26
1
NO:-168B/A05

UNIT -II: CYBER OFFENSES

2.1 How Criminals Plan Them –Introduction

2.2 How Criminals Plan the Attacks

2.3 Social Engineering

2.4 Cyber stalking

2.5 Cyber cafe and Cybercrimes

2.6 Botnets: The Fuel for Cybercrime

2.7 Attack Vector

2.8 Cloud Computing

Dept. of CSE- RGAN

Prepared By Mr. Isaac Paul. P, Department of CSE- RGAN

www.Jntufastupdates.com

2.1 How Criminals Plan Them –Introduction

- Technology is a "double-edged sword" as it can be used for both good and bad purposes.
- People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose.
- Computers and tools available in IT are also used as either target of offense.
- In today's world of Internet and computer networks, a criminal activity can be carried out across national borders.
- Chapter 1 provided an overview of *hacking*, *cyberterrorism*, *network intrusions*, *password sniffing*, *computer viruses*, etc. They are the most commonly occurring crimes that target the computer.
- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyberlaws among the people who are constantly using the IT infrastructure for official and personal purposes.
- People who commit cybercrimes are known as "Crackers" (Box 2.1).

Box 2.1 | Hackers, Crackers and Phreakers
Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defi nes someone who breaks into computers (refer to Box 2.2).
Brute force hacking: It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.
Cracker: A cracker is a person who breaks into computers. Crackers should not be confused with hackers. The term "cracker" is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.
Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called "phreaking"). These sites usually display warnings such as "These fi les are illegal; we are not responsible for what you do with them."
Cracker tools: These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.
Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.
War dialer: It is program that automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in.

www.Jntufastupdates.com

- An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.
- The categories of vulnerabilities that hackers typically search for are the following:
  1. Inadequate border protection (border as in the sense of network periphery);
  2. remote access servers (RASs) with weak access controls;
  3. application servers with well-known exploits;
  4. misconfigured systems and systems with default configurations.
- To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

