UNIT VI

6 Introduction to Cyber Security

Syllabus

Basic Cyber Security Concepts, Layers of security, Vulnerability, Threat, Harmful Acts-Malware, Phishing, MIM Attack, DOS Attack, SQL Injection, Internet Governance - Challenges and Constraints, Computer Criminals, Assets and Threat, Motive of Attackers, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber Stalking, Cyber Terrorism, Cyber Espionage, Comprehensive Cyber Security Policy.

Contents

6.1 Basic Cyber Security Concepts
6.2 Attack Vector
6.3 DOS and DDOS Attack
6.4 Man-in-the-Middle Attack
6.5 Malware (Malicious Software)
6.6 Phishing
6.7 SQL Injection
6.8 Cyber Crime
6.9 Cyber Stalking
6.10 Cyber Crime and Information Security
6.11 Cloud Computing and Cybercrime
6.12 Cyber Terrorism
6.13 Cybercrime against Property
6.14 Cybersquatting
6.15 Cyber Security Policy
6.16 Short Answered Questions
6.17 Mutliple Choice Questions

6.1 Basic Cyber Security Concepts

- Cyber safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- There is no standard definition for "**CYBER**". This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.
- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Cyberspace : The impression of space and community formed by computers, computer networks, and their users ; the virtual "world" that Internet users inhabit when they are online.
- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.
- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.
- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybercrime** is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.
- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).
- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

- When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world.
- The ingenuity of cyber criminals is becoming obvious when we look at the clever ways in which online frauds are being perpetrated. Phishing, a particularly crafty fraud attack perpetrated by cyber criminals combines elements of forgery, misrepresentation and misplaced trust to obtain sensitive personal data like PIN numbers, credit card details and passwords of victims. The attackers then rob the victim's money by using such personal information.
- Other forms of cyber crimes include hacking, unauthorized access to data or resources, alteration of information and electronic mail based offences.

6.2 Attack Vector

- An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

1. **Code tampering :** This type of attacks are conducted from outside of a client's, by probing open ports and trying to force the code behind those ports to do unwanted actions, allowing hackers either remote execution, illegal upload with further execution, or system crash.
2. **Brute force :** An attacker uses techniques that are trying multiple combinations of passwords and keys trying to pick correct combination.
3. **Denial attack :** When an attacker creates either a large number of requests or specifically crafted requests or both at the same time to cause a client's system to stop responding.
4. **Floods :** An attacker creates large amount of traffic, produced by hacker's controlled infected machines - "bots or zombies" to simply overflow capacities of the client networks or their ISPs.
5. **Browser scripting attacks :** During this attack, a hacker is convincing a user to go to a malicious website. Such website has a java or other scripting code that cause client's browser to perform unwanted actions, infect the computer, download unwanted software, etc.
6. **Email attacks :** During this attack, a hacker tricks a user to open an attachment that has a code that causes the opening program such as MS Office, Adobe

PDF viewer, etc. to perform unwanted actions, such as infect the computer, download unwanted software etc.

6.3 DOS and DDOS Attack

- The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource.
- The DDoS attack uses multiple computers and Internet connections to flood the targeted resource.
- Fabrication causes Denial Of Service (DOS) attacks. DOS prevents the normal use or management of communications facilities.
- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.
- The sudden increase in traffic can cause the site to load very slowly for legitimate users. Sometimes the traffic is enough to shut the site down completely. This kind of an attack is called a **Distributed Denial of Service (DDoS)** attack.
- DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a DoS attack.
- Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.
- The DoS attack typically uses one computer and one Internet connection to flood a targeted system or resource.
- The DDoS attack uses multiple computers and Internet connections to flood the targeted resource.
- DDoS attacks are often global attacks, distributed via botnets.

6.4 Man-in-the-Middle Attack

- In cryptography, a **Man-In-The-Middle attack (MITM)** is an attack in which an attacker is able to read, insert and modify at will, meassages between two parties without either party knowing that the link between them has been compromised.
- The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.

- The MITM attack may include one or more of
  1. Eavesdropping, including traffic analysis and possibly a known-plaintext attack.
  2. Chosen ciphertext attack, depending on what the receiver does with a message that it decrypts.
  3. Substitution attack.
  4. Replay attacks.
  5. Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties. The defense is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.
- MITM is typically used to refer to active manipulation of the meassages, rather than passively eavesdropping.

Example of a successful MITM attack against public-key encryption

- Suppose Alice wishes to communicate with Bob and that Mallory wishes to eavesdrop on the conversation, or possibly deliver a false message to Bob. To get started. Alice must ask Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a Man-In-The-Middle attack can begin.
- Mallory can simply send Alice a public key for which she has the private, matching, key Alice, believing this public key to be Bob's, then encrypts her message with Mallory's key and sends the enciphered message back to Bob.
- Mallory again intercepts, deciphers the message, keeps a copy and reenciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he will believe it came from Alice.
- This example shows the need for Alice and Bob to have some way to ensure that they are truly using the correct public keys of each other. Otherwise, such attacks are generally possible in principle, against any message sent using public-key technology.

Defenses against the attack

- The possibility of a man-in-the-middle attack remains a serious security problem even for many public-key based cryptosystems. Various defenses against MITM attacks use authentication techniques that are based on :
  1. Public keys
  2. Stronger mutual authentication
  3. Secret keys (high information entropy secrets)
  4. Passwords (low information entropy secrets)

5. Other criteria, such as voice recognition or other biometrics

- The integrity of public keys must generally be assured in some manner, but need not be secret, whereas passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a certificate authority, whose public key is distributed through a secure channel.

6.5 Malware (Malicious Software)

- The generic term for threats is malicious software or malware. **Malware** is software designed to cause damage to or use up the resources of a target computer.

Malicious Programs

- Fig. 6.5.1 provides an overall taxonomy of malicious software. These threat can be divided into two categories those that need a host program and those that are independent. Which requires host programs are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program.

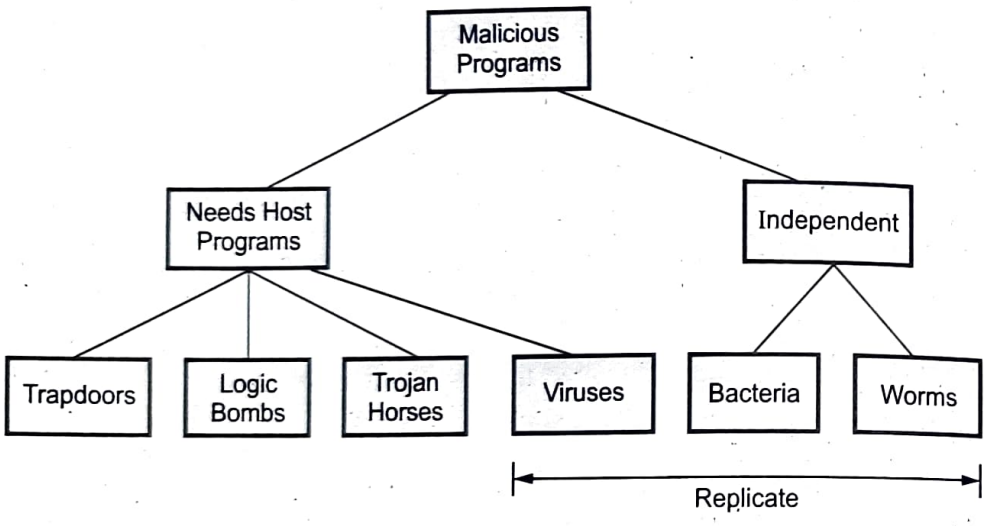


Fig. 6.5.1 Taxonomy of malicious programs

- Second category i.e. independent programs are self contained programs that can be scheduled and run by the operating system.

