Lecture 1
Basics

Prepared by

Dr. Risala T Khan

Professor

IIT, JU

Information, Computer & Network Security

- **Information Security** refers to the protection of available information or information resources from **unauthorized access, attack, theft, or data damage**.
    - Responsible individuals and organizations must secure their confidential information.
- **Computer security** is the protection of computer systems and information from harm, theft, and unauthorized use.
- **Network security** is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft.

Key Objectives of Computer Security

- **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
- This term covers two related concepts:
  - **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:**
  - 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.
- This term covers two related concepts:
  - **Data integrity**: Assures that information (both stored and in transmitted packets) 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.

CIA Triad

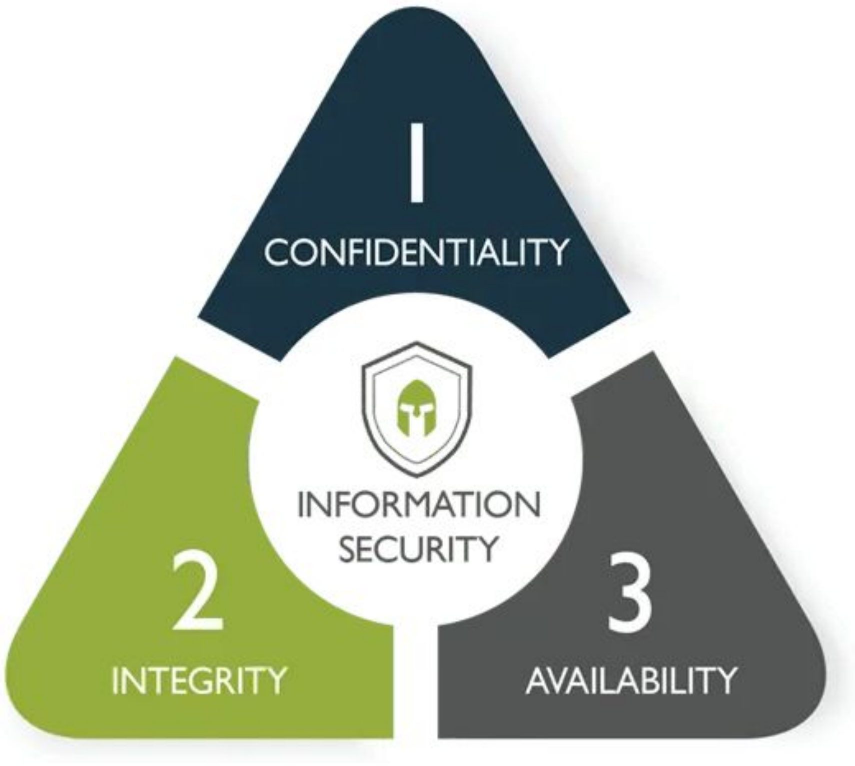


Figure 1: CIA Triad

- **Confidentiality, integrity** and **availability**, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

CIA Triad

Principle	Description
Confidentiality	This is the fundamental principle of keeping information and communications private and protected from unauthorized access. Confidential information includes trade secrets, personnel records, health records, tax records, and military secrets. Confidentiality is typically controlled through encryption, access controls, and steganography
Integrity	This is the fundamental principle of keeping organizational information accurate, free of errors, and without unauthorized modifications. Integrity is typically controlled through hashing, digital signatures, certificates, and change control.
Availability	This is the fundamental principle of ensuring that computer systems operate continuously and that authorized persons can access the data that they need. Availability is typically controlled through redundancy, fault tolerance, and patching

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture (as shown in the figure). Two of the most commonly mentioned are as follows:

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. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action recovery and legal action.

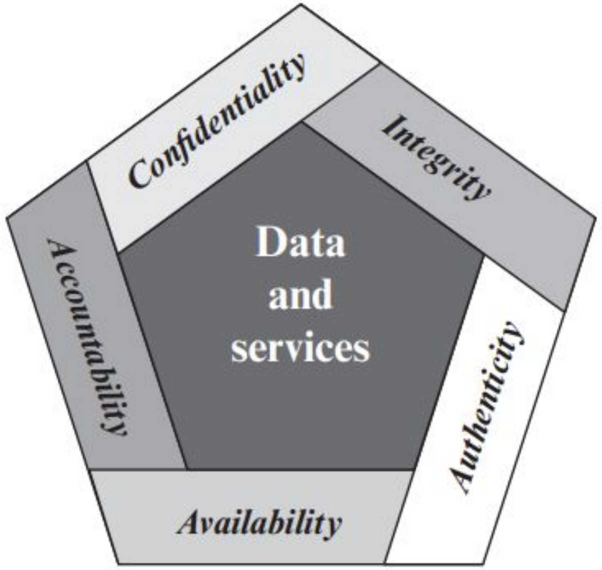


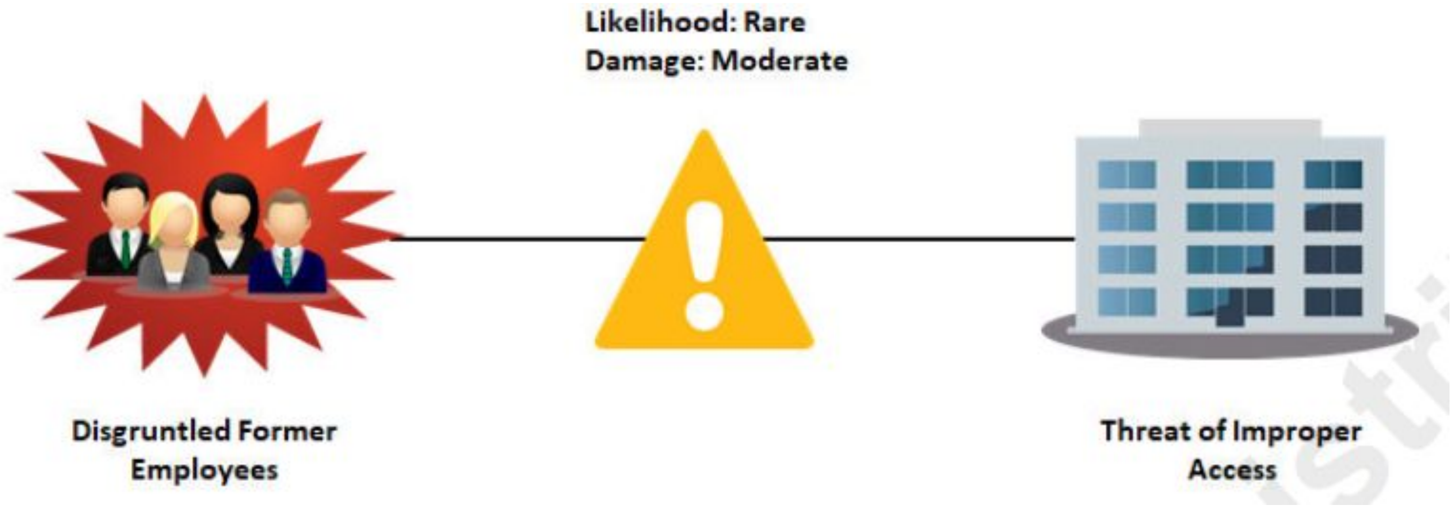
Figure 1.1 Essential Network and Computer Security Requirements

Goal of Information Security

Information Security Goal	Description
Prevention	Personal information, company information, and information about intellectual property must be protected.
Detection	Detection occurs when a user is discovered trying to access unauthorized data or after information has been lost
Recovery	When there is a disaster or an intrusion by unauthorized users, system data can become compromised or damaged. It is in these cases that you need to employ a process to recover vital data from a crashed system or data storage devices

