Introduction to Information Security

Dr. Amina SOUYAH

2021-2022

Chapter 1

Introduction to Security

Why study Information Security (InfoSec) ?

- You can not be an IT expert without also knowing IT security.
- Developing IT systems without considering security will lead to vulnerable IT systems.
- "Security by design" is a requirement in system design and is a prerequisite for privacy by design.
- Information security is a political issue (InfoSec is mandatory in Government , IT education).

Security certification for professionals

- Many different types of certifications available.
  - vendor neutral or vendor specific, profit or not-profit, e.g.,
    - $(ISC)^2$ https://www.isc2.org/
    - ISACA https://www.isaca.org/
    - SANS https://www.sans.org/
    - CISCO https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html
- Certification gives assurance of knowledge and skills
  - needs in job functions
  - gives credibility for consultants, applying for job,…
- Certification types reflect current topics in IT Security
  - Generally kept up-to-date
- Sometimes required
  - US Government IT Security jobs

What is Information ?

- Information can be considered as some meaning conveyed (conducted) by a sequence of symbols.

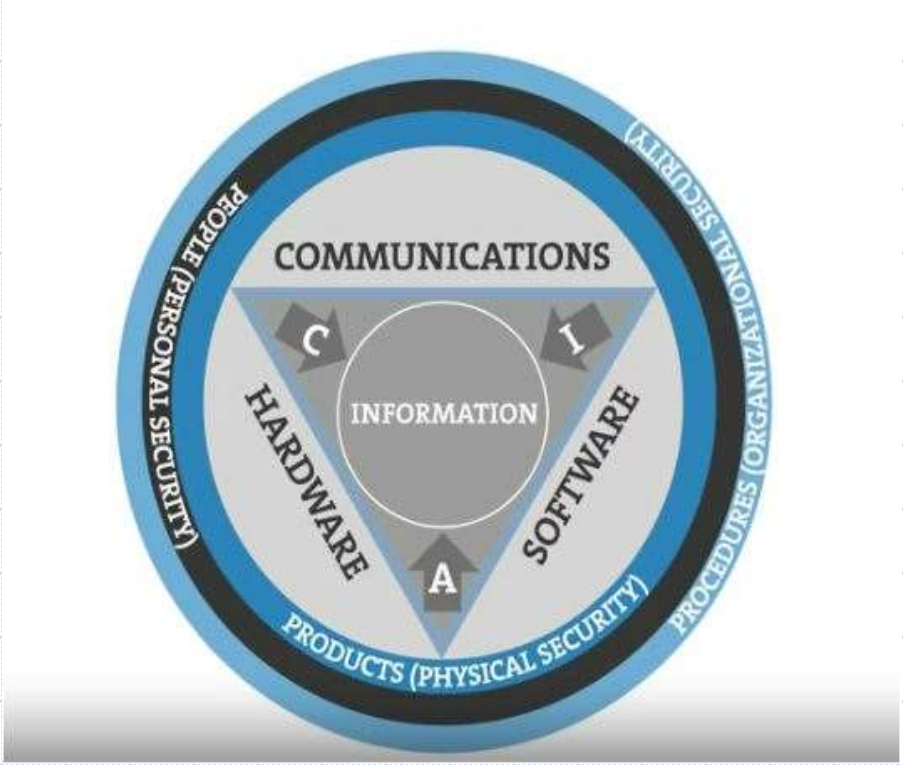
- These symbols can be:
  - Alphabetics (characters; numbers ; punctuations; etc),
  - Genetic sequence (such a book or something on computer),
  - Measurable, a discipline called information theory that developed from the work of Claude Shannon in the 1940s.

What is Information Security ?

- The states of being free from danger or threats.
- Regarding the Cambridge English dictionary: " security is the protection of a building, a person, an organization or a country against threads such as crime".
- We often use information security in the context of computer systems.
- In recent years, the term Cyber Security has been coined (invented).
- **ACM** (**A**ssociation of **C**omputer **M**achinery) has **J**oint **T**ask **F**orce (**JTF**) defines Cyber Security as: " a computing-based discipline involving, technology, people, information, and processes to enable assured operations of an organization".
- Information/Cyber Security is an interdisciplinary course comprising elements of law, policy, human factors, ethics, and risk management.

CIA Triad

- The classical model used to describe the key concepts in **I**nformation **S**ecurity (**IS**) is called the **CIA**.
- **CIA** stands for **C**onfidentiality, **I**ntegrity and **A**vailability.

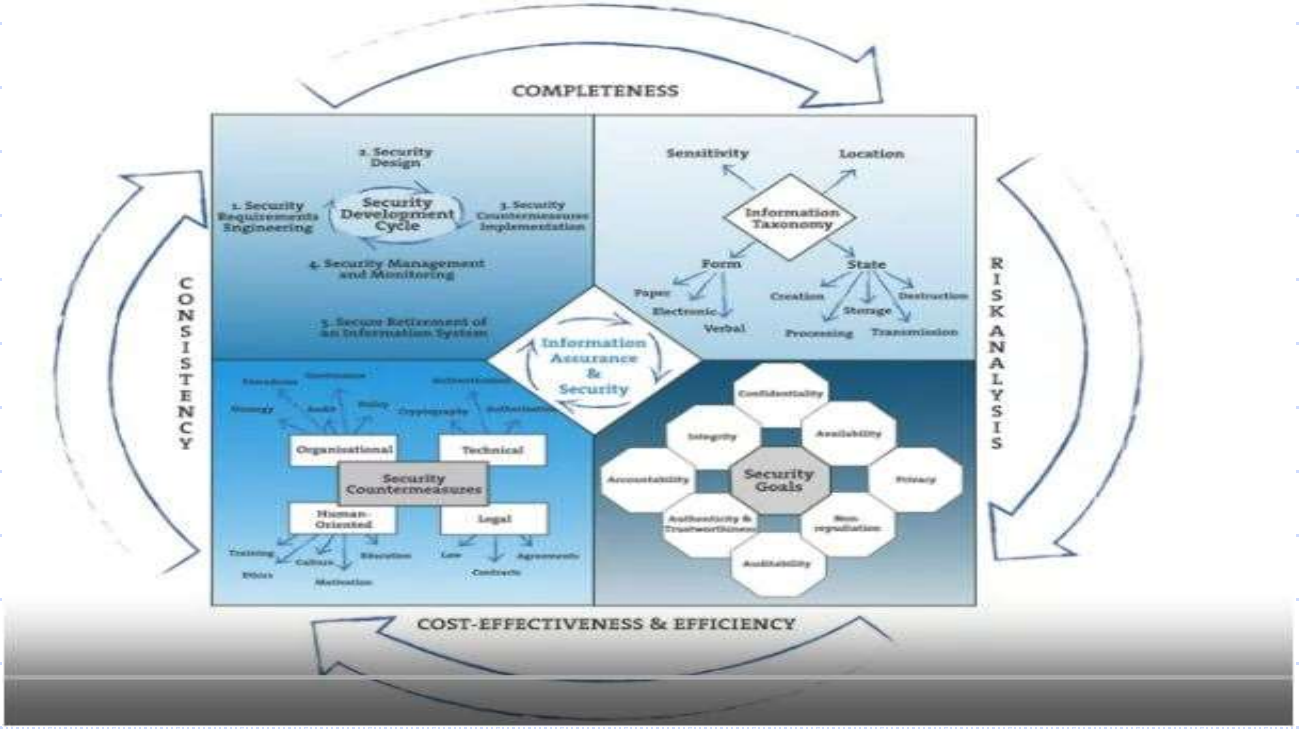


CIA Triad (cont'd)

- Confidentiality : a system should ensure that only authorized users access information.
  - (Symmetric-key Cryptography, Asymmetric-key Cryptography)
- Integrity : a system should ensure completeness, accuracy and an absence of unauthorized modifications in all its components.
  - (Hash functions)
- Availability : a system and all system components are available and operational when requires, as requested by authorized users.

