CHAPTER 3

Threats and Vulnerabilities

LEARNING OUTCOMES

By the end of this chapter, you should be able to:

1. Define the meaning of computer criminals and psychology in computer systems.
2. Define the meaning of information warfare and computer penetration.
3. Determine the attacker involve in information warfare and computer penetration.
4. Determine malicious code and denial attacks associated with computer systems.
5. Explain the malicious code concepts.
6. Identify the physical threats in computer security.

INTRODUCTION

Source: http://www.youtube.com/watch?v=YqMt7aNBTq8

From the news video above, identify the issues relating to the topic threats and vulnerabilities.

Threats and vulnerabilities pose on-going risks to enterprise networks. Finding vulnerabilities on our systems and networks is the first step to mitigating potentially extensive damage through network attacks. It is important to pro-actively look for vulnerabilities on a regular basis so that they can be resolved before persistent threats exploit them.

Computer vulnerability is a weakness in an operating system, application code, or configuration that makes it possible for threats to exploit the system (or underlying network) thereby creating negative impact or damage. Threats are entities that act upon vulnerabilities for the purpose of trying to exploit it. A threat may be an unauthorised user such as a hacker, or even a system administrator trying to obtain access above and beyond their authorised level of privilege. Errant application or system processes can also act as threats and could possible erase valuable data if files and directories are not set with the correct permissions.

Today's threats can prevent organisations from accomplishing their mission by causing significant downtime, altering information and inserting fraudulent information in its place, or removing and destroying information altogether. While it is clearly illegal to destroy data that does not belong to us, this has not stopped hackers from taking part in these irreverent and disruptive crimes.

3.1 COMPUTER CRIMINALS AND PSYCHOLOGY

Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterised as falling in one or more.

Additionally, although the terms computer crime and cyber crime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important.

Figure 3.1 displays the definition of computer crime:

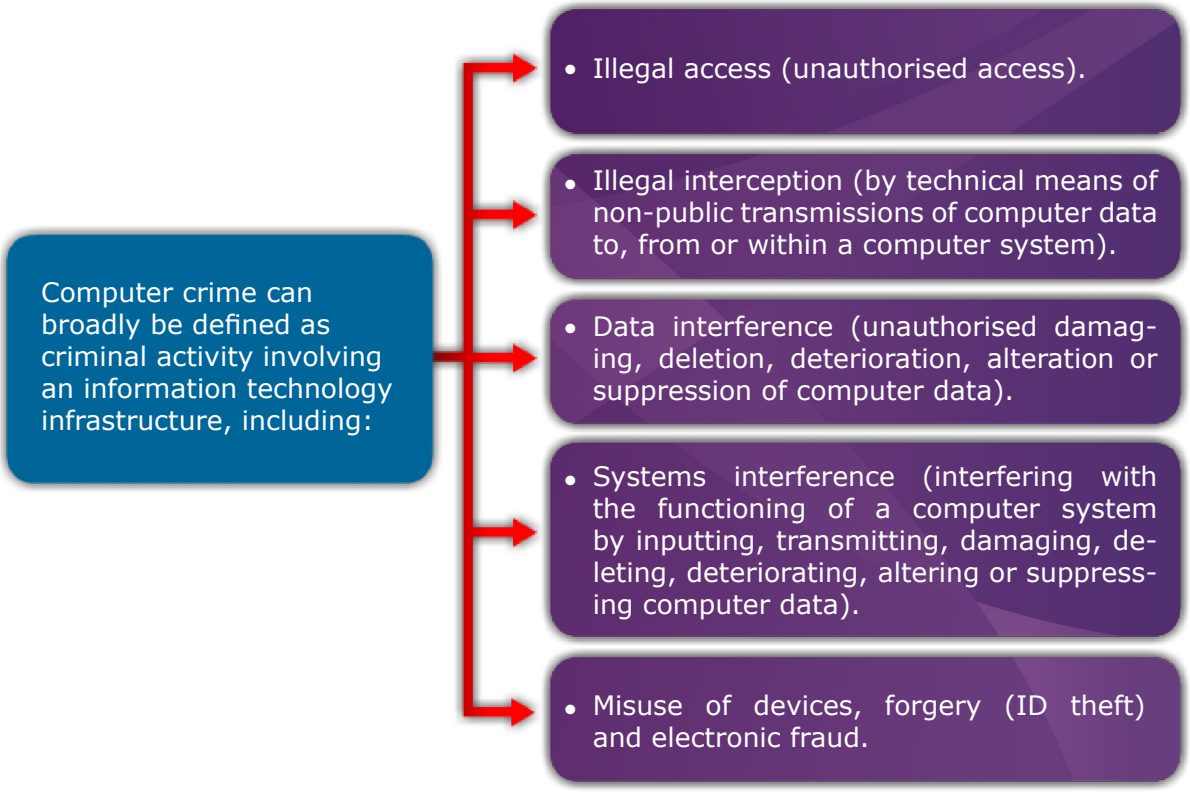


Figure 3.1: Definition of computer crime

Computer crime issues have become high-profile, particularly those surrounding hacking, copyright infringement through warez, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

3.1.1 Types of Computer Crimes

Computer-crimes are primarily grouped into four categories. However, in practice, multiple crimes, that is, concurrent criminality or lesser offences can occur during any given criminal transaction, resulting in an overlap between the classifications. These four categories of computer crimes are described in Figure 3.2:

Figure 3.2: The four types of computer crime

Let us look into details each of the types provided in Figure 3.2.

1. Computer as the Target

Crimes in which the computer is the target include offences such as:

- Theft of intellectual property;
- Theft of marketing information (e.g., customer lists, pricing data, or marketing plans); or
- Blackmail based on information gained from computerised files (e.g., medical information, personal history, or sexual preference).

These crimes also could entail sabotage of intellectual property, marketing, pricing, or personnel data or sabotage of operating systems and programs with the intent to impede a business or create chaos in a business' operations. Unlawful access to criminal justice and other government records is another crime that targets the computer directly. This crime covers:

- Changing a criminal history;
- Modifying want and warrant information;
- Creating a driver's license, passport, or another document for identification purposes;
- Changing tax records; or
- Gaining access to intelligence files.

Techno-vandalism occurs when unauthorised access to a computer results in damage to files or programs, not so much for profit but for the challenge. In such cases, the damage or loss may be intentional or accidental.

Another crime in this category is techno-trespass that is, "walking" through a computer just to explore. In such cases, the intruder only looks at a file, but even this violates the owner's privacy. This would be the technological equivalent of a criminal trespass. In all of these crimes, the offender uses the computer to obtain information or to damage operating programs. The offender commits the crime either by "super zapping" or by becoming a "super user." These labels mean that the offender accesses the operating program by masquerading as the system's manager, thus giving the intruder access to virtually every file in the system.

Not surprisingly, becoming a super user is relatively easy for individuals experienced in computer operations, because virtually every operating system has a trap door that allows individuals to enter a system and declare them as the system's manager. Trapdoors permit access to systems should a problem, either a human or technological one, arise. Unfortunately, this device also poses a threat to the system's integrity.

2. Computer as the Instrumentality of the Crime

In common law, instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime. In this category, the processes of the computer, not the contents of computer files, facilitate the crime.