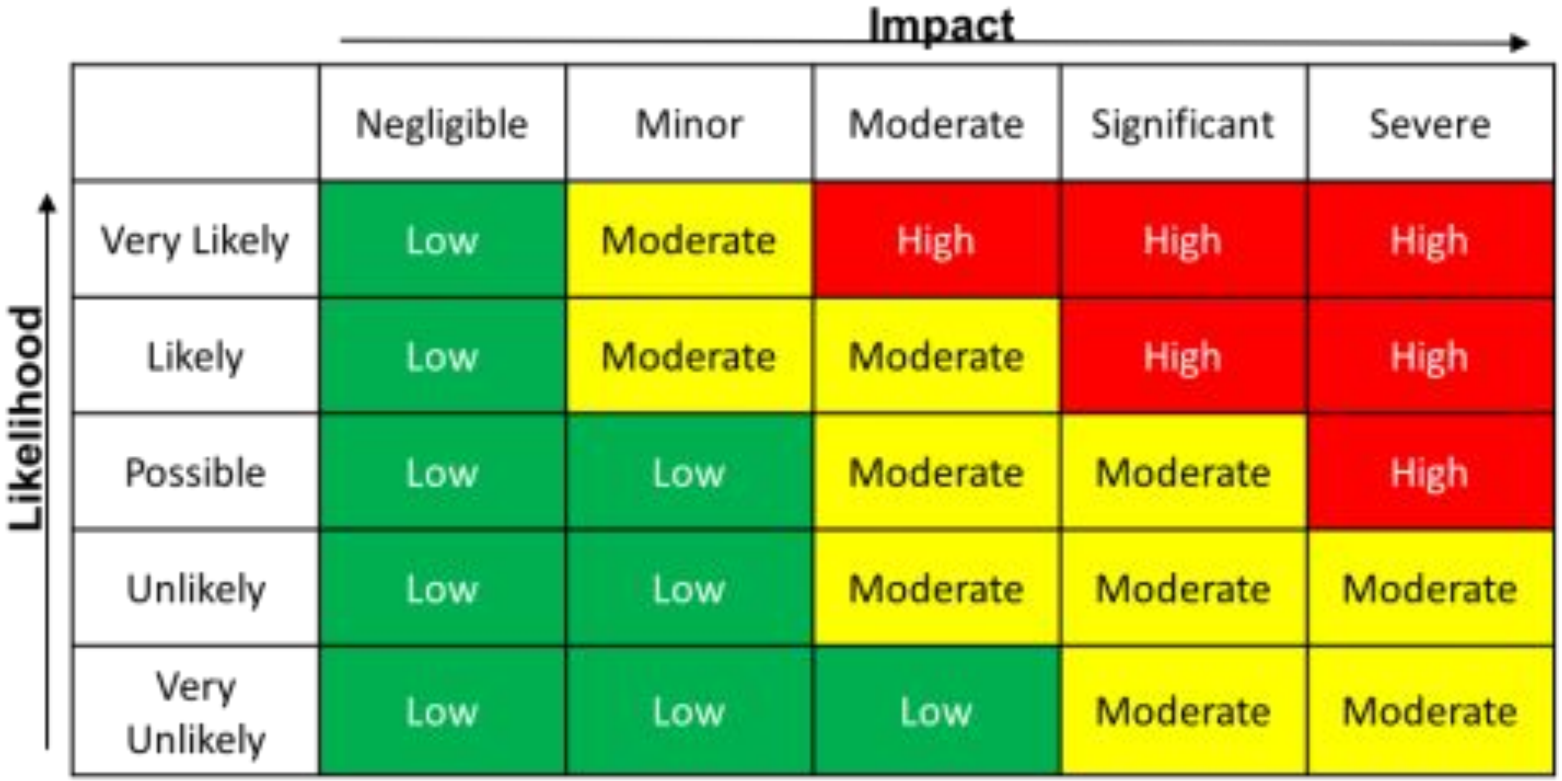
Risk

- As applied to information systems, risk is a concept that indicates exposure to the chance of damage or loss. It signifies the likelihood of a hazard or dangerous threat occurring.



Risk

- Risk = Likelihood X Impact



Impact

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

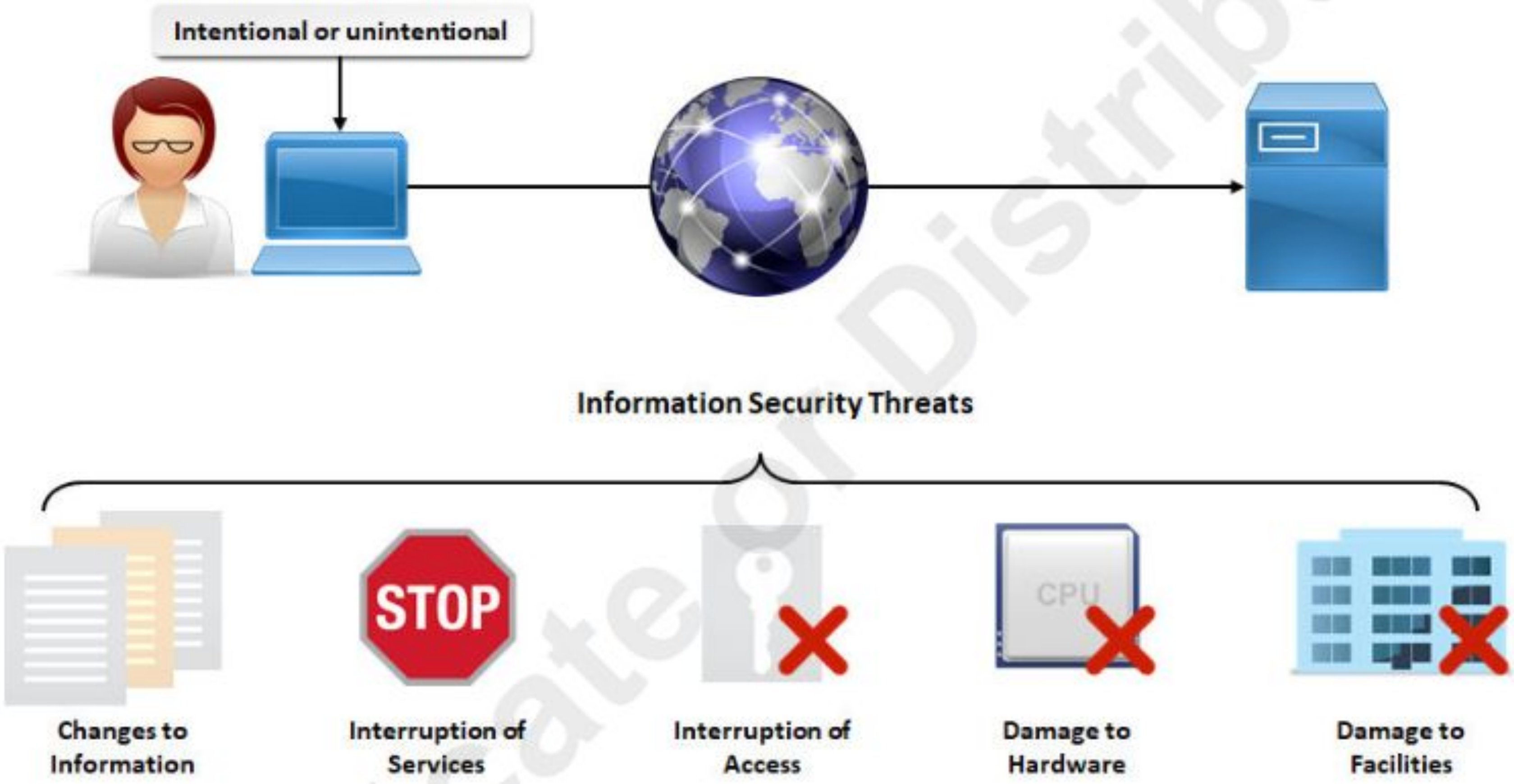
Vulnerabilities

- At the most basic level, a vulnerability is any condition that leaves an information system open to harm.
- Vulnerabilities can come in a wide variety of forms, including:
  - Improperly configured or installed hardware or software.
  - Delays in applying and testing software and firmware patches.
  - Untested software and firmware patches.
  - Bugs in software or operating systems.
  - The misuse of software or communication protocols.
  - Poorly designed networks.
  - Poor physical security.
  - Insecure passwords.
  - Design flaws in software or operating systems.
  - Unchecked user input

Threats

- In the realm of computer security, a threat is any event or action that could potentially cause damage to an asset.
- Threats are often in violation of a security requirement, policy, or procedure.
- Regardless of whether a violation is intentional or unintentional, malicious or not, it is considered a threat.
- Potential threats to computer and network security include:
  - Unintentional or unauthorized access or changes to data.
  - The interruption of services.
  - The interruption of access to assets.
  - Damage to hardware.
  - Unauthorized access or damage to facilities.

Threats

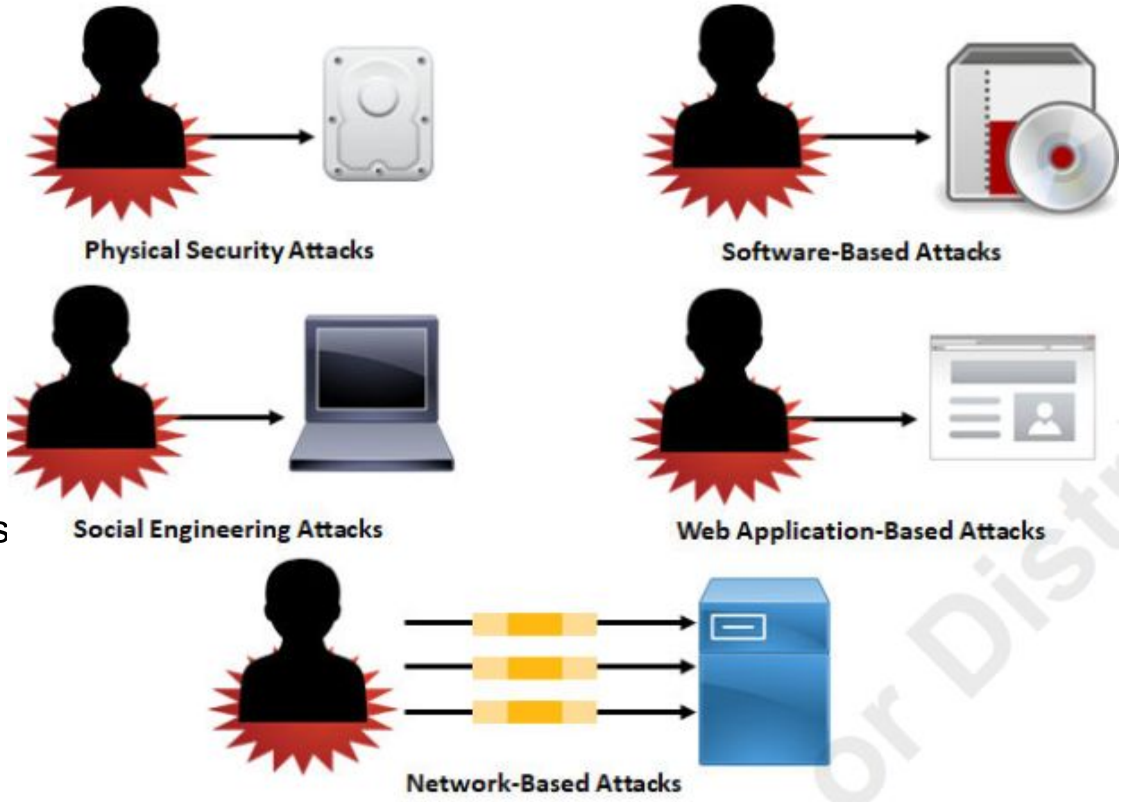

Intentional or unintentional
Information Security Threats
Changes to Information
STOP
Interruption of Services
Interruption of Access
CPU
Damage to Hardware
Damage to Facilities

Attacks

In the realm of computer security, an attack is a technique used to exploit a vulnerability in any application or physical computer system without the authorization to do so.

