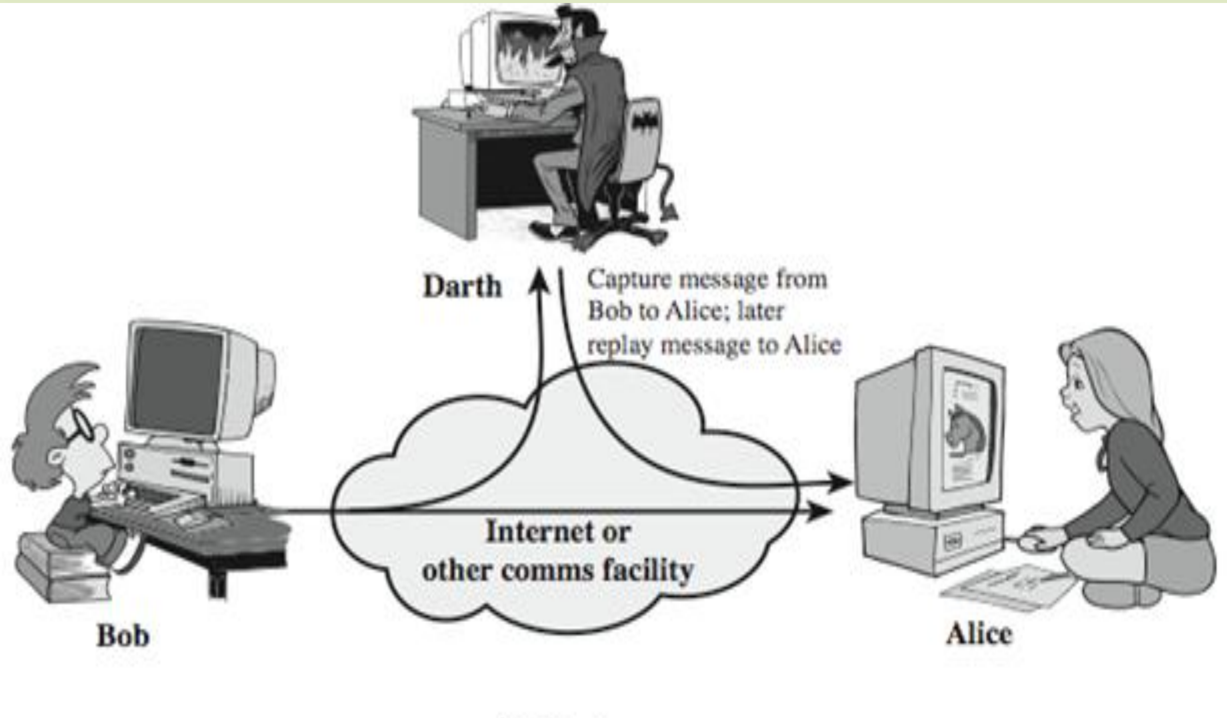
An **active attack** is one in which an unauthorized change of the system is attempted. This could include, for example, the modification of transmitted or stored data, or the creation of new data streams

Masquerade attacks relate to an entity (usually a computer or a person) taking on a false identity in order to acquire or modify information, and in effect achieve an unwarranted privilege status.

Message replay involves the re-use of captured data at a later time than originally intended in order to repeat some action of benefit to the attacker.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