6.5.1 Trap Door

- Secret undocumented entry point into a program used to grant access without normal methods of access authentication.
- Trap doors have been used legitimately for many years by programmers to debug and test programs.

- Trap door can be caused by a flow in the system design or they can be installed there by a system programmer for future use. Trap door including backdoor passwords are unspecified and non documented entry points to the system. A clever trap door could be included in a compiler.
- The compiler could generate standard object code as well as a trap door regardless of the source code being compiled. Trap door may also be a incorporated into the system by a destructive virus or by a Trojan horse program.
- Trap door is one type of program threat.
- Trap door is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.
- It is difficult to implement operating system controls for trap doors. Security measures must focus on the program development and software update activities.

6.5.2 Logic Bomb

- Logic embeded in a computer program that checks for a certain set of conditions to be present on the system. When these conditions are met, it executes some functioning that result in unauthorized actions.
- Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application.
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

6.5.3 Trojan Horse

- Trojan horse is a virus that's disguised as a legitimate or harmless program that sometimes carries within itself the mean to allow the programs creator to secretly access the users system.
- Trojan horse attack may either be passive or active depending on the activities performed by the clandestine code.
- For example, if the clandestine code simply steals information then it is of the passive type. But if it does something more harmful like destroying or corrupting files, then it is of the active type. A variation of the Trojan horse is a program that emulates a login program.
- Many systems have mechanisms for allowing programs written by users to be used by other users. These programs can improperly use the access rights of an executing user and leak information.

- For example an intruder may wriute an editor program that works perfectly as an editor but also creates a copy of the edited file to a special area accessible to the intruder. The user is ignorant of the theft being made because the editor program performs all jobs in a perfectly normal fashion.

6.5.4 Virus

- A Virus is **a block of code** that inserts copies of itself into other programs. A virus generally carries a payload, which may have nuisance value, or serious consequences. To avoid early detection, viruses may delay the performance of functions other than replication.
- Virus is one type of system threats.
- A virus is any unauthorized program that is designed to gain access to a computer system. Viruses need other programs to spread. Due to its spreading nature, a virus can cause severe damage to a system.
- Virus attacks are active type Trojan horse attacks. A macro virus is embedded in a word processing. When the recepient of an email or data file with embedded virus opens the document, the macro defined as an auto exec file, execute and immediately infects the systems. Viruses have even been found in legitimate applications software.
- Most viruses include a string of characters that acts as a marker showing that the program has been infected. When an uninfected program is found, the virus infects it by attaching a copy of itself to the end of the program and replacing the first instruction of the program with a jump to the viral code.
- Virus does not infect an already infected file in order to prevent an object file growing ever longer. This allows the virus to infect many programs without noticeably increasing disk space usage.

Precautions to prevent virus problems

1. Buying software only from respectable store.
2. Avoid uploading of free software from public domain.
3. Avoid borrowing programs for someone whose security standards are less.

Nature of virus

- Once a virus is executing, it can perform any function, such as erasing files and programs, that is allowed by the privileges of the current user.
- During its lifecycle, a typical virus goes through the following four stages.

Viruses

- A computer virus is a program that inserts itself into one or more files and then performs some action.

Phases of viruses

During its lifecycle, virus goes through these phases

1. Dormant phase
2. Propagation phase
3. Triggering phase
4. Execution phase.

- **Dormant phase :** The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.
- **Propagation phase :** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase :** The virus is activated to perform the function for which it was intended.
- **Execution phase :** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

Types of Viruses

1. **Parasitic virus :** A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
2. **Memory-resident virus :** Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.
3. **Boot sector virus :** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
4. **Stealth virus :** A form of virus explicitly designed to hide itself from detection by antivirus software.
5. **Polymorphic virus :** A virus that mutates with every infection, making detection by the signature of the virus impossible.
6. **Metamorphic virus :** A metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

Macro Viruses

- Macro viruses are particularly threatening for a number of reasons
  1. A macro virus is platform independent virtually all of the macro viruses infect MS Word documents.
  2. Macro viruses infect documents, not executable portions of code.
  3. Macro viruses are easily spread. A very common method is by electronic mail.
- Macro viruses take advantage of a feature found in Word and other office applications such as Microsoft Excel, namely the macro.

E-mail Viruses

- If the recipient opens the email attachment, the Word Macro is activated. The e-mail virus sends itself to everyone on the mailing list in the user's e-mail package. The virus does local damage.
- The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft Word Macro embedded in an attachment.

6.5.5 Worms

- Worm is a program that replicates itself by installing copies of itself on other machines across a network.
- An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.
- Network worm programs use network connections to spread from system to system. To replicate itself, a network worm uses some sort of network vehicle. Examples include the following -
  1. Electronic mail facility
  2. Remote execution capability
  3. Remote login capability
- A network worm exhibits the same characteristics as a computer virus a dormant phase a propagation phase, a triggering phase and an execution phase.
- The propagation phase generally performs the following functions.
  1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
  2. Establish a connection with a remote system.
  3. Copy itself to the remote system and cause the copy to be run.

State of Worm Technology

- Worm technology includes,

1. **Multiplatform :** Newer worms are not limited to windows machines but can attack a variety of platforms, especially the popular varieties of UNIX.
2. **Multiexploit :** New worms penetrate systems in a variety of ways, using exploits against web servers, browsers, e-mail, file sharing.
3. Ultrafast spreading
4. Polymorphic
5. Metamorphic
6. Transport vehicles
7. Zero-day exploit.

6.5.6 Difference between Worm and Virus

- A virus is a piece of code that adds itself to other programs, including operating systems.
- Virus cannot run independently, host program is required to run it.
- Alters system file or any other file that is to be used in future.
- Until the user (inadvertently) activates the virus or the altered file is called, the virus is unable to do any activity.
- It needs to be carried from one computer to another.
- A *worm* is a program that can run by itself and can propagate a fully working version of itself to other machines.
- When a worm gains access to a computer (usually by breaking into it over the Internet) it launches a program which searches for other Internet locations, infecting them if it can.
- At no time does the worm need user assistance in order to operate its programming.

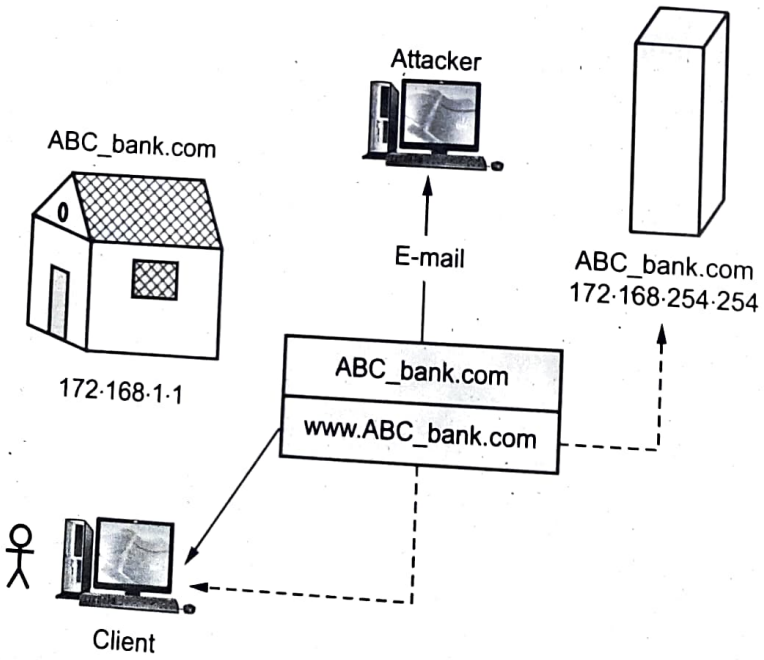
6.6 Phishing

- Phishing and pharming attacks have become sophisticated and are being used to cause real harm to a wide range of organizations.