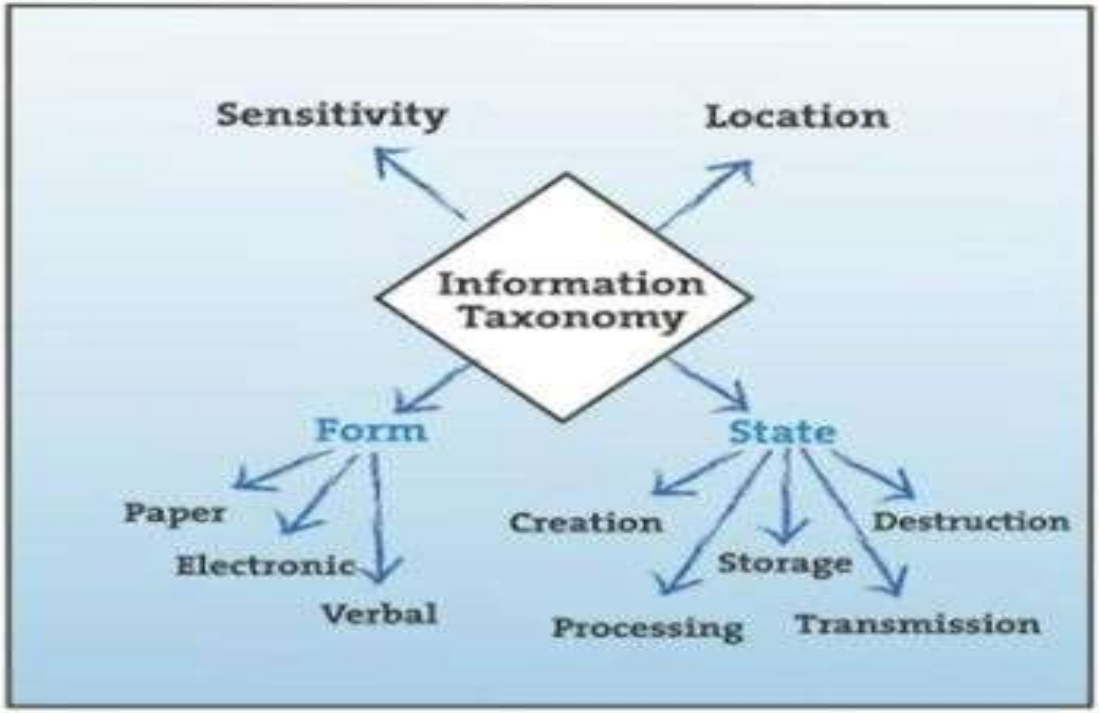
RMIAS model (cont'd)

- **RMIAS** stands for **R**eference **M**odel of **I**nformation **A**ssurance and **S**ecurity.
- Proposed in 2013, has combined a number of different viewpoints, or models that expand on the **CIA** classical model.



RMIAS model : Information Taxonomy (cont'd)

- Information form: paper, electronic,…
- Information state: created, processed, destroyed,…
- Information sensitivity: normal, secret, top secret,…
- Information location : different areas within the organization

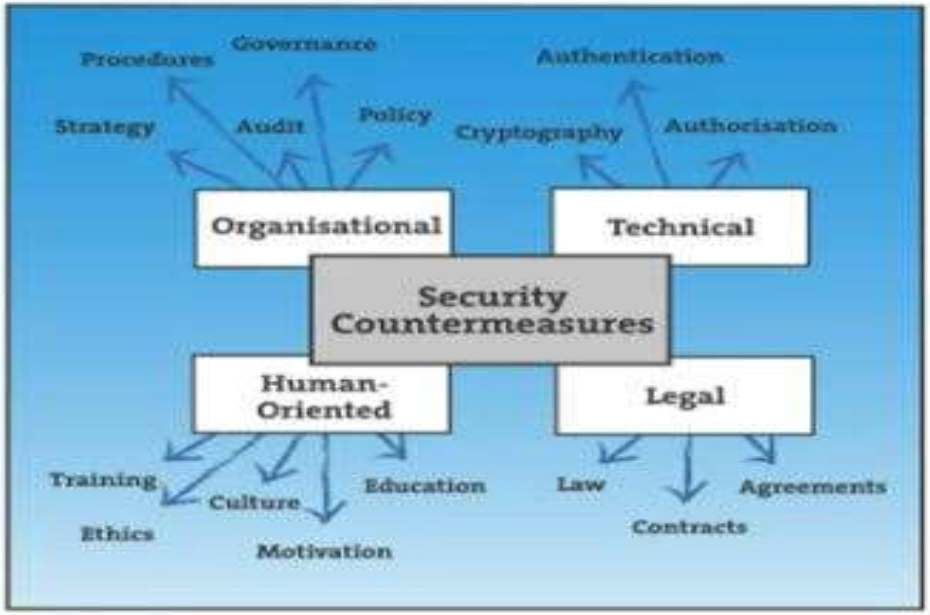


RMIAS model : Information Assurance Security (cont'd)

- In addition to CIA more security goals should be determined which are :
  - Accountability
  - Auditability
  - Non-repudiation
  - Authenticity and Trustworthiness
  - Privacy

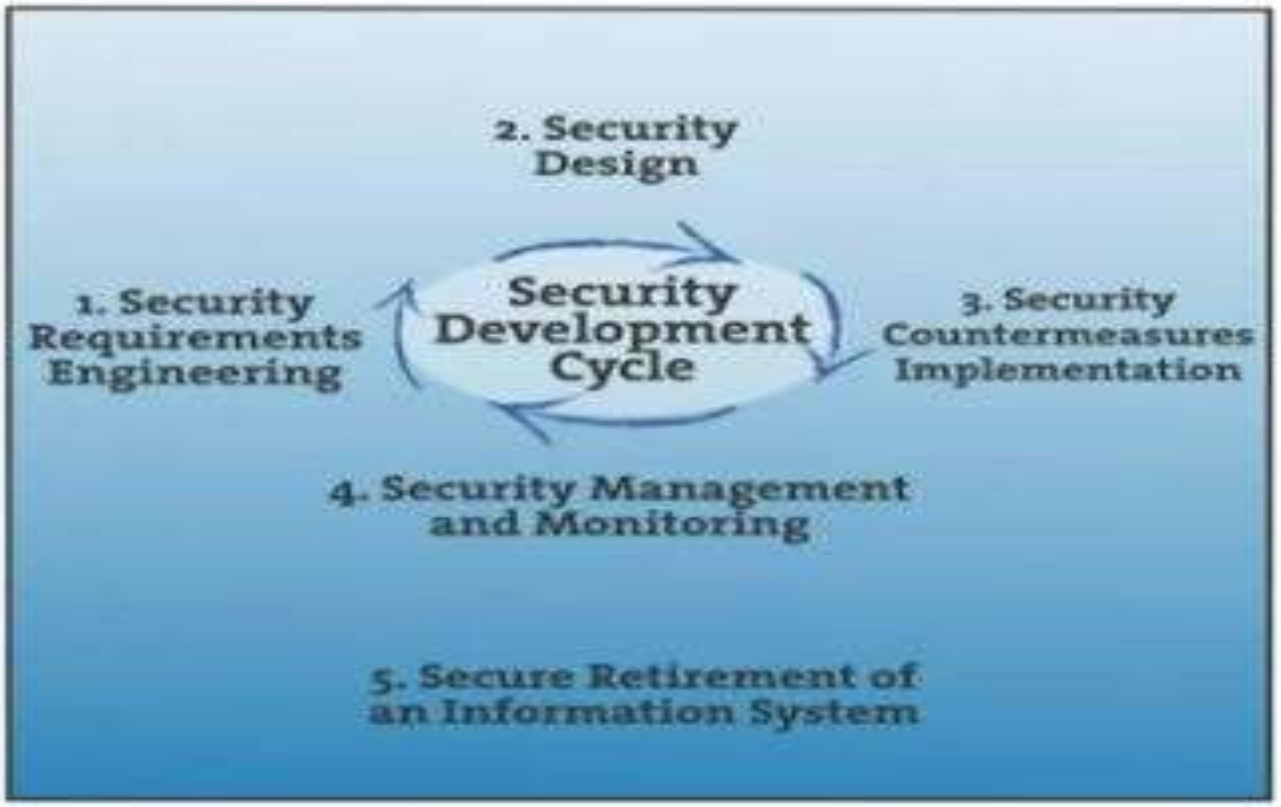
RMIAS model : Security countermeasures (cont'd)