Attacks on a computer system and network security include:

- Physical security attacks.
- Software-based attacks.
- Social engineering attacks.
- Web application-based attacks.
- Network-based attacks, including wireless networks


Physical Security Attacks
Software-Based Attacks
Social Engineering Attacks
Web Application-Based Attacks
Network-Based Attacks

Security Controls

- In the realm of computer security, controls are the countermeasures that you need to put in place to avoid, mitigate, or counteract security risks due to threats or attacks.
- In other words, controls are solutions and activities that enable an organization to meet the objectives of an information security strategy.

Types of Security Controls

Mainly 3 types

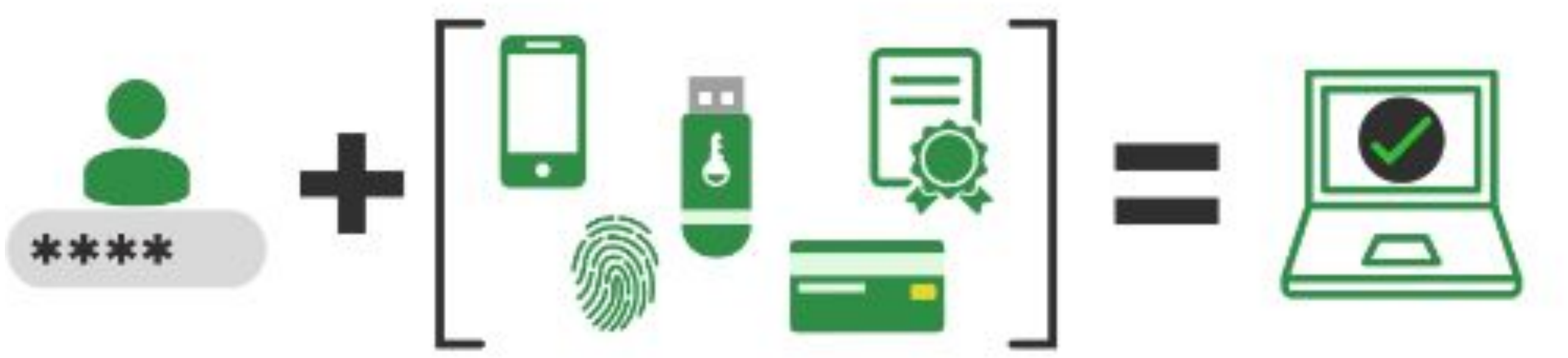
Prevention Controls	Detection Controls	Correction Controls
• These help to prevent a threat or attack from exposing a vulnerability in the computer system. • For example, a security lock on a building's access door is a prevention control.	• These help to discover if a threat or vulnerability has entered into the computer system. • For example, surveillance cameras that record everything that happens in and around a building are detection controls.	• These help to mitigate the consequences of a threat or attack from adversely affecting the computer system. • For example, a security officer who responds to a silent alarm detecting an intrusion and who then stops the intruder is a correction control.

Non-Repudiation

- Non-repudiation is the goal of ensuring that the party that sent a transmission or created data remains associated with that data and cannot deny sending or creating that data.
- You should be able to independently verify the identity of a message sender, and the sender should be responsible for the message and its data.

Identification

- In security terms, identification is the process by which a claim is made about the nature of a particular entity.
- Identification is what you show when someone wants proof of who you are.



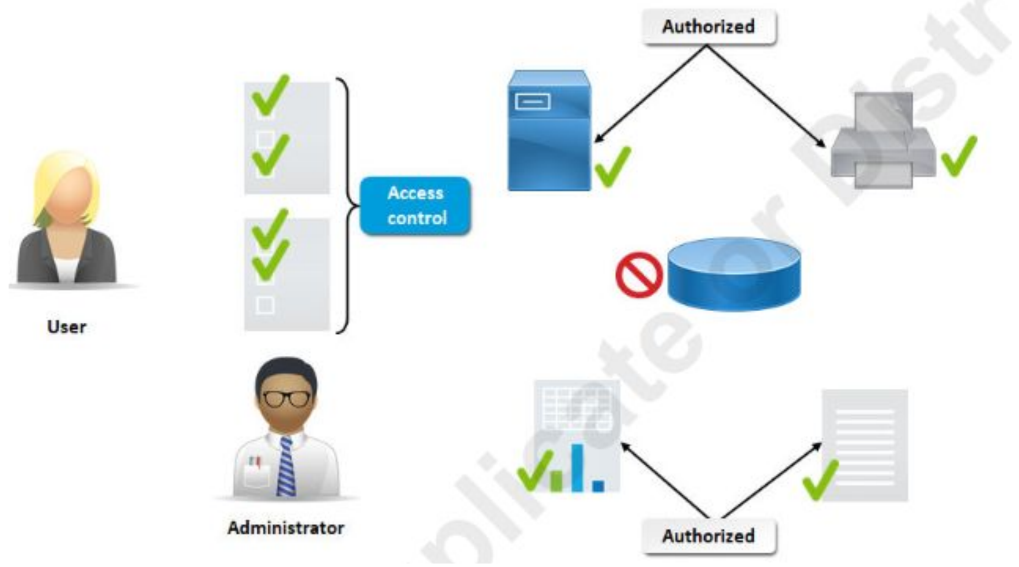
Authentication

- Authentication is the method of validating a particular entity's or individual's identity and unique credentials.
- Authentication concentrates on identifying if a particular individual has the right credentials to enter a system or secure site.
- Authentication credentials should be kept secret to keep unauthorized individuals from gaining access to confidential information.

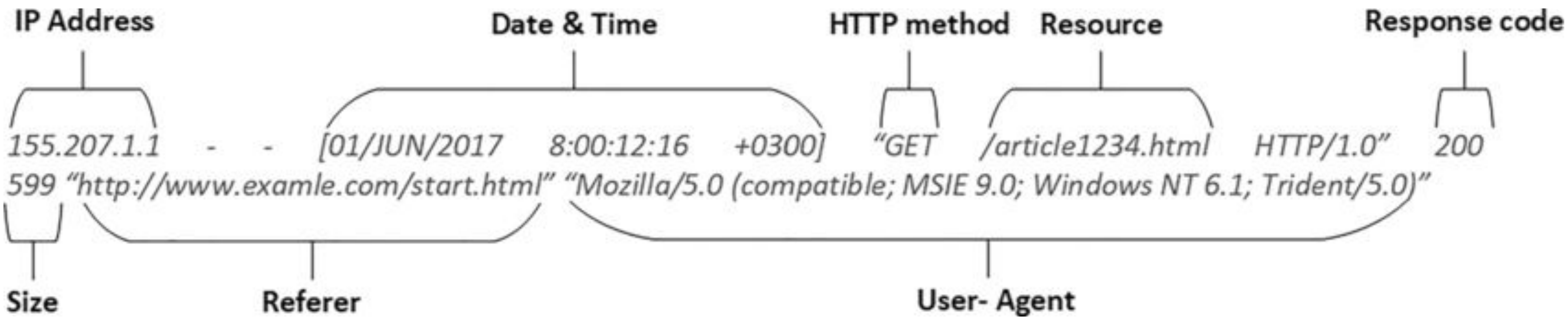
Authorization

- In security terms, authorization is the process of determining what rights and privileges a particular entity has.
- Authorization is equivalent to a security guard checking the guest list at an exclusive gathering, or checking for your ticket when you go to the movies.
- After a user has been identified and authenticated, a system can then determine what rights and privileges that user should have to various resource:
    - Access Control
    - Accounting and Auditing
    - Principle of Least Privilege
    - Privilege Management