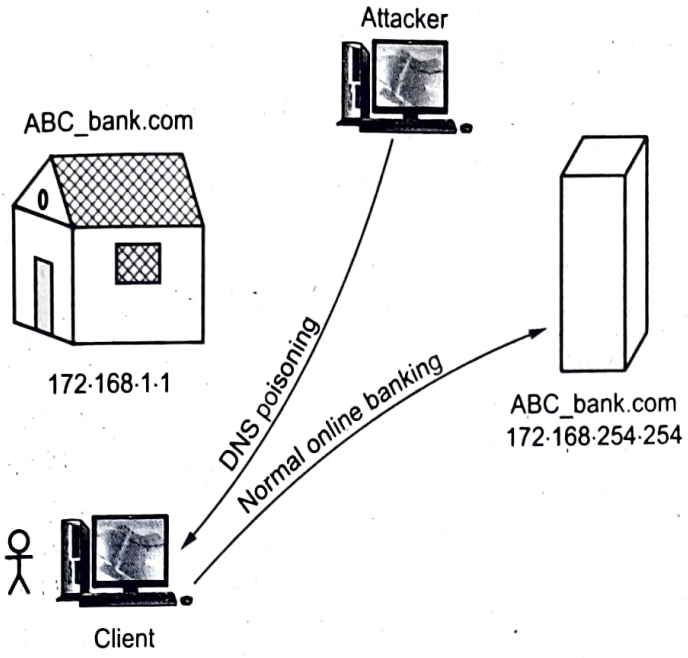
- Attackers' objectives are both to steal confidential information and to gain access to and control over sensitive systems, whether for political or financially-motivated reasons. Phishing and pharming attacks are increasingly being used as a means of delivering malicious software into target organizations, with this malware then used to achieve the attackers' ultimate goals.
- **Phishing** : Attempting to criminally acquire sensitive information, such as usernames and passwords, by masquerading as trustworthy entities.
- **Pharming** is an attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct web address.

Difference between phishing and pharming :

- Fig. 6.6.1 shows phishing and pharming attacks.
- Phishing attacks usually will involve an email that appears to be from a company with which user do business prompting user to take action and log in to account with the link provided in the email. The Web site user visit is not the real site but a cleverly designed imposter site that may seem real to you, so user will enter your username and password, which is then captured by the attacker.
- Pharming is different in that it can happen when you are going to a legitimate Web site, even when user have typed the URL of the Web site yourself. In a pharming attack, the criminal "hijacks" the intended site's DNS server. The result is



(a) Phishing



(b) Pharming

Fig. 6.6.1

that users are redirected an imposter site that looks like your intended site. Many won't notice any difference, will enter their username and password as usual and the attacker captures it.

6.6.1 Phishing Attacks

- **Phishing** is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.
- Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies. The purpose of a phishing message is to acquire sensitive information about a user. For doing so the message needs to deceive the intended recipient.

How to avoid being a phishing victim ?

1. Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name. Never respond to requests for personal information via email. When in doubt, call the institution that claims to have sent you the email.

   For example, "Dear Sir or Madam" rather than "Dear Dr. Phatak".

2. If you suspect the message might not be authentic, don't use the links within the email to get to a web page. Retype the address in a new window.
3. Never fill out forms in email messages that ask for confidential information.
4. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your web browser.
   - Check the beginning of the Web address in your browsers address bar
   - It should be 'https://' rather than just 'http://'
   - Look for the locked padlock icon on your URL bar.
5. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate and if anything is suspicious, contact your bank and all card issuers immediately.
6. Ensure that your browser and OS software is up-to-date and that latest security patches are applied. Keep antivirus definitions updated.
7. Verify the real address of a website. Phishers also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the URL "www.microsoft.com" could appear instead as :

   www.micosoft.com ?

   www.mircosoft.com ?

   www.verify-microsoft.com

6.6.2 Buffer Overflow

- A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- It may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information.

- Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
- In July 2000, a vulnerability to buffer overflow attack was discovered in Microsoft Outlook and Outlook Express. A programming flow made it possible for an attacker to compromise the integrity of the target computer by simply it sending an e-mail message.
- Unlike the typical e-mail virus, users could not protect themselves by not opening attached files; in fact, the user did not even have to open the message to enable the attack.
- The programs message header mechanisms had a defect that made it possible for senders to overflow the area with extraneous data, which allowed them to execute whatever type of code they desired on the recipient's computers. Because the process was activated as soon as the recipient downloaded the message from the server, this type of buffer overflow attack was very difficult to defend. Microsoft has since created a patch to eliminate the vulnerability.
- Buffer overflow vulnerabilities are one of the most common vulnerabilities. These kinds of vulnerabilities are perfect for remote access attacks because they give the attacker a great opportunity to launch and execute their attack code on the target computer.
- A buffer overflow attack occurs when the attacker intentionally enters more data than a program was written to handle. The data runs over and overflows the section of memory that was set aside to accept it.
- The extra data overwrites on top on another portion of memory that was meant to hold something else, like part of the program's instructions. This allows an attacker to overwrite data that controls the program and can takeover control of the program to execute the attacker's code instead of the program.
- In exploiting the buffer overflow vulnerability, the main objective is to overwirte some control information in order to change the flow of control in the program. The usual way of taking advantages of this is to modify the control information to give authority to code provided by the attacker to take control.
- The stack is a section of memory used for temporary storage of information. In a stack-based buffer overflow attack, the attacker adds more data than expected to the stack, overwriting data. For example, "Let's say that a program is executing and reaches the stage where it expects to use a postal coder or zip code, which it gets from a Web-based form that customers filled out."
- The longest postal code is fewer than twelve characters, but on the web form, the attacker typed in the letter "A" 256 times, followed by some other commands. The

data overflows the buffer allotted for the zip code and the attacker's commands fall into the stack. After a function is called, the address of the instruction following the function call is pushed onto the stack to be saved so that the function knows where to reutrn control when it is finished.

- A buffer overflow allows the attacker to change the return address of a function to a point in memory where they have already inserted executable code. Then control can be transferred to the malicious attack code contained with the buffer, called the **payload**.
- The payload is normally a command to allow remote access or some other command that would get the attacker closer to having control of the system.
- The best defense against any of these attacks is to have perfect programs. In ideal circumstances, every input in every program would do bounds checks to allow only a given number of characters. Therefore, the best way to deal with buffer overflow problems is to not allow them to occur in the first place.

6.6.2.1 Exploitation

- The techniques to exploit a buffer overflow vulnerability vary per architecture, operating system and memory region.