- Technical solutions : (E.g., the use of cryptography to preserve data confidentiality),
- A set of requirements on us as an organization : (E.g., laws, contracts),
- Human : (E.g., developing an ethical framework),
- Organizational : (E.g., defining a policy, processes, procedures,…).



RMIAS model : Security Development Cycle (cont'd)

- Security requirements, security design, security implementation, security monitoring and management and security mechanism evolving and updating.



What is Cyber Security

- The **ACM** Joint Task Force defines Cyber Security as a computer based discipline in evolving technology, people, information and processes to enable assured operations. It evolves the creation, operation, analysis and testing of secured computer systems.

- It is an interdisciplinary course of study including aspects of law, policy, human factors, ethics and risk management in the context of adversaries. *So, what are the knowledge areas that have been identified ?*

What is Cyber Security (cont'd)

- Cyber defense : which includes aspects such like cryptography, computer security, network security, data security and information assurance.
- Cyber operations : this covers cyber attack, and penetration testing (i.e., behave as attacker and estimate what can be done to a system), cryptanalysis.
- Digital forensics : which includes hardware and software forensics on hosts and services, embedded systems (looking to identify incursions into our system by attackers).
- Cyber physical systems : **S**upervisory **C**ontrol and **D**ata **A**cquisition (so called **SCADA** systems), IOT systems, industrial control systems.

What is Cyber Security (cont'd)

- Secure software development : secure systems design, secure coding, secure deployment, maintainability, usability of secure systems.
- Cyber policy, governance and law : as set of laws and regulations that are identified for a cyber system, a range of regulations that apply for cyber systems and operations.
- Cyber risk management : cyber resiliency and assurance (E.g., we need to think about disaster recovery and business continuity as an organization. How to achieve this in the face of an attack, or a failure of a system).
- Human behaviors relating to cyber systems and operations : social engineering, social networks, user experience, organization behavior.

What is Information/Cyber Security (cont'd)

- as conclusion :

Information security is a multi disciplinary study and professional activity

- In which :

We are concerned with the developments and implementations of secure mechanisms of all types, namely Technical, Organizational, Human and Legal.

Information Security terminologies

- **A Threat (Menace)** : is described as the capacity of an adversary to attack a system, it is the adversary's goal, or what an adversary might try to do to the system.
- **Vulnerability (Vulnèrabilitè)** : consists of weaknesses (flaws) whether in the system or elsewhere, which can be exploited by the attackers that may lead to dangerous impacts.
- **An Attack** : occurs when some entity attempts to exploit a vulnerability.
- **An Adversary (Attacker)** : is a subject who tries to gain unauthorized access.
- **An asset** : is any data, device or other component of the system that is valuable.

A risk is when a Threat is associated to a vulnerability

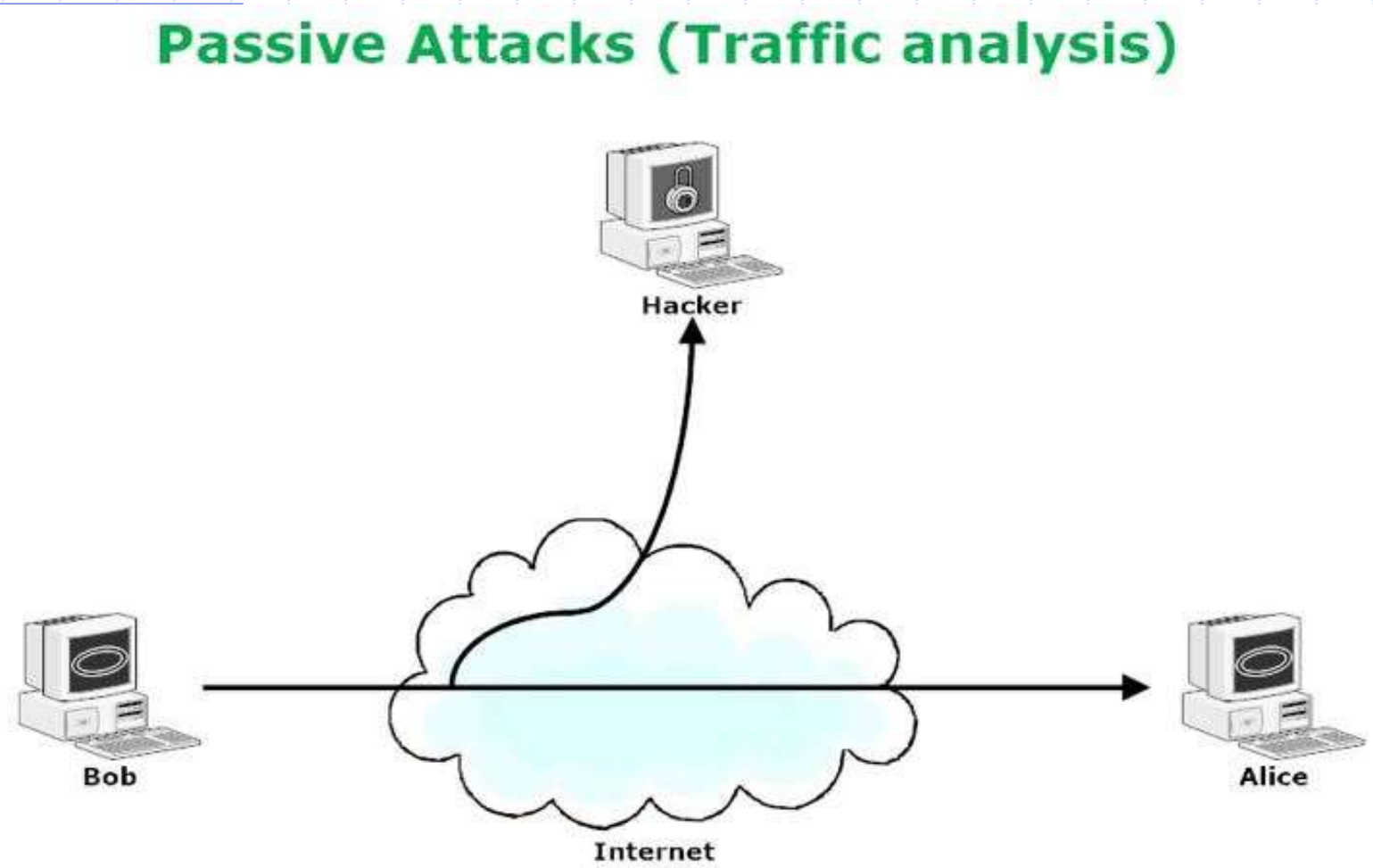
Threats

- A threat can be considered as a mechanism that the attacker employs to gain unauthorized access.
- Threats can be observed and classified based on different criteria:
  - Security threat source : the origin of the threat is either internal or external.
  - Security threat motivation : the goal of attackers on the system can be either malicious or non-malicious.
    - Malicious Threats : consist of inside or outside attacks caused by legitimate parties or non-legitimate parties to harm and disrupt a system like Viruses, Trojan horses and worms.
    - Non-malicious Threats : occur due to poor security policies and controls that allow vulnerabilities and errors to take place. It is caused by ignorant legitimate parities.