Essentially, the criminal introduces a new code (programming instructions) to manipulate the computer's analytical processes, thereby facilitating the crime. Another method involves converting legitimate computer processes for illegitimate purposes. Crimes in this category include:

- Fraudulent use of automated teller machine (ATM) cards and accounts;
- Theft of money from accrual, conversion, or transfer accounts;
- Credit card fraud;
- Fraud from computer transactions (stock transfers, sales, or billings); and
- Telecommunications fraud.

One example of using a computer as the instrument to commit a crime is the growing problem of individuals' using cellular phones and electronically billing charges to other customers. In these cases, offenders obtain cellular billing identification codes by using scanning devices, which a small parabolic (curve-shaped) antennae connected to portable computers. When activated, these scanners capture and store account numbers transmitted by cellular phones.

The offenders operate near highways, because motorists frequently make calls from their cars. Once they capture the computerised billing codes, they program these codes into other cellular phones simply by hooking up the phone to a personal computer. Then, using software originally developed by programmers in London, they reprogram the signal chip in the cellular phone. The use of this software, which is easy to copy and to use, is spreading across the United States and Canada, sometimes being shared through underground computer bulletin board services (BBS).

3. Computer is Incidental to Other Crimes

In this category of computer crime, the computer is not essential for the crime to occur, but it is related to the criminal act. This means that the crime could occur without the technology; however, computerisation helps the crime to occur faster, permits processing of greater amounts of information, and makes it more difficult to identify and trace the crime. Such crimes include:

- Money laundering and unlawful banking transactions;
- Bulletin Board Services supporting unlawful activity;
- Organised crime records or books; and
- Bookmaking.

In one case, a suspect committed murder by changing a patient's medication information and dosage in a hospital computer.

Cases involving drug raids, money laundering seizures, and other arrests also have produced computers and electronic storage media containing incriminating information. Many times, the criminals encrypt the data or design the files to erase themselves if not properly accessed. In some instances, criminals even destroy the storage media, such as disks, to eliminate evidence of their illegal activities.

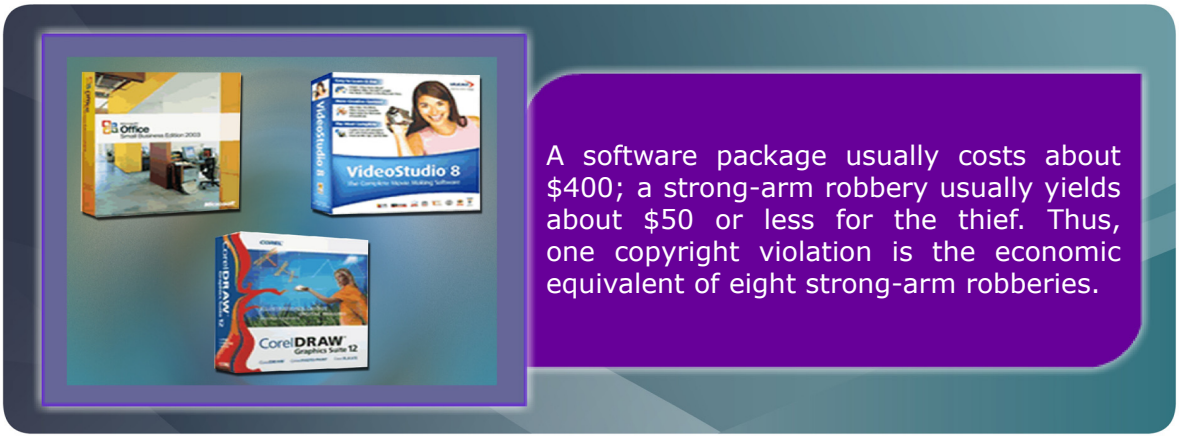
All of these situations require unique data recovery techniques in order to gain access to the evidence. And, in every case, the crimes could occur without the computers; the systems merely facilitate the offences.

Another illustration of how criminals use technology to further their illegal activities involves child pornography. Historically, consumers of ***child pornography*** *have trafficked photographs and related information through newsletters and tightly controlled exchange networks. Now, with the advancement of computer technology, child pornographers exchange this information through Bulletin Board Systems (BBS). Recently, U.S. Customs agents raided 40 locations in 15 States serviced by a Denmark-based, child pornography BBS. These criminals used the computer to facilitate the distribution of pornographic material and to increase the efficiency of criminal activity already occurring via other methods.*

4. Crimes Associated With the Prevalence of Computers

The simple presence of computers, and notably the widespread growth of microcomputers, generates new versions of fairly traditional crimes. In these cases, technological growth essentially creates new crime targets. Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment fall into this category of computer crime.

One offence in this category occurs with relative frequency - the violation of copyright restrictions of commercial software. Initially, these offences may not seem like a serious crime; yet, the potential loss to businesses can be quite staggering.



A software package usually costs about $400; a strong-arm robbery usually yields about $50 or less for the thief. Thus, one copyright violation is the economic equivalent of eight strong-arm robberies.

However, because the emotional trauma experienced in a piracy is almost nonexistent, many people do not view this as a serious crime. Evidence exists that software also is being written and sold explicitly to help hackers break into computers. In another area, successful computer programs, notably word processing, spreadsheets, and databases are being duplicated, packaged, and sold illegally on a large scale, just as audio and video tapes are pirated. Similarly, counterfeit computers and peripherals (items such as modems and hard disks) are being manufactured and sold as originals in much the same manner as imitation Rolex watches and Gucci shoes.

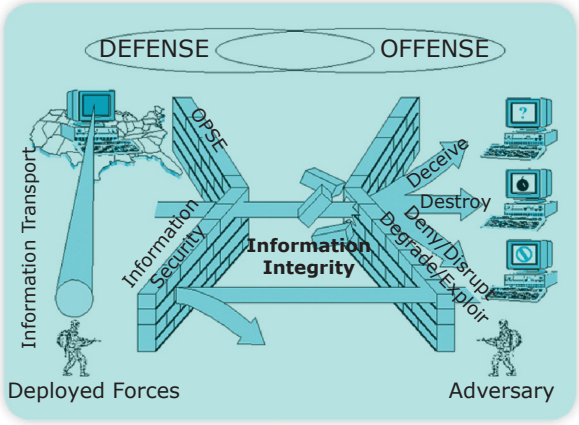
Criminals have adapted the advancements of computer technology to further their own illegal activities. Unfortunately, their actions have outpaced the ability of police to respond effectively. Protocols must be developed by law enforcement that addresses the various categories of computer crime. Investigators must know the materials to search and seize the electronic evidence to recover, and the chain of custody to maintain. Without question, law enforcement must be well prepared to deal with the many aspects of computer-related crimes and the techno-criminals who commit them.

SELF-CHECK

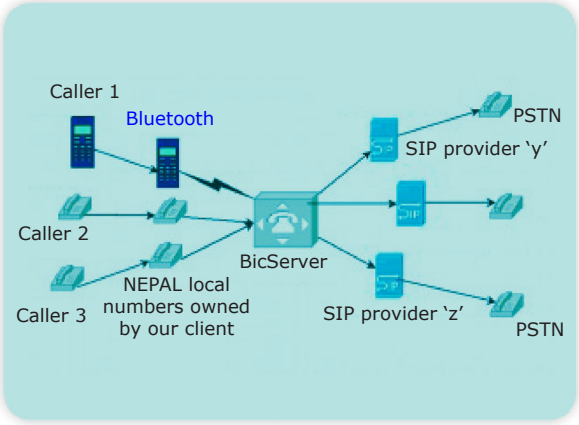
Use the internet to find an example of the types of computer crimes as described above. Share your findings in the LMS Forum.

