UNIT-II:CYBER OFFENSES

2.1 How CriminalsPlanThem–Introduction

- Technology is a“double-edged sword”asit can be used for both good and bad purposes.
- People with the tendency to cause damages or carryingout 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 outacrossnational borders.
- Chapter1 provided an over view of *hacking*, *cyberterrorism*, *networkintrusions*, *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 storedata, contacts, account information, etc.
- The criminals take advantage of the widespread lack of awareness about cybercrimes andcyberlaws among the people who are constantly usingtheIT infrastructure for officialandpersonal purposes.
- People who commit cybercrimes are known as“Crackers”(Box2.1).

Box2.1|Hackers,CrackersandPhreakers

Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting withthem. Hackers are usually very talented,smartpeople who understand computers better than others.The term is often confused with cracker that defines someone who Breaks into computers(refertoBox2.2).

Bruteforce hacking: It is a technique used to find passwords or encryption keys. Bruteforce 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 subjectonthe 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 phonelines(called“phreaking”).These sites usually display warnings such as “These files are illegal; we are not responsible for what you do with them.”

Crackertools: These are programs used to breakintocomputers.Crackertoolsarewidely distributedontheInternet.Theyincludepasswordcrackers,Trojans,viruses,wardialersandworms.

Phreaking: Thisisthenotoriousartofbreakingintophoneorothercommunicationsystems. PhreakingsitesontheInternetarepopularamongcrackersandothercriminals.

Wardialer: Itisprogramthatautomaticallydialsphonenumberslookingforcomputersonthe otherend.It catalogsnumbersso thatthehackerscancall backandtrytobreakin.

- Anattackerwouldlooktoexploitthevulnerabilitiesinthenetworks,mostoftensobecausethenetworks arenot adequatelyprotected.
- Thecategoriesof vulnerabilitiesthathackers typicallysearchforarethefollowing:
    1. Inadequateborderprotection(borderasinthesenseofnetworkperiphery);
    2. remoteaccessservers (RASs)withweakaccess controls;
    3. applicationserverswithwell-knownexploits;
    4. misconfiguredsystemsandsystemswithdefaultconfigurations.
- Tohelpthereaderunderstandthenetworkattackscenario,Fig.2.2illustratesasmallnetworkhighlightingspecificoccurrencesof severalvulnerabilities describedabove.

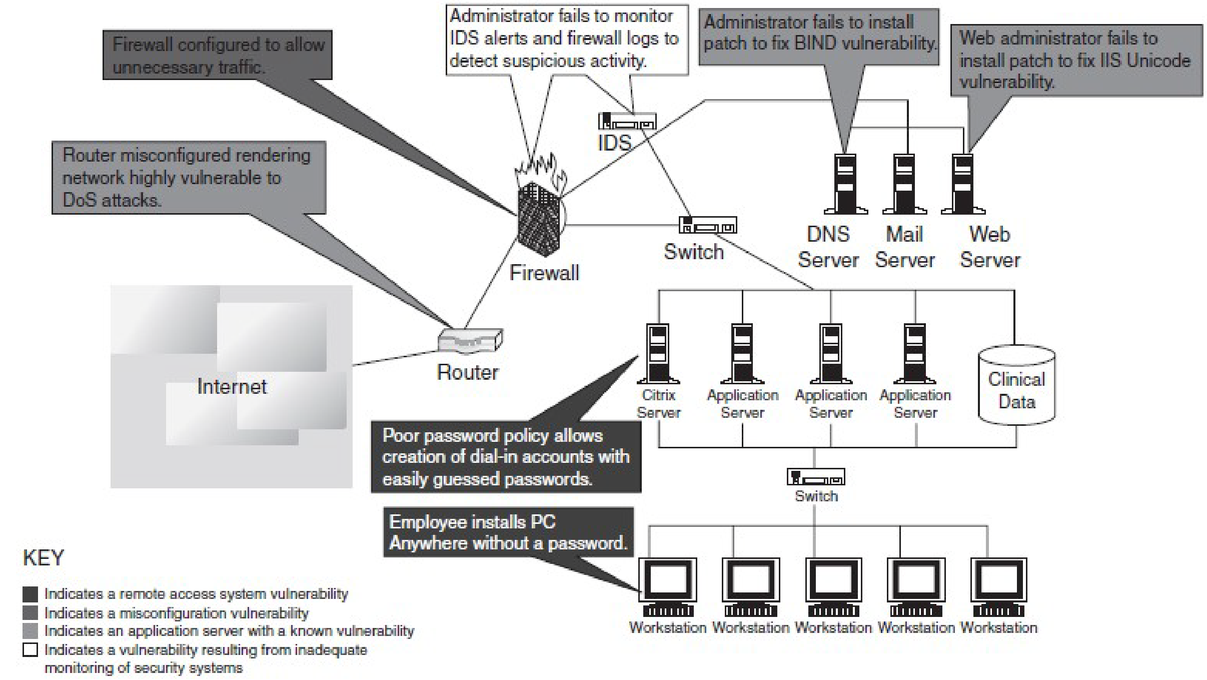
Firewall configured to allow unnecessary traffic.
Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.
Administrator fails to install patch to fix BIND vulnerability.
Web administrator fails to install patch to fix IIS Unicode vulnerability.
Router misconfigured rendering network highly vulnerable to DoS attacks.
IDS
Firewall
Switch
DNS Server
Mail Server
Web Server
Internet
Router
Citrix Server
Application Server
Application Server
Application Server
Clinical Data
Poor password policy allows creation of dial-in accounts with easily guessed passwords.
Switch
Employee installs PC Anywhere without a password.
Workstation
Workstation
Workstation
Workstation
Workstation
KEY
■ Indicates a remote access system vulnerability
■ Indicates a misconfiguration vulnerability
■ Indicates an application server with a known vulnerability
□ Indicates a vulnerability resulting from inadequate monitoring of security systems

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.