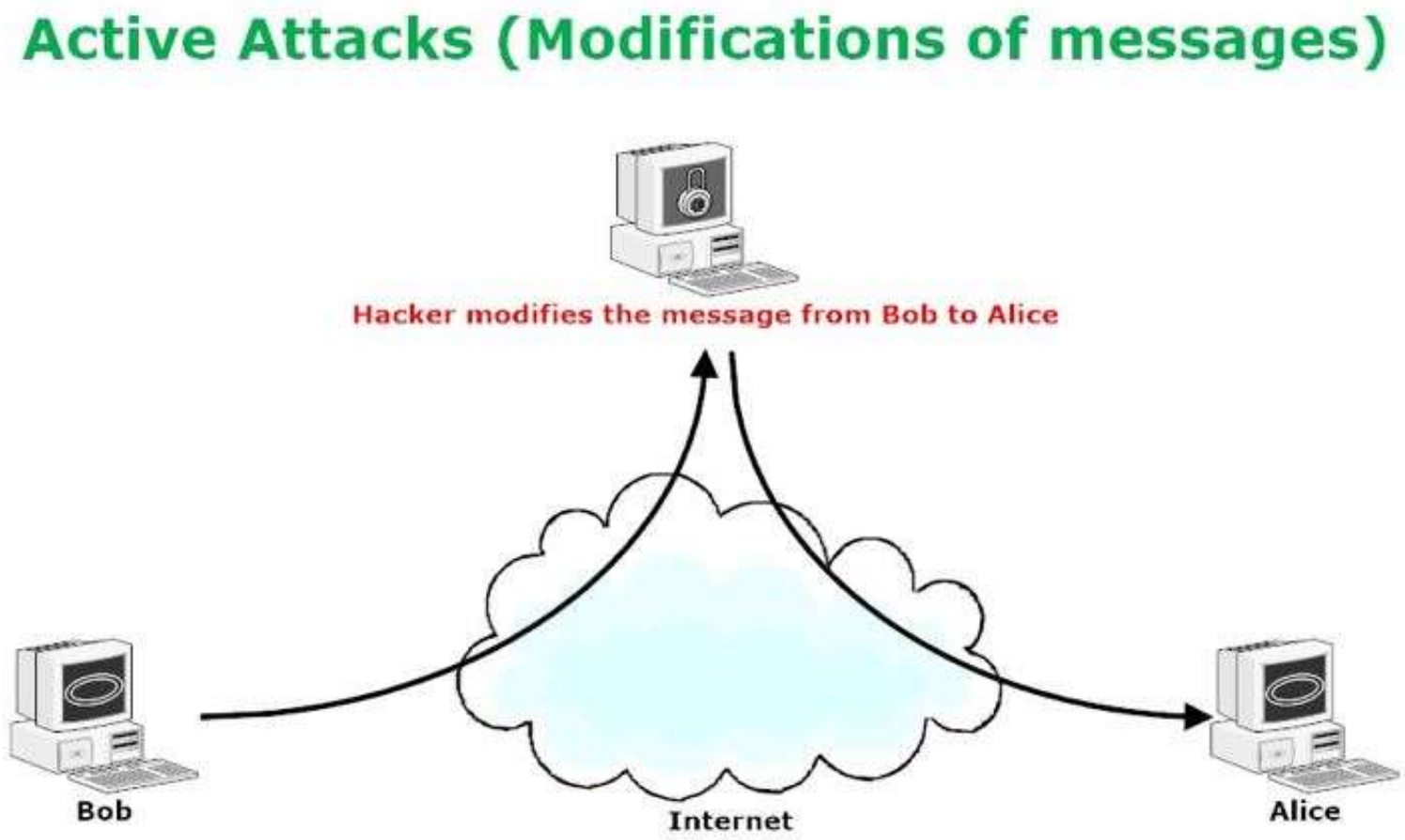
Threats (cont'd)

- Security threat intent : represents the intent of the entity that caused the threat.
  - Intentional Threats : it represents threats that are result of a harmful decision, e.g., computer crimes, or when some entity purposely damages property or information.
  - Unintentional Threats : it represents threats that are introduced without awareness, e.g., these threats basically include accidental modifications of a software or else what for example as programming errors,…
- Also intentional Threats or attacks can further more subdivided into : passive or active.
  - Passive attack : an attacker only observes/copies data over the system (data is always unchanged).
  - Active Attack : an attacker tries to modify data-content, aiming to achieve data or scan open ports or vulnerabilities over the system.

Threats (Passive attack) (cont'd)



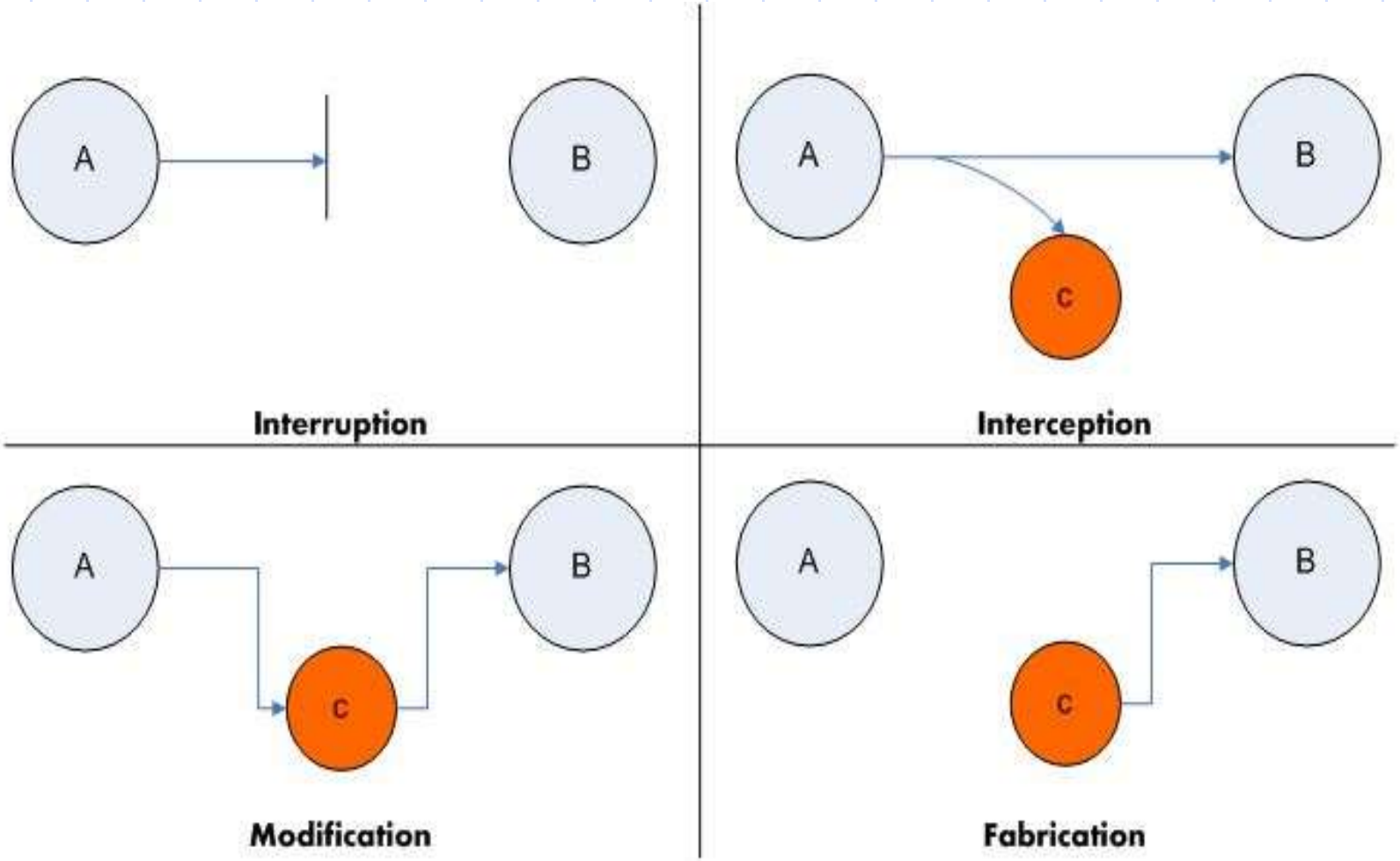
Threats (Active attack) (cont'd)