3.2 INFORMATION WARFARE AND COMPUTER PENETRATION

Observe these two photos.



Information Warfare



Computer Penetration

These two photos displays an example of Information Warfare and Computer Penetration. From these photos, identify the differences between these two process.

3.2.1 What is Information Warfare?

Information Warfare (IW) is the process of protecting your information and network resources while potentially denying the adversary access to his or hers.

In a military setting it is a strategy for undermining an enemy's data and information system while defending and leveraging one's own information edge. In an organisational setting, it primarily means protecting your information assets from a variety of adversaries. The most obvious of these, although not necessarily the most dangerous, is intrusion.

In practice, information warfare may not only be the target of an adversary, it may also used as a weapon. Information warfare falls into the highly structured threat category. This type of threat is characterised by a much longer period of preparation, tremendous financial backing, and a large and organised group of attackers. The threat may not only include attempts to subvert insiders but might also consist of attempt.

3.2.2 What is Computer Penetration?

A ***computer penetration*** is a method done by potential attacker (Black Hat, Hacker or Cracker) to attack the computer system or network.

This process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

3.2.3 Who Are The Attackers?

There are several potential IW attackers which are criminal attacks, terrorist attack, hackers, scripts kiddies, programmers and rogue users. This is an active attack which has bypassed certain rules and policies that may result the same threats to the organisation. Table 3.1 describes the types of IW attackers followed by the description.

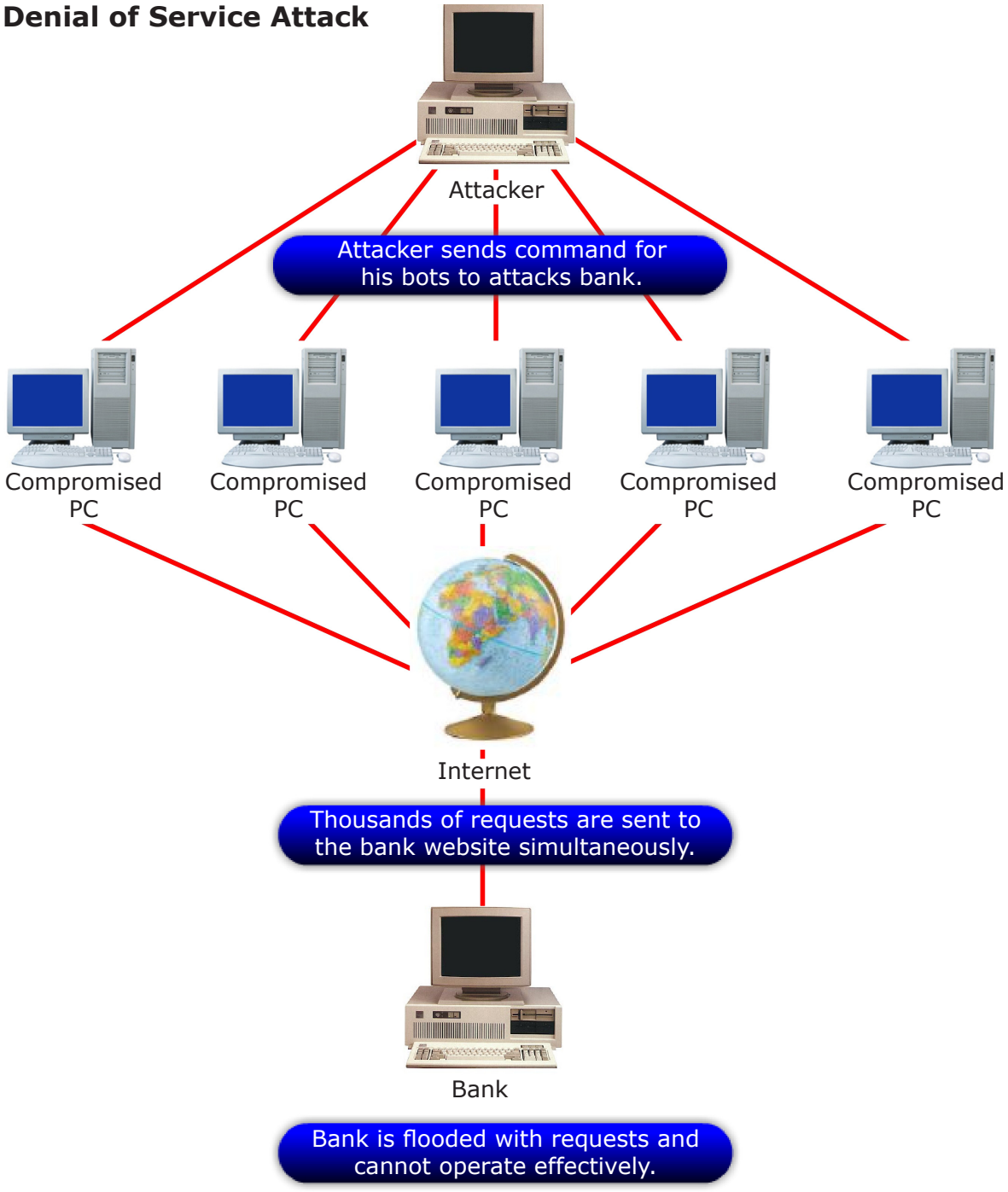
Table 3.1: IW Attackers

Attacker	Description
Criminal Attacks	It allows a crime to be committed without being at the scene of the event. It involves deliberate attacks on computer and telecommunications systems that range from data tampering to fraud and extortion. A criminal attack is one where the intent is financial gain for the attacker.

Terrorist Attack	It is an act of terrorism which is designed to specifically cause harm to people, systems, infrastructures or nations. There are two types of terrorism which is physical and virtual. Physical terrorism need a physical presence and is guarded against with physical security while virtual terrorism does not require physical presence, it is the most dangerous from of intrusion as it can be launched from anywhere on earth.
Hackers	It describes a person wish to break into another's computer or network. It is a form of attack that poses threats of data destruction, fraud, spread of viruses and so forth. Hackers are a primary adversary in industrial information warfare.
Script Kiddies	It is a term given to would-be hackers who do not possess the knowledge or skill to write their own programs but rely on ready-to-use kits form the Internet or programs written by others.
Programmers	Programmers sometimes bypass or disable security mechanisms, install insecure systems, install default passwords and backdoor provisions and circumvent established procedures. Hardware operating systems can have flaws that make data vulnerable to loss or interception. Hardware and its software must work together to ensure they do not contribute to lack of security.
Rogue Users	They are dishonest or unethical people, or perhaps users getting around some of the rules. They do things to be mischievous or damaging and may range from intruders to disgruntled or dismissed employees. Whether the hacking occurred via wired or wireless access, the addition of the rogue as a legitimate user will make further unauthorised wired or wireless accesses very easy.

3.3 MALICIOUS CODE AND DENIAL OF ATTACKS

Observe the next diagram.



Based from the diagram given, in your on words, describe how the malicious code and denial of attacks invades the computer system.

3.3.1 Malicious Code

Malicious codes are the general name for unanticipated or undesired effects in programs or program parts generated by an agent on the intent on damage. This does not include

unintentional damage although these errors could also have a serious negative effect. A bug or an error in a program is not considered as a malicious code. The agent is the writer of a program or the person that causes the distribution of the program.

Figure 3.3 shows the definition of malicious code and who developes it.