1. Stack-based exploitation

- A technically inclined and malicious user may exploit stack-based buffer overflows to manipulate the program in one of several ways :

1. By overwriting a local variable that is near the buffer in memory on the stack to change the behaviour of the program which may benefit the attacker.
2. By overwriting the return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input filled buffer.
3. By overwriting a function pointer or exception handler, which is subsequently executed.

2. Heap-based exploitation

- A buffer overflow occurring in the heap data area is referred to as a heap overflow and is exploitable in a different manner to that of stack-based overflows. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
- Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc meta data) and uses the resulting pointer exchange to overwrite a program function pointer.

6.7 SQL Injection

- **SQL injection** is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.
- SQL injection is subset of the an unverified/unsanitized user input vulnerability and the idea is to convince the application to run SQL code that was not intended. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

Forms of the vulnerability

1. Incorrectly filtered escape characters
2. Incorrect type handling
3. Blind SQL injection
4. Parameterized statements
5. Escaping

6.7.1 SQL Injection Remedies

- There are two complementary and successful methods of mitigating SQL Injection attacks :
  1. Parameterized queries using bound, typed parameters
  2. Careful use of parameterized stored procedures.
- Parameterized queries are the easiest to adopt, and work in fairly similar ways among most web technologies in use today, including :
  1. Java
  2. .NET
  3. Perl
  4. PHP.

6.8 Cyber Crime

- Cyber safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- There is no standard definition for "**CYBER**". This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.

- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Cyberspace : The impression of space and community formed by computers, computer networks, and their users ; the virtual "world" that Internet users inhabit when they are online.
- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man.
- Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world.
- Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.
- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security.
- Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.
- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybercrime** is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.
- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).
- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

6.8.1 Types of Cyber Crimes

- There are many types of cyber crimes and the most common ones are explained below :

1. **Hacking :** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.

2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
4. **Identity theft :** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **Malicious software :** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and abuse :** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Example of cyber crime :

a. Online banking fraud
b. Fake antivirus
c. 'Stranded traveler' scams
d. 'Fake escrow' scams
e. Advanced fee fraud
f. Infringing pharmaceuticals
g. Copyright-infringing software
h. Copyright-infringing music and video
i. Online payment card fraud
j. In-person payment card fraud
k. Industrial cyber-espionage and extortion
l. Welfare fraud.

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important cybercrimes known today.
- Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest cybercrimes known till date.

6.8.2 Botnets

- A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals.

- They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices around the world.
- Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and they perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Fig. 6.8.1 shows botnet.

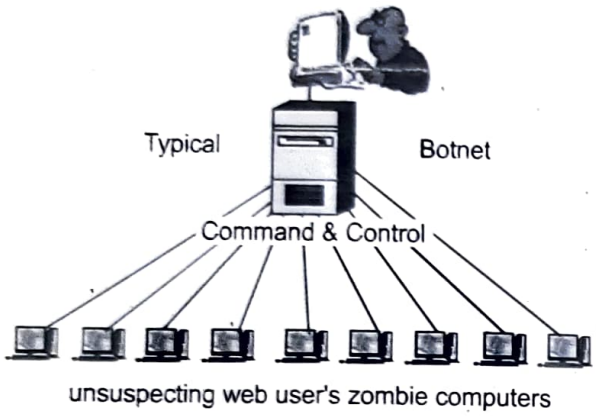


Fig. 6.8.1 Botnet

- Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.
- The word Botnet is formed from the words 'robot' and 'network'. Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage.
- A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation. At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.

- Botnets can be used to :
  1. Send out spam emails
  2. Launch a distributed denial of service attack
  3. Commit advertising fraud
  4. Distribute malware, or spyware.
- Keep phishing websites active and frequently change their domains to remain anonymous and undetected by law enforcement.

6.8.3 Zombie

- Zombie computer is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.
- Zombie network (Botnet) refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centers to perform illegal activities.
- If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.
- Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.
- The following steps are used to create zombie networks :
  1. A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
  2. The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
  3. The zombie network operator leases zombie network services to a customer.
  4. The customer provides the zombie network operator with spam or any other material, which is run through the zombie network.
- Another botnet called, Gameover Zeus Botnet, allows cyber criminals to retrieve banking passwords from infected machines, or use the botnet to infect more computers.

How and Why Do Cyber Criminals Use Botnets ?

- The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.
- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.

- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans, and purchase charges under the user's name.
- Cyber criminals may use botnets to create Denial-of-Service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations.
- Revenue from DoS attacks come through extortion and leasing botnets. The criminals will rent botnets to groups interested in inflicting damage to another entity.
- The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks.

6.8.4 Classification of Cybercrime

1. Cyber pornography

- Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computer for producing obscene materials. Such material tends to pervert the thinking 'of adolescents and corrupt their mind set.
- A person who publishes or transmits or causes to be published in the electronic form any material which is lascivious, or if its effects in such as to tend to deprave or corrupt the persons who are likely to see, wad or hear the matter contained or embodied in it, is liable to punishment.
- The important ingredients of such an offence are publication and transmission through any electronic medium, of pornographic material in any electronic form.
- Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.
- Pornography has no legal or consistent definition. The definition of pornography depends how the society, norms and their values are reacting to the pornographic content.

2. Email spoofing

- A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called **spoofing**. The hacker able to the by, having previously actual password or having created a new identity by fooling the computer into thinking he is the system's operator.

- A spoofed a may email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates.
- For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student "A" would a be quality of email spoofing.

3. Identity theft

- Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains.
- When this is done online on the Internet, its is called **Online Identity Theft.**
- The most common source to steal identity information of others, are data breaches affecting government or federal websites.
- It can be data breaches of private websites too, that contain important information such as, credit card information, address, email ID's, etc.

4. Data diddling

- This offence involves changing or reusing of data in sub till of ways which makes of it different to put the data subtitle ways which data back of or be curtain of its accuracy.
- This is resorted to for the purpose of illegal monetary gains or for community of fraud of financial scam. In case of scan the criminal are change of data which is relate[d] on the scan.
- In th data are changed of computer system, record are destroy of and alterations of i rmation of and other type of frauds.

5. Email bombing

- This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

6. Internet time thefts

- This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case-in this incident the Internet hours were used up by a unauthorized person.

7. Salami attacks

- This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack.
- This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.
- This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace.

8. Web jacking

- This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means.

9. Hacking

- In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.

10. Software piracy

- Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries.
- Piracy includes casual copying of particular software by an individual or business.
- Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated software forfeit some practical benefits as well. Those who use pirate software :
  a) Increase the chances that the software will not function correctly or will fail completely;
  b) Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
  c) Have no warranty to protect themselves;
  d) Increase their risk of exposure to a debilitating virus that can destroy valuable data;
  e) May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;

f) Are subject to significant fines for copyright infringement; and

g) Risk potential negative publicity and public and private embarrassment.

- The software licensure agreement is a contract between the software user and the software developer. Usually, this agreement has certain terms and conditions the software user must follow.
- When the user doesn't follow the rules and regulations, they are guilty of software piracy. Some of these terms and conditions prohibit :
  1. Using multiple copies of a single software package on several computers
  2. Passing out copies of software to others without the proper documentation
  3. Downloading or uploading pieces of software via bulletin boards for others to copy
  4. Downloading and installing shareware without paying for it.
- Examples of documents that support the information security program include a configuration management plan, a contingency plan, an incident response plan, a security awareness and training plan, rules of behavior, a risk assessment , a security test and evaluation results, system interconnection agreements, security authorizations and accreditations, and a plan of action and milestones.
- This step provides the necessary security authorization of an information system to process, store, or transmit information that is required.
- This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.
- **Monitoring** ensures that controls continue to be effective in their application through periodic testing and evaluation.
- Security control monitoring, such as verifying the continued effectiveness of those controls over time, and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program.
- Assessment may be internal or external. The internal assessment is a controlled network attack simulation that is used to gauge the exposure present on internal systems, applications, and network devices.
- The assessment provides a more structured approach to identifying vulnerabilities that may go undetected.
- The goal of an external assessment is to quantify the security risk that is associated with Internet-connected systems.