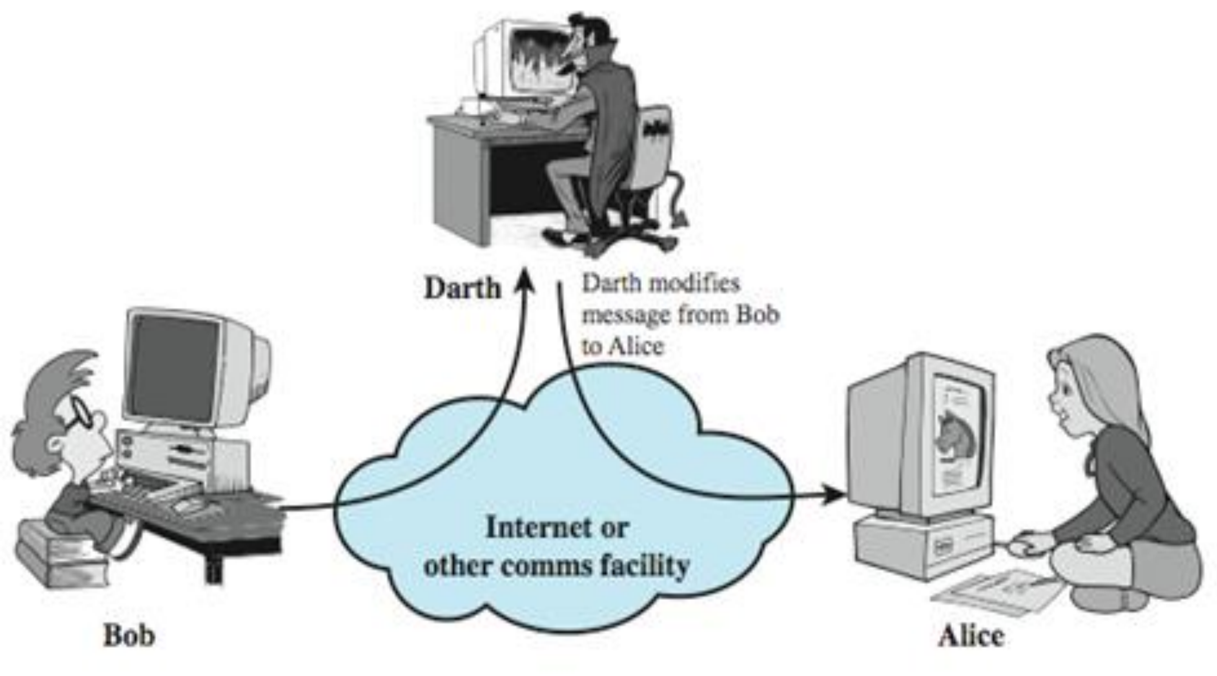

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

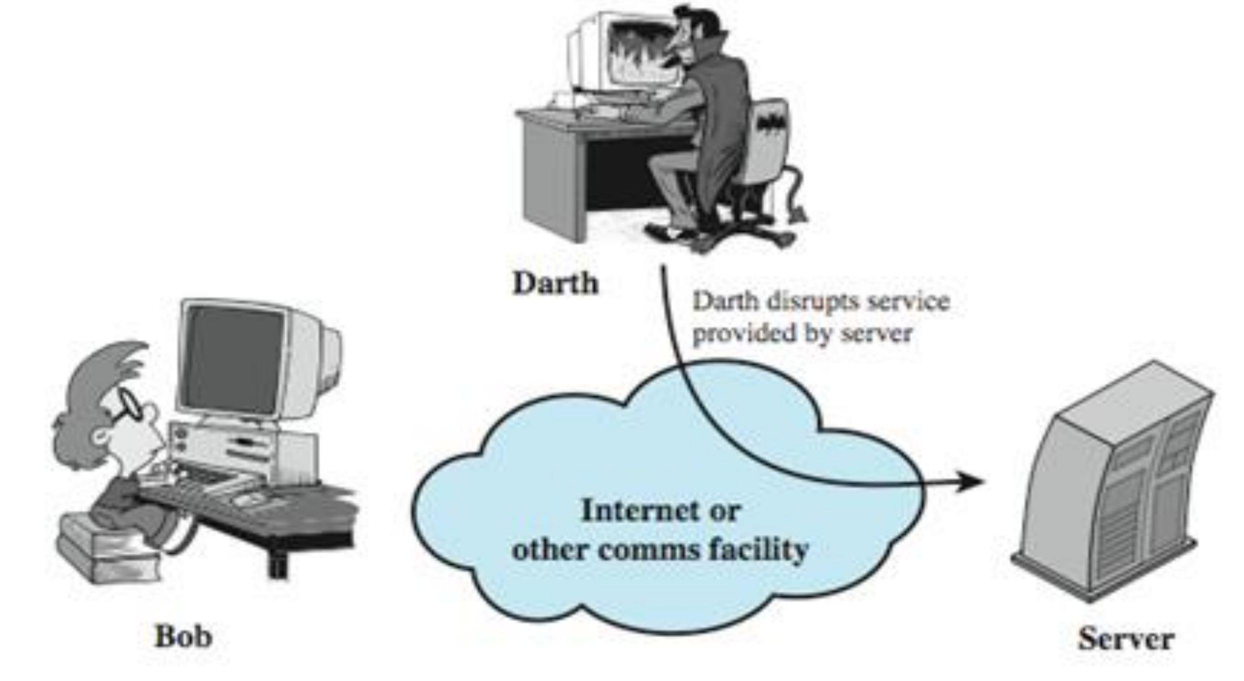
Active Attacks

Message modification could involve modifying a packet header address for the purpose of directing it to an unintended destination or modifying the user data.

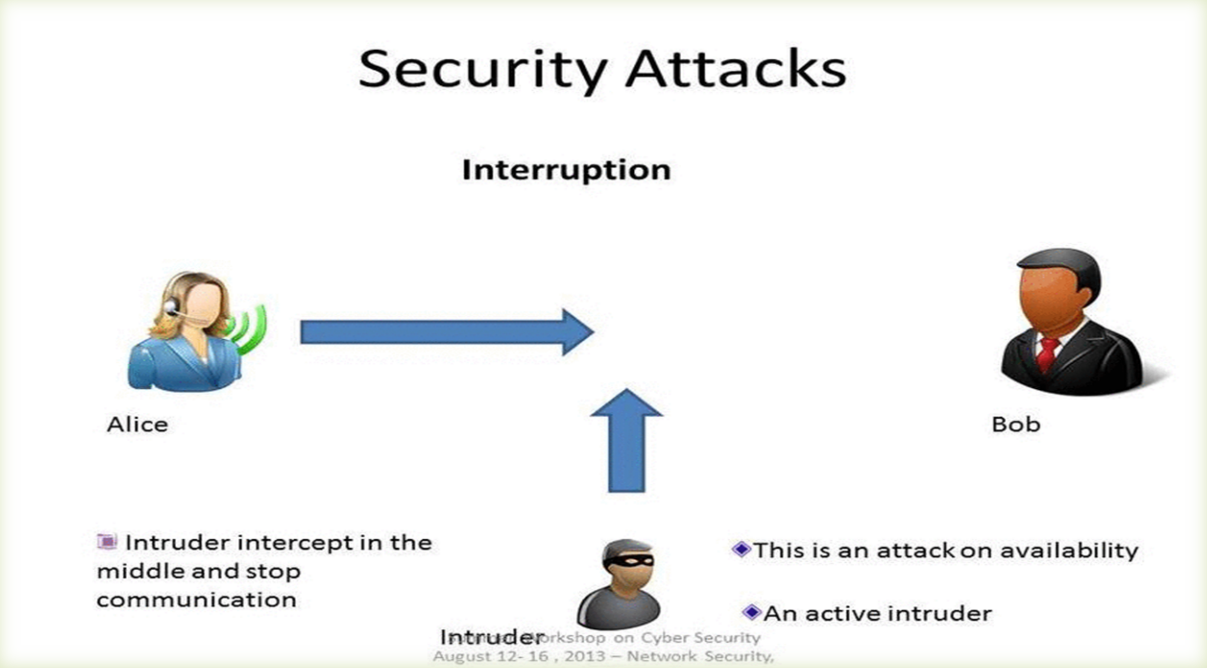
Denial-of-service attacks prevent the normal use or management of communication services, and may take the form of either a targeted attack on a particular service or a broad, incapacitating attack.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