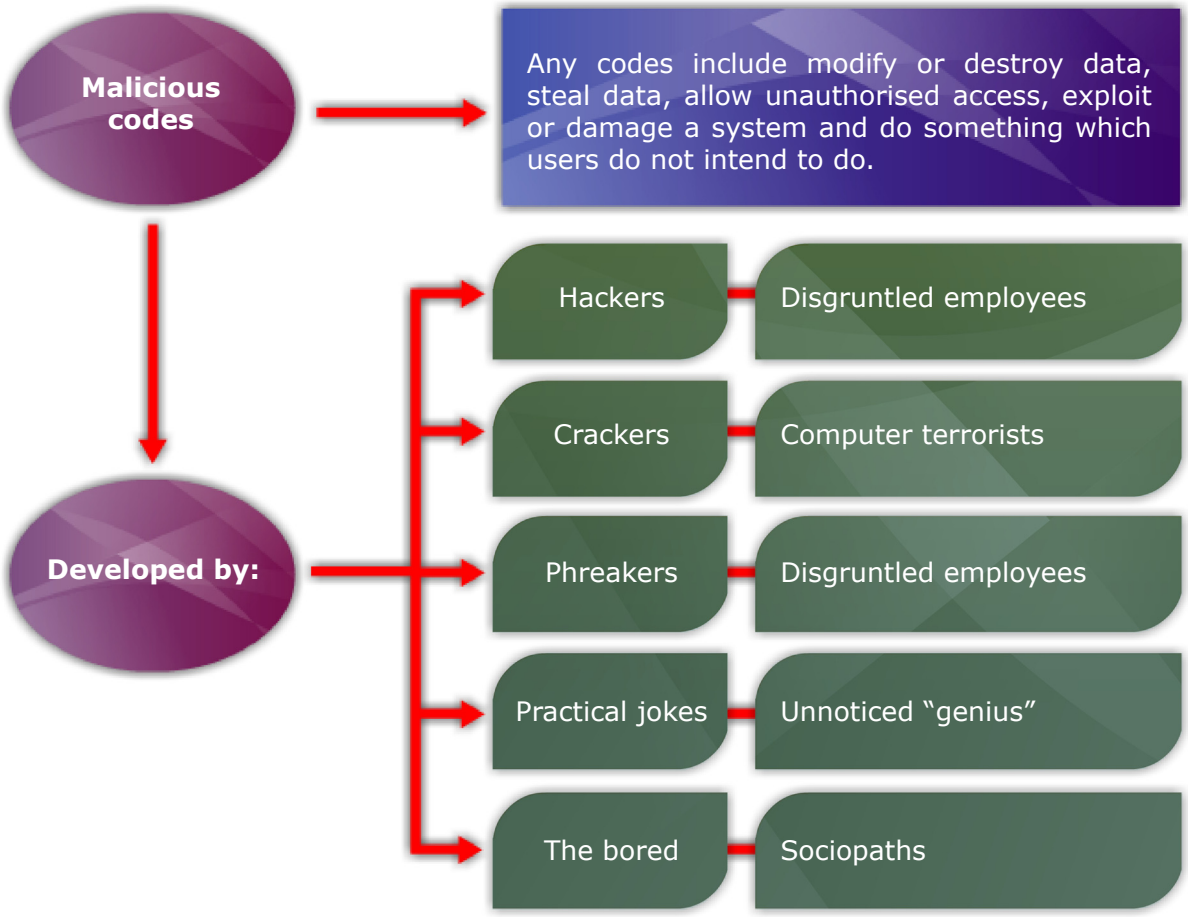


Figure 3.3: Definition of malicious code and who develops it

Malicious codes are any codes include modify or destroy data, steal data, allow unauthorised access, exploit or damage a system and do something which users do not intend to do. These malicious codes are developed by hackers, crackers, phreakers, practical jokes, disgruntled employees, computer terrorists, publicity/attention seekers, the bored, unnoticed "genius" and sociopaths.

Malicious codes can be measured using virus scanner and scanner shortfalls. No scanner is 100% accurate or effective, but new viruses appear weekly and may be undetectable. Therefore, user should have most current version of scanning software at all times.

The sourcesof malicious code infection include bulletin boards, shareware, commercial software packages, networks, sabotage by employees, terrorists, crackers or spies, pirated software and public domain software.

The examples of malicious codes are shown in Figure 3.4.

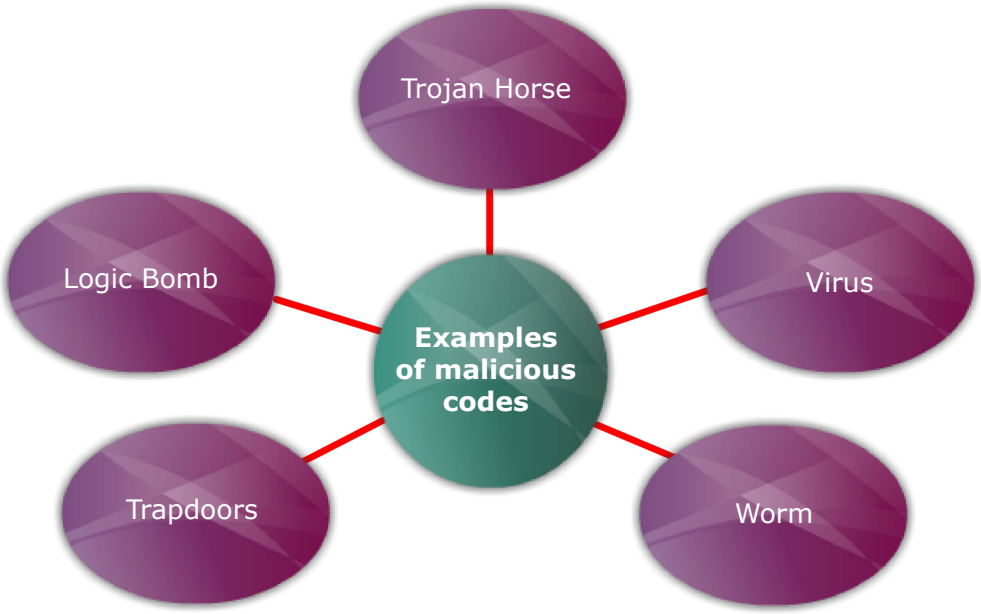


Figure 3.4: Examples of malicious codes

3.3.1.1 Trojan Horse

***Trojan horse** is a Greek mythology, which means **a gift that carried an unannounced and unexpected visitor**. In a computer, a Trojan Horse performs a hidden function in addition to its stated, obvious function.*

Trojan horse is any program that causes unexpected effects when willing installed or run by an unsuspecting user. These programs are generally deeply buried in the code of the target program and lie dormant for a specified period. The code in a Trojan Horse waits until some predetermined time or condition to act. They are triggered by any number of events such as time of day, date or number of accesses to a file. These programs perform a useful function but also perform an unexpected action as well.

A Trojan horse also is disguised as a useful program, when in reality it is not. Behind the scenes it may be downloading information to a third party, deleting, changing or crashing information, etc. The important thing to remember that it appears as a useful program and the destructiveness of it is hidden.

1. Examples of Trojan Horse

As an example, suppose a programmer wants to modify the protection level associated with files belonging to other users. The programmer writes a program that ostensibly produces a listing of files in a desirable format. Then, the programmer offers it to the manager of the computing system as a utility program for the benefit of all users. What the programmer does not say is that the utility will also alter the protection level of those files.

