Threats And Attacks (Chapter 2, BCIS)

Threat

A Threat is a possible security violation that might exploit the vulnerability of a system or asset. The origin of threat may be accidental, environmental (natural disaster), human negligence or human failure. Difference types of security threats are interruption, interception, fabrication and modification.

Attack

Attack is a deliberate unauthorized action on a system or asset. Attack can be classified as active and passive attack. An attack will have a motive and will follow a method when opportunities arise.

Threat Vs. Attack

Threat	**Attack**
Can be intentional or unintentional	Is intentional
May or may not be malicious	Is malicious
Circumstance that has ability to cause damage	Objective is to cause damage
Information may or may not be altered or damaged	Chance for information alteration and damage is very high
Comparatively hard to detect	Comparatively easy to detect
Can be blocked by control of vulnerabilities	Cannot be blocked by just controlling the vulnerabilities; no one knows what an outsider is capable of.
Can be initiated by system itself as well as outsider	Is always initiated by outsider (system or user)

Types of Threats

1. Compromises to Intellectual property

I**ntellectual property (IP):** The creation, ownership, and control of original ideas as well as the representation of those ideas. IP includes trade secrets, copyrights, trademarks, and patents. IP is protected by copyright law and other laws, carries the expectation of proper attribution or credit to its source, and potentially requires the acquisition of permission for its use, as specified in those laws. One might need to pay royalties to the original creator for the use of certain creations.

Software piracy: The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property. One must not make copies of software and it's license and install those in more devices than agreed.

Copyright protection and User Registration: A number of technical mechanisms—digital watermarks, embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws. The most common tool is a unique software registration code in combination with an end-user license agreement (EULA). Another effort to combat piracy is online registration.

In the context of Nepal, copyright is protected by "copyright law 2059" and the "Nepal Copyright Registrar's office" is responsible for its implementation.

2. Deviations in Quality of Service

Key Terms

availability disruption: An interruption in service, usually from a service provider, which causes an adverse event within an organization.

downtime: The percentage of time a particular service is not available; the opposite of uptime.

service level agreement (SLA): A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

uptime: The percentage of time a particular service is available; the opposite of downtime

An organization's information system depends on the successful operation of many interdependent support systems, including power grids, data and telecommunications networks, parts suppliers, service vendors, and even janitorial staff and garbage haulers. Any of these support systems can be interrupted by severe weather, employee illnesses, or other unforeseen events. Deviations in quality of service can result from such accidents as a backhoe taking out an ISP's fiber-optic link. The backup provider may be online and in service, but may be able to supply only a fraction of the bandwidth the organization needs for full service. This degradation of service is a form of availability disruption. Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems.

2.1 Internet Service issues

An organization that relies on the use of the internet for its operation will be heavily impacted by the interruption or degradation in the Internet service.

2.2 Communications and Other Service Provider Issues

Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services. The loss of these services can impair the ability of an organization to function.

2.3 Power Irregularities

Key Terms

blackout: A long-term interruption (outage) in electrical power availability.
brownout: A long-term decrease in electrical power availability.
fault: A short-term interruption in electrical power availability.
noise: The presence of additional and disruptive signals in network communications or electrical power delivery.
sag: A short-term decrease in electrical power availability.
spike: A short-term increase in electrical power availability, also known as a swell.
surge: A long-term increase in electrical power availability.

Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses. These fluctuations can pose problems for organizations that provide inadequately conditioned power for their information systems equipment. When power voltage levels vary from normal, expected levels, such as during a spike, surge, sag, fault, noise, brownout, or blackout, an organization's sensitive electronic equipment—especially networking equipment, computers, and computer based systems, which are vulnerable to fluctuations—can be easily damaged or destroyed. With small computers and network systems, quality power-conditioning options such as surge suppressors can smooth out spikes. The more expensive uninterruptible power supply (UPS) can protect against spikes and surges as well as sags and even blackouts of limited duration.

3. Espionage or Trespass

Key Terms

competitive intelligence: The collection and analysis of information about an organization's business competitors through legal and ethical means to gain business intelligence and competitive advantage.
industrial espionage: The collection and analysis of information about an organization's business competitors, often through illegal or unethical means, to gain an unfair competitive advantage. Also known as corporate spying, which is distinguished from espionage for national security reasons.
shoulder surfing: The direct, covert observation of individual information or system use.