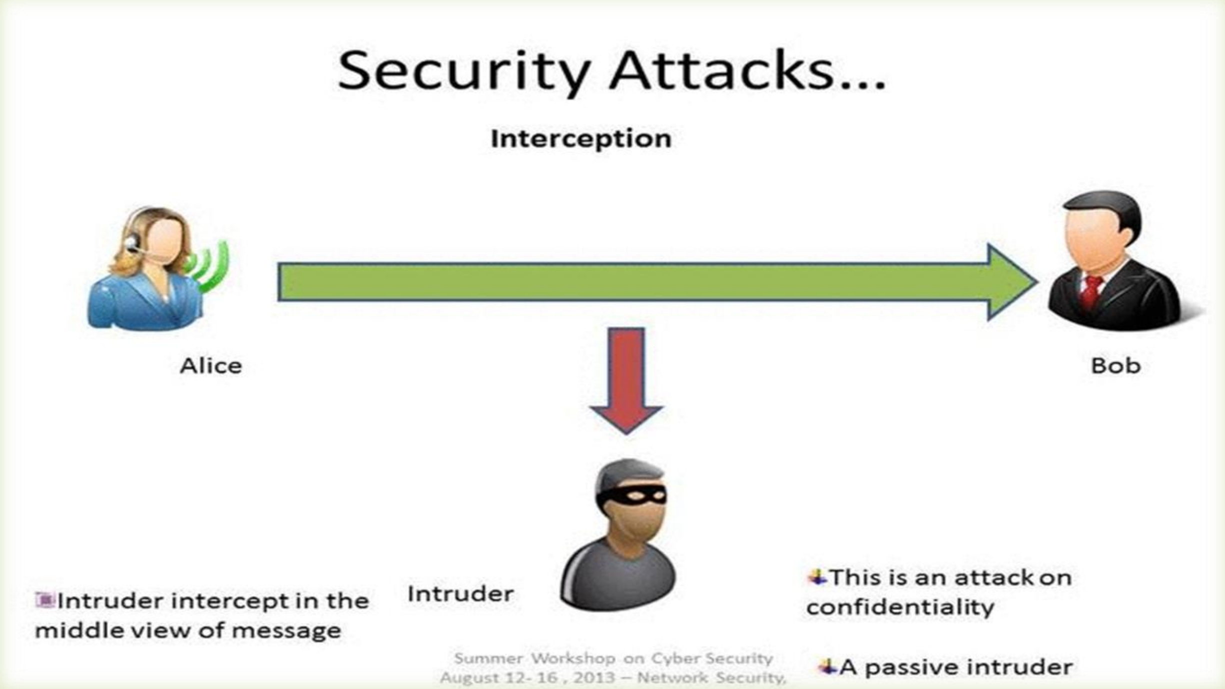


Security Attacks

Interruption

- Intruder intercept in the middle and stop communication

- This is an attack on availability
- An active intruder

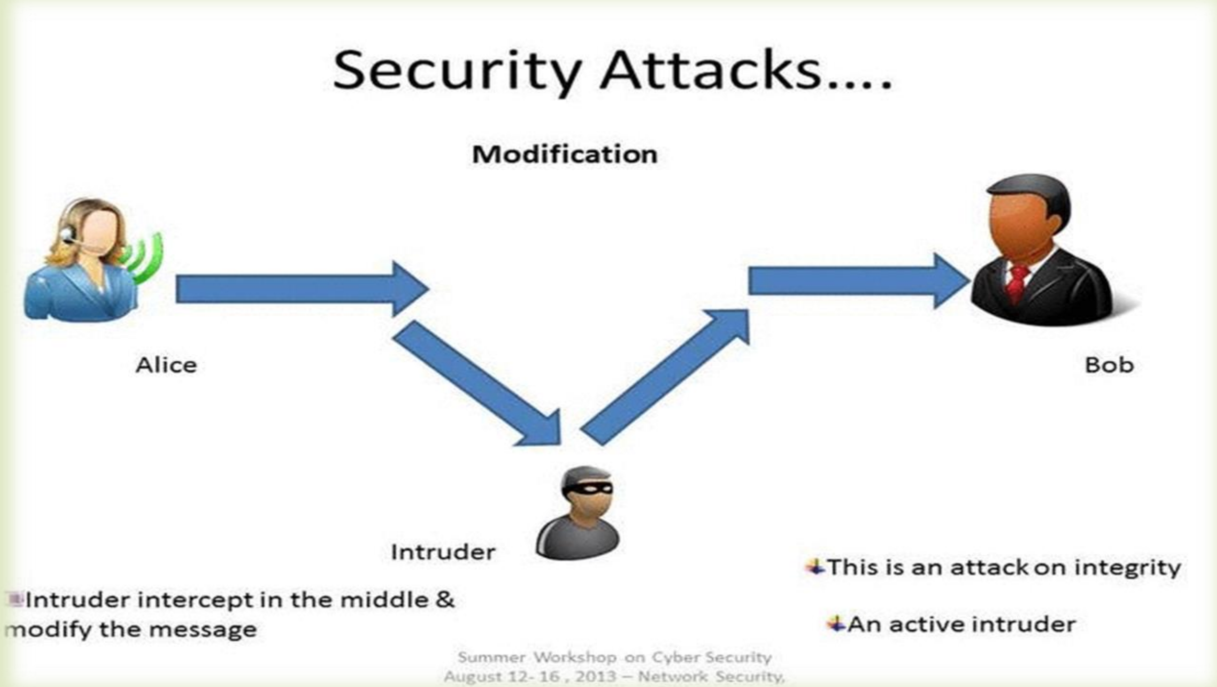


Security Attacks...

Interception

- Intruder intercept in the middle view of message

- This is an attack on confidentiality
- A passive intruder

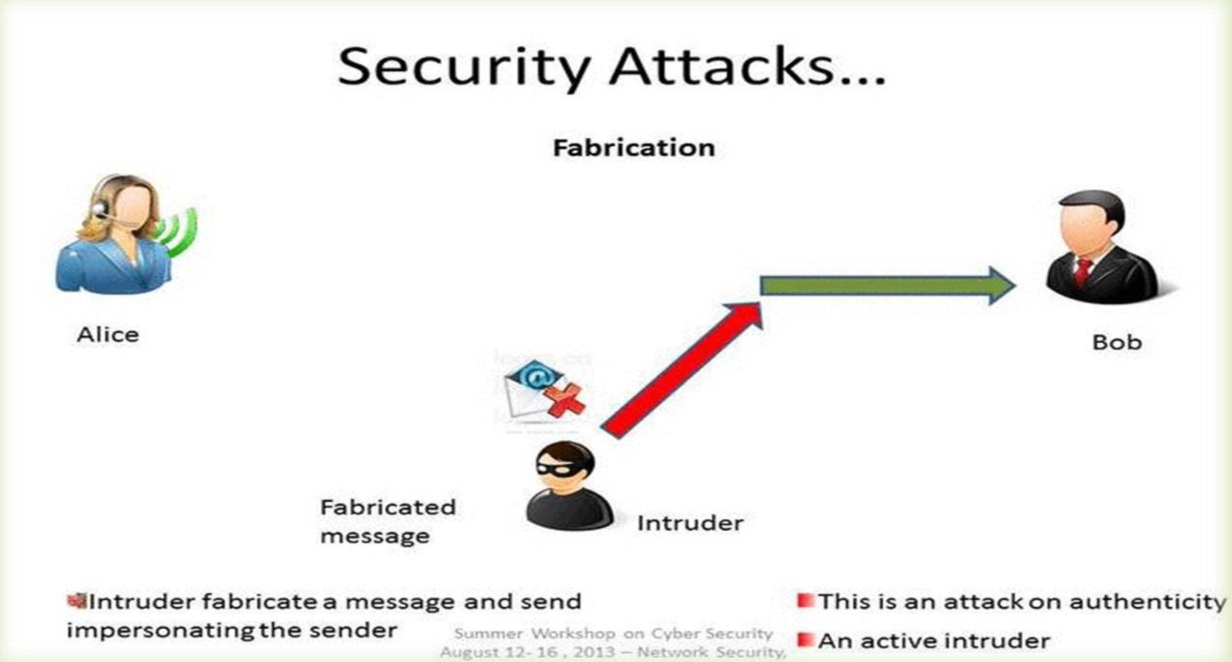


Security Attacks....

Modification

- Intruder intercept in the middle & modify the message

- This is an attack on integrity
- An active intruder



Security Attacks...