- Preliminary risk assessment : This step results in an initial description of the security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

6.9 Cyber Stalking

Definition of stalking : *Threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications.*

- Cyber stalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.
- Stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person.
- Stalkers use victim information like mobile numbers, telephone numbers, addresses, and personal preferences to impinge upon their normal life. Some time cyber stalkers can learn what sorts of things upset their victims and can use this knowledge to harass the victims further.
- Stalkers target victims through chat rooms, WhatsApp, Hangouts, e-mail, facebook etc.
- Different forms of cyber stalking : Threatening e-mails, spam, and online verbal abuse, inappropriate messages on message boards, computer viruses, tracing internet activity, and identity theft.
- Effects of cyber stalking on person :
  1. Changes in sleeping and eating patterns
  2. Nightmares
  3. Hyper vigilance
  4. Anxiety
  5. Helplessness
  6. Fear for safety
  7. Shock and disbelief.
- Cyber stalking damages multiple aspects of victims' lives, from study to professional activity to their relationships with others. Survey respondents reported changing or losing jobs, isolating themselves by giving up social activities and having important relationships break up.
- The Delhi police registered India's first case of cyber stalking. A case was registered under section 509 of the Indian Penal Code. One Mrs. Neha (Name changed) complained to the police against a person who was using her identity to chat over the Internet. She also complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was giving her telephone number to other chatters encouraging them to call her at odd hours.

- Stalkers usually make harassing phone calls, leave written messages or objects, or vandalize a person's property. Cyber stalkers meet or target their victims by using different search engines, bulletin and discussion boards, and online forums.
- Cyber stalkers use different social network sites and self publishing media such as Facebook, Twitter, Friendster, Bebo, Myspace and Indymedia etc. They try to damage the reputation of their victims by posting false information on websites, blogs or user pages. Many cyber stalkers use third parties to encourage them to join in their pursuit.
- They may order pornographic materials and sex toys, having them sent to their victim's address. Some cyber stalkers may arrange to meet their victims, especially young people who are at high risk of becoming their victims.
- Most stalking behavior is not a crime, at least not by itself. Calling someone over and over, texting numerous messages and leaving gifts are common behaviors that, on their own, do not constitute a crime.
- Section 354D says that anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail.
- India is finally waking up to cyber stalking with the Criminal Law (Amendment) Bill, 2013, saying that stalking includes monitoring of a person's use of internet, email and electronic communication.
- Section 66A of the IT Act deals with cyber stalking. "A person who repeatedly sends emails can be booked under 66A, but not many know this,"
- Two different kinds of cyber stalking situations which can occur.
  1. Online harassment and cyber stalking that occurs and continues on the internet.
  2. Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address. Always be careful what details you give out over the web and to whom.
- The increasing use of the Internet and the ease with which it allows others unusual access to personal information, have made this form of stalking ever more accessible. Potential stalkers may find it easier to stalk via a remote device such as the Internet rather than to confront an actual person. You cannot stop the contact with a request. In fact, the more you protest or respond, the more rewarded the cyber stalker feels. The best response to cyber stalking is not to respond to the contact.

6.9.1 Motivates of Cyber Stalker

1. **Sexual harassment :** Sexual harassment is also a very common experience offline. The internet reflects real life and consists of real people. It's not a separate, regulated or sanctified world. A common form of sexual harassment on the Internet occurs when a harasser sends unwanted, abusive, threatening, or obscene messages to a victim via e-mail or instant messaging.
2. **Obsession for love :** This category is characterized by stalkers who develop a love obsession or fixation on another person with whom they have no personal relationship. It could also be an online romance that moves to real life, only to break-up once the persons really meet.
3. **Ego and power trips :** stalkers online showing off their skills to themselves and their friends. They do not have any grudge against you - they are rather using you to 'show-off' their power to their friends or doing it just for fun and you have been unlucky enough to have been chosen.

- Some other forms of cyber stalking are listed below :
  1. Sending inappropriate electronic greeting cards.
  2. Sending viruses.
  3. Sending harassing messages to the victim's.
  4. Hacking into the victim's computer.
  5. Posting personal advertisements in the victim's name.

6.9.2 Types of Stalkers

- There are three main types of stalkers :
  1. Simple obsessional 2. Delusional 3. Vengeful

Simple obsessional stalkers or domestic

- This is the most common type of stalker.
- Stalker, usually male, knows victim as an ex-spouse, ex-lover, or former boss, who they attempt to establish a relationship with and when rebuffed begin a campaign of harassment.
- This category represents 70 - 80 % of all stalking cases and is distinguished by the fact that some previous personal or romantic relationship existed between the stalker and the victim before the stalking behavior began.
- This kind of stalker may or may not have psychological disorders, all clearly have personality disorders. They refuse to believe that the relationship is over despite being told several times. They may have a history of other criminal behaviors.

- The love-obsessional stalker, who is typically a psychotic stalker targeting famous people or total strangers; and most common. Stalker is a stranger to the victim but is obsessed with the victim and when rejected mounts a campaign of harassment to make the victim aware of the stalker's feelings.

Delusional stalkers

- Often have little contact with their victims
- Could have a mental disorder
- Often are unmarried, socially immature, isolated loners
- Typically choose a victim that is unattainable or who has shown them kindness in some way...a therapist, celebrity, clergy, teacher, doctor, etc.
- Can be dangerous and usually the rarest category of stalker.
- False belief that the victim shares the stalker's feelings and desire for a relationship.
- Here relationship based on stalker's psychological fixation. It also based on idealized love or spiritual union rather than sexual attraction.
- Target is usually a person with high visibility and a higher status.
- The danger period for a delusional is when they are falling out of love with one victim and in love with another victim.

Vengeful stalkers

- **Vengeful stalkers** may or may not have contact with their victims. They become angry with their victims over some real or perceived event or insult.
- They are as dangerous as delusional stalkers and are violent.
- Vengeful stalkers thinks you did them wrong and they want to make you pay for it.
- These stalkers may be stalking to get even and take revenge and believe that "they" have been victimized. Ex-spouses can turn into this type of stalker.

6.9.3 Typology of Cyber Stalking

- The typology of the stalker is defined by what the relationship is/was between the suspect and the victim. Stalker, usually female, falsely believes that the victim, usually someone famous or wealth is in love with them. The target is usually unobtainable by the suspect.
- Primarily, there are three ways of cyber stalking :
  1. **E-mail stalking :** Direct communication through e-mail
  2. **Internet stalking :** Global communication through internet

3. **Computer stalking :** Unauthorized control of another person's computer

- Cyber stalkers use email as the primary means to harass and threaten victims, far more than any other electronic communication device.
- Emailing allows an offender to repeatedly transmit harassing, threatening, hateful, or obscene messages, including pictures, videos, or audio.