Since a user other than the original programmer calls this utility, the program will probably execute with the protection level of the user. Therefore, the utility will have access to the users' files and may have the right to alter the access rights to those files for other users.

Another example of a Trojan horse is a login script that solicits a user's identification and password, and then passes it to the rest of the system to complete the remaining of the login process. This program then redirects all the login information into a separate file and uses it later to break into users' accounts. The user only sees the login script and he or she has nothing to suspect otherwise.

2. How Do Trojan Horses Occur?

Basically, the easiest way for Trojan horse happen is the programmer prepares a Trojan horse source program and compiles the source code. Then, the programmer gives only the object code and documentation on the overt use of the program to the computing centre staff. So, the true operation of the utility program is hidden and the computer centre staff just knows that by using this utility, it can gives benefits to all users.

In other words, a Trojan horse is a piece of malicious code that fools a user. It acts as an innocent program but has a non-obvious malicious effect.

3.3.1.2 Virus

Virus is a code segment, which replicates by attaching copies to existing executables. Viruses are currently designed to attack single platforms. A platform is defined as the combination of hardware.

As an example, a virus can be referred to as an IBM-PC virus, referring to the hardware, or a DOS virus, referring to the operating system.

A virus is a program than can "infect" other programs by modifying them. It can pass on malicious code to other non-malicious program. The term virus arises because the

infected program can be modified to include a copy of the virus program itself. The infected program then begins to act as a virus, infecting other programs. This is similar to its biological nature. A virus attaches itself or co-existing with it. The infection of a virus spreads at a geometric rate. The virus can eventually over take the whole system and spread to all other connected systems in a networked environment.

A virus can be planted in shared system utilities to access common data, such as electronic mail, system news bulletins and lists of users on the system. Because many users access these utilities, a virus planted in one can spread quickly.

A virus could be either transient or resident. A transient virus runs when its attached program executes and it terminates when its attached program ends. A resident virus is located permanently in the memory and remains active even after its attached programs ends. Figure 3.5 shows how viruses will be separated to another application.

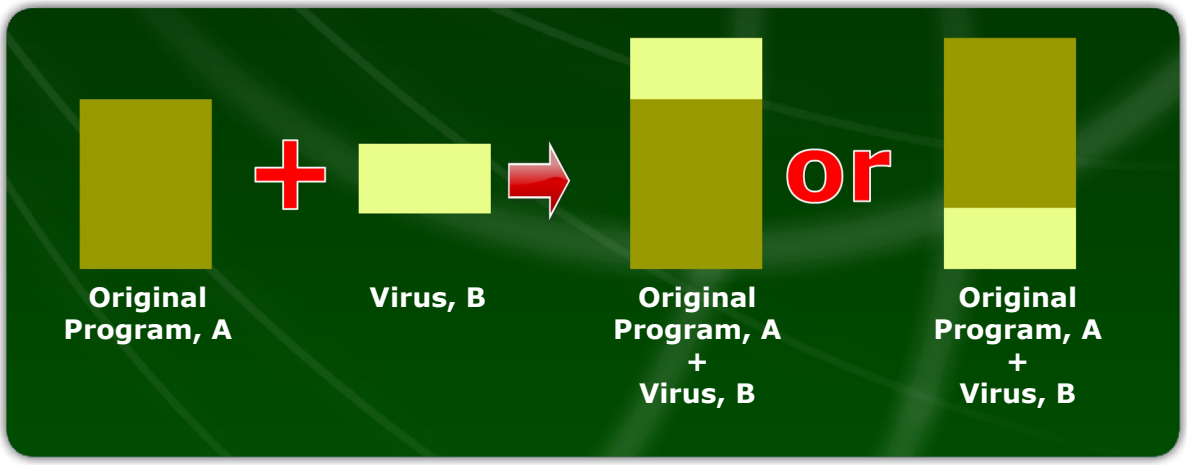


Figure 3.5: Viruses separated to another application

1. Characteristics of a Virus

A virus has several characteristics which are:

- Replication;
- Requires a host program as a carrier;
- Activated by external action; and
- Replication limited to (virtual) system.

2. Types of Viruses

The following are the types of virus:

- ***Boot Infectors/Boot Sector Virus*** - infects the boot sector of a disk, and spreads when the operating system boots up (original DOS viruses).
- ***File Infectors***.
- ***Partition Infectors***.

- ***Parasitic Virus*** - attaches itself to executable files as part of their code. Runs whenever the host program runs.
- ***Memory-resident Virus*** - Lodges in main memory as part of the residual operating system.
- ***Stealth Virus*** - explicitly designed to hide from Virus Scanning programs.
- ***Polymorphic Virus*** - mutates with every new host to prevent signature detection.

3. Virus Phases

- ***Dormant phase*** - the virus is idle.
- ***Propagation phase*** - the virus places an identical copy of itself into other programs.
- ***Triggering phase*** - the virus is activated to perform the function for which it was intended.
- ***Execution phase*** - the function is performed.

4. Examples of viruses

Not all viruses are bad. For example, a virus might locate uninfected programs, compress them so that they occupy less memory and insert a copy of a routine that decompresses the program when its execution begins, as well as spreading the compression function to other programs. It means, this virus could substantially reduce the amount of storage required for stored programs possibly by up to 50 percent. However, the compression would be done at the request of the virus, not at the request or even to the knowledge of the program owner.

3.3.1.3 Worm

A "***worm***" is a program that travels independently along computer cables. It spread copies of itself through a network. Most computers are connected via cabling, so these can do a lot of damage in a short time.

It is also a program, which replicates itself and causes execution of the new copy. It is not a Trojan horse. It is a program designed to replicate and may perform any variety of additional tasks as well. The first network worms were intended to perform useful network management functions. The worms use the network management mechanism of a computing system to identify free machine on the network and to pass the worm program to the free machines. Once active, the worm tries to find another free machine to which it will transfer a segment of itself. The difference between a worm and a virus is that a worm operates through a network and a virus spread through any medium, usually copied program or data files.

Additionally a worm spread copies of itself as a standalone program; where else a virus spread copies of itself as a program that is attached to other programs as shown in the Figure 3.6.

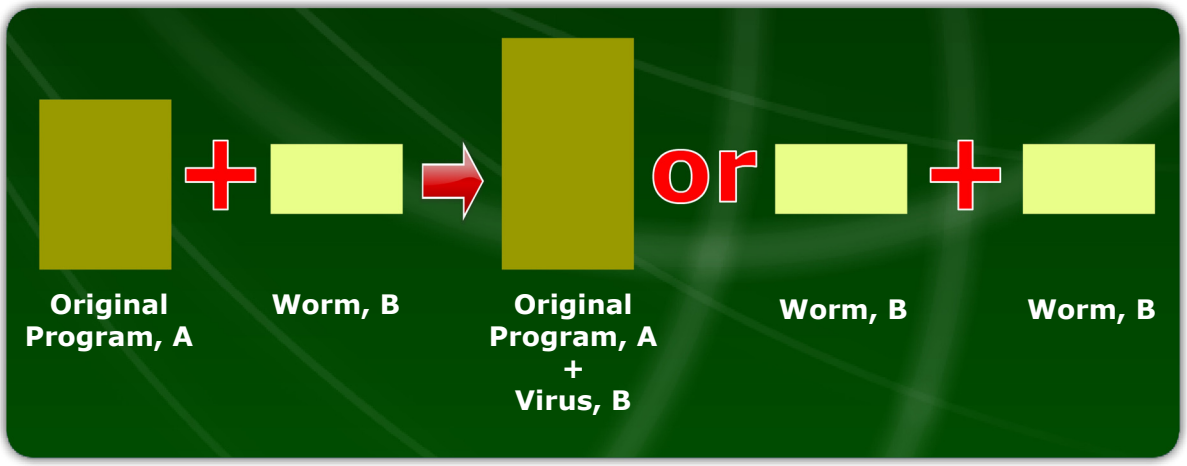


Figure 3.6: Virus is attached to other programs

1. Characteristics of a Worm

- Replication;
- Self-contained, does not require a host; and
- For network worms, replication occurs across communication links.