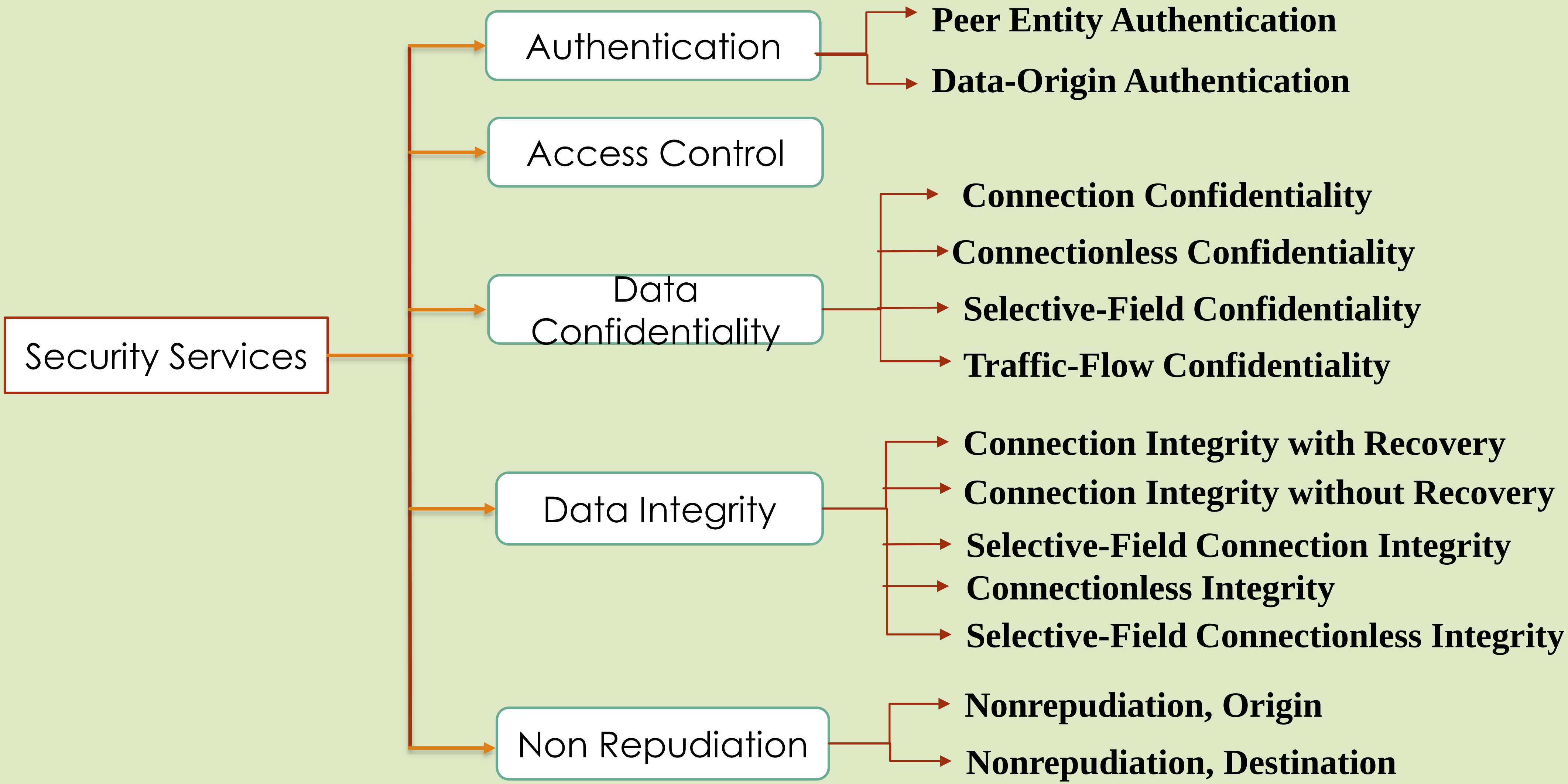
Fabrication

- Intruder fabricate a message and send impersonating the sender

- This is an attack on authenticity
- An active intruder

Security Services

RFC 2828 defines Security Service as a processing or communication service that is provided by a system to give a specific kind of protection to system resources.



- Security Services
  - Authentication
    - Peer Entity Authentication
    - Data-Origin Authentication
  - Access Control
  - Data Confidentiality
    - Connection Confidentiality
    - Connectionless Confidentiality
    - Selective-Field Confidentiality
    - Traffic-Flow Confidentiality
  - Data Integrity
    - Connection Integrity with Recovery
    - Connection Integrity without Recovery
    - Selective-Field Connection Integrity
    - Connectionless Integrity
    - Selective-Field Connectionless Integrity
  - Non Repudiation
    - Nonrepudiation, Origin
    - Nonrepudiation, Destination

X.800 divides security services into five categories and fourteen specific services. Security Services intend to counter security attacks and make use of one or more security mechanisms to provide the service

Security Services

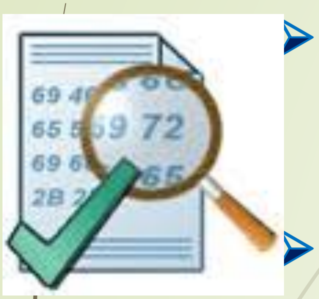
Authentication – Authentication service is concerned with assurance that communicating entity is the one claimed. It helps in establishing proof of identification. Two specific authentication services are defined:

- *Peer Entity Authentication* - provides corroboration of the identity of a peer entity in an association. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection.
- *Data Origin Authentication* - provides corroboration of the source of a data unit. In a connectionless transfer, provides assurance that the source of received data is as claimed

Data Confidentiality – It is the protection of transmitted data from passive attacks, and the protection of traffic flow from analysis.

- *Connection Confidentiality*: The protection of all user data on a connection
- *Connectionless Confidentiality*: The protection of all user data in a single data block
- *Selective-Field Confidentiality:* The confidentiality of selected fields within the user data on a connection or in a single data block
- *Traffic Flow Confidentiality:* The protection of the information that might be derived from observation of traffic flows

Security Services



Data Integrity – It assures that messages are received as sent by an authorized entity, with no duplication, insertion, modification, reordering, replay, or loss.

- *Connection Integrity with Recovery:* Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted
- *Connection Integrity without Recovery:* As above, but provides only detection without recovery.

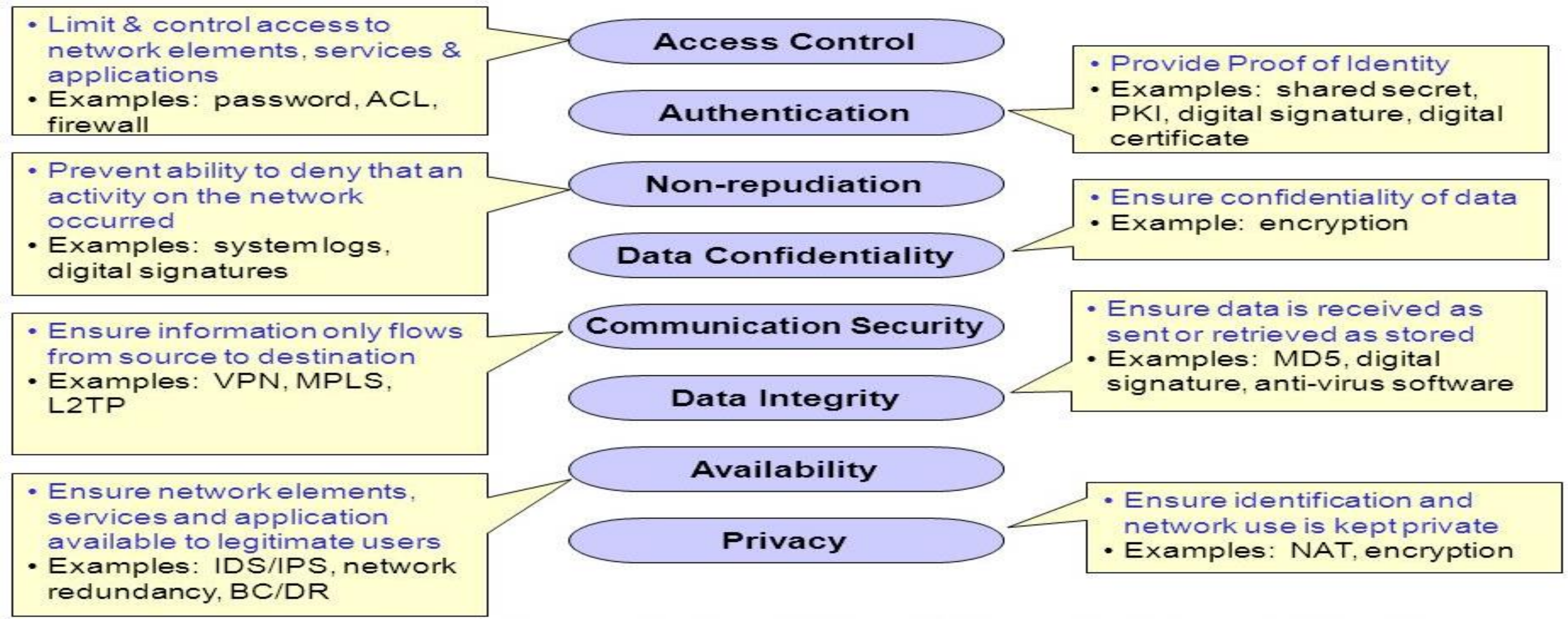
- *Selective-Field Connection Integrity:* Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- *Connectionless Integrity:* Provides for the integrity of a single connectionless data block and may take the form of detection of data modification.
- *Selective-Field Connectionless Integrity:* Provides for the integrity of selected fields within a single connectionless data block

Access Control – It is the ability to limit and control the access to host systems and applications via communications links. The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

Nonrepudiation: This service does not allow the sender or receiver of a message to refuse the claim of not sending or receiving that message.