Threats (Active attack) (cont'd)

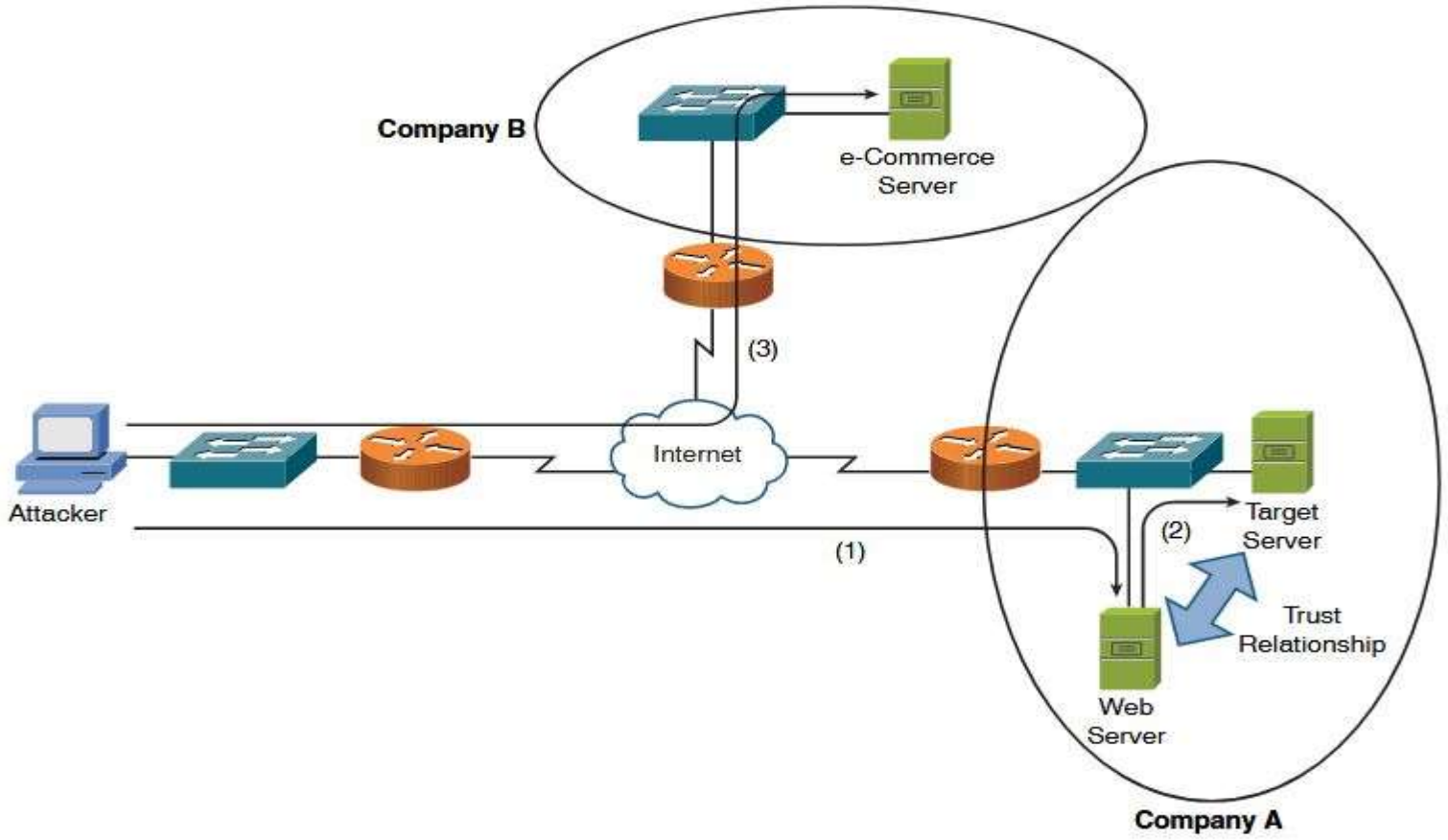
- **Interruption** : an asset of the system is destroyed or becomes unavailable. It is an attack on availability, e.g., User/Credential counterfeiting , Email spoofing,…
- **Interception** : an unauthorized party gains access to an asset. It is an attack on confidentiality, e.g., Eavesdropping on communication, packet sniffing to capture data, obtaining copies of messages,…
- **Modification** : when an unauthorized party gains access and tampers (alters) an asset. It is an attack on integrity, e.g., change existing information (Insertion attacks, Deletion attacks).
- **Fabrication** : an unauthorized party inserts a counterfeit object (a copy that is represented as the origin) into the system. It is an attack on authenticity, e.g., Overloading a server host so that it can not respond , blocking access to a service by overloading device/network,…

Threats (Active attack) (cont'd)