2. Uses of Worm

Some worm programs have legitimate purposes such as running system bulletin boards or alarm clocks. Worms can also be applied to perform parallel computation on a network of serial machines.

3.3.1.4 Trapdoors

*A **trapdoor** is a secret, undocumented entry point into a module. In other words, it is a feature in a program by which someone can access the program other than by obvious, direct call, perhaps with special privileges.*

The trapdoor is inserted sometime during code development perhaps to test the module, or as a 'hook' to connect for future modifications or enhancements and perhaps to allow access in the event of future errors. In addition to this legitimate use, trapdoors can allow a programmer to access a program once it is placed into production.

The trapdoor becomes vulnerability if it is not noticed and no one acts to prevent or control its use in vulnerable situations. It is because trapdoors expose the system to modification during execution. The original programmer can exploit trapdoors. Trapdoors can also be used by anyone who discovers them by accident or through exhaustive trials.

The trapdoor is inserted sometime during code development perhaps to test the module, or as a 'hook' to connect for future modifications or enhancements and perhaps to allow access in the event of future errors. In addition to this legitimate use, trapdoors can allow a programmer to access a program once it is placed into production.

The trapdoor becomes vulnerability if it is not noticed and no one acts to prevent or control its use in vulnerable situations. It is because trapdoors expose the system to modification during execution. The original programmer can exploit trapdoors. Trapdoors can also be used by anyone who discovers them by accident or through exhaustive trials.

1. Causes of Trapdoors

The programmer usually removes trapdoors during program development. However, trapdoors can persist in production programs because the programmer:

i. Forgets to remove them.
ii. Intentionally leaves them in the program to assist in the rest of testing.
iii. Intentionally leaves them in the program to assist in maintenance of the finished program.
iv. Intentionally leaves them in the program in order to have a covert means of access to the routine after it becomes an accepted production program.

The (i) case is an unintentional security blunder, (ii) and (iii) cases are serious exposures of the security of a system and (iv) is the first step in an outright attack.

2. Examples of Trapdoors

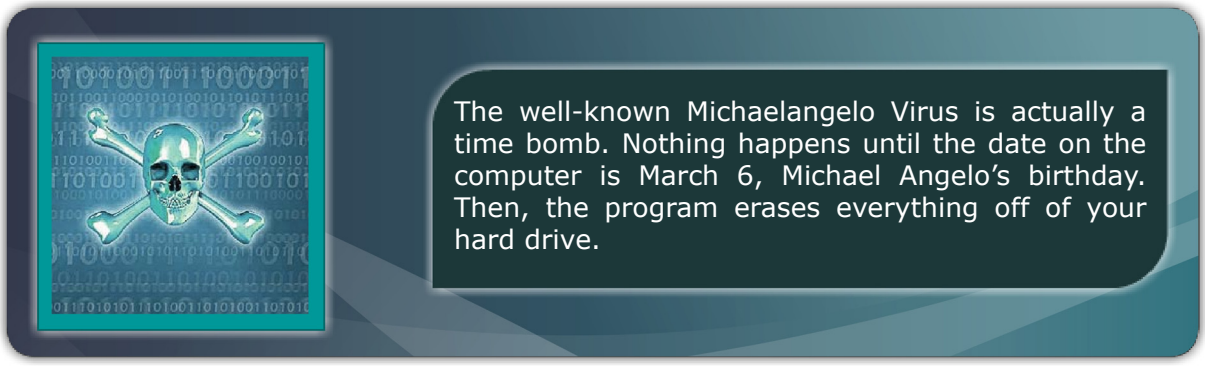
An example of this is by pressing some special characters or words on the keypad at an ATM machine site, a person is able to see all the transactions which occur at that machine and all their private information. This can be done for maintenance purposes or it could be a way for the implementer to change a record of a crime.

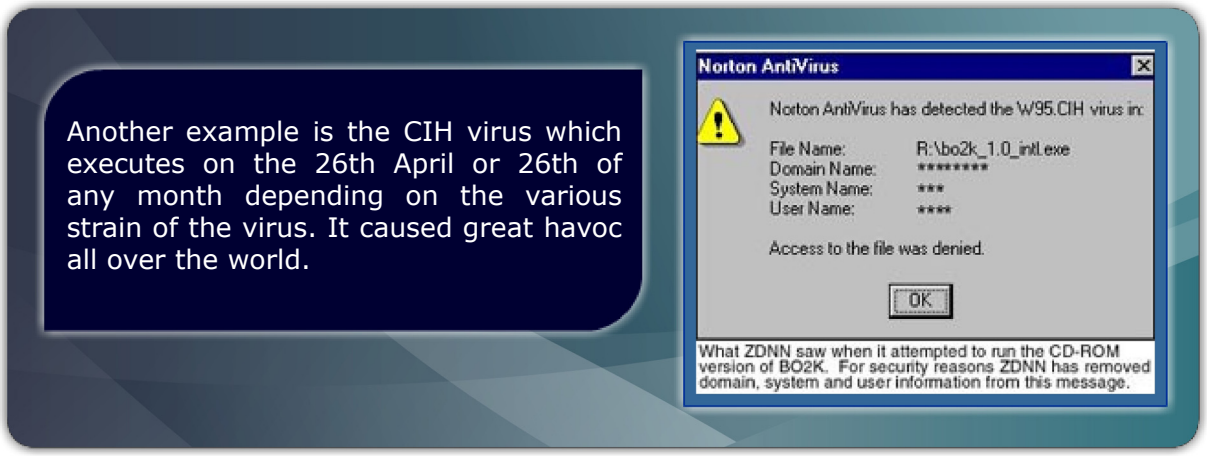
3.3.1.5 Logic Bomb

A "***logic bomb***" is a program that sits on your computer and does nothing, until…. The 'until' could be pressing a key, like the ESC key.

Nothing would happen until the ESC key was pressed, but after it could crash your hard drive, erase files or other destructive act. The 'until' could be a specific date. It is a classification for malicious codes that denotes or goes off when a specified condition occurs. A time bomb is a subset of a logic bomb that will trigger at a given time.