- *Nonrepudiation, Origin*: Proof that the message was sent by the specified party.
- *Nonrepudiation, Destination*: Proof that the message was received by the specified part.

Availability - It is the property of a system / resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. A variety of attacks can result in the loss of or reduction in availability.



Access Control
- Limit & control access to network elements, services & applications
- Examples: password, ACL, firewall

Authentication
- Provide Proof of Identity
- Examples: shared secret, PKI, digital signature, digital certificate

Non-repudiation
- Prevent ability to deny that an activity on the network occurred
- Examples: system logs, digital signatures

Data Confidentiality
- Ensure confidentiality of data
- Example: encryption

Communication Security
- Ensure information only flows from source to destination
- Examples: VPN, MPLS, L2TP

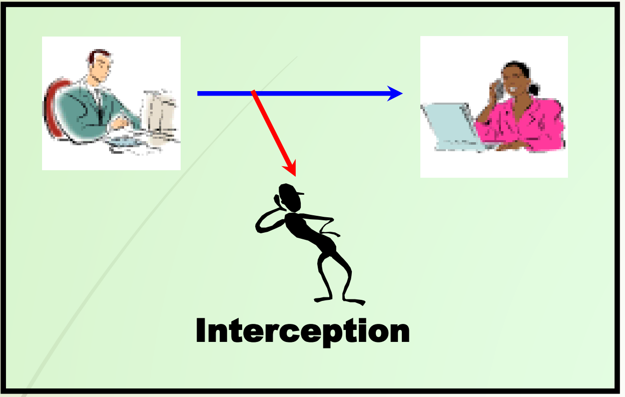
Data Integrity
- Ensure data is received as sent or retrieved as stored
- Examples: MD5, digital signature, anti-virus software

Availability
- Ensure network elements, services and application available to legitimate users
- Examples: IDS/IPS, network redundancy, BC/DR

Privacy
- Ensure identification and network use is kept private
- Examples: NAT, encryption

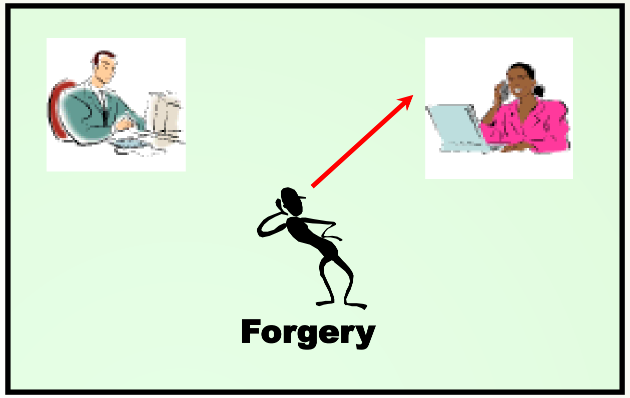
Security Needs for Network Communications

Confidentiality



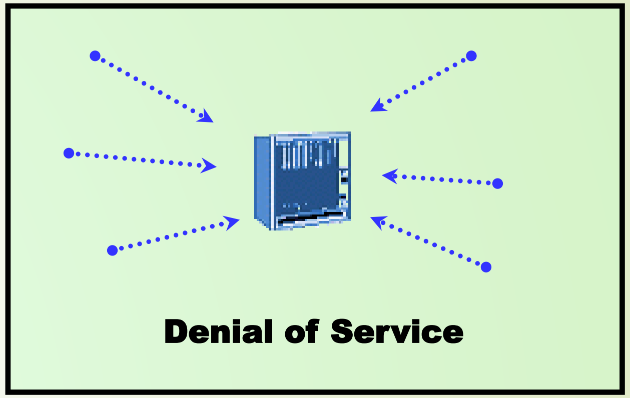
Is Private?

Authentication



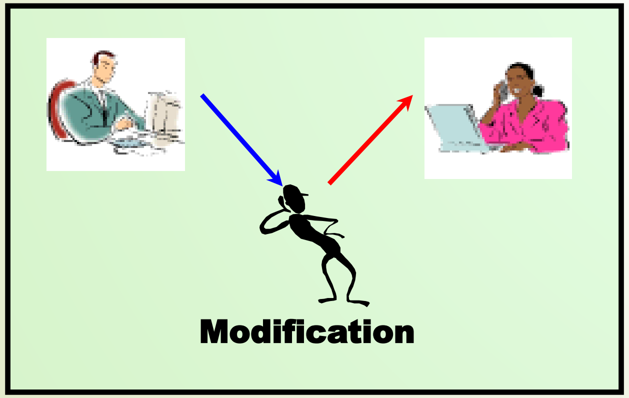
Who am I dealing with?

Availability



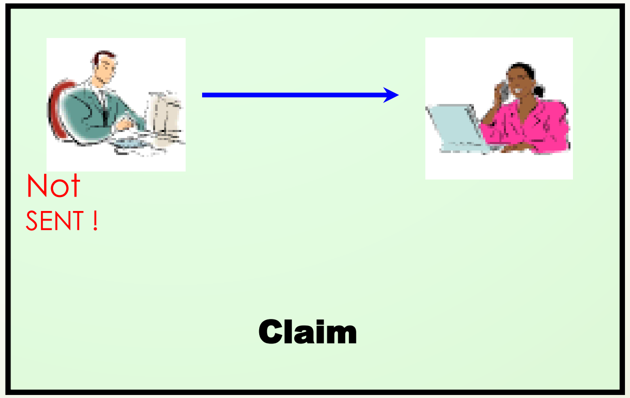
Wish to access!!

Integrity



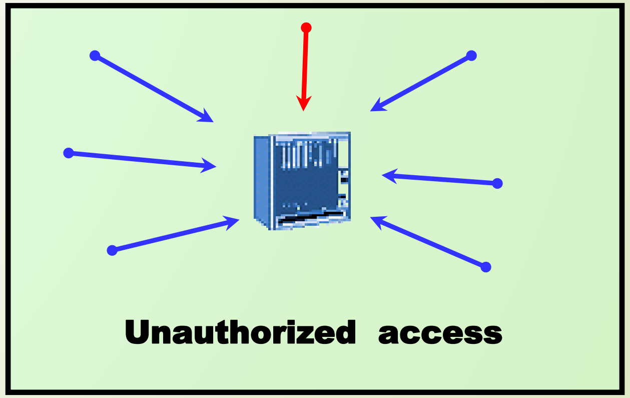
Has been altered?

Non-Repudiation



Who sent/received it?