Access Control



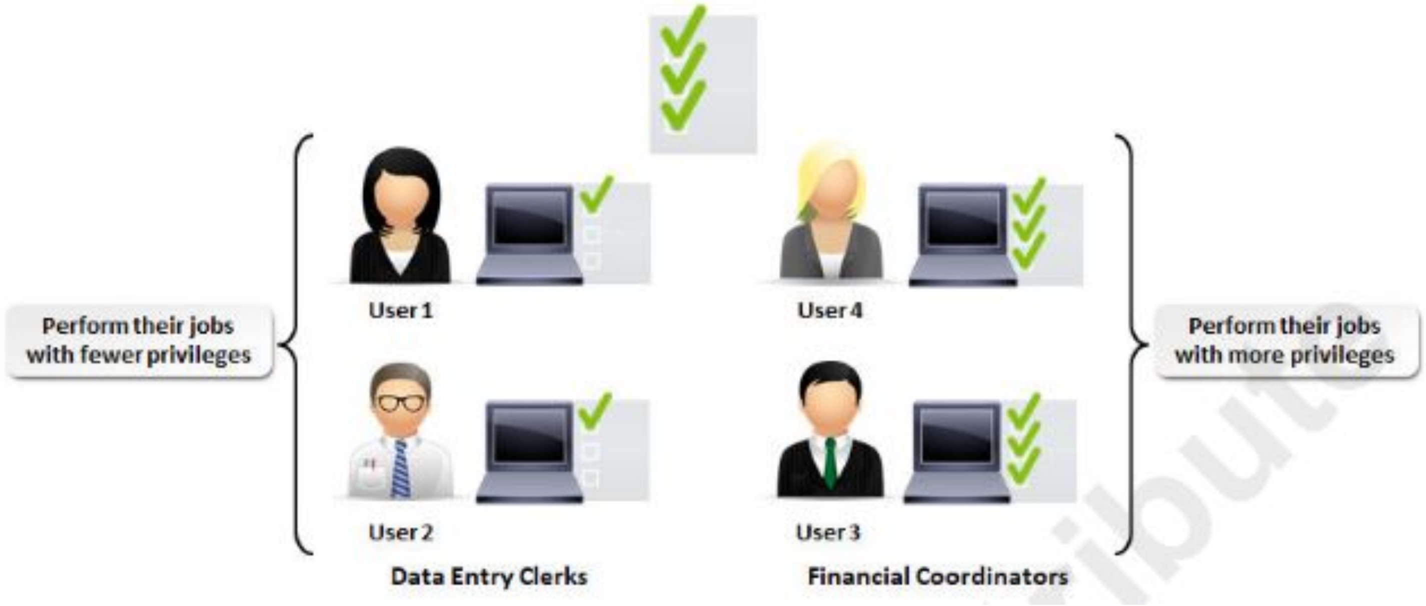
- Access control is the process of determining and assigning privileges to various resources, objects, or data.



```
155.207.1.1   -   -   [01/JUN/2017   8:00:12:16   +0300]   “GET   /article1234.html   HTTP/1.0”   200
599 “http://www.examle.com/start.html” “Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)”
```

Accounting and Auditing

- In security terms, accounting is the process of tracking and recording system activities and resource access.
- Auditing is the part of accounting in which a security professional examines logs of what was recorded.


Perform their jobs with fewer privileges
User 1
User 2
Data Entry Clerks
User 4
User 3
Financial Coordinators
Perform their jobs with more privileges

Least Privilege Model

- The principle of least privilege dictates that users and software should have the minimal level of access that is necessary for them to perform the duties required of them.
- This level of minima access includes access to facilities, computing hardware, software, and information.

Privilege Bracketing

The term *privilege bracketing* is used when privileges are granted only when needed, then revoked as soon as the task is finished or the need has passed.

Privilege Management

Privilege management is the use of authentication and authorization mechanisms to provide centralized or decentralized administration of user and group access control. Privilege management should include an auditing component to track privilege use and privilege escalation. *Single sign-on (SSO)* can offer privilege management capabilities by providing users with one-time authentication for browsing resources such as multiple servers or sites.

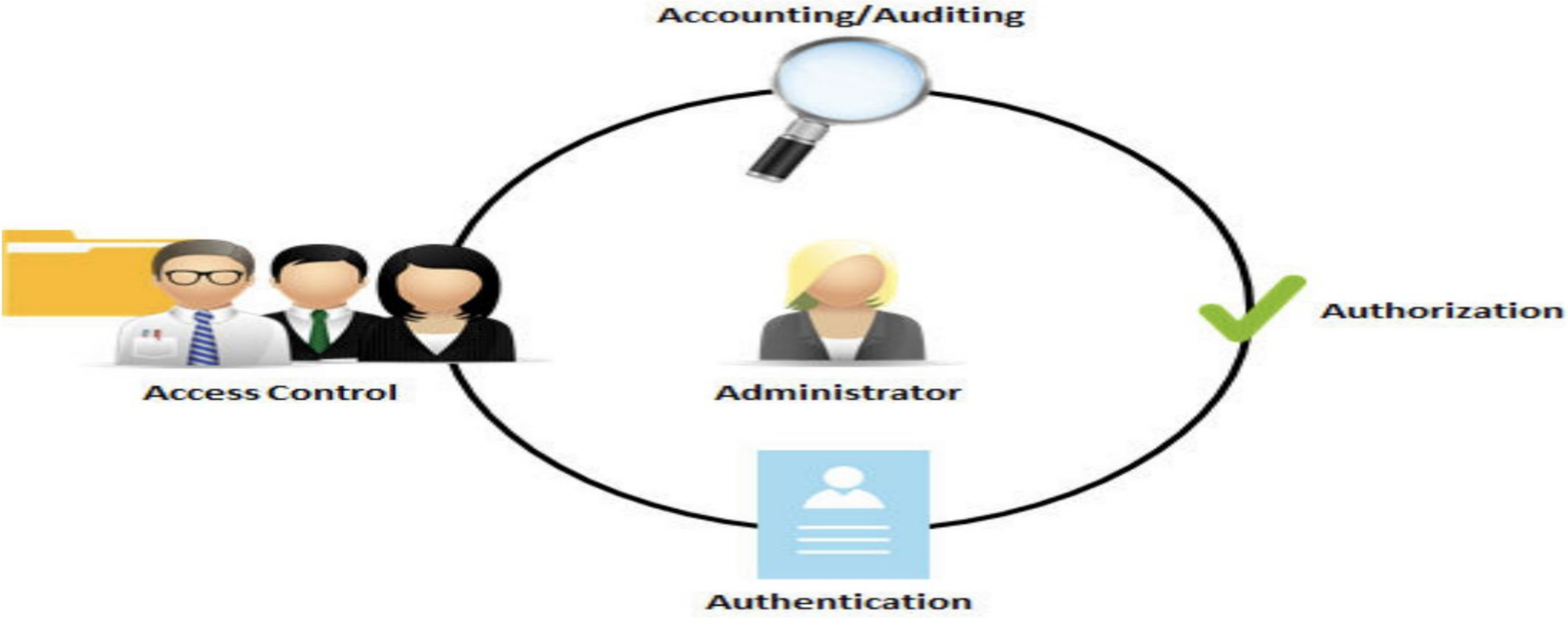


Figure 1–12: Privilege management.

DAD Triad

- Like every concept in security, the CIA Triad can be a double edged sword.
- Where there is a good side, there is an opposite bad side to consider as well.
- **In the lack of each of the CIA Triad, you are given the DAD triad.**

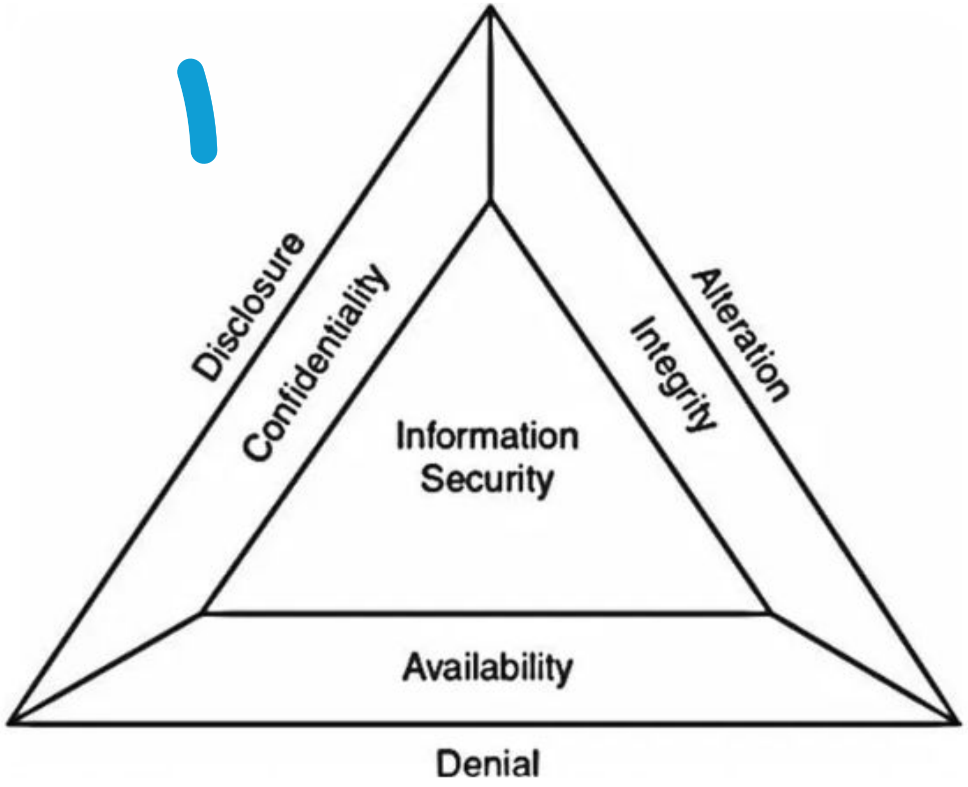


Figure 2: DAD triad

DAD Triad

- **Disclosure :**
  - Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users.
  - Depending on the context, websites may leak all kinds of information to a potential attacker, including:
    1. Data about other users, such as usernames or financial information
    2. Sensitive commercial or business data

DAD Triad

- **Alteration:**
  - An unauthorized change of information, covers three classes of threats.
  - The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released.
  - If the modified data controls the operation of the system, the threats of disruption and usurpation arise.
  - Unlike snooping, modification is active; it results from an entity changing information.