Preventing cyber stalking

1. Do not post your personal information online.
2. Do not use your real name as a screen name.
3. Find out if your chat client or ISP network has a policy against cyber stalking.
4. Be careful about meeting friends that you have talked to online.

6.9.4 Types of Stalkers

1. **The resentful / rejected stalker :** The rejected suitor is when someone stalks their ex lover because in their mind they think that it is the only relationship they will ever have and believe that there is no other possibility except for that one relationship. In some cases these types of stalkers have some type of psychological disorder.
2. **The intimacy** seeker is similar to the rejected suitor except that this stalker is trying to create a relationship with what he or she believes is their one and only and the rejected suitor is a person that is trying to get back an old recent relationship.
3. **The incompetent** suitor is usually a man that has been turned down by a woman that they would like to develop a relationship with. After being turned down the stalker begins to repeatedly bother her and hope that his actions with let the women see that he is willing to work for the relationship and she will change her mind.
4. **The perdatory stalker** is a stalker that usually chooses victims at random with intent to commit a sexual crime with their victim. The initial motivation is to gather information about the potential victim and gain access to their life. This is to most dangerous type of stalker.

6.9.5 Investigating Cyber Stalking

- Following are the some of the methods for investigating the cyber stalking :
  1. Take interview of victim person
  2. Take interview of other persons
  3. Check risk assessment

4. Find out any other additional digital evidence
5. Purpose of the crime or characteristics
6. Motivation
7. Repeat the steps until.

- **Take interview of victim person :** Victim has to submit the proof about cyber stalking. The investigator has to check proof before taking any action. Collect the initial information from victim and develop victimology.
- After gathering all information, investigation will move forward. The whole story needs to be heard from the perspective of the complainant's history with the suspect in order to properly.
- **Take interview of other persons :** If suppose other persons involved in this case, investigator will take interview of all that peoples. It will help to understand the case.
- **Check risk assessment :** Check the relationship between victim and an offender.
- **Find out any other additional digital evidence :** What is known about the victim and cyber stalker to perform a thorough search of the Internet ? Aim of this stage is to collect detail information about victim, cyber stalker and crime.
- **Purpose of the crime or characteristics :** Find out the depth of crime scenes. Find the location where the cyber stalker and victim meet. There is any physical location and over the internet they meet without knowing to each other.
- **Motivation :** Determine personal interest of cyber stalker.
- Repeat the steps until you reach to the cyber stalker.

6.10 Cyber Crime and Information Security

- Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.
- Cybercrime may also be referred to as computer crime. A **cybercriminal** is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.
- The department of justice categorizes computer crime in three ways :
  1. The computer as a target : Attacking of other computers. For example, spreading viruses in the computer.

2. The computer is used like a weapon : Using a computer to commit "traditional crime" that like in the physical world. For example, it is like fraud or illegal gambling.
3. The computer as an accessory : Using a computer as a "fancy filing cabinet" to store illegal or stolen information.

- Cybercrime requires no physical contact with victims. They can be located anywhere in the world. This both reduces the chances of being caught and makes it very difficult for law enforcement to fingerprint a cybercriminal. It also greatly increases the potential number of victims of an attack and the return on investment.

Reasons for success of cyber criminals

- Today's cyber security paradigm is a reactive cycle : when a threat is exposed, it is analyzed and a counter-solution is designed with response times varying from weeks to years. The trouble is that attackers can easily reuse pieces of previous malware, modify them, and create a brand new threat, bypassing the newly updated security measures.
- Attackers can simply copy pieces of code from previous malware, such as exploits, decryptors or modules (keyloggers, backdoors etc.), and incorporate them into the new malware they are developing. Alternatively, attackers can imitate the operational methods performed by other malware, needed for the success of the operation.
- Cybercriminals often work in organized groups. They are as follows :
  1. **Programmers :** Write code or programs used by cybercriminal organization
  2. **Distributors :** Distribute and sell stolen data and goods from associated cybercriminals
  3. **IT experts :** Maintain a cybercriminal organization's IT infrastructure, such as servers, encryption technologies and databases
  4. **Hackers :** Exploit systems, applications and network vulnerabilities
  5. **Fraudsters :** Create and deploy schemes like spam and phishing
  6. **System hosts and providers :** Host sites and servers that possess illegal contents
  7. **Cashiers :** Provide account names to cybercriminals and control drop accounts.
- There are many reasons why cyber-criminals are doing cyber-crime. Some of the reasons are given below :
  1. Difficulty in personal identification.
  2. For the sake of recognition.

3. For earning quick money.
4. Low marginal cost of online activity due to global reach.
5. Start as hobby and then any reason.
6. Catching by law and enforcement agency is less effective and more expensive.
7. New opportunity to do legal acts using technical architecture.
8. Official investigation and criminal prosecution is rare.

6.10.1 Types of Cyber Crimes

- There are many types of cyber crimes and the most common ones are explained below :

1. **Hacking :** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.
2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
4. **Identity theft :** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **Malicious software :** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and abuse :** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Example of Cyber Crime :

a. Online banking fraud
b. Fake antivirus
c. `Stranded traveler' scams
d. `Fake escrow' scams
e. Advanced fee fraud
f. Infringing pharmaceuticals

g. Copyright-infringing software
h. Copyright-infringing music and video
i. Online payment card fraud
j. In-person payment card fraud
k. Industrial cyber-espionage and extortion
l. Welfare fraud.

- The trafficking, distribution, posting and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important cybercrimes known today. Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest cybercrimes known till date.

6.10.2 Information Security Life Cycles

- Fig. 6.10.1 shows information security life cycle.

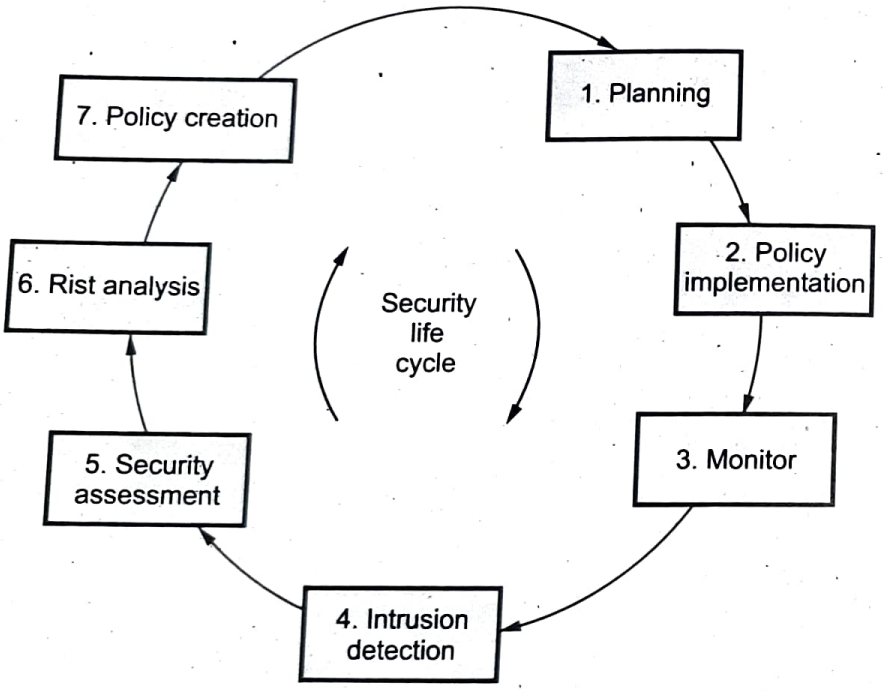


Fig. 6.10.1 Security life cycle

- Security in development and support processes is an essential part of a comprehensive quality assurance and production control process and usually involves training and continuous oversight by the most experienced staff. Rules for system and software development should be developed. These rules should incorporate secure software development techniques such as user authentication, session control, logging, and data validation and sanitization.