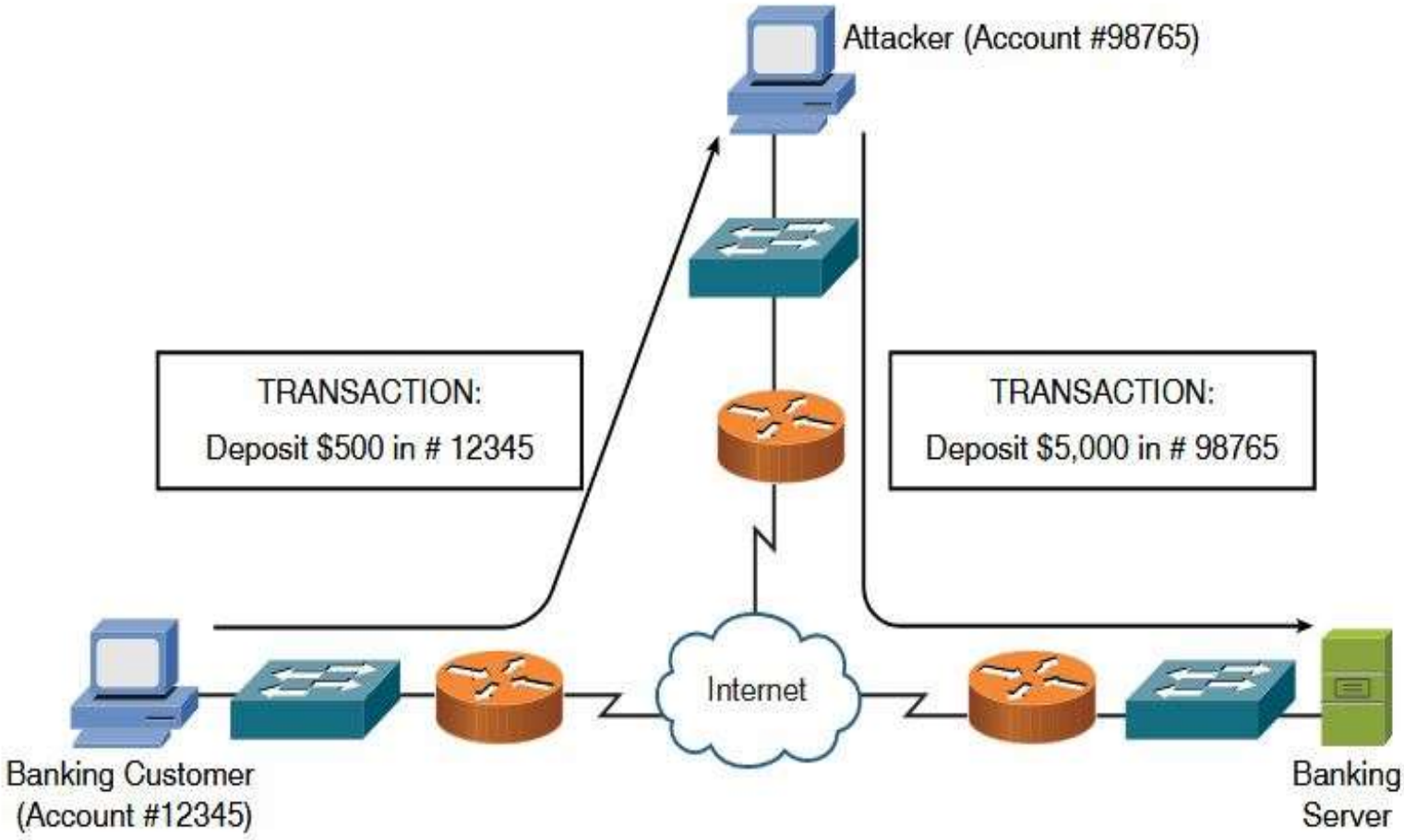
Types of Attacks (Attack targeting Confidentiality) (cont'd)

- A confidentiality attack attempts to make confidential data viewable by unauthorized parties.



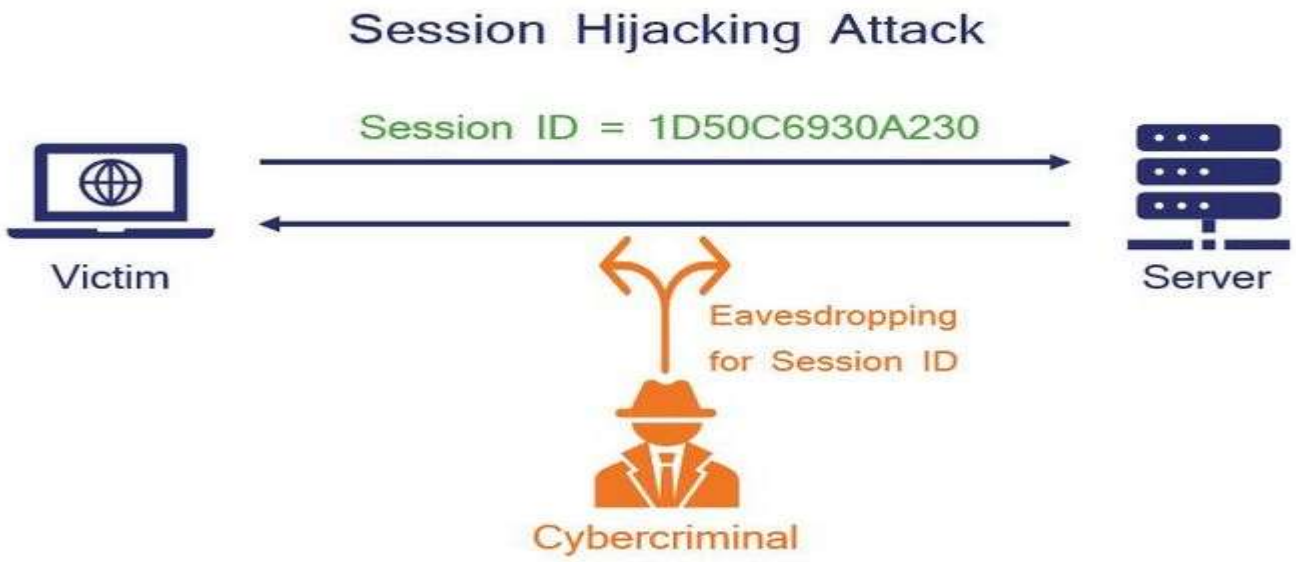
Attack targeting Confidentiality (MitM attack) (cont'd)

- Man in the Middle Attack (MitM) : can comprise both confidentiality and Data integrity.



Types of Attacks (Attack targeting Authentication)

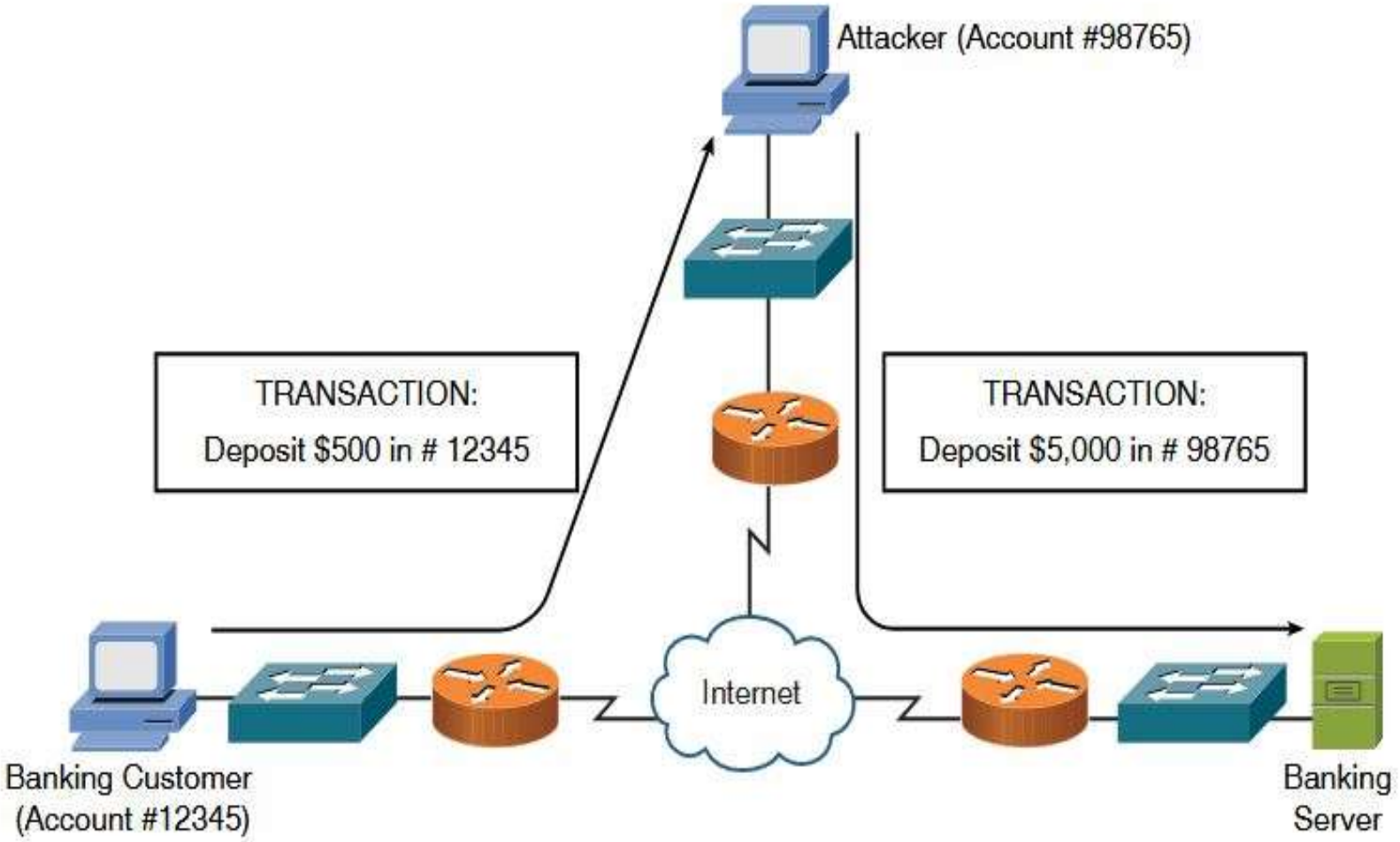
- Authentication and authorization attacks aim at gaining access to resources without the correct credentials (also named Impersonation attacks).
- Authentication specifically refers to how an application determines who you are (i.e., confirm legitimate party's identity).
- Authorization refers to the application limiting your access to only which you should see.