DAD Triad

- **Denial** :
  - It is an type of a aspect which is targeted towards depriving legitimate users from online services.
  - It is done by flooding the network or server with useless and invalid authentication requests which eventually brings the whole network down, resulting in no connectivity.
  - As a result of this, users are prevented from using a service.

CIA and DAD Relationship

- Each point of the CIA and DAD triangle are exact opposites of each other.
- If one a CIA principle is absent, then a DAD principle is present.
- Thus, you cannot have both at the same time.
- You could not have both a Denial and Availability at the exact same time, it is either one or the other.

a) **Disclosure**: Attempts to defeat confidentiality
b) **Alteration:** Attempts to defeat integrity
c) **Destruction:** Attempts to defeat availability

Data Loss Prevention

- **Data Loss Prevention (DLP)** is a technology that helps prevent data breaches and unauthorized data transmission.

What Does DLP Do?

1. Identifies Sensitive Data: DLP tools help you recognize what data needs extra protection.
2. Prevents Data Loss: Monitor and block data transfer and exfiltration, whether accidental or intentional

Data Classification

While the definition of sensitive data can differ, some types are universally recognized, and often governed by laws:

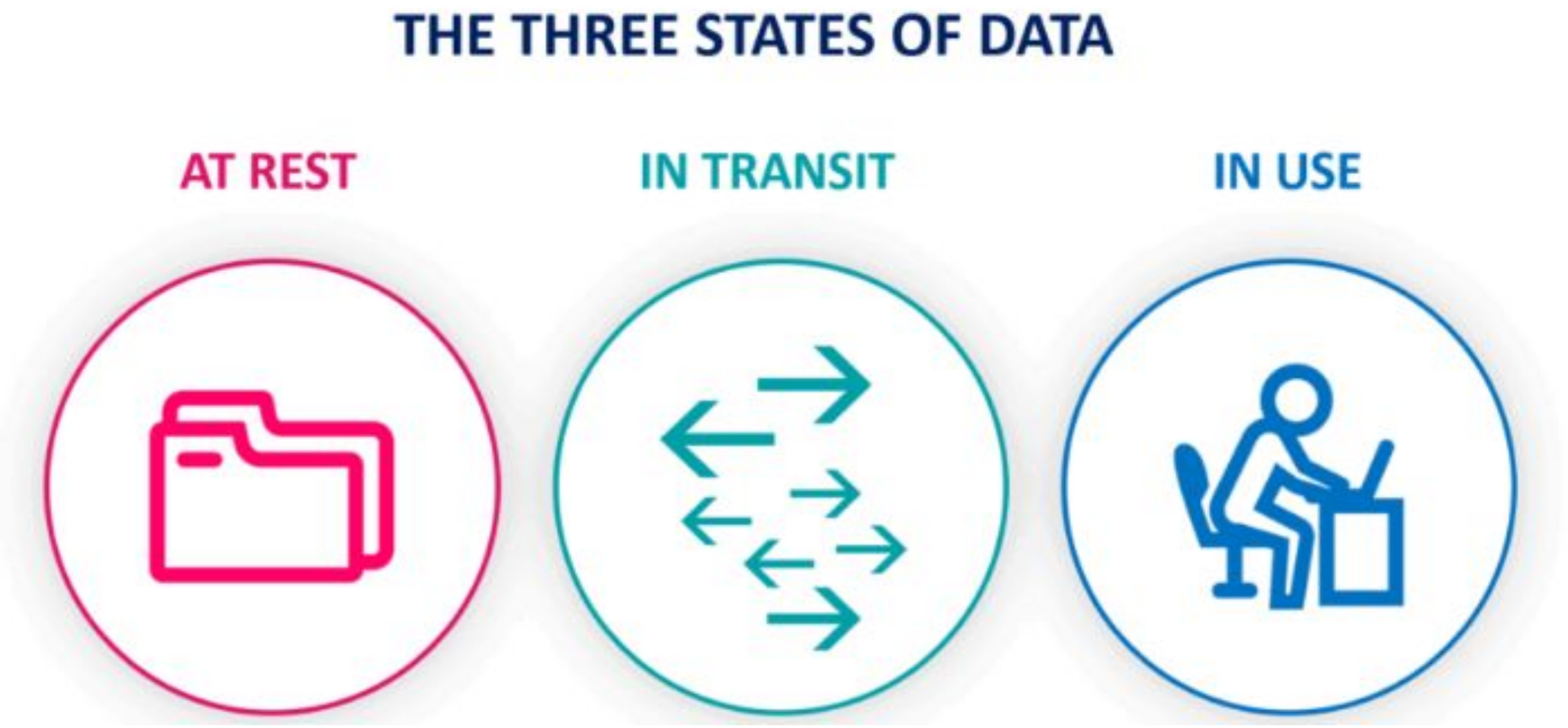
- **Personally Identifiable Information (PII):** Primarily defined in the United States, PII includes data that can trace an individual's identity – name, Social Security number, and biometric data, among others.
- **Personal Data:** A broader term, especially in the context of Europe's General Data Protection Regulation (GDPR), encompassing any information related to an identifiable person, like location data or online identifiers.
- **Sensitive Personal Information (SPI):** Defined under the California Privacy Rights Act (CPRA), this term may extend to include IP addresses, which are generally not considered PII or Personal Data.
- **Nonpublic Personal Information (NPI):** Originating from the Gramm-Leach-Bliley Act (GLBA), NPI could include names, income, credit scores, and even data collected via cookies

Sensitive Data

Aside from personal data, businesses often need to protect various types of intellectual property (IP):

- Source Code: Especially important in software development.
- Formulas: Crucial for industries like pharmaceuticals.
- Diagrams, Videos, and More: Varied forms of intellectual assets critical to different business types.

Data Security State



THE THREE STATES OF DATA

AT REST

IN TRANSIT

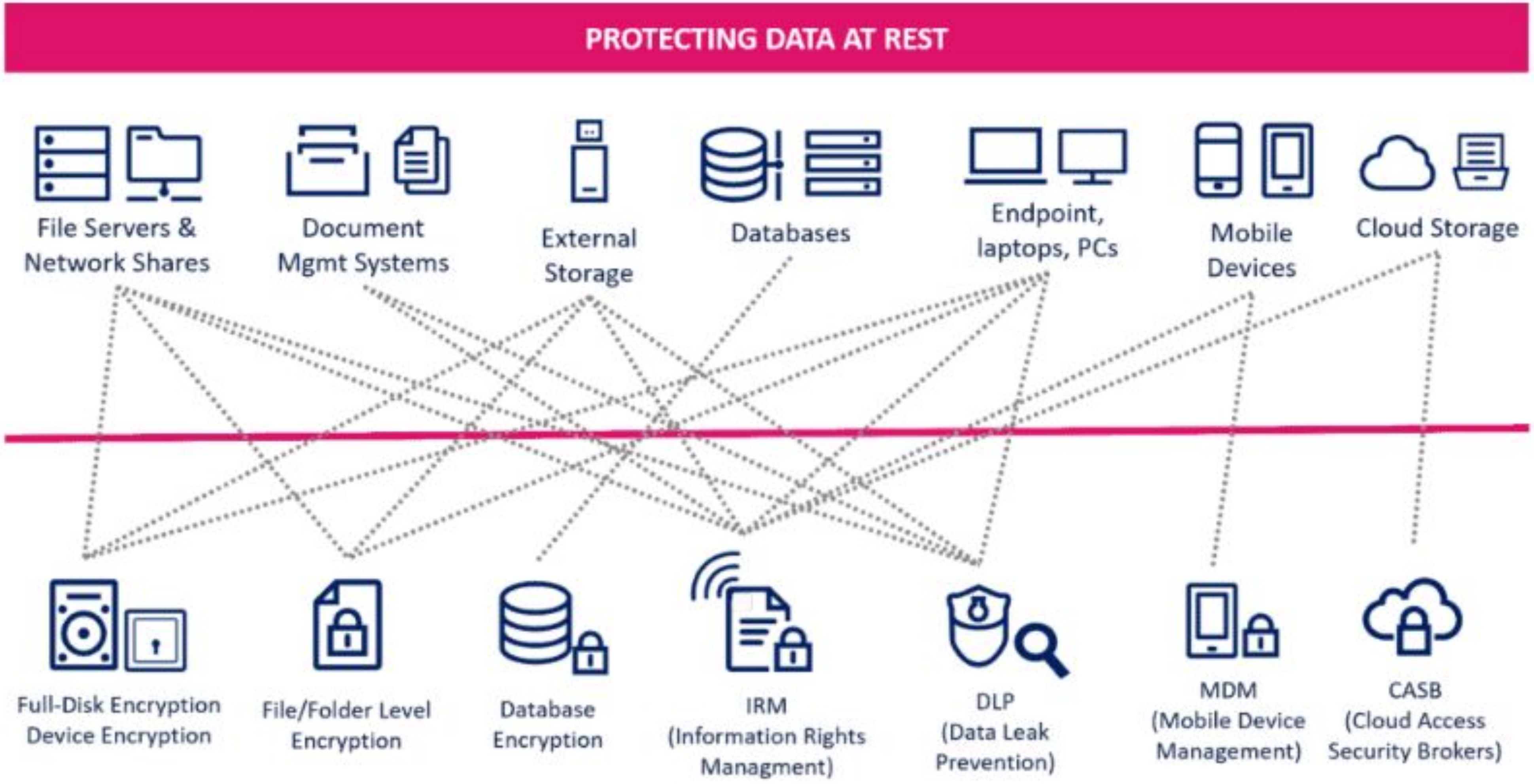
IN USE

Data Security State

We can consider three states for information or data:

- **Data at rest**: By this term we mean data that is not being accessed and is stored on a physical or logical medium. Examples may be files stored on file servers, records in databases, documents on flash drives, hard disks etc.
- **Data in transit**: Data that travels through an email, web, collaborative work applications such as Slack or Microsoft Teams, instant messaging, or any type of private or public communication channel. It’s information that is traveling from one point to another.
- **Data in use**: When it is opened by one or more applications for its treatment or and consumed or accessed by users.