Access Control

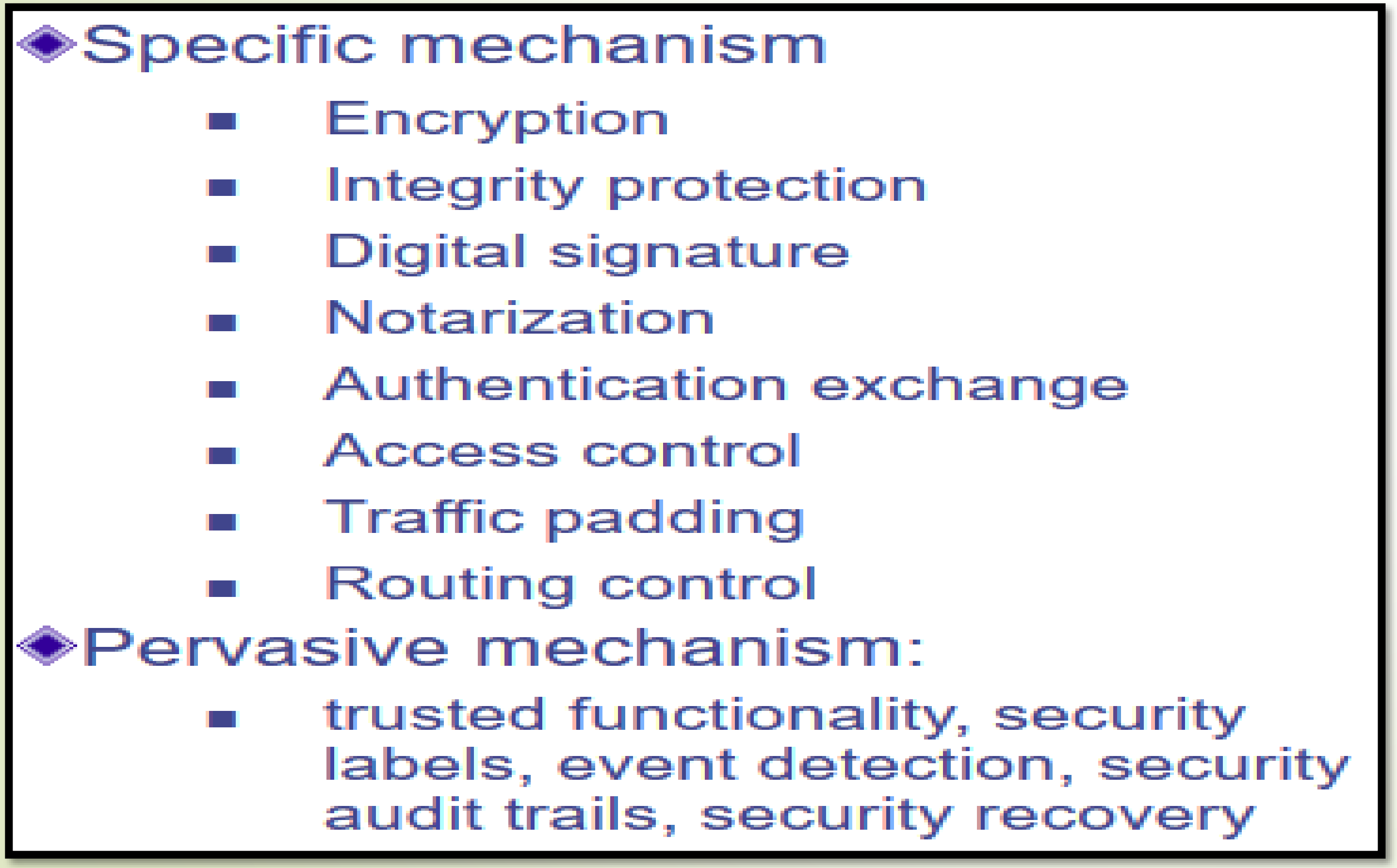


Have you privilege?

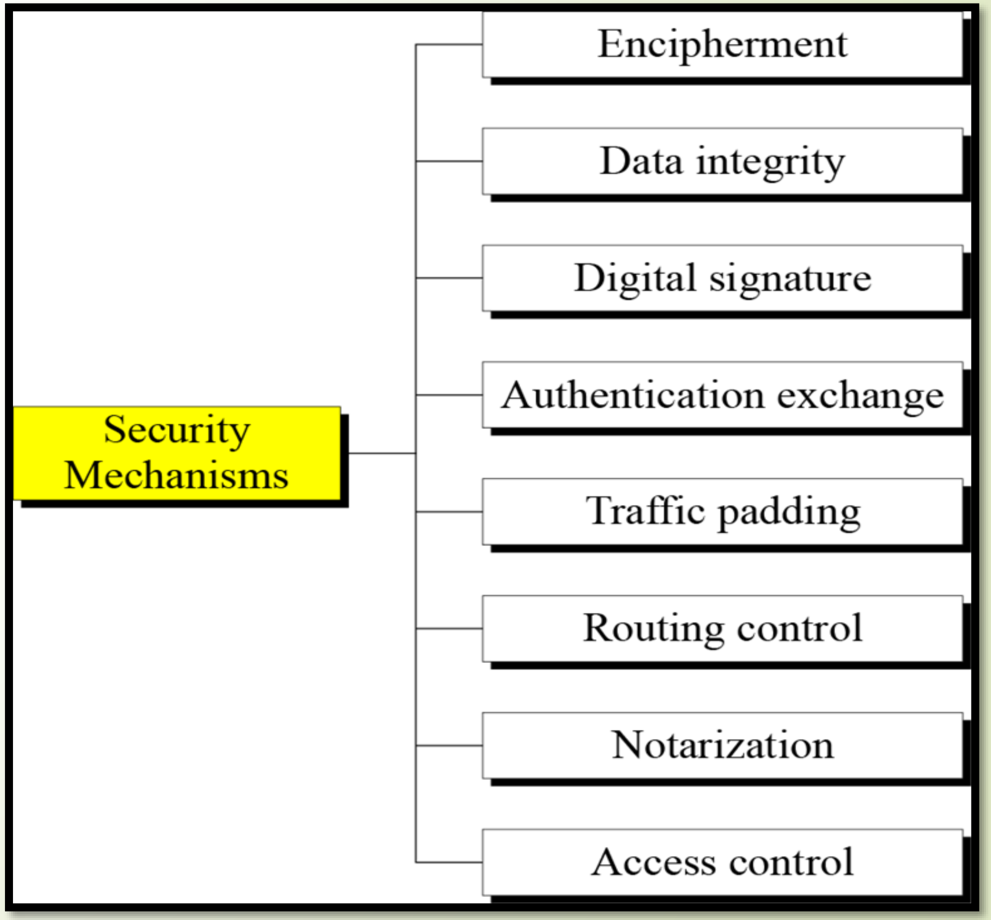
Security Mechanisms

Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack. No single mechanism that will support all functions required.

❖ The security mechanisms are divided into those that are implemented in a specific protocol layer called Specific Security Mechanisms and those that are not specific to any particular protocol layer or security service called Pervasive Security Mechanisms.



- Specific mechanism
  - Encryption
  - Integrity protection
  - Digital signature
  - Notarization
  - Authentication exchange
  - Access control
  - Traffic padding
  - Routing control
- Pervasive mechanism:
  - trusted functionality, security labels, event detection, security audit trails, security recovery