Types of Attacks (Attack targeting Data Integrity) (cont'd)

- Integrity attacks aim to gain unauthorized access with intentions to alter (modify) data.
- The attacker not only intercepts data by manipulates it as well.
- Integrity attacks : Salami attack, Data diddling, Password attack,….
- Man in the Middle Attack (MitM) : can comprise both confidentiality and Data integrity.

Types of Attacks (Attack targeting Data Integrity) (cont'd)



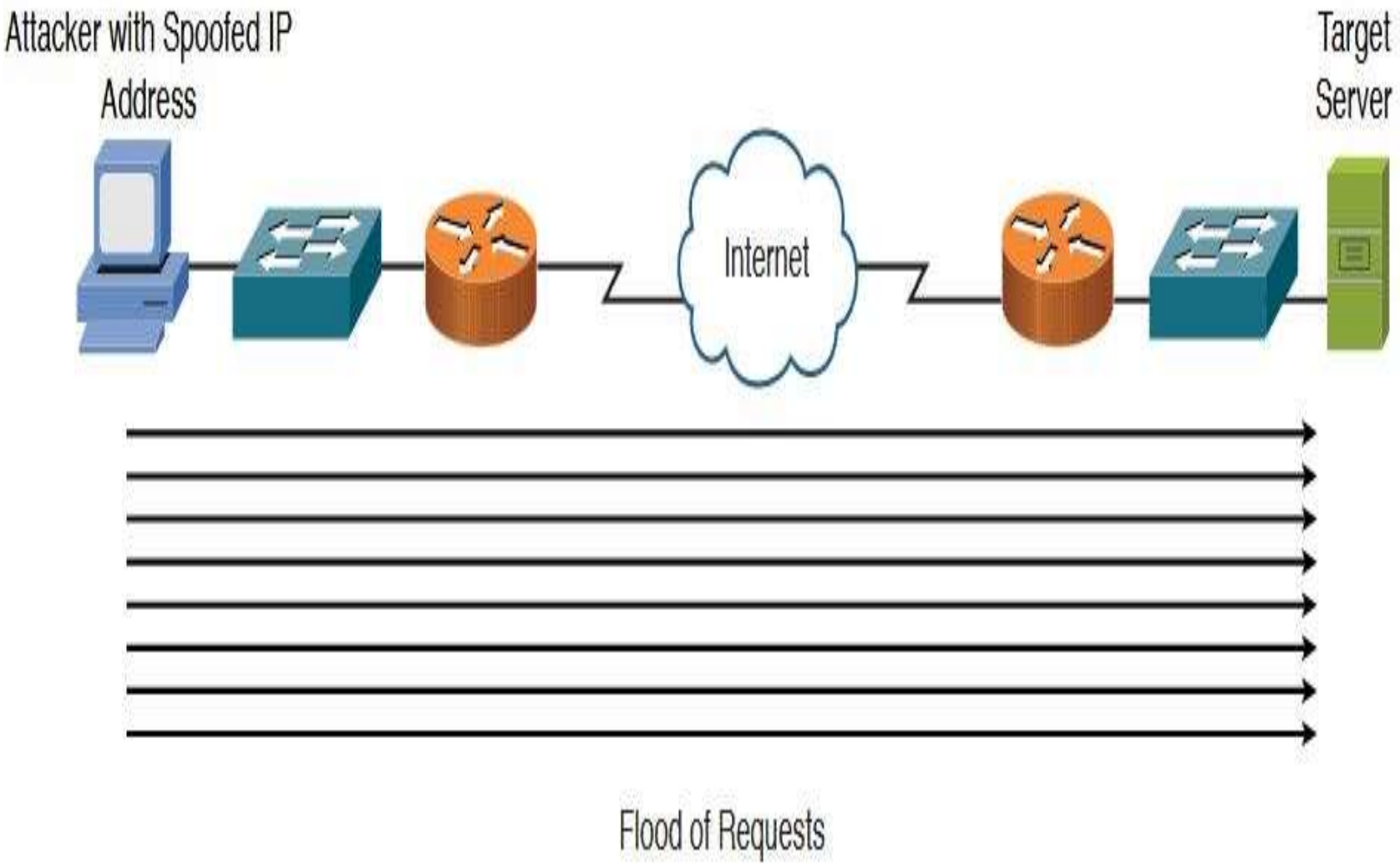
Types of Attacks (Attack targeting Availability) (cont'd)

- Availability attacks attempts to limit the accessibility and usability of a system (e.g., an asset, a service).
- Availability attacks vary widely, from consuming the resources of a target system, to do physical damage to that system.
- It is worth mentioning that fabrication attacks primary affect integrity but could be considered an availability attack as well.
- Examples of Availability (fabrication) attacks :
  - **D**enial of **S**ervice (**DoS**) is a one-to-one availability attack.
  - **D**istributed **D**enial **o**f **S**ervice (DDoS) is a many-to-one availability attack.

Attack targeting Availability (DoS attack) (cont'd)

- An attacker can launch DoS attack on a system by sending the target system a flood of data/requests that consume the target system's resources.
- Some OSs and applications crash when receiving a flood of data/requests (such vulnerability is exploited by attacker to make the system/application inoperable).
- An attacker often uses IP spoofing to conceal his identity when launching DoS attack.