Secure Data in Different States (At Rest)


PROTECTING DATA AT REST
File Servers & Network Shares
Document Mgmt Systems
External Storage
Databases
Endpoint, laptops, PCs
Mobile Devices
Cloud Storage
Full-Disk Encryption Device Encryption
File/Folder Level Encryption
Database Encryption
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
MDM (Mobile Device Management)
CASB (Cloud Access Security Brokers)

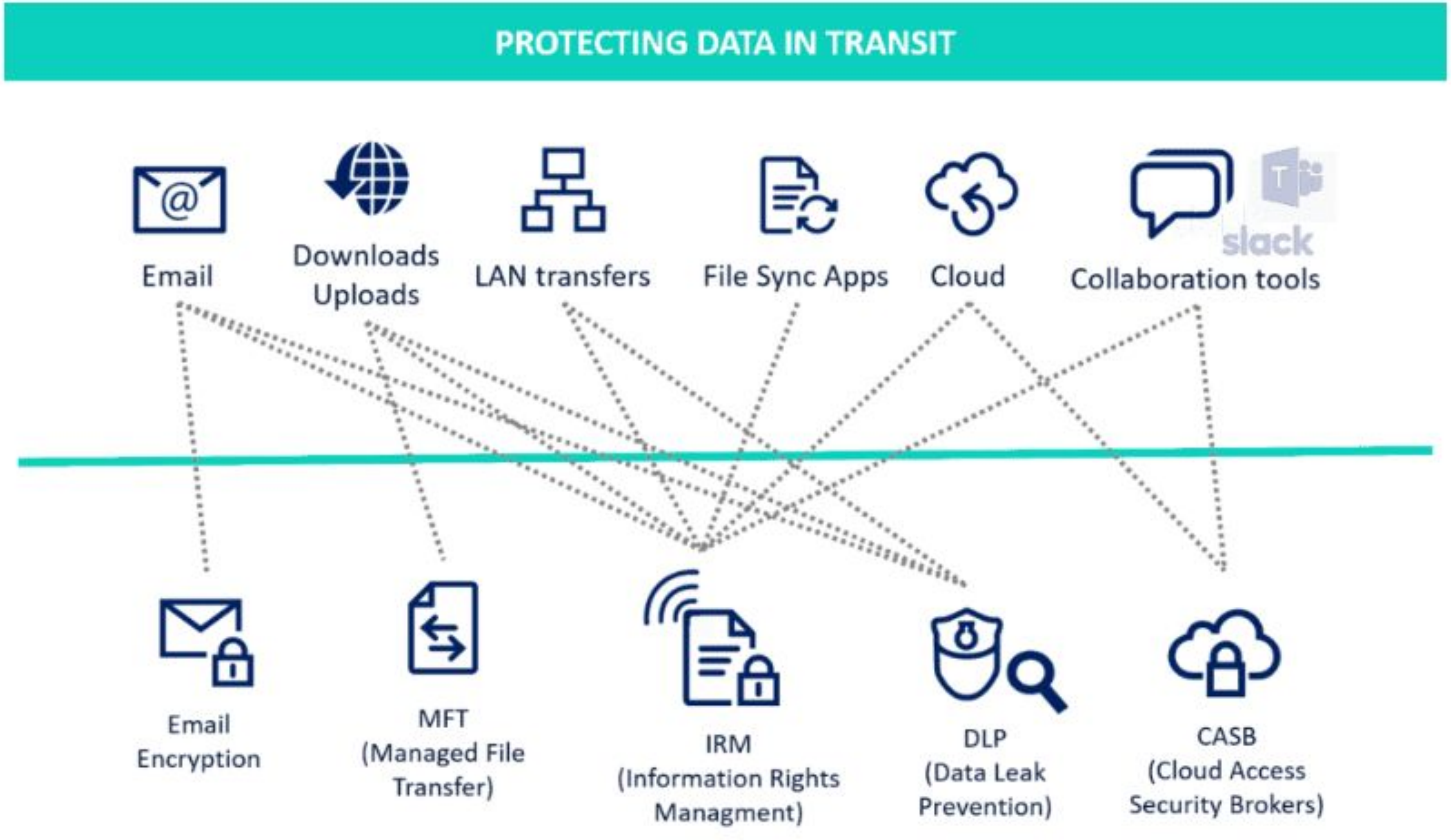
Secure Data in Different States (At Rest)

Documentation is considered secure at rest when it is encrypted (so that it requires an unworkable amount of time in a brute-force attack to be decrypted), the encryption key is not present on the same storage medium, and the key is of sufficient length and level of randomness to make it immune to a dictionary attack.

In this area we find different data protection technologies. For example:

- **Full disk encryption or device**
- **File-level encryption**
- **Database Encryption**
- **MDM (Mobile Device Management)**
- **DLPs (Data Leak Prevention)**

Secure Data in Different States (in Transit)


PROTECTING DATA IN TRANSIT
Email
Downloads Uploads
LAN transfers
File Sync Apps
Cloud
slack
Collaboration tools
Email Encryption
MFT (Managed File Transfer)
IRM (Information Rights Managment)
DLP (Data Leak Prevention)
CASB (Cloud Access Security Brokers)

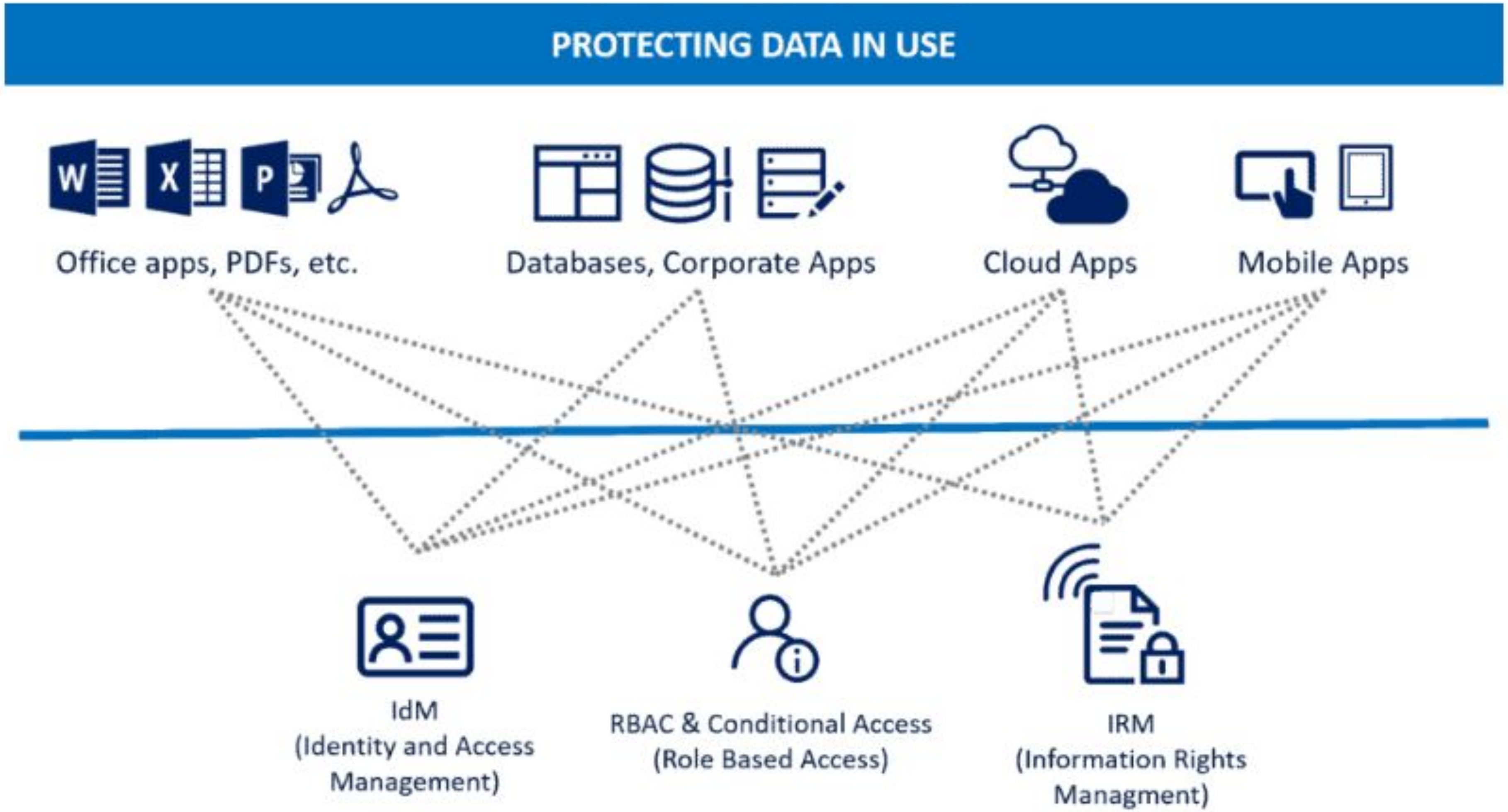
Secure Data in Different States (in Transit)

This describes data that is actively being transferred from one location to another across a network. This includes data transmissions over the internet, local area networks (LANs), or any communication channel.