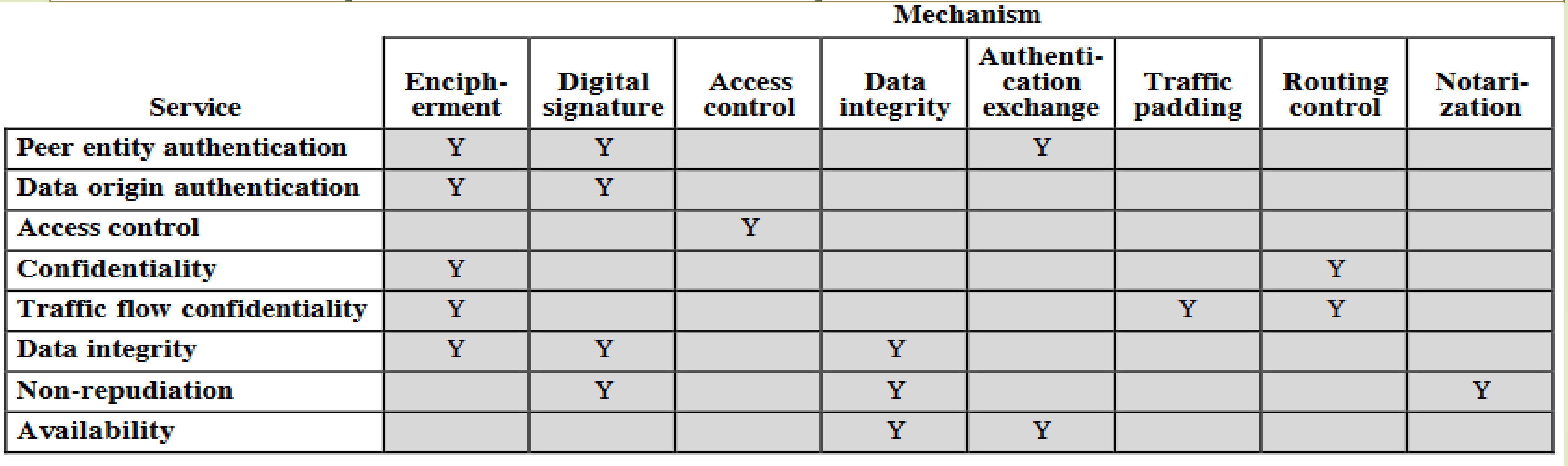
Specific Security Mechanisms

Security Mechanism	Description
Encipherment	The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
Access Control	A variety of mechanisms that enforce access rights to resources.
Data Integrity	A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
Authentication Exchange	A mechanism intended to ensure the identity of an entity by means of information exchange
Traffic Padding	The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
Routing Control	Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
Notarization	The use of a trusted third party to assure certain properties of a data exchange.

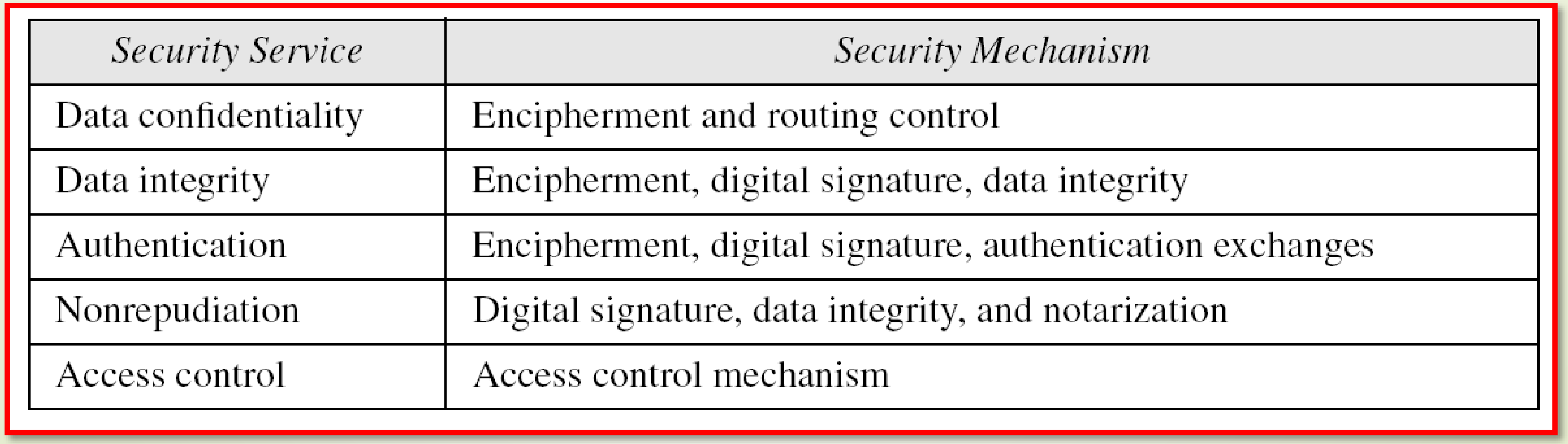
Pervasive Security Mechanisms

Security Mechanism	Description
Trusted Functionality	That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Security Label	The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Event Detection	Detection of security-relevant events
Security Audit Trail	Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Security Recovery	Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Relationship between security Services and Mechanisms



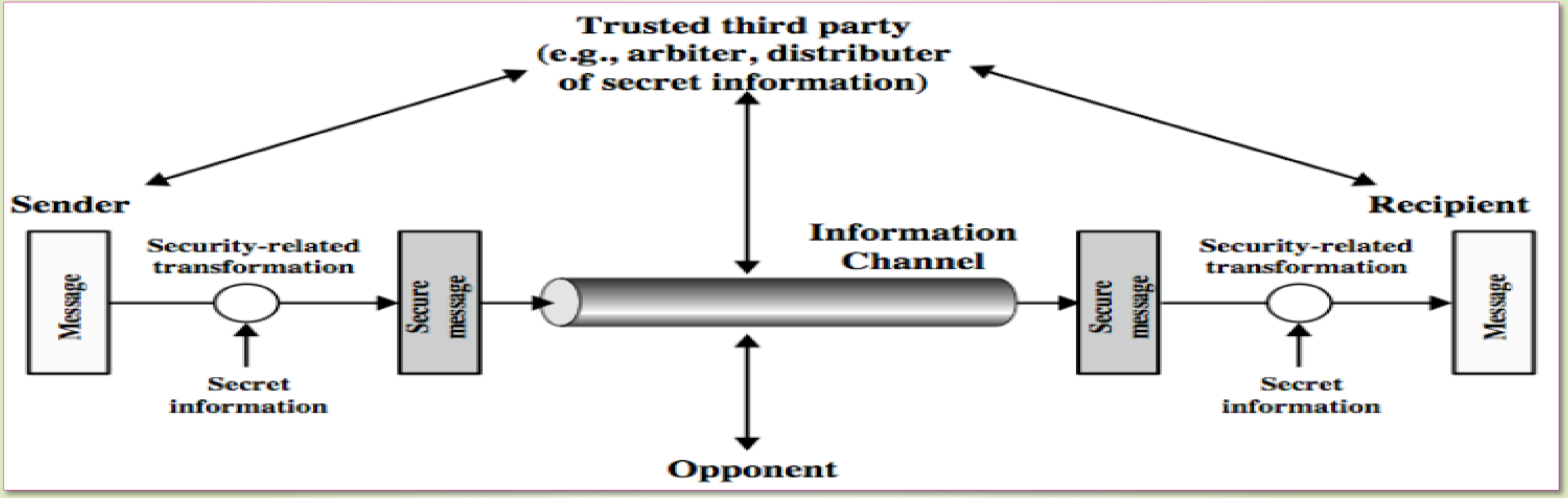
	Mechanism							
Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			



Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

A Model for Network Security

Data is transmitted over network between two communicating parties, who must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination by use of communication protocols by the two parties.



Two components are present in almost all the security providing techniques.

