1.1.3 Security Introduction

Security is the degree of protection against danger, damage, loss, and criminal activity. In regards to information security, computers, and IT networks, modern day security challenges include the following:

Challenge	Description
Sophisticated Attacks	Sophisticated attacks are complex, making them difficult to detect and thwart. Sophisticated attacks: ▪ Use common internet tools and protocols, making it difficult to distinguish an attack from legitimate traffic. ▪ Vary their behavior, making the same attack appear differently each time.
Proliferation of Attack Software	A wide variety of attack tools are available on the internet, allowing anyone with a moderate level of technical knowledge to download the tools and run an attack.
Attack Scale and Velocity	The scale and velocity of an attack can grow to millions of computers in a matter of minutes or days due to its ability to proliferate on the internet. Because modern attacks are not limited to user interactions, such as using a floppy disk, to spread an attack from machine to machine, the attacks often affect very large numbers of computers in a relatively short amount of time.

Common security terms include the following:

- *Confidentiality*, which ensures that data is not disclosed to unintended persons. This is provided through *encryption*, which converts the data into a form that makes it less likely to be usable by an unintended recipient.
- *Integrity*, which ensures that data is not modified or tampered with. This is provided through *hashing*.
- *Availability*, which ensures the uptime of the system so that data is available when needed.
- *Non-repudiation*, which provides validation of a message's origin. For example, if a user sends a digitally signed email, they cannot claim later that the email was not sent. Non-repudiation is enforced by *digital signatures*.

The CIA of Security refers to confidentiality, integrity, and availability. These are often identified as the three main goals of security.

Key security components include the following:

- *Physical security*, which includes all hardware and software necessary to secure data, such as firewalls and antivirus software.
- *Users* and *administrators*, which are the people who use the software and the people who manage the software, respectively.
- *Policies*, which are the rules an organization implements to protect information.

Risk management is the process of identifying security issues and deciding which countermeasures to take in reducing risk to an acceptable level. The main objective is to reduce the risk for an organization to a level that is deemed acceptable by senior management. Risk management generally takes the following items into account:

- An *asset* is something that has value to the person or organization, such as sensitive information in a database.
- A *threat* is an entity that can cause the loss of an asset or any potential danger to the confidentiality, integrity, or availability of information or systems, such as a data breach that results in a database being stolen.
- A *threat agent* (sometimes known as an *attacker*) is an entity that can carry out a threat, such as a disgruntled employee who copies a database to a thumb drive and sells it to a competitor.
- A *vulnerability* is a weakness that allows a threat to be carried out, such as a USB port that is enabled on the server hosting the database or a server room door that is frequently left ajar. USB devices pose the greatest threat to the confidentiality of data in most secure organizations. There are so many devices that can support file storage that stealing data has become easy, and preventing it is difficult.
- An *exploit* is a procedure or product that takes advantage of a vulnerability to carry out a threat, such as when a disgruntled employee waits for the server room door to be left ajar, copies the database to a thumb drive, and then sells it.

Types of threat agents include the following:

Type	Description
Employee	Employees can be the most overlooked yet most dangerous threat agent because they have greater access to information assets than anyone on the outside trying to break in. Employees are also known as *internal* threats. Employees can: ▪ Become disgruntled with their employer ▪ Be bribed by a competitor ▪ Be an unintentional participant in an attack ▪ Accidentally delete or cause data corruption
Spy	Spies can be employed in corporate espionage to obtain information about competitors for commercial purposes. Spies are typically deployed in the following scenarios: ▪ A spy applies for a job with a commercial competitor and then exploits internal vulnerabilities to steal information and return it to their client.

	▪ A spy attacks an organization from the outside by exploiting external vulnerabilities and then returns the information to their client.
Hacker	In general, a *hacker* is any threat agent who uses their technical knowledge to bypass security mechanisms to exploit a vulnerability to access information. Hacker subcategories include the following: ▪ *Script kiddies*, who download and run attacks available on the internet, but generally are not technically savvy enough to create their own attacking code or script. ▪ *Cybercriminals*, who usually seek to exploit security vulnerabilities for some kind of financial reward or revenge. ▪ *Cyber terrorists*, who generally use the Internet to carry out terrorist activities, such as disrupting network-dependent institutions.