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized person gains access to information an organization is trying to protect, the act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information-gathering techniques are legal—for example, using a Web browser to perform market research. These legal techniques are collectively called competitive intelligence. When information gatherers employ techniques that cross a legal or ethical threshold, they are conducting industrial espionage.

3.1 Hacker

Acts of trespass can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems without permission. Sound principles of authentication and authorization can help organizations protect valuable information and systems.

The classic perpetrator of espionage or trespass is the **hacker.**

Key terms related to Hackers

expert hacker: A hacker who uses extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

hacker: A person who accesses systems and information without authorization and often illegally.

jailbreaking: Escalating privileges to gain administrator-level or root access control over a smartphone operating system (typically associated with Apple iOS smartphones). See also rooting.

novice hacker: A relatively unskilled hacker who uses the work of expert hackers to perform attacks. Also known as a neophyte, n00b, or newbie. This category of hackers includes script kiddies and packet monkeys.

packet monkey: A script kiddie who uses automated exploits to engage in denial-of-service attacks.

Hacker Skills and Abilities Hackers possess a wide range of skill levels, as with most technology users. However, most hackers are grouped into two general categories: the expert hacker and the novice hacker. The expert hacker is usually a master of several programming languages, networking protocols, and operating systems, and exhibits a mastery of the technical environment of the chosen targeted system.

A new category of hacker has emerged over the last few years. The **professional hacker** seeks to conduct attacks for personal benefit or the benefit of an employer, which is typically a crime organization or illegal government operation (see the section on cyberterrorism). The professional hacker should not be confused with the **penetration tester**, who has authorization from an organization to test its information systems and network defense, and is expected to provide detailed reports of the findings. The primary differences between professional hackers and penetration testers are the authorization provided and the ethical professionalism displayed.

Escalation of Privileges Once an attacker gains access to a system, the next step is to increase his or her privileges (privilege escalation). While most accounts associated with a system have only rudimentary “use” permissions and capabilities, the attacker needs administrative or “root” privileges. These privileges allow attackers to access information, modify the system itself to view all information in it, and hide their activities by modifying system logs. A common example of privilege escalation is called **jailbreaking** or **rooting**.

3.2 Password attacks

Password attacks fall under the category of espionage or trespass just as lock-picking falls under breaking and entering. Attempting to guess or reverse-calculate a password is often called cracking. There are a number of alternative approaches to password cracking:

- Brute force
    - The application of computing and network resources to try every possible password combination is called a brute force password attack. Brute force password attacks are rarely successful against systems that have adopted the manufacturer's recommended security practices.
- Dictionary
    - The dictionary password attack, or simply dictionary attack, is a variation of the brute force attack that narrows the field by using a dictionary of common passwords and includes information related to the target user, such as names of relatives or pets, and familiar numbers such as phone numbers, addresses, and even Social Security numbers. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against passwords that are easy to guess. In addition, rules requiring numbers and special characters in passwords make the dictionary attack less effective
- Rainbow tables
    - A far more sophisticated and potentially much faster password attack is possible if the attacker can gain access to an encrypted password file, such as the Security Account Manager (SAM) data file. While these password files contain hashed representations of users' passwords—not the actual passwords, and thus cannot be used by themselves—the hash values for a wide variety of passwords can be looked up in a database known as a rainbow table.
- Social engineering
    - Attackers posing as an organization's IT professionals may attempt to gain access to systems information by contacting low-level employees and offering to help with their computer issues. After all, what employee doesn't have issues with computers? By posing as a friendly helpdesk or repair technician, the attacker asks employees for their usernames and passwords, then uses the information to gain access to organizational systems. Some even go so far as to actually resolve the user's issues. Social engineering is much easier than hacking servers for password files.

4. Forces of Nature

Forces of nature, sometimes called acts of God, can present some of the most dangerous threats because they usually occur with little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, landslides, mudslides, windstorms, sandstorms, solar flares, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only people's lives but the storage, transmission, and use of information. Because it is not possible to avoid threats from forces of nature, organizations must implement controls to limit damage and prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans.