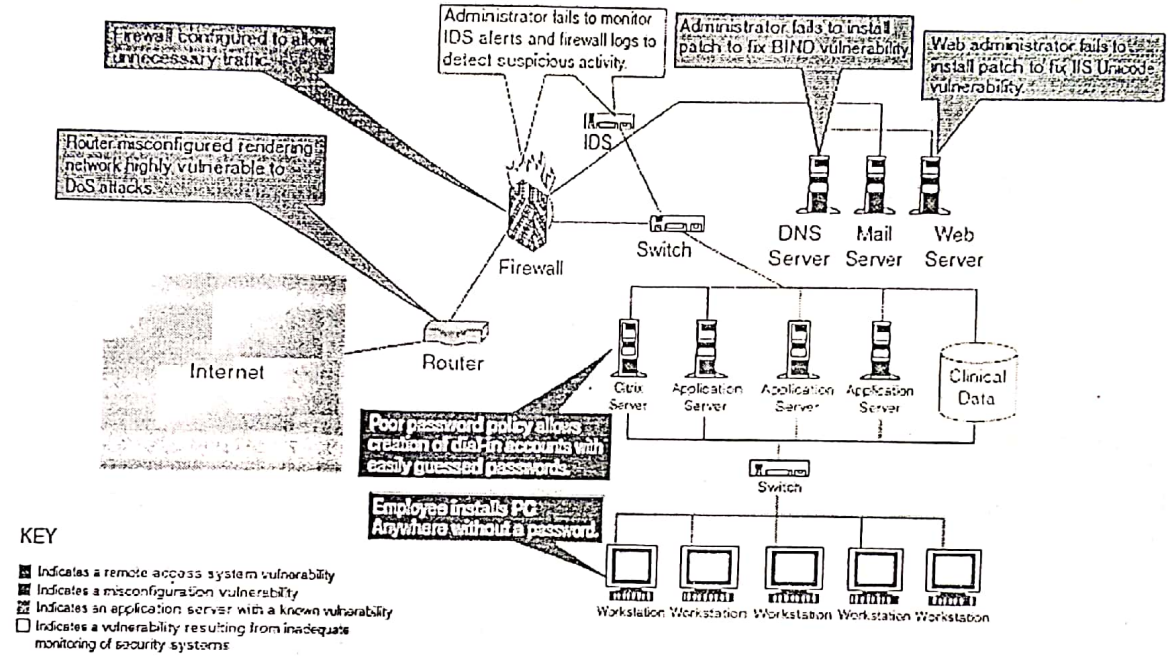


Figure 2.2 | Network vulnerabilities – sample network.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 11.6), Wiley India.

www.Jntufastupdates.com

Box 2.2 | What Color is Your Hat in the Security World?

A black hat is also called a "cracker" or "dark side hacker." Such a person is a malicious or criminal hacker. Typically, the term "cracker" is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

A white hat hacker is considered an *ethical hacker*. In the realm of IT, a "white hat hacker" is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a "white hat" generally focuses on securing IT systems, whereas a "black hat" (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

A brown hat hacker is one who thinks before acting or committing a malice or non-malice deed. *A grey hat* commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

2.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

- Cybercrime can be targeted against individuals (persons), assets (property) and/or organizations (government, business and social).
  1. **Crimes targeted at individuals:** The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography (explained in Section 1.5.13, Chapter 1), copyright violation, harassment, etc. with the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims. However, this also makes difficult to trace and apprehend the criminals.
  2. **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive, etc.
  3. **Crimes targeted at organizations:** Cyberterrorism is one of the distinct crimes against organizations/ governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and files or plant programs to get control of the network and/or system (see Box 2.3).

SREC-CSE-CYBER

4. **Single event of cybercrime:** It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
5. **Series of events:** This involves attacker interacting with the victims repetitively. For example, attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault.

Box 2.3 | Patriot Hacking

Patriot hacking[1] also known as *Digital Warfare*, is a form of vigilante computer systems' cracking done by individuals or groups (usually citizens or supports of a country) against a real or perceived threat. Traditionally, Western countries, that is, developing countries, attempts to launch attacks on their perceived enemies.

Although patriot hacking is declared as illegal in the US, however, it is reserved only for government agencies [i.e., Central Intelligence Agency (CIA) and National Security Agency (NSA)] as a legitimate form of attack and defense. Federal Bureau of Investigation (FBI) raised the concern about rise in cyberattacks like website defacements (explained in Box 1.4, Chapter 1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel into increase in international tension and gets mirrored it into the online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe and Israel. These are countries that have the greatest threat to Islamic terrorism and its aforementioned digital version.

The People's Republic of China is allegedly making attacks upon the computer networks of the US and the UK. Refer to Box 5.15 in Chapter 5. For detailed information visit www.patriothacking.com

not official

2.2 How Criminals Plan the Attacks

- Criminals use many methods and tools to locate the vulnerabilities of their target.
- The target can be an individual and/or an organization.
- Criminals plan passive and active attacks
- Active attacks are usually used to alter the system (i.e., computer network) whereas passive attacks attempt to gain information about the target.
- Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to violation of confidentiality.

The following phases are involved in planning cybercrime:
1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

2.2.1 Reconnaissance

(*reconnaissance*= నిఘా)

- The literal meaning of "Reconnaissance" is *an act of finding something or somebody (especially to gain information about an enemy or potential enemy)*.
- In the world of "hacking," reconnaissance phase begins with "*Footprinting*" – this is the preparation toward pre-attack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.
- Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.
- The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.
- Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

2.2.2 Passive Attacks

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It can be as simple as watching a building to identify what time employees enter the building premises.
- However, it is usually done using Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

  1. Google or Yahoo search: People search to locate information about employees.
  2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
  3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target (see Section 2.3).
  4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.