1. Examples of Logic Bombs



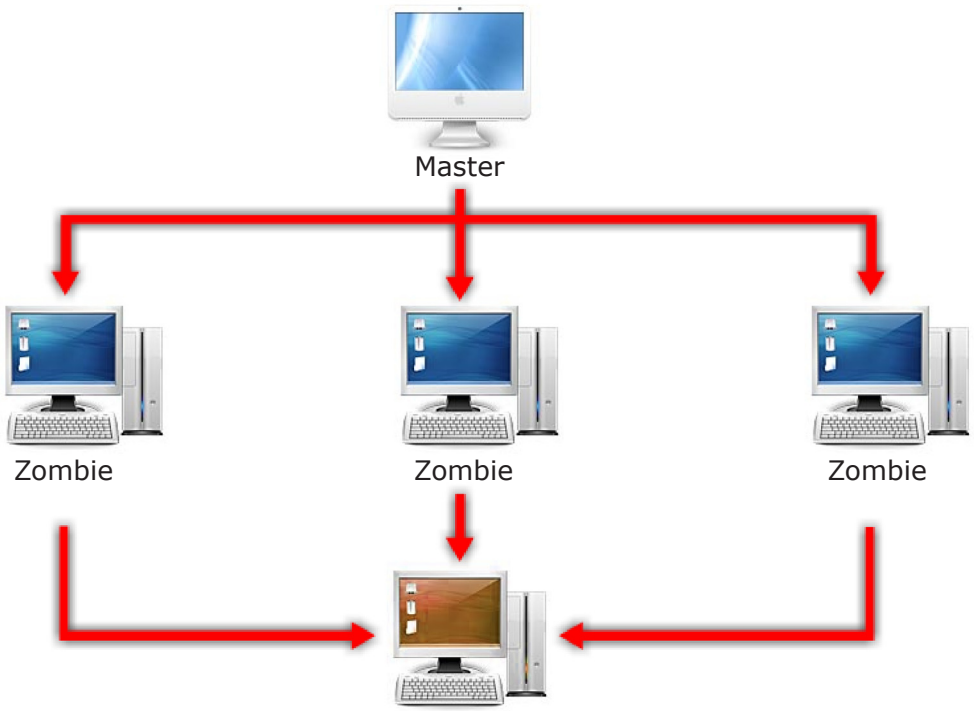


A rabbit is a worm or virus that self replicates itself without bound with the intention of exhausting the system resources. A good example of this will be intentionally clogging up a network or an email servers' disk space. This can cause the other users to have problem either when sending or receiving emails or other form of data. This is called flooding.

Two or more malicious codes can be combined to produce a malicious code. An example is a rabbit could be activated at a certain time and date in the future. This is a combination of a time bomb which is a subset of a logic bomb, with a rabbit which is part of a virus or worm that replicates to congest computer system resources.

3.3.2 Denial Attacks

Multi-user, multi-tasking operating systems are subject to "denial of service" attacks where one user can render the system unusable for legitimate users by "hogging" a resource or damaging or destroying resources so that they cannot be used. Denial of service attacks may be caused deliberately or accidentally. Taking precautions to prevent a system against unintentional denial of service attacks will help to prevent intentional denial of service attacks.



Systems on network are vulnerable to overload and destructive attacks as well as other types of intentional or unintentional denial of service attacks. The three common forms of network denial of service attacks are listed in Figure 3.7.

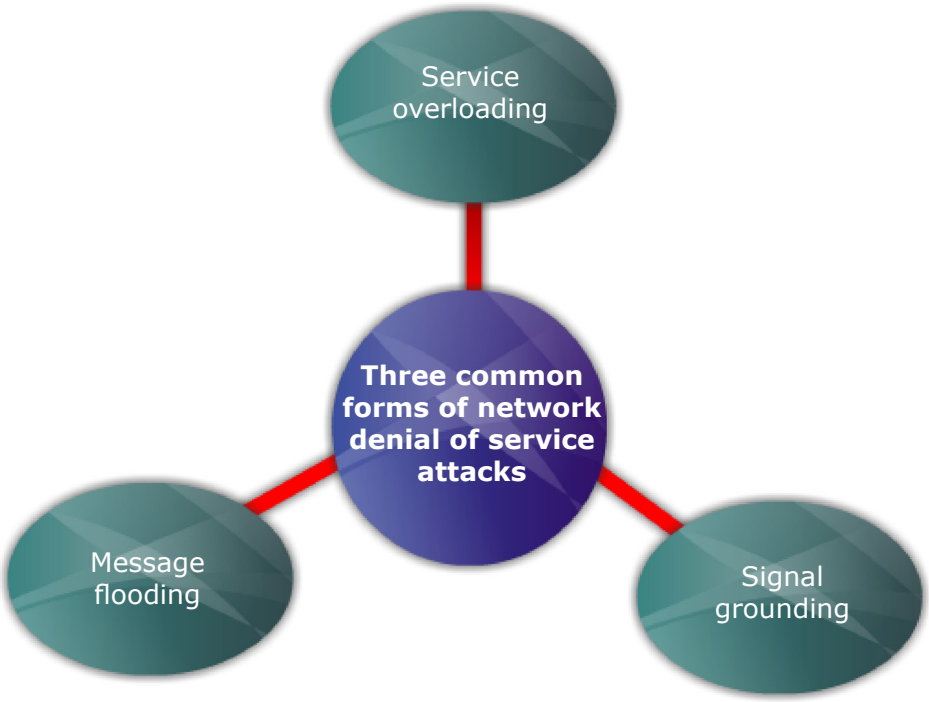


Figure 3.7: The three common forms of network denial of service attacks

It is important for system administrators to protect against denial of service threats without denying access to legitimate users. In general, denials of service attacks are hard to prevent. Many denials of service attacks can be hindered by restricting access to critical accounts, resources, and files, and protecting them from unauthorised users.

3.4 PHYSICAL SECURITY THREATS

Physical security is the term used to describe protection needed outside the computer system. It concerns the physical aspects of computing that's the devices themselves and harm that can come to them because of the buildings in which they are contained. Physical security addresses two branches of threats: natural threats to buildings and the infrastructure, and the human threats.

Physical security is the lifeblood of all security controls. If physical security is compromised, all other controls are irrelevant. This is because, if someone manages to get into our server, physically accessing our computers, he or she can cause serious damage. Some examples of damage possible can include removing the hard drives from our computer, stealing computer backup tapes, or simply shutting down the power to our servers.

All of these can be accomplished in the blink of an eye, without involving serious technical skills. Therefore, do not overlook physical security. To understand physical security, it is good idea to primarily understand physical threats. There are three types of physical threats as depicted in Figure 3.8.