SECURITY CONSIDERATION:

- ○ **Encryption in Transit:** Encrypting data in motion using protocols like Secure Sockets Layer (SSL)/Transport Layer Security (TLS) scrambles data during transmission, preventing eavesdropping or interception.
- ○ **Virtual Private Networks (VPNs):** VPNs create a secure tunnel over a public network like the internet, encrypting all data traffic within the tunnel.
- ○ **Firewalls:** Firewalls act as security barriers, filtering incoming and outgoing network traffic based on predefined rules, protecting against unauthorized access attempts.

Secure Data in Different States (in Use)



PROTECTING DATA IN USE

Office apps, PDFs, etc.

Databases, Corporate Apps

Cloud Apps

Mobile Apps

IdM
(Identity and Access
Management)

RBAC & Conditional Access
(Role Based Access)

IRM
(Information Rights
Managment)

Secure Data in Different States (in Use)

To protect the data in use, controls should normally be put in place “before” accessing the content. For example, through:

- **Conditional Access or Role Based Access Control (RBAC) tools**
- **Through digital rights protection or IRM**
- **Identity management tools**

The Challenges of Computer Security

1. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
2. Because of point 1, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.
3. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP [Transmission Control Protocol/Internet Protocol] should mechanisms be placed).

Security Challenges (Cont…)

1. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.
2. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
3. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
4. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.
5. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

OSI Security Architecture

OSI Model

- The OSI (Open Systems Interconnection) Security Architecture provides a framework for implementing security at each layer of the OSI model. This layered approach ensures a comprehensive security posture for network communications.

Understanding the OSI Model:

The OSI model is a conceptual framework that defines seven layers for communication between network devices. Each layer has specific functionalities:

1. **Physical Layer:** Deals with the physical transmission of data (cables, connectors).
2. **Data Link Layer:** Handles error-free data transfer across a physical link.
3. **Network Layer:** Routes data packets across networks.
4. **Transport Layer:** Provides reliable data transfer between applications.
5. **Session Layer:** Establishes, manages, and terminates sessions between communicating applications.
6. **Presentation Layer:** Handles data formatting and encryption/decryption.
7. **Application Layer:** Provides network services to user applications (e.g., HTTP, FTP).

The OSI Security Architecture

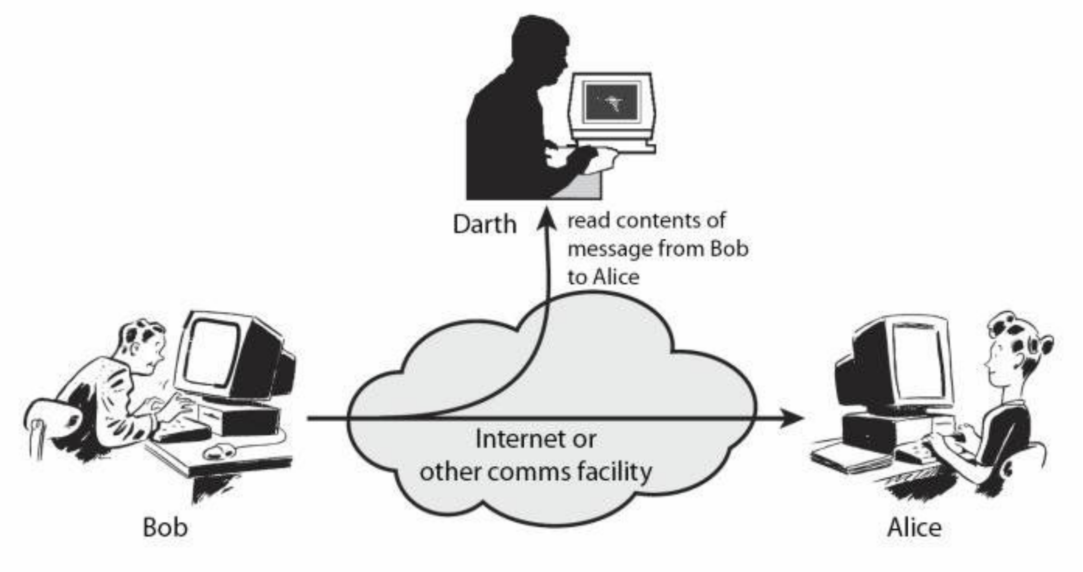
- The OSI security architecture focuses on **security attacks, mechanisms, and services**.
- These can be defined briefly as
- **Security attack:**
  - Any action that compromises the security of information owned by an organization.
- **Security mechanism:**
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:**
  - A capability that supports one, or many, of the security goals.
  - Examples of security services are key management, access control, and authentication.
  - The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security at Each OSI Layer

- The OSI Security Architecture defines how security services and mechanisms can be applied at each layer of the OSI model:
- **Lower Layers (Physical & Data Link):** Focus on physical security measures to prevent unauthorized access to network devices and ensure data transmission integrity.
- **Network Layer:** Implements routing protocols with security features like authentication and encryption for secure data routing.
- **Transport Layer:** Provides secure communication channels between applications using protocols like TCP/IP with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for encryption.
- **Upper Layers (Session, Presentation, Application):** Implement access control mechanisms, user authentication, and data encryption specific to the applications.

Security Attacks

- **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 the **release of message contents** and **traffic analysis.**
  - **The release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.

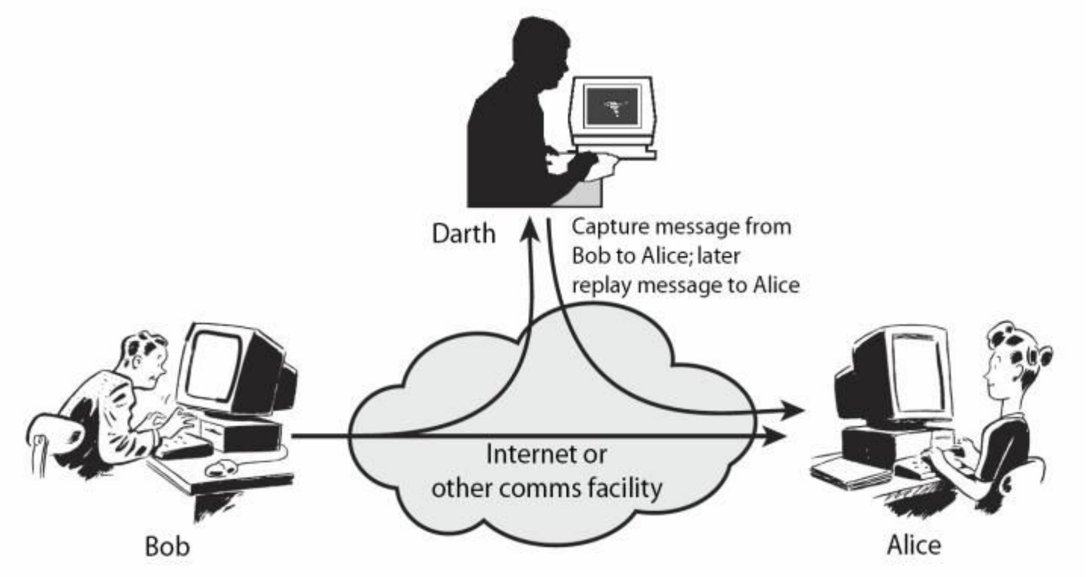

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Passive Attacks (Cont…)

- **Traffic analysis attack**, is less noticeable.
  - Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
- Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
- Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usually by means of encryption.

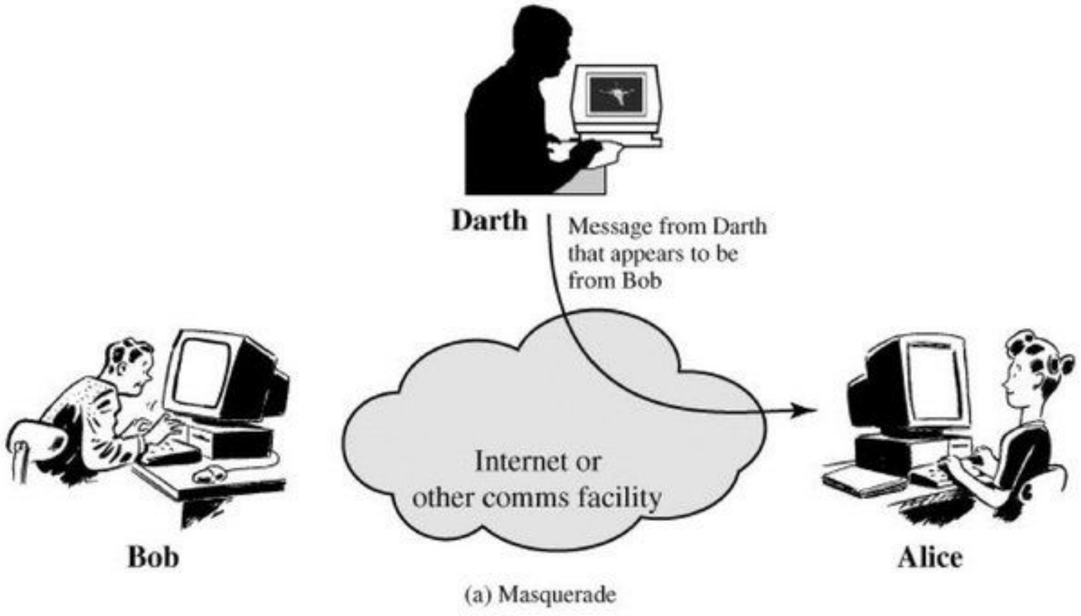
Security Attacks

- **Active Attacks:**
  - Active attacks involve some modification of the data stream or the creation of a false stream.
  - Active attacks can be subdivided into four categories: **masquerade, replay, modification of messages, and denial of service.**