5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

2.2.3 Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase.
- It involves the risk of detection and is also called "*Rattling the doorknobs*" or "*Active reconnaissance*."
- Active reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

2.2.4 Scanning and Scrutinizing Gathered Information

- Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:
  1. **Port scanning:** Identify open/close ports and services. Refer to Box 2.5.
  2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
  3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

2.2.5 Attack (Gaining and Maintaining the System Access)

- After the scanning and enumeration, the attack is launched using the following steps:
  1. Crack the password.
  2. exploit the privileges.
  3. execute the malicious commands/applications.
  4. hide the files (if required).
  5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

Dept of CSE-RGAN

2.3 Social Engineering

- Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes.
- It is generally agreed that people are the weak link in security and this principle makes social engineering possible.
- A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.
- The goal of a social engineer is to fool someone into providing valuable information or access to that information.
- Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.
- The sign of truly successful social engineers is that they receive information without any suspicion.
- A simple example is calling a user and pretending to be someone from the service desk working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on… (see Box 2.6).

Box 2.6 | Social Engineering Example
Mr. Joshi: Hello? **The Caller:** Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk space constraints on the file server, we will be moving few user's home directories to another disk. This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move and will be unavailable temporarily.
Mr. Joshi: Ohh … okay. I will be at my home by then, anyway. **Caller:** Great!!! Please ensure to log off before you leave offi ce. We just need to check a couple of things. What is your username?
Mr. Joshi: Username is "pjoshi." None of my fi les will be lost in the move, right? **Caller:** No sir. But we will have to check your account to ensure the same. What is the password of that account?
Mr. Joshi: My password is "ABCD1965," all characters in upper case. **Caller:** Ok, Mr. Joshi. Thank you for your cooperation. We will ensure that all the fi les are there.
Mr. Joshi: Thank you. Bye. **Caller:** Bye and have a nice day.

www.Jntufastupdates.com

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information.
- An example is calling the help desk and trying to find out a password.

1. **Impersonating an employee or valid user:**
   - "Impersonation" is perhaps the greatest technique used by social engineers to deceive people.
   - Social engineers "take advantage" of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who "forgot" his/her badge, etc., or pretending to be an employee or valid user on the system.
2. **Posing as an important user:**
   - The attacker pretends to be an important user — for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
   - The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.
3. **Using a third person:**
   - An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.
4. **Calling technical support:**
   - Calling the technical support for assistance is a classic social engineering example.
   - Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.
5. **Shoulder surfing:**
   - It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.
6. **Dumpster diving:**
   - It involves looking in the trash for information written on pieces of paper or computer printouts.
   - This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded.
   - It is also called dumpstering, binning, trashing, garbing or garbage gleaning.
   - "Scavenging" is another term to describe these habits.
   - In the UK, the practice is referred to as " binning" or "skipping" and the person doing it is a "binner" or a "skipper."

CSE-RGAN

Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.
- For example, sending a **fake E-Mail** to the user and asking him/her to re-enter a password in a webpage to confirm it.

1. **Fake E-Mails:**

- The attacker sends fake E-Mails (see Box 2.7) to users in such that the user finds it as a real e-mail.
- This activity is also called "Phishing".
- It is an attempt to attract the Internet users (netizens) to reveal their personal information, such as **usernames, passwords and credit card details** by impersonating as a trustworthy and legitimate organization or an individual.
- Banks, financial institutes and payment gateways are the common targets.
- Phishing is typically carried out through E-Mails or instant messaging and often directs users to enter details at a website, usually designed by the attacker with abiding the look and feel of the original website.
- Thus, Phishing is also an example of social engineering techniques used to fool netizens.
- The term "Phishing" has been evolved from the analogy that Internet scammers are using E-Mails attract to *fish* for passwords and financial data from the sea of Internet users (i.e., netizens).
- The term was coined in 1996 by hackers who were stealing AOL Internet accounts by scamming passwords without the knowledge of AOL users.
- As hackers have a tendency of replacing "f" with "ph," the term "Phishing" came into being.