- Security life cycle involves following phases :
  1. Planning
  2. Policy implementation
  3. Monitoring
  4. Intrusion detection
  5. Security assessment
  6. Risk analysis
  7. Security policy creation.
- Security categorization standards help organizations make the appropriate selection of security controls for their information systems. Security planning ensures that user fully document any agreed upon security controls, whether they are just planned or in place. The security plan also provides a complete characterization or description of the information system and attachments of or references to key documents that support the information security program of the agency.
- Examples of documents that support the information security program include a configuration management plan, a contingency plan, an incident response plan, a security awareness and training plan, rules of behavior, a risk assessment , a security test and evaluation results, system interconnection agreements, security authorizations and accreditations, and a plan of action and milestones.
- This step provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.
- **Monitoring** ensures that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring, such as verifying the continued effectiveness of those controls over time, and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program.
- Assessment may be internal or external. The internal assessment is a controlled network attack simulation that is used to gauge the exposure present on internal systems, applications, and network devices. The assessment provides a more structured approach to identifying vulnerabilities that may go undetected. The goal of an external assessment is to quantify the security risk that is associated with Internet-connected systems.
- Preliminary risk assessment : This step results in an initial description of the security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

6.11 Cloud Computing and Cybercrime

- In a cloud computing environment, individuals and businesses work with applications and data stored and/or maintained on shared machines in a web-based environment rather than physically located in the home of a user or a corporate environment.
- The increasing popularity of cloud computing moreover has made conventional crime detection even more difficult. The data in the clouds is constantly shifted from one server to the next, moving within or across different countries at any time. Also, data in the clouds might be mirrored for security and availability reasons, and therefore could be found in multiple locations within a country or in several separate countries.
- Due to this and to cached versions of data, not even the cloud computing provider might know where the sought-after data is exactly located.
- With cloud computing, law enforcement does not have physical control of the media nor the network on which it resides. Many users will have access to a particular cloud. How does law enforcement seize only that portion of the media where the evidence may exist ? How will they know if they have gotten everything that they will need during the analysis, interpretation, documentation and presentation phases.
- Clouds are massively complex systems that can be reduced to simple primitives that are replicated thousands of times. These complexities create many issues related to security as well as all aspects of cloud computing.
- Clouds typically have single security architecture but have many customers with different demands. Cloud security issues may drive and define how we adopt and deploy cloud computing solutions
- Highly sensitive data is likely to be on private clouds where organizations have complete control over their security model. Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties.
- An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), all the way to the information and applications (application security).
- Additionally controls are implemented at the people and process levels, such as separation of duties and change management, respectively.

- It is clear that the security issue has played the most important role in hindering cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, pose serious threats to organization's data and software.
- Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use cloud to organize botnet as cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.
- Physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. For cloud computing providers to gain from the efficiencies of virtualization, virtual machines from multiple organizations will need to be co-located on the same physical resources.
- One of the most important characteristics of cloud computing is that it offers "self-service" access to computing power, most likely via the Internet. In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in system control.
- In cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines. Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also be readily cloned and seamlessly moved between physical servers.
- Cloud computing servers use the same operating systems, enterprise and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments.
- In addition, co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention systems need to be able to detect malicious activity at the virtual-machine level, regardless of the location of the VM within the virtualized cloud environment.
- Unlike a physical machine, when a virtual machine is offline, it is still available to any application that can access the virtual machine storage over the network and is therefore susceptible to malware infection.

- The attack surface in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are not being tampered with nor compromised, particularly when residing on shared physical infrastructure. Operating system and application files and activities need to be monitored.
- To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself.

6.12 Cyber Terrorism

- **Cyber terrorism** is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

What is Terrorism ?

- Most governments in the world cannot agree on one single definition for terrorism. The ambiguity in the definition brings indistinctness in action; as the old maxim goes "one man's terrorist is another man's freedom fighter".
- The US FBI defines terrorism as "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."
- The US department of state defines terrorism as "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents".
- It is interesting to note that some definitions of terrorism also include targets to computer systems and its services.
- The traditional terrorism and cyber terrorism share the same attributes. One approach of understanding cyber terrorism is by breaking it down to its fundamental elements. The above definitions suggest that there are at least five elements which must be satisfied to construe **cyber terrorism :**

1. Politically motivated attacks that lead to death or bodily injury;
2. Cause fear and/or physical harm through attack techniques
3. Serious attacks against critical information infrastructures such as financial, energy, transportation and government operations;
4. Attacks that disrupt non-essential services are not considered as terrorism; and.
5. Attacks that are not primarily focused on monetary gain.

- At the moment, there has been no known publicly reported incident of actual cyber terrorism. Most reported cases are related to cyber threats and the use of the Internet as a tool by terrorists.

Internet as an Ideal Tool for Terrorists

- Several works on cyber terrorism and the Internet have been conducted by researchers including experiments on cyber terrorism activities on major websites and blogs such as YouTube and Second Life.
- The researchers also studied popular hosting service providers such as blogspot.com and wordpress.com. Their findings indicate that :

1. There have been several cases reported in the media where the Internet has helped terrorists in their activities.
2. The virtual world is indeed used to promote terrorism activities. Some of the videos published on the Net are related to explosives, attacks, bombing and hostage-taking.
3. Some terrorist groups use the Internet for the purpose of inter-group communication and inter-networked grouping.
4. The Internet is used to release manifestos and propaganda statements.
5. Aside from generating propaganda, the Net is also used to coordinate missions or call meetings and to recruit new members.

Cyber Terrorism in India

- Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.
- Cyber terrorism is an attractive option for modern terrorists for several reasons,
  1. It is cheaper than traditional terrorist methods.
  2. Terrorism is more anonymous than traditional terrorist methods.
  3. The variety and number of targets are enormous.
  4. Terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
  5. Terrorism has the potential to affect directly a larger number of people.

Review Question

1. *Write short note on cyber terrorism.* **SPPU : Dec.-14, Marks 6**

6.13 Cybercrime against Property

- Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs and unpossession of computerized information.
- Property crime is a category of crime that includes, among other crimes, burglary, larceny, theft, motor vehicle theft, arson, shoplifting and vandalism.
- Property crime involves the taking of property and does not involve force or threat of force against a victim.

Intellectual property crimes

- Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is a crime.
- The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- The property transaction scams come against a backdrop of instances of con artists pretending to be solicitors, using either fake names or stealing the identities of genuine firms.

THEFT :

A person commits an offense if he unlawfully appropriates property with intent to deprive the owner of property,

- Cybercrime is nothing but where the computer used as an object or subject of crime. Cybercrime is an evil having its origin in the growing dependence on computers in modern life.
- In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers.
- Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs.
- Whoever intentionally causes damage to any physical property of another without the person's consent is guilty of a class A misdemeanor.
- Whoever intentionally causes damage to, intentionally marks, draws or writes with ink or another substance on or intentionally etches into any physical property of another, with-out the person' s consent and with knowledge of the character of the property, is guilty of a class I felony if the property consists of one or more of the following :

1) Any church, synagogue or other building, structure or place primarily used for religious worship or another religious purpose.