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

Active Attacks

- A **masquerade** takes place when one entity pretends to be a different entity.
- A masquerade attack usually includes one of the other forms of active attack.
  - For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

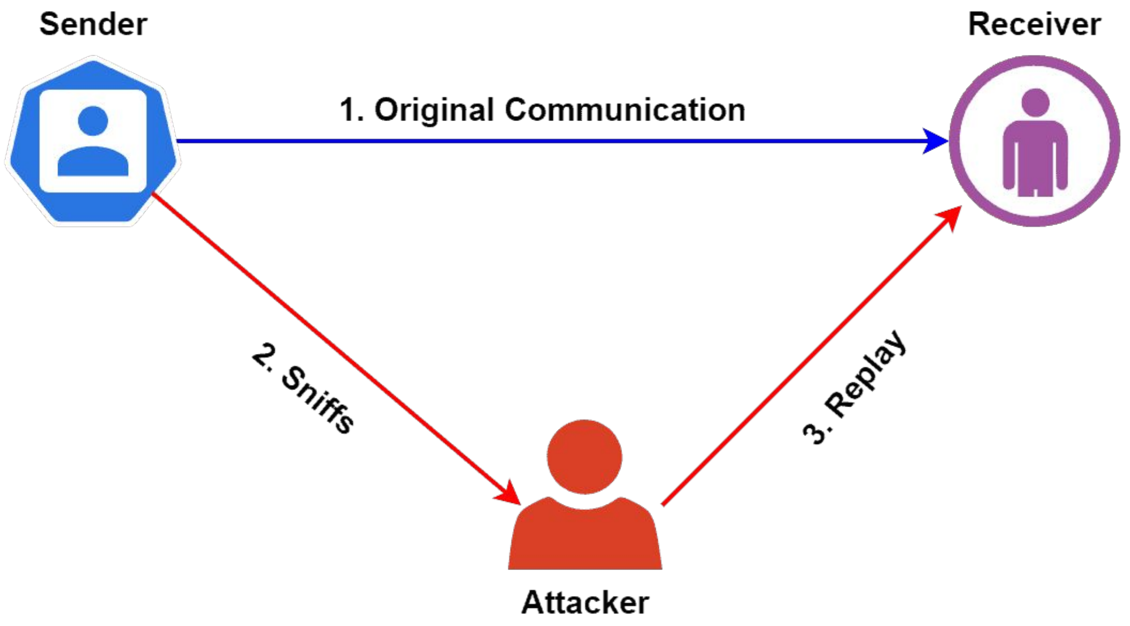

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Active Attack – Masquerade

Active Attacks (Cont..)

- A **replay attack** is a type of network attack in which an attacker captures a valid network transmission and then retransmit it later.
- **The main objective is to trick the system into accepting the retransmission of the data as a legitimate one.**
- Additionally, replay attacks are hazardous because it's challenging to detect.
- Furthermore, it can be successful even if the original transmission was encrypted.
- An attacker can lunch a replay attack to gain unauthorized access to systems or networks.



Active Attacks (cont..)

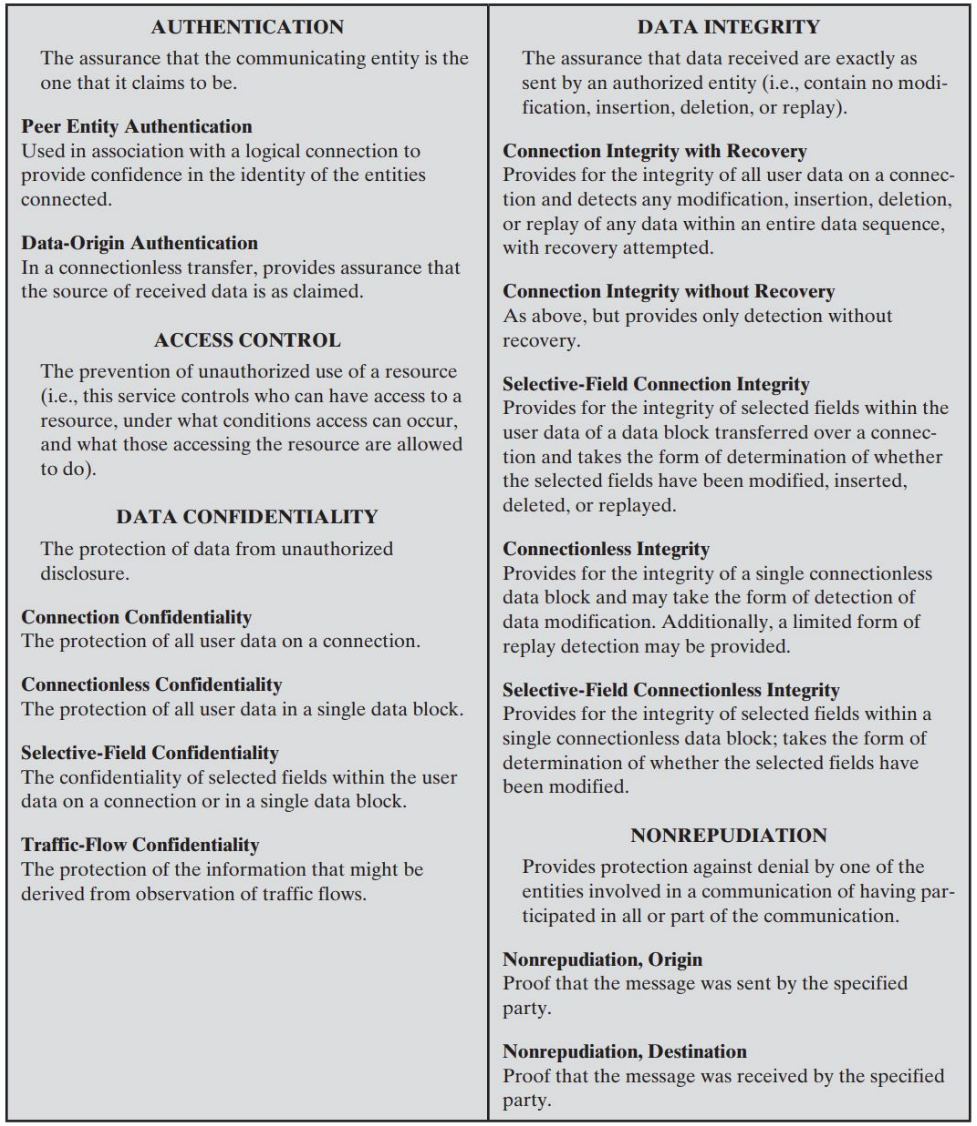
- **Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect .
  - For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”
- **The denial of service** prevents or inhibits the normal use or management of communications facilities .
  - This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).
  - Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

Security Services

- X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.
- X.800 divides these services into **five categories** and **fourteen specific services.**
- The five categories are:

1. Authentication
2. Access Control
3. Data Confidentiality
4. Data Integrity
5. Nonrepudiation

Table 1.2 Security Services (X.800)



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

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).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

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.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

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. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Authentication

- Authentication is the method of validating a particular entity's identity and unique credentials.
- Authentication concentrates on identifying if a particular individual has the right credentials to enter a system or a secure site.
- Two specific authentication services are defined in X.800:

■ **Peer entity authentication:**

- Provides the evidence of the identity of a peer entity in an association.
- Two entities are considered peers if they implement to same protocol in different systems; for example two TCP modules in two communicating systems.
- Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection.
- It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

□ **Data origin authentication:**

- **data origin authentication** is an assurance that the source of the information is indeed verified.
- Data origin authentication guarantees data integrity because if a source is corroborated, then the data must not have been altered. Various methods, such as **Message Authentication Codes** (**MACs**) and digital signatures are most commonly used.
- It does not provide protection against the duplication or modification of data units.
- This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.

Access Control

- Access control is the process of determining and assigning privileges to various resources, objects or data.
- In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links.
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data Confidentiality

- Confidentiality is the protection of transmitted data from passive attacks.
- The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data Integrity

- **Data integrity** is the accuracy, completeness, and quality of data as it’s maintained over time and across formats.
- A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.
- The destruction of data is also covered under this service.
- Thus, the connection-oriented integrity service addresses both message stream modification and denial of service.
- On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.
- We can make a distinction between service with and without recovery.
- Because the integrity service relates to active attacks, we are concerned with detection rather than prevention.
- If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation.
- Alternatively, there are mechanisms available to recover from the loss of integrity of data, as we will review subsequently. The incorporation of automated recovery mechanisms is, in general, the more attractive alternative