2. **E-Mail attachments:**

- E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed.
- Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

3. **Pop-up windows:**

- Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

Property of R-GIAN

2.4 Cyberstalking

- The dictionary meaning of "stalking" is an "*act or process of following prey stealthily – trying to approach somebody or something.*"
- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.
- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

1. Online stalkers:
   - They aim to start the interaction with the victim directly with the help of the Internet.
   - E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
   - The stalker makes sure that the victim recognizes the attack attempted on him/her.
   - The stalker can make use of a third party to harass the victim.

2. Offline stalkers:
   - The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
   - Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
   - The victim is not aware that the Internet has been used to perpetuate an attack against them.

2.4.2 Cases Reported on Cyberstalking

- The majority of cyberstalkers are men and the majority of their victims are women.
- Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking.
- In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-lover, ex-spouse, boss/subordinate, and neighbor.
- However, there also have been many instances of cyberstalking by strangers.

Prepared By Mr. Isaac Paul. P, Department of CSE- RGAN

www.Jntufastupdates.com

2.4.3 How Stalking Works?

It is seen that stalking works in the following ways:

1. Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. Th e letters may have the tone of loving, threatening or can be sexually explicit. Th e stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details (telephone numbers/cell phone numbers/E-Mail address) to have sexual services. The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details (telephone/cell phone nos), asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

2.4.4 Real-Life Incident of Cyberstalking

Case Study
The Indian police have registered first case of cyberstalking in Delhi – the brief account of the case has been mentioned here. To maintain confidentiality and privacy of the entities involved, we have changed their names.
• Mrs. Joshi received almost 40 calls in 3 days mostly at odd hours from as far away as Kuwait, Cochin, Bombay, and Ahmadabad.
• The said calls created havoc in the personal life destroying mental peace of Mrs. Joshi who decided to register a complaint with Delhi Police.
• A person was using her ID to chat over the Internet at the website www.mirc.com, mostly in the Delhi channel for four consecutive days.
• This person was chatting on the Internet, using her name and giving her address, talking in obscene language.
• The same person was also deliberately giving her telephone number to other chatters encouraging them to call Mrs. Joshi at odd hours.
• This was the first time when a case of cyberstalking was registered.
• Cyberstalking does not have a standard definition but it can be defined to mean threatening, unwarranted behavior, or advances directed by one person toward another person using Internet and other forms of online communication channels as medium.

SCANNED

Box 2.8 | Cyberbullying

The National Crime Prevention Council defi nes *Cyberbullying* as "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person."

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defi nes cyberbullying as "a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology."

The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults.[4]
Source: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009)

Dept. of CSE- RGAN

2.5 Cybercafe and Cybercrimes

- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students.
- Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes.
- In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.
- **First**, we do not know what programs are installed on the computer – that is, risk of malicious programs such as *keyloggers* or *Spyware*, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior.
- **Second**, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.
- Indian Information Technology Act (ITA) 2000, does not define cybercafes and interprets cybercafes as "network service providers" referred to under the Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network.
- Cybercriminals prefer cybercafes to carry out their activities.
- The criminals tend to identify one particular personal computer (PC) to prepare it for their use.
- Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.
- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.
- A recent survey conducted in one of the metropolitan cities in India reveals the following facts:

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button. Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack was carried out, to retrieve logged files.
4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is

CSE-RGAN

down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.

5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security. There are thousands of cybercafes across India.

In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe.

Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:**
2. **Stay with the computer:**
3. **Clear history and temporary fi les:**
4. **Be alert:**
5. **Avoid online financial transactions:**
6. **Change passwords:**
7. **Use Virtual keyboard:**
8. **Security warnings:**

2.6 Botnets: The Fuel for Cybercrime

2.6.1 Botnet

- The dictionary meaning of Bot is

"(*computing*) *an automated program for doing some particular task, often over a network.*"

- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer program One can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access.
- Computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "*Zombie networks*" have become a source of income for entire groups of cybercriminals.

Prof. of CSE- RGAN

www.Jntufastupdates.com

- The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.
- If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums.
- 'encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet. Figure 2.8 explains how Botnets create business.
- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.

