German University in Cairo
Faculty of Media Engineering and Technology
Mervat Abu-Elkheir
Mohamed Abdelrazik
Ahmad Helmy

CSEN1001: Computer and Network Security

Spring Term 2019

Tutorial 1

Problem 1

Discuss the three fundamental objectives of information security as abstracted by the CIA triad.

Answer

The three concepts embody the fundamental security objectives:

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity	Data integrity involves guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity. System integrity is ensuring a system performs its intended function in an impaired manner free from unauthorized manipulation of the system.
Availability	Ensuring timely and reliable access to and use of information.

Problem 2

Discuss the main types of threats on Confidentiality.

Answer

An unauthorized disclosure of information is considered a threat to confidentiality. The following types of attacks could result in this threat:

Exposure	A type of threat action whereby sensitive data is directly released to an unauthorized entity. This type of threat action includes the following subtypes: □ **Deliberate Exposure**: Intentional release of sensitive data to an unauthorized entity. □ **Scavenging**: Searching through data residue in a system to gain unauthorized knowledge of sensitive data. □ **Human error**: Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data. There have been

	numerous instances of this, such as universities accidentally posting student’s confidential information on the Web. □ **Hardware or software error**: System failure that unintentionally results in an entity gaining unauthorized access to confidential information.
Interception	A type of threat action whereby an unauthorized entity directly accesses sensitive data while the data is traveling between authorized sources and destinations This type of threat action includes the following subtypes: □ **Theft**: Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data. □ **Wiretapping**: Monitoring and recording data that is flowing between two points in a communication system. □ **Emanations analysis**: Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but was not intended to communicate the data (e.g. electromagnetic emanations, acoustics emanations, etc.).
Inference	□ A type of threat action that reasons from characteristics or byproducts of communication and thereby indirectly accesses sensitive data, but not necessarily the data contained in the communication (e.g. Traffic analysis Attacks). *For example:* Onion routing systems are systems that are used to gain anonymity. Traffic analysis can be used to attack anonymous communication systems in that case traffic-analysis allows adversaries to infer which nodes relay the anonymous streams. This reduces the anonymity. □ A type of threat action that indirectly gains unauthorized access to sensitive information in a database management system by correlating query responses with information that is already known. In other words, an Inference attack occurs when a user is able to infer from trivial information more robust information about a database without directly accessing it.
Intrusion	An example of intrusion is an adversary gaining unauthorized access to sensitive data by overcoming the system’s access control protections. This type of threat action includes the following subtypes: □ Trespass: Gaining physical access to sensitive data by circumventing a system's protections. □ ⍰ Penetration: Gaining logical access to sensitive data by circumventing a system's protections.

Problem 3

Discuss the main types of threats on Integrity.

Answer

An unauthorized modification or destruction of information is considered a threat to Integrity. The following two types of attacks could result in this threat:

First, Deception:

A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. This is a type of threat consequence, and it can be caused by the following types of threat actions:

Masquerade	An unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. This type of threat action includes the following subtypes: □ **Spoof**: Attempt by an unauthorized entity to gain access to a system by posing as an authorized user. □ **Malicious logic**: In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.
Falsification	A type of threat action whereby false data deceives an authorized entity. This type of threat action includes the following subtypes: □ **Substitution**: Altering or replacing valid data with false data that serves to deceive an authorized entity. □ **Insertion**: Introducing false data that serves to deceive an authorized entity. □ **Deletion**: Unauthorized deletion of data.
Repudiation	Denial of sending, receiving or possessing some data

Secondly, Usurpation:

A circumstance or event that results in control of system or functions by an unauthorized entity. This type of threat consequence can be caused by the following types of threat actions:

Misappropriation	A type of threat action whereby an entity assumes unauthorized logical or physical control of a system resource. This type of threat action includes the following subtypes: □ **Theft of data**: Unauthorized acquisition and use of data in a system. □ **Theft of service**: Unauthorized use of a system service. □ **Theft of functionality**: Unauthorized acquisition of actual hardware, firmware, or software of a system component.
Misuse	□ The intentional use (by authorized users) of system resources for other than authorized purposes. Example: An authorized system administrator creates an unauthorized account for a friend. □ A type of threat action that causes a system component to perform a function or service that is detrimental to system security.

Problem 4

Discuss the main types of threats on Availability.

Answer

Disruption is a type of threat consequence; it can be caused by the following types of threat action:

Incapacitation	A type of threat action that prevents or interrupts system operation by disabling a system component. This type of threat action includes the following subtypes: □ **Malicious logic**: In context of incapacitation, any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources. □ **Physical destruction**: Deliberate destruction of a system component to interrupt or prevent system operation. □ **Human error**: Action or inaction that unintentionally disables a system component. □ **Hardware or software error**: Error that unintentionally causes failure of a system component and leads to disruption of system operation. □ **Natural disaster**: "act of God" that disables a system component (e.g. fire, flood, earthquake, lightning, or wind).
Corruption	A type of threat action that undesirably alters system operation by adversely modifying system functions or data. □ **Tampering**: Deliberately altering a system's logic, data, or control information to interrupt or prevent correct operation of system functions. □ **Malicious logic**: Any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data. □ **Human error**: Human action or inaction that unintentionally results in the alteration of system functions or data. □ **Hardware or software error**: Error that results in the alteration of system functions or data. □ **Natural disaster**: Any "act of God" that alters system functions or data (e.g. power surge caused by lightning).
Obstruction	A type of threat action that interrupts delivery of system services by hindering system operations. This type of threat action includes the following subtypes: □ **Interference**: Disruption of system operations by blocking communication of user data or control information. □ **Overload**: Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

Problem 5

Information Security aims to achieve some main objectives. Which of these objectives is violated in the following scenarios?

a) You hear from your friends that the final grades for the Information Security course are online. You access the GUC system, the site loads for a long time then you get an error page.

Answer: Availability

b) A group of hackers issue a lot of parallel ping requests to www.yahoo.com, the server gets overloaded and as a result, no one is able to access the site's services.

Answer: Availability

c) A programmer working at Facebook, accessed a database and was able to extract your password.

Answer: Confidentiality

d) A student hacks into the GUC system and changes his grades.

Answer: Integrity

Problem 6

Identify the malicious software in the following cases:

a) A person downloads a game, upon installing the game, a program launches in the background that sends all of the user's keystrokes to someone's email.

Answer: Trojan

b) A malware that hides within files, once these files are accessed it infects nearby files and reachable computers.

Answer: Virus

c) A malware that copies itself to accessible computers on its own.

Answer: Worm