- ***A security-related transformation on the information to be sent making it unreadable by the opponent, and the addition of a code based on the contents of the message, used to verify the identity of sender.***
- ***Some secret information shared by the two principals and, it, unknown to the opponent. A trusted third party may be needed to distribute the secret information or to arbitrate disputes between the principals.***

The general model shows that there are four basic tasks in designing a particular security service:

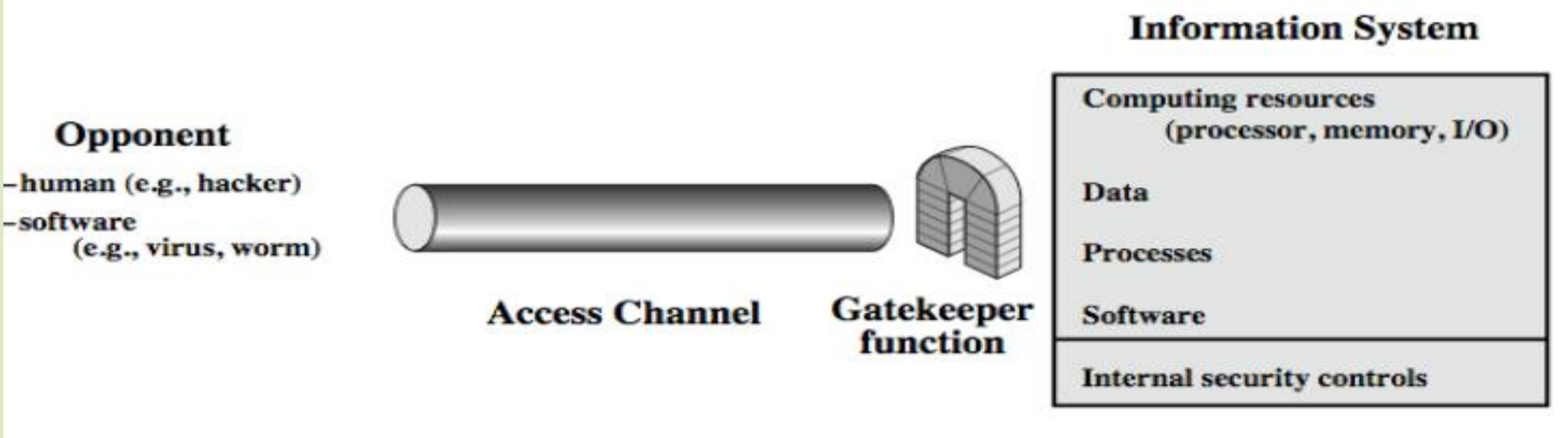
1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose
2. Generate the secret information to be used with the algorithm
3. Develop methods for the distribution and sharing of the secret information
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service

Various other threats to information system like unwanted access still exist. The existence of hackers attempting to penetrate systems accessible over a network remains a concern. Another threat is placement of some logic in computer system affecting various applications and utility programs. This inserted code presents two kinds of threats.

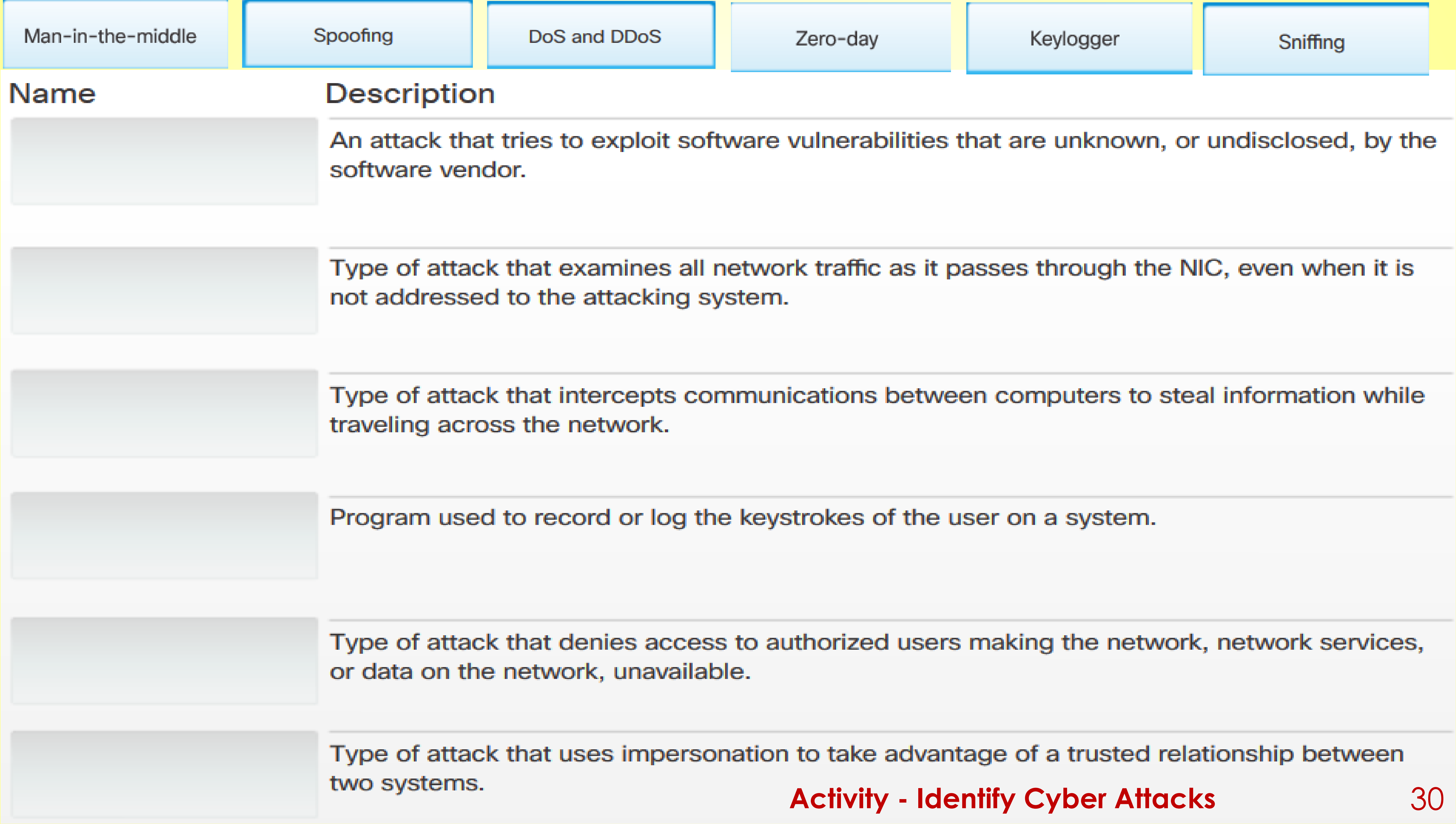
- **Information access threats** intercept or modify data on behalf of users who should not have access to that data
- **Service threats** exploit service flaws in computers to inhibit use by legitimate users

A Model for Network Access Security

Viruses and **worms** are two examples of software attacks inserted into the system by means of a disk or also across the network.



- ➔ Placing a gatekeeper function, which includes a password-based login methods that provide access to only authorized users and screening logic to detect and reject worms, viruses etc.
- ➔ An internal control, monitoring the internal system activities analyzes the stored information and detects the presence of unauthorized users or intruders.



Name	Description
	An attack that tries to exploit software vulnerabilities that are unknown, or undisclosed, by the software vendor.
	Type of attack that examines all network traffic as it passes through the NIC, even when it is not addressed to the attacking system.
	Type of attack that intercepts communications between computers to steal information while traveling across the network.
	Program used to record or log the keystrokes of the user on a system.
	Type of attack that denies access to authorized users making the network, network services, or data on the network, unavailable.
	Type of attack that uses impersonation to take advantage of a trusted relationship between two systems.

Activity - Identify Cyber Attacks