4.1 Fire : Explain the threat by fire by yourself.

4.2 Floods

4.3 Earthquakes

4.4 Lightning

4.5 Landslides

4.6 Tornados

4.7 Hurricanes

4.8 Tsunamis

4.9 Electrostatic Discharge

4.10 Dust Contamination

4.11 Solar Activity

5. Human Error or Failure

This category includes acts performed without intent or malicious purpose or in ignorance by an authorized user. When people use information systems, mistakes happen. Similar errors happen when people fail to follow established policy. Inexperience, improper training, and incorrect assumptions are just a few things that can cause human error or failure. Regardless of the cause, even innocuous mistakes can produce extensive damage. Employee mistakes can easily lead to revelation of classified data, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information. Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat as a person who seeks to exploit the information, because the carelessness can create a vulnerability and thus an opportunity for an attacker. However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

Human error or failure often can be prevented with training, ongoing awareness activities, and controls. These controls range from simple activities, such as requiring the user to type a critical command twice, to more complex procedures, such as verifying commands by a second party. Many military applications have robust, dual-approval controls built in. Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs.

5.1. Social Engineering

Key Terms

advance-fee fraud (AFF): A form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer.

phishing: A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually email), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information. **pretexting:** A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information.

Pretexting: is commonly performed by telephone. social engineering The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.

spear phishing: Any highly targeted phishing attack

In the context of information security, social engineering is used by attackers to gain system access or information that may lead to target system access. There are several social engineering techniques, which usually involve a perpetrator posing as a person who is higher in the organizational hierarchy than the victim. To prepare for this false representation, the perpetrator already may have used social engineering tactics against others in the organization to collect seemingly unrelated information that, when used together, makes the false representation more credible.

5.1.1 Advance Fee Fraud

Also known as the 4-1-9 fraud, is named after a section of the Nigerian penal code. The perpetrators of 4-1-9 schemes often use the names of fictitious companies, such as the Nigerian National Petroleum Company. Alternatively, they may invent other entities, such as a bank, government agency, long-lost relative, lottery, or other nongovernmental organization. The scam is notorious for stealing funds from credulous people, first by requiring them to participate in a proposed money-making venture by sending money up front, and then by soliciting an endless series of fees. These 4-1-9 schemes are even suspected to involve kidnapping, extortion, and murder. According to Ultrascan Advanced Global Investigations, more than $82 billion had been swindled from victims as of 2014.

5.1.2 Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Pretexting, sometimes referred to as phone phishing or voice phishing (vishing), is pure social engineering. The attacker calls a potential victim on the telephone and pretends to be an authority figure in order to gain access to private or confidential information, such as health, employment, or financial records. The attacker may impersonate someone who is known to the potential victim only by reputation. Pretexting is generally considered pretending to be a person you are not, whereas phishing is pretending to represent an organization via a Web site or HTML e-mail. This can be a blurry **distinction**.

6. Information Extortion

Key Terms

information extortion: The act of an attacker or trusted insider who steals or interrupts access to information from a computer system and demands compensation for its return or for an agreement not to disclose the information.

ransomware: Computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption

Information extortion, also known as cyber extortion, is common in the theft of credit card numbers. The latest type of attack in this category is known as **ransomware**. **Ransomware** is a malware attack on the host system that denies access to the user and then offers to provide a key to allow access back to the user's system and data for a fee. There are two types of ransomware: lockscreen and encryption. Lockscreen ransomware denies access to the user's system simply by disabling access to the desktop and preventing the user from bypassing the ransom screen that demands payment. Encryption ransomware is far worse, in that it encrypts some or all of a user's hard drive and then demands payment.

7. Sabotage or Vandalism

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization. Although they might not be financially devastating, attacks on the image of an organization are serious. Vandalism to a Web site can erode consumer confidence, diminishing an organization's sales, net worth, and reputation.

7.1 Online Activism

Key Terms

cyberactivist: See hacktivist.