One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date:
2. Set the OS to download and install security patches automatically:
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet:

   A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.
4. Disconnect from the Internet when you are away from your computer:
5. Downloading the freeware only from websites that are known and trustworthy:
6. Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send:
7. Take an immediate action if your system is infected:

Box 2.9 | Technical Terms
Malware: It is malicious *software*, designed to damage a computer system without the owner's informed consent. Viruses and worms are the examples of malware.
Adware: It is *advertising-supported software*, which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Few Spywares are classifi ed as Adware.
Spam: It means unsolicited or undesired E-Mail messages
Spamdexing: It is also known as search Spam or search engine Spam. It involves a number of methods, such as repeating unrelated phrases, to manipulate the relevancy or prominence of resources indexed by a search engine in a manner inconsistent with the purpose of the indexing system.
DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods

UNSOLD COPY

2.7 Attack Vector

- **An "attack vector" is a path,** which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- **Attack vectors** enable attackers to exploit system vulnerabilities, including the human element.
- **Attack vectors** include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defenses.
- To some extent, firewalls and antivirus software can block attack vectors.
- However, no protection method is totally attack-proof.
- A defense method that is effective today may not remain so for long because attackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers. Refer to Box 2.10.
- The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
- In the technical terms, *payload* is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e., attack vector) payload means the malicious activity that the attack performs.
- From the technical perspective, payload does not include the "overhead" data required to get the packet to its destination. Payload may depend on the following point of view: "What constitutes it?" To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include that part of the overhead data that this layer handles.

The attack vectors described here are how most of them are launched.

1. **Attack by E-Mail:** The content is either embedded in the message or linked to by the message. Sometimes attacks combine the two vectors, so that if the message does not get you, the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or malicious action of some kind. Any link that offers something "free" or tempting is a suspect.
2. **Attachments (and other files):** Malicious attachments install malicious computer code. The code could be a virus, Trojan Horse, Spyware, or any other kind of malware. Attachments attempt to install their payload as soon as you open them.
3. **Attack by deception:** Deception is aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor. Fraud, scams, and to some extent Spam, not to mention viruses, worms and such require the unwitting cooperation of the computer's operator to succeed. Social engineering are other forms of deception that are often an attack vector too.
4. **Hackers:** Hackers/crackers are a formidable attack vector because, unlike ordinary Malicious Code, people are flexible and they can improvise. Hackers/crackers use a variety of hacking tools, heuristics, Cyberoffenses: How and social engineering to gain access to computers and online accounts. They often install a Trojan Horse to commandeer the computer for their own use.

Prepared By Mr. Isaac Paul. P, Department of CSE- RGAN

www.Jntufastupdates.com

5. Heedless guests (attack by webpage): Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate. One may think he/she is doing business with someone you trust. However, he/she is really giving their personal information, like address, credit card number, and expiration date. They are often used in conjunction with Spam, which gets you there in the first place. Pop-up webpages may install Spyware, Adware or Trojans.

6. Attack of the worms: Many worms are delivered as E-Mail attachments, but network worms use holes in network protocols directly. Any remote access service, like file sharing, is likely to be vulnerable to this sort of worm. In most cases, a firewall will block system worms. Many of these system worms install Trojan Horses.

7. Malicious macros: Microsoft Word and Microsoft Excel are some of the examples that allow macros. A macro does something like automating a spreadsheet, for example. Macros can also be used for malicious purposes. All Internet services like instant messaging, Internet Relay Chart (IRC), and P2P fi le-sharing networks rely on cozy connections between the computer and the other computers on the Internet. If one is using P2P software then his/her system is more vulnerable to hostile exploits.

8. Foistware (sneakware): Foistware is the software that adds hidden components to the system with cunning nature. Spyware is the most common form of foistware. Foistware is partial- legal software bundled with some attractive software. Sneak software often hijacks your browser and diverts you to some "revenue opportunity" that the foistware has set up.