2) Any cemetery, mortuary or other facility used for burial or memorializing the dead.

6.14 Cybersquatting

- Cybersquatting is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses.
- Internet Corporation for Assigned Names and Numbers (ICANN) coordinates assignment of domain names by various entities, which generally allocate domain names on a first-come, first-served basis for a modest fee.
- A cybersquatter takes advantage of the domain registration companies' 'first come, first served' policy by submitting a large list of very popular words and names all at once.
- While the domain registration company is in the process of entering these names, the cybersquatter uses profits from individual domain resales to finance the required registration fees.
- A cybersquatter can literally sit on a popular domain name for years, causing grief to the actual celebrity or company it represents.
- As the internet started becoming popular, internet users knew businesses would need a website. Some users started buying domains to create sites that looked like they were from reputable companies.
  Example : A cybersquatter could buy Heinz.com if the company hadn't created a website yet, looking to sell the domain to Heinz at a later date for profit, or use the domain name to attract traffic and generate money through advertising.
- If a business has a good reputation but no website, the company either pays the owner of the domain name to transfer the domain or contacts a trademark attorney to start a lawsuit.
- The second way is time - and cost - intensive, so trying to buy the domain directly from the cybersquatter is usually the preferred method. .
- Today, opportunities for cybersquatters aren't as common since most businesses make the purchasing of their domain a high priority, especially if they have a strong trademark.

6.15 Cyber Security Policy

- The Indian government has created the necessary legal and administrative framework through the enactment of Information Technology Act 2000, which

combines the e-commerce transactions and computer misuse and frauds rolled into an Omnibus Act.

- While on the one hand it seeks to create the Public Key Infrastructure for electronic authentication through the digital signatures, on the other hand, it seeks to build confidence among the public that the frauds in the cyber space will not go unpunished.
- The Controller of Certifying Authority (CCA) has been put in place for the effective implementation of the IT Act, 2000.
- The Act also enables e-governance applications for the electronic delivery of services to the public, business and government.
- The Information technology Act, 2000 has been enacted by the legislators with the prime intention of ensuring that the communication through electronic medium is facilitated and all sorts of ambiguity regarding the authenticity of the communication is fixed for once and all.

6.15.1 Indian IT Act

- In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology act, 2000. Cyber laws are contained in the IT act, 2000.
- This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand the various perspectives of the IT act, 2000 and what it offers.
- The Information Technology act, 2000 also aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- Some highlights of the act are listed below :

a. Chapter-II of the act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

b. Chapter-III of the act details about electronic governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

- Rendered or made available in an electronic form; and
- Accessible so as to be usable for a subsequent reference

The said chapter also details the legal recognition of Digital Signatures.

c. Chapter-IV of the said act gives a scheme for regulation of certifying authorities. The act envisages a controller of certifying authorities who shall perform the function of exercising supervision over the activities of the certifying authorities as also laying down standards and conditions governing the certifying authorities as also specifying the various forms and content of digital signature certificates. The act recognizes the need for recognizing foreign certifying authorities and it further details the various provisions for the issue of license to issue digital signature certificates.

d. Chapter-VII of the act details about the scheme of things relating to digital signature certificates. The duties of subscribers are also enshrined in the said Act.

e. Chapter-IX of the said act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding ₹ 1,00,00,000 to affected persons. The act talks of appointment of any officers not below the rank of a director to the government of India or an equivalent officer of state government as an adjudicating officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said adjudicating officer has been given the powers of a civil court.

f. Chapter-X of the act talks of the establishment of the cyber regulations appellate tribunal, which shall be an appellate body where appeals against the orders passed by the adjudicating officers, shall be preferred.

g. Chapter-XI of the act talks about various offences and the said offences shall be investigated only by a police officer not below the rank of the deputy superintendent of police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form and hacking.

The act also provides for the constitution of the cyber regulations advisory committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.

The said act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

6.15.2 Cyber Laws and Crimes as per the Indian IT Act

- The IT act covers cyber laws and crimes, which are subject to the Indian Penal Code. Such cyber crimes include :
  - Crimes related to technical aspects, such as unauthorized access and hacking, trojan attack, virus and worm attack, email related attacks (email spoofing and email spamming, email bombing) and Denial Of Service attacks (DOS). DOS include :

1. Consumption of limited or non-renewable resources like NW bandwidth and RAM, alteration or destruction of configuration information, destruction or alteration of network components and pornography.
2. Forgery
3. IPR violations, which include software piracy, copyright infringement, trademark violations, etc. This also includes cyber terrorism, Banking and credit card related crimes, e-Commerce and investment frauds, sale of illegal articles, defamation.
4. Cyber stacking, identity theft, data diddling, theft of internet hours.
5. Breach of privacy and confidentiality.

6.15.3 Advantages of Cyber Law

- The IT act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Such laws are required so that people can perform purchase transactions over the net through credit cards without fear of misuse.
- The act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format.
- The act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT act 2000 and its provisions contain many positive aspects.
- Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the act.
- Digital signatures have been given legal validity and sanction in the act.
- The act throws open the doors for the entry of corporate companies in the business of being certifying authorities for issuing digital signatures certificates.
- The act now allows government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate government in electronic form by means of such electronic form as may be prescribed by the appropriate government.
- The IT act also addresses the important issues of security, which are so critical to the success of electronic transactions. The act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the government at a later date.
- Under the IT act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the act is in the form of monetary damages, not exceeding ₹ 1 crore.

6.15.4 A Global Perspective on Cybercrimes

- The rapid development of Internet and computer technology globally has led to the growth of new forms of transnational crime especially Internet related.
- These crimes have virtually no boundaries and may affect any country across the globe.
- Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crime.
- Globally Internet and computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries.

- This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law - making and law - enforcing authorities find this new environment deeply threatening.

6.16 Short Answered Questions

Q.1 What is phishing ?

Ans. : Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information by masquerading as a trustworthy entity in an electronic communication.

Q.2 Define Cross-site scripting.

Ans. : Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other users. An exploited cross - site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy.

Q.3 Design SQL injection.

Ans. : SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

Q.4 What is brute force attack ?

Ans. : Brute force attack :

- The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.
- Brute force attack is an automated process of trial and error used to guess a person's user name, password, credit-card number of cryptographic key.

6.17 Mutliple Choice Questions

Q.1 _____ refers to the security flaws in a system that allows an attack to be successful.

[a] Vulnerability [b] Availability

[c] Integrity [d] Confidential

Q.2 Information is _____ when it is in the same state in which it was created, placed, stored, or transferred.

[a] authorized [b] authentic

[c] secure [d] available

Q.3 **Information has _____ when it is free from mistakes or errors and it has the value that the end user expects.**

a authentic
b availability
c accuracy
d all of these

Q.4 **Which of the following is NOT a malicious code ?**

a Virus
b Worms
c Anti-virus
d Back door

Q.5 **What is the software called that's designed to exploit a computer user and is a broad term covering computer viruses, worms, Trojan, adware, etc.?**

a Backdoors
b Key-logger
c Malware
d Bots

Q.6 **Which of the following is the type of software that has self-replicating software that causes damage to files and system?**

a Viruses
b Trojan horses
c Bots
d Worms

Answer Keys for Multiple Choice Questions :

Q.1	a	Q.2	b	Q.3	b	Q.4	c
Q.5	c	Q.6	d				

❑❑❑