Cyberterrorism: Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

cyberterrorist: A hacker who attacks systems to conduct terrorist activities via networks or Internet pathways.

cyberwarfare: Formally sanctioned offensive operations conducted by a government or state against information or systems of another government or state. Sometimes called information warfare.

hacktivist: A hacker who seeks to interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

Internet activism, also known as **web activism**, **online activism**, **digital campaigning**, **digital activism**, **online organizing**, **electronic advocacy**, **e-campaigning**, and **e-activism**, is the use of electronic communication technologies such as social media, e-mail, and podcasts for various forms of activism to enable faster and more effective communication by citizen movements, the delivery of particular information to large and specific audiences as well as coordination. This form of activism is known as **positive internet activism.**

When the platform of the internet is misused for defacement and defamation of websites or exposure of sensitive personal data, it can be considered as a serious information threat.

8. Technological Obsolescence

Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of losing data integrity from attacks. Management's strategic planning should always include an analysis of the technology currently in use. Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is clear, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence. For eg. Windows 7 is the most popular and most used operating system in the context of Nepal due to its stability and available accessories softwares.

9. Theft

The illegal taking of another's property, which can be physical, electronic, or intellectual. The threat of theft is a constant. The value of information is diminished when it is copied without the owner's knowledge. Physical theft can be controlled easily using a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft, however, is a more complex problem to manage and control. When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the crime is not always readily apparent. If thieves are clever and cover their tracks carefully, the crime may remain undiscovered until it is too late. Theft is often an overlapping category with software attacks, espionage or trespass, information extortion, and compromises to intellectual property. A hacker or other individual threat agent could access a system and commit most of these offenses by downloading a company's information and then threatening to publish it if not paid.

10. Technical software failures or errors

Software used by systems may have purposeful or unintentional errors that result in failures, which can lead to loss of availability or unauthorized access to information. There are many to mention but in brief we may list them as below:

- **Buffer Overruns:** Getting memory of server full by the improperly handled and created entities. Eg. DOS attack, etc.

- **Catching Exceptions:** Exceptions (expected but irregular situations at runtime), when not handled for all the possible inputs, leads to undefined state of program.
- **Command Injection:** Injection of commands by the hackers/users when a simple string is expected.
- **Cross-Site Scripting (XSS):** Hacker first injects/encodes malicious code in the target server/website and when a common user visits it to the infected site it would look normal to the visitor. Hence, Cross-site scripting allows the attacker to acquire valuable information, such as account credentials, account numbers, or other critical data from common visitors of a website through the legitimate website without the knowledge/consent of the site owner and the visitor.
- **Failure to Handle Errors:** Errors in code is a situation when a program is not prepared to face a situation. For eg. There is a form for collection of mobile numbers in the user interface but there is no code to save it to the database, no declaration of variable prior its use, etc. There are many of its kind.
- **Failure to protect Network Traffic:** Most publicly available wireless networks are backed by no to weak security measures. Any hacker may intercept those. Even in the case of a wired network where hubs are used instead of switches it's possible to listen to all the packets with packet sniffers.
- **Failure to Store and Protect Data Securely**: Access controls, regulate who, what, when, where, and how users and systems interact with data. Failure to properly implement sufficiently strong access controls makes the data vulnerable. Overly strict access controls hinder business users in the performance of their duties, and as a result the controls may be administratively removed or bypassed. To mention a few "hard coding" of passwords, encryption keys, or other sensitive information—can put that information at risk of disclosure.
- **Failure to Use Cryptographically Strong Random Numbers:** Most of the modern cryptographic technologies make use of random numbers. To generate those a seed is required, which could be some static value or the timestamp. But one with great experience in this field may regenerate the random number for the particular timestamp.
- **Format String Problems:** While copying strings of codes from untrusted sources one must verify that it does not contain any formatting identifier, such as '%' in C.
- **Improper file access:** If an attacker changes the file to be used in a program by the bogus one instead of a legitimate one. It is certain that the server itself or the clients of the application are forced to compromise.
- **Improper Use of SSL** Programmers use Secure Sockets Layer (SSL) to transfer sensitive data, such as credit card numbers and other personal information, between a client and server. While most programmers assume that using SSL guarantees security, they often mishandle this technology. SSL and its successor, Transport Layer Security (TLS), both need certificate validation to be truly secure. We will learn more about this in the chapter of encryption.
- **Information Leakage** One of the most common methods of obtaining inside and classified information is directly or indirectly from one person, usually an employee. Attackers may gather intelligence related to the next movement, plot through employees, close ones to employees, bars and restaurants where employees hang out.