Attack targeting Availability (DoS attack) (cont'd)

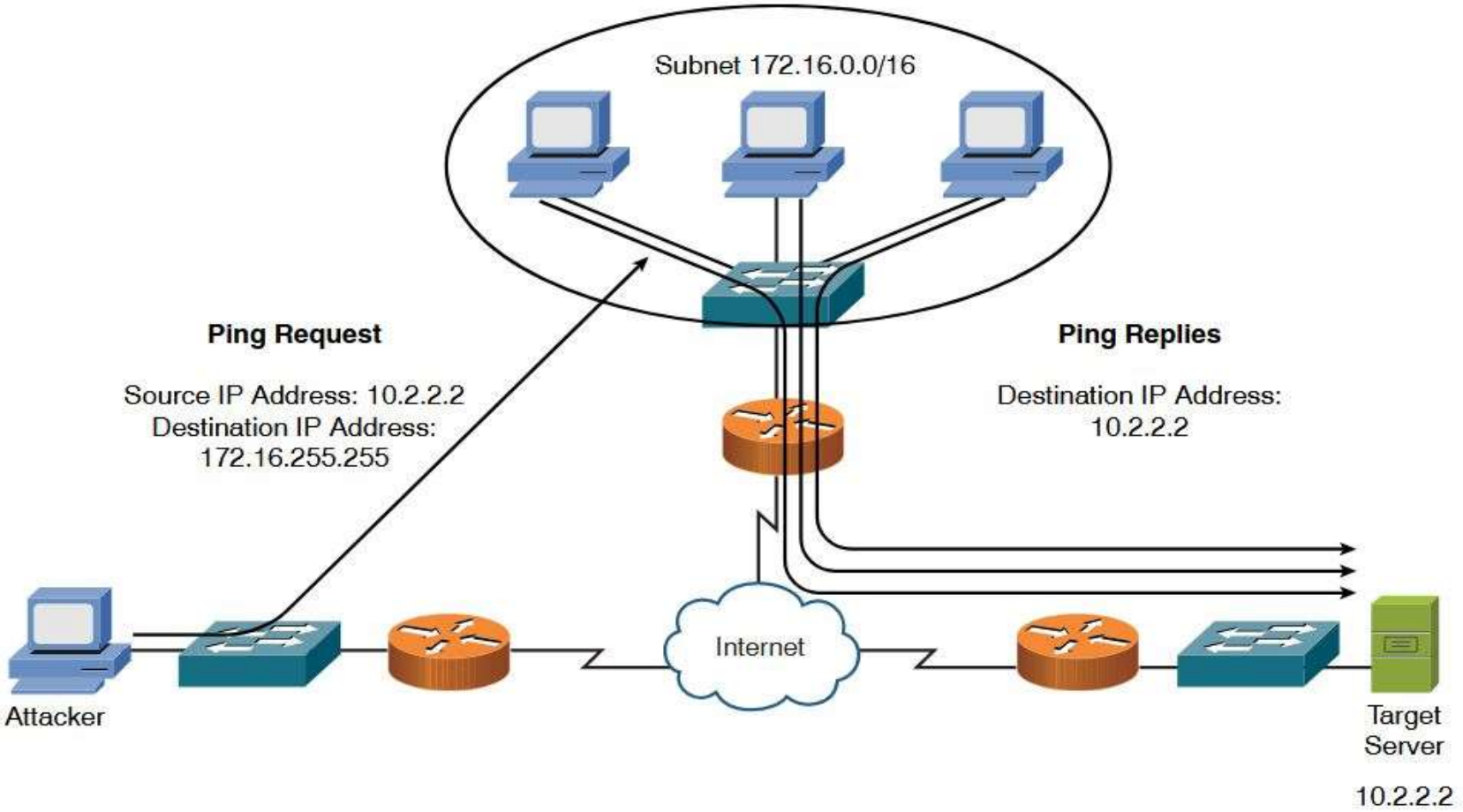


Attack targeting Availability (DDoS attack) (cont'd)

- DDoS can increase the amount of the traffic flooded to a target system.
- An attacker comprises multiple systems, and those comprised systems can be instructed by the attacker to simultaneously launch a DDoS attack against a target system .
- E.g., Smurf Attack , TCP SYN Flood Attack

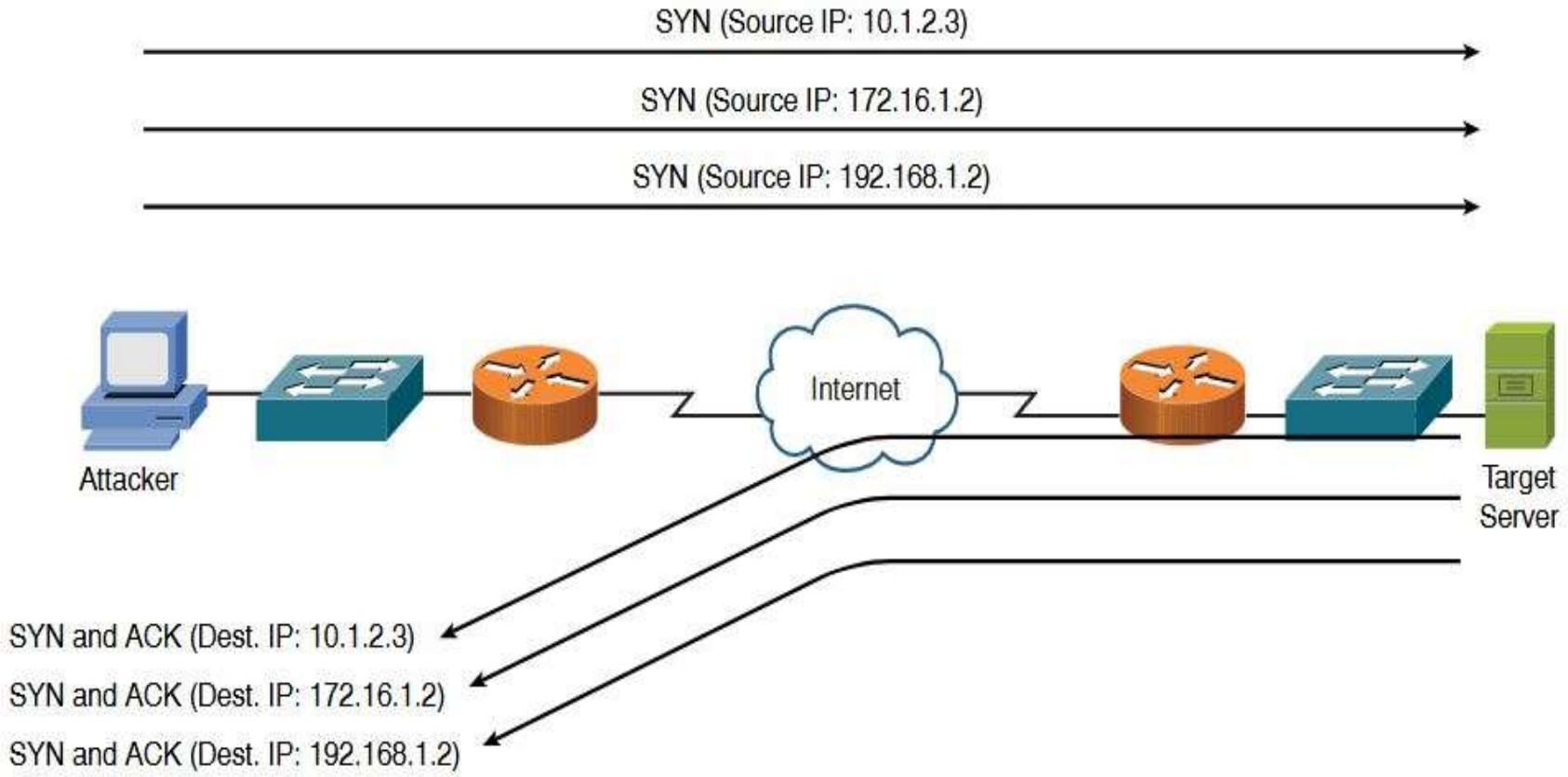
Attack targeting Availability (DDoS attack) (cont'd)

- E.g., Smurf Attack



Attack targeting Availability (DDoS attack) (cont'd)

- E.g., TCP SYN Flood



Conclusion

- Information Security is a critical problem for individuals and organizations, this issue turned to be more and more difficult to attain especially in the era of Internet of Thing (IoT).

- In what follows, we will be concerned by cryptography as a tool to employ for responding to Information Security problems and goals,….