9. Viruses: These are malicious computer codes that hitch a ride and make the payload. Nowadays, virus vectors include E-Mail attachments, downloaded files, worms, etc.

Box 2.10 | Zero-Day Attack

A zero-day (or zero-hour) attack[17] is a computer threat which attempts to exploit computer application vulnerabilities that are unknown to anybody in the world (i.e., undisclosed to the software vendor and software users) and/or for which no patch (i.e., security fi x) is available. Zero-day exploits are used or shared by attackers before the software vendor knows about the vulnerability.

Sometimes software vendors discover the vulnerability but developing a patch can take time. Alternatively, software vendors can also hold releasing the patch reason to avoid the flooding the customers with numerous individual updates. A "zero-day" attack is launched just on or before the first or "zeroth" day of vendor awareness, reason being the vendor should not get any opportunity to communicate/distribute a security fi x to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fi xes commonly known as patches) are collected and then release them together as a package. Malware writers are able to exploit zero-day vulnerabilities through several different attack vectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who work to release non-vendor patches for zero-day exploits. Nevada is attempting to provide support with the Zeroday Project at www.zerodayproject.com, which purports to provide information on upcoming attacks and provide support to vulnerable systems. Also visit the weblink http://www.isotf.org/zert to get more information about it.

SECURED

2.8 Cloud Computing

- The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals.
- Cloud computing services, while offering considerable benefits and cost savings, move servers outside the organizations security perimeter, which make it easier for cybercriminals to attack these systems.
- Cloud computing is Internet ("cloud")-based development and use of computer technology ("computing").
- The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.
- Cloud computing is a term used for hosted services delivered over the Internet.
- A cloud service has three distinct characteristics which differentiate it from traditional hosting:

1. It is sold on demand – typically by the minute or the hour;
2. It is elastic in terms of usage – a user can have as much or as little of a service as he/she wants at any given time;
3. The service is fully managed by the provider – a user just needs PC and Internet connection.

Significant innovations into distributed computing and virtualization as well as improved access speed over the Internet have generated a great demand for cloud computing.

2.8.1 Why Cloud Computing?

The cloud computing has following advantages.

1. Applications and data can be accessed from anywhere at any time. Data may not be held on a hard drive on one user's computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space. Cloud computing gives the option of storing data on someone else's hardware, thereby removing the need for physical space on the front end.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware. The cloud computing services can be either private or public.

2.8.2 Types of Services

Services provided by cloud computing are as follows:

1. **Infrastructure-as-a-service (IaaS):** It is like Amazon Web Services that provide virtual servers with unique IP addresses and blocks of storage on demand. Customers benefit from an Application Programmable Interface (API) from which they can control their servers. As customers can pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.
2. **Platform-as-a-service (PaaS):** It is a set of software and development tools hosted on the provider's servers. Developers can create applications using the provider's APIs. Google Apps is one of the most famous PaaS providers. Developers should take notice that there are not any interoperability standards; therefore, some providers may not allow you to take your application and put it on another platform.

Prepared By Mr. Isaac Paul. P, Department of CSE- RGAN

www.Jntufastupdates.com

3. Software-as-a-service (SaaS): It is the broadest market. In this case, the provider allows the customer only to use its applications. The **software interacts with the user through a user interface.** These applications can be anything from Web-based E-Mail to applications such as Twitter or Last.fm.

2.8.3 Cybercrime and Cloud Computing

- Nowadays, prime area of the risk in cloud computing is protection of user data. Although cloud computing is an emerging field, the idea has been evolved over few years.
- Risks associated with cloud computing environment are as follows

1. Elevated user access	Any data processed outside the organization brings with it an inherent level of risk.
2. Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments.
3. Location of the data	User doesn't know where the data is stored or in which country it is hosted.
4. Segregation of data	Data of one organization is scattered in different locations.
5. Recovery of the data	In case of any disaster, availability of the services and data is critical.
6. Information security violation reports	Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity
7. Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.

Dept. of CSE