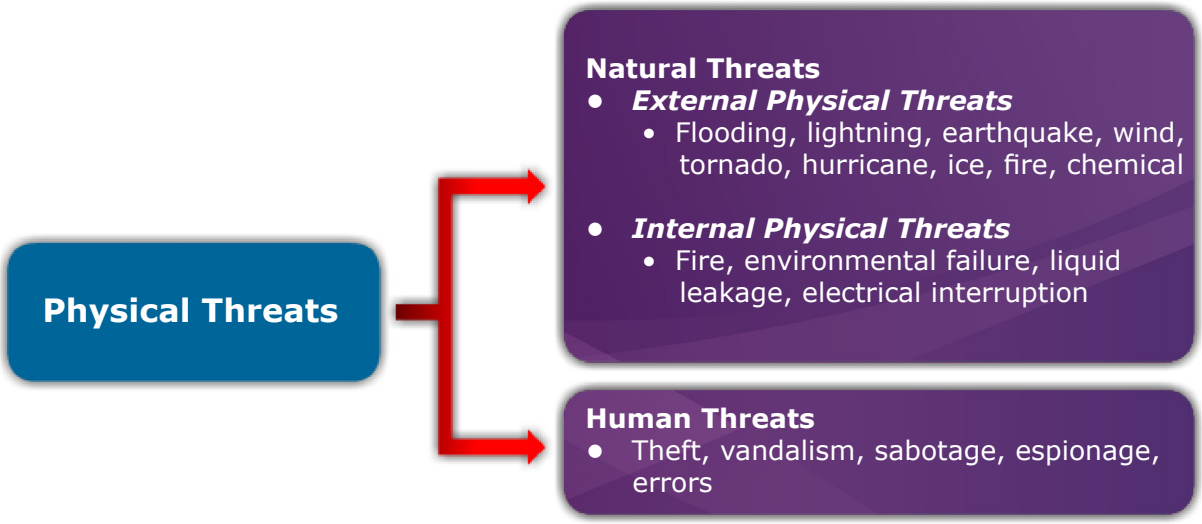


Figure 3.8: The three types of physical threats

3.4.1 Natural Threats

Natural threats can occur to homes, stores, and automobiles. They can be flooded, burned, melted, hit by falling objects and destroyed by earthquakes, storms and tornadoes. Additionally, computers are sensitive to their operating environment, so excessive heat or inadequate power is also a threat. It is impossible to prevent natural threat, but through careful planning it is possible to reduce the damage they inflict.

Some measures can be taken to reduce their impact. This is because many of these perils cannot be prevented or predicted. Issues to be considered include the need for offsite backups, the cost of replacing equipment, the speed with which equipment can be replaced, the need for available computing power, and the cost or difficulty of replacing data and programs.

Figure 3.9 display examples of natural threats.

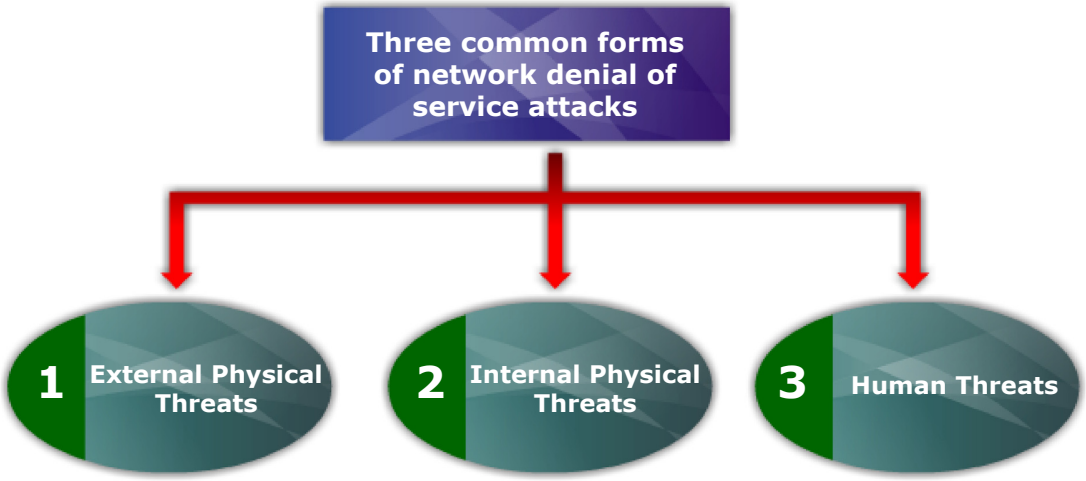


Figure 3.9: Examples of natural threats

Let us look in details each of the threats described in Figure 3.9.

1. External Physical Threats

In environmental,not only needed to secure our systems from human interference, but also need to secure them from the interference of natural disasters such as fires, hurricanes, tornados, and flooding, which fall under the realm of environmental threat. Environmental issues also come from extreme temperature or humidity.

2. Internal Physical Threats

In electrical vulnerabilities are seen in things such as spikes in voltage to different devices and hardware systems, or brownouts due to an insufficient voltage supply. Electrical threats also come from the noise of unconditioned power and, in some extreme circumstances, total power loss.

3. Human Threats

Electronic defences, especially perimeter defences, can be defeated if attackers gain physical.

If an attacker can reach an office, the attacker could:

- Install hardware key loggers to capture keystrokes, including usernames and passwords.
- Pose as a driver from a parcel delivery service and pickup backup tapes and disks.
- Engage in social engineering with office staff to learn about security procedures, office policies, and the names of executives and managers in the office.
- Use a rogue device to access a poorly secured wireless network.

Any one of these ploys might not be enough to compromise a system or result in a disclosure, but they can provide pieces to the security puzzle that attacker is trying to assess. Physical access controls, surveillance, and security awareness training are countermeasures to this type of threat. From increasingly sophisticated malware to social engineering to physical threats, there are many ways to fall victim to information security attacks. To prevent these threats from becoming reality, ***Physical Security Controls (PSC)*** should be implemented.

Some examples of effective physical security controls are shown in Table 3.2. All of these controls require detailed and careful planning prior to setting up an office with computing facilities.

Table 3.2: Effective Examples of Physical Security Controls

Type of PSC	Examples of PSC
Exterior PSC	• Fences, Barriers
Entrance PSC	• Doors and Gates with Locks
Administrative PSC	• Badges and Escorts
Property PSC	• Monitoring/Detection Systems, Lighting
Environmental PSC	• HVAC System, Power Protection, Water and Fire Protection

SUMMARY

1. Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime.
2. There are grouped into four categories (Computer as the target, Computer as the instrumentality of the crime, Computer is incidental to other crimes and Crimes associated with the prevalence of computers). Some classifications can be overlap.
3. Information Warfare (IW) is the process of protecting your information and network resources while potentially denying the adversary access to his or hers while a computer penetration is a method done by potential attacker (Black Hat, Hacker or Cracker) to attack the computer system or network.
4. Malicious codes are the general name for unanticipated or undesired effects in programs or program parts generated by an agent on the intent on damage.
5. Physical security is the term used to describe protection needed outside the computer system. It concerns the physical aspects of computing that's the devices themselves and harm that can come to them because of the buildings in which they are contained.
6. Physical security addresses two branches of threats: natural threats to buildings and the infrastructure, and the human threats.

GLOSSARY

Adversary	Enemy.
Attack	Any attempt to gain unauthorised access to a system or to deny authorised users from accessing the system.
DoS Attack	Denial of Service (DoS) is an attack that renders a system unavailable for its intended use.
Warez	Copyrighted works traded in violation of copyright law.

DISCUSSION QUESTION

1. Explain briefly what the difference between Virus and Worm is.
2. Give an example of Trojan horse (not included in notes) and explain briefly why we call it Trojan horse.
3. Define the aspects are used in software engineering for security purposes.
4. Explain briefly what the difference between Trojan horse and Trapdoors is.
5. Explain how to control the program threats and explain briefly the differences between modularity, encapsulation and information hiding.
6. From question 5, identify the advantages of modularity, encapsulation and information hiding from security aspect.
7. What are some ways to detect malicious codes? How are these codes vulnerable?
8. Describe in detail how an executable infecting computer virus might append itself to an executable. What changes must it make to the executable? Why?
9. In what ways is DoS a vulnerability to users of single-user personal computer?
10. Identify the two of most probable threats to personal computing system in an office with fewer than ten employees. Identify the two vulnerabilities most likely to be exploited.
11. List two different sources of electricity to a computing systems, and state a control for each.

REFERENCES

Carr I Snyder (2007). *Data Communications & Network Security*. New York: Mc Graw Hill.

Charles P. Pfleeger (2003). *Security in Computing*. New Jersey, United States: Prentice Hall.