- **Poor usability:** Employees prefer doing any job in an easier way rather than a more secure way. Hence their work must be guided and audited in a serious manner.
- **Race Condition:** It is the state when two or more independent programs make use of the same resource. In such cases the common resource is manipulated independently. The change made by one program might hamper the operation of another.
- **SQL Injection** SQL injection occurs when developers fail to properly validate user input before using it to query a relational database.
  For example,

  Accept USER-ID from console;
  SELECT USERID, NAME FROM USERS WHERE USERID = USER-ID;
  // if attacker input "200 or 1==1" in console then the second line may be synthesized as: SELECT USERID, NAME FROM USERS WHERE USERID = "200 or 1==1";

  In above example 1==1 is always true and there is no any query validation between input and query to the server, hence the attacker is able to list the names and ids of all the users in the table.
- **Trusting Network Address Resolution:** The DNS is a function of the World Wide Web that converts a URL like www.course.com into the IP address of the Web server host. This distributed model is vulnerable to attack or "poisoning." DNS cache poisoning involves compromising a DNS server and then changing the valid IP address associated with a domain name into one the attacker chooses, usually a fake Web site designed to obtain personal information or one that accrues a benefit to the attacker—for example, redirecting shoppers from a competitor's Website. Such attacks are usually more sinister, however; for instance, a simulated banking site used for a phishing attack might harvest online banking information.
- **Use of Weak Password-Based Systems**
- **Web Client-Related Vulnerability (XSS):** One of the issues in programming Web Based applications is bugs that affect either the client side or the server side. Client-side cross-site scripting errors can cause problems that allow an attacker to send malicious code to the user's computer by inserting the script into an otherwise normal Web site. The user's Web browser, not knowing the code is malicious, runs it and inadvertently infects the client system. Some code can read a user's Web information, such as his or her Web history, stored cookies or session tokens, or even stored passwords.
- **Web Server-Related Vulnerabilities (XSS, XSRF, and Response Splitting):** The same cross-site scripting attacks that can infect a client system can also be used to attack Web servers. Cross-site request forgery (XSRF or CSRF) attacks cause users to attack servers they access legitimately, on behalf of an outside attacker. For example, on banking Websites, this could include changing a fund transfer account number to the attacker's account number. "HTTP response splitting occurs when data enters a Web application through an untrusted source, most frequently an HTTP request, or data is included in an HTTP response header sent to a Web user without being validated for malicious characters.

10. Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. This attack can consist of specially crafted software that attackers trick users into installing on their systems. This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means.

10.1 Malware

Malware is referred to as **malicious code** or **malicious software**. Other attacks that use software, like redirect attacks and denial-of-service attacks, also fall under this threat. These software components or programs are *designed to damage, destroy, or deny service* to targeted systems. Note that the terminology used to describe malware is often not mutually exclusive; for instance, Trojan horse malware may be delivered as a virus, a worm, or both. Malicious code attacks include the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. The most state-of-the-art malicious code attack is the polymorphic worm, or multivector worm. When an attack makes use of malware that is not yet known by the anti-malware software companies, it is said to be a **zero-day attack**. Other forms of malware include covert software applications—bots, spyware, and adware— that are designed to work out of users' sight or be triggered by an apparently innocuous user action.

10.1.1 Virus and worms

The primary difference between a virus and a worm is that viruses must be triggered by the activation of their host; whereas worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system. Worms do not require activation—or any human intervention—to execute or spread their code.

Viruses are often attached or concealed in shared or downloaded files, both executable files—a program that runs script—and non-executable files such as a Word document or an image file. When the host file is accepted or loaded by a target system, the virus remains dormant until the infected host file is activated. Only after the host file is activated, can the virus run, executing malicious code and replicating to infect other files on your system.

In contrast, worms don't require the activation of their host file. Once a worm has entered your system, usually via a network connection or as a downloaded file, it can then run, self-replicate and propagate without a triggering event. A worm makes multiple copies of itself which then spread across the network or through an internet connection. These copies will infect any inadequately protected computers and servers that connect—via the network or internet—to the originally infected device. Because each subsequent copy of a worm repeats this process of self-replication, execution and propagation, worm-based infections spread rapidly across computer networks and the internet at large.

10.1.2 Trozan Horse

It's a brilliant trick and a masterful feat of engineering is nowadays regarded as a malicious digital pest whose sole aim is to wreak havoc on its victims' computers unnoticed. It does this by reading passwords, recording keyboard strokes or opening the door for further malware that can even take the entire computer hostage. These actions can include:

- Deleting data

- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of computers or computer networks

Unlike computer viruses and worms, Trojans are not able to self-replicate.

10.1.3 Polymorphic Threats

Malware (a virus or worm) that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. One of the biggest challenges to fighting viruses and worms has been the emergence of polymorphic threats. A polymorphic threat actually evolves, changing its size and other external file characteristics to elude detection by antivirus software programs.

10.2 Backdoors

A malware payload that provides access to a system by bypassing normal access controls. A back door may also be an intentional access control bypass left by a system designer to facilitate development. It's also called a maintenance hook or trap door.

Using a known or newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Viruses and worms can have a payload that installs a back door or *trap door* component in a system, allowing the attacker to access the system at will with special privileges. Sometimes these doors are left behind by system designers or maintenance staff; such a door is referred to as a *maintenance hook*.

10.3 Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

bot: An abbreviation of robot, an automated software program that executes certain commands when it receives a specific input.

denial-of-service (DoS) attack: An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems.

distributed denial-of-service (DDoS) attack: A form of DoS attack in which a coordinated stream of requests is launched against a target from many locations at the same time using bots or zombies.

10.4 E-mail attacks

Spam is unsolicited bulk messages, spamming is the act of sending these messages, and a person who engages in the practice is a spammer. Most of the time, spamming is commercial in nature, and though the spam is bothersome, it isn't necessarily malicious or fraudulent (though it can be).Spam is always unrequested. It's annoying, it's usually promotional, it's sent to loads of people, and it's coming whether you asked for it or not. If you've signed up for a marketing newsletter and later gotten sick of it, that's unfortunate, but it isn't spam.

Another form of e-mail attack that is also a DoS attack is called a **mail bomb**. It can be accomplished using traditional e-mailing techniques or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageably large volume of unsolicited e-mail. By sending large e-mails with forged header information, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them

into sending many e-mails to an address of the attackers' choice. If many such systems are tricked into participating, the target e-mail address is buried under thousands or even millions of unwanted e-mails. Although phishing attacks occur via e-mail, they are much more commonly associated with a method of social engineering designed to trick users to perform an action, rather than simply making the user a target of a DoS e-mail attack.

10.5 Communications Interception Attacks

10.5.1 Packet Sniffer

A packet sniffer (or simply sniffer) can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This feature makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks. Sniffers add risk to network communications because many systems and users send information on local networks in clear text. A sniffer program shows all the 2 Software Attacks 101 Copyright 2018 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. WCN 02-300 data going by, including passwords, the data inside files (such as word-processing documents), and sensitive data from applications.

10.5.2 Spoofing

A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage. Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message, leaving them vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. IP spoofing and ARP spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

10.5.3 Pharming

Pharming attacks often use Trojans, worms, or other virus technologies to attack an Internet browser's address bar so that the valid URL the user types is modified to be that of an illegitimate Web site. A form of pharming called Domain Name System (DNS) cache poisoning targets the Internet DNS system, corrupting legitimate data tables. It modifies the user's traffic without the user's knowledge or active participation.

10.5.4 Man in the middle attack

A man-in-the-middle attack is a type of eavesdropping attack, where attackers interrupt an existing conversation or data transfer. After inserting themselves in the "middle" of the transfer, the attackers pretend to be both legitimate participants. This enables an attacker to intercept information and data from either party while also sending malicious links or other information to both legitimate participants in a way that might not be detected until it is too late.

Man-in-the-middle attacks:

- Are a type of session hijacking
- Involve attackers inserting themselves as relays or proxies in an ongoing, legitimate conversation or data transfer
- Exploit the real-time nature of conversations and data transfers to go undetected
- Allow attackers to intercept confidential data
- Allow attackers to insert malicious data and links in a way indistinguishable from legitimate data