Box2.2 |WhatColorisYour Hatin theSecurity World?

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

*A****whitehathacker***isconsideredan***ethicalhacker***.IntherealmofIT,a“whitehathacker”is a person who is ethically opposed to the abuse of computer systems. It is said that the term isderivedfromAmericanwesternmovies,wheretheprotagonisttypicallyworeawhitecowboyhat 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 tobreakinto them, so this sounds likean age-oldgame ofathief and apolice.

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

2.1.1Categoriesof Cybercrime

Cybercrimecanbe categorizedbasedonthefollowing:

1. Thetargetofthecrime and

2. whetherthe crimeoccursasasingle eventorasaseriesof events.

- Cybercrimecanbetargetedagainstindividuals(**persons**),assets(**property**)and/or **organizations**(government,businessandsocial).
  1. **Crimes targeted at individuals:** The goal is to exploit human weakness such as greedand naivety. These crimes include financial frauds, sale of non-existent or stolen items,childpornography(explainedinSection1.5.13,Chapter1),copyrightviolation,harassment, etc. with the development in the IT and the Internet; thus, criminals have anew tool that allows them to expand the pool of potential victims. However, this alsomakesdifficult to traceand apprehend thecriminals.
  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 wipeout data from hard disk, and can create the malfunctioning of the attached devices in thesystemsuchas modem, CD drive, etc.
  3. **Crimes targeted at organizations:** Cyberterrorism is one of the distinct crimes againstorganizations/governments.Attackers(individualsorgroupsofindividuals)usecomputer tools and the Internet to usually terrorize the citizens of a particular country bystealing the private information, and also to damage the programs and files or plantprogramstoget controlof thenetworkand/or system (seeBox2.3).

4. **Single event of cybercrime:** It is the single event from the perspective of the victim. Forexample, unknowingly open an attachment that may contain virus that will infect thesystem(PC/laptop).This is known as hackingor fraud.
5. **Series of events:** This involves attacker interacting with the victims repetitively. Forexample,attackerinteractswiththevictimonthephoneand/orviachatroomstoestablish relationship first and then they exploit that relationship to commit the sexualassault.

Box2.3|PatriotHacking

Patriot hacking[1] also known as ***Digital Warfare***, is a form of vigilante computer systems’crackingdonebyindividualsorgroups(usuallycitizensorsupportsofacountry)againstarealor perceived threat. Traditionally, Western countries, that is, developing countries, attempts tolaunchattacks on their perceivedenemies.

Althoughpatriothacking isdeclaredasillegalinthe US, however, itisreservedonly forgovernment 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) raisedtheconcernaboutriseincyberattackslikewebsitedefacements(explainedinBox1.4,Chapter1) and denial-of-service attacks (DoS – refer to Section 4.9, Chapter 4), which adds as fuel intoincreasein international tension andgets mirroredit intothe online world.

After the war in Iraq in 2003, it is getting popular in the North America, Western Europe andIsrael.Thesearecountriesthathavethegreatestthreattolslamicterrorismanditsaforementioneddigital version.

The People’s Republic of China is allegedly making attacks upon the computer networks of theUSandtheUK.RefertoBox5.15inChapter5.Fordetailedinformationvisitwww.patriothacking.com

2.2 HowCriminalsPlantheAttacks

- Criminals use many methods andtools to locate the vulnerabilities of their target.
- Thetargetcanbe anindividualand/oranorganization.
- Criminalsplanpassiveandactiveattacks
- **Activeattacks**areusuallyusedtoalterthesystem(i.e.,computernetwork)whereas**passiveattacks**attempt to gain information about the target.
- **Activeattacks**mayaffecttheavailability,integrityandauthenticityofdatawhereas**passiveattacks**lead to violationofconfidentiality.

Thefollowingphases areinvolved inplanningcybercrime:
1. Reconnaissance(informationgathering)isthefirstphaseandis treatedas**passiveattacks.**
2. Scanningandscrutinizingthegatheredinformationforthevalidityoftheinformationaswellasto identifytheexistingvulnerabilities.
3. Launchinganattack(gainingandmaintainingthesystemaccess).

2.2.1 Reconnaissance

- Theliteralmeaningof“Reconnaissance”is*anactof****findingsomethingorsomebody*** (*especiallytogaininformation aboutanenemyorpotentialenemy*).
- In the world of “hacking,” reconnaissance phase begins with “*Footprinting*” – this is thepreparationtowardpre-attackphase,andinvolvesaccumulatingdataaboutthetarget’senvironmentand 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 andservices,andanyother aspects ofitssecuritythatareneedful forlaunching the attack.
- Thus, anattacker attempts to gatherinformationin two phases: passiveand activeattacks.Letus understandthesetwo phases.

2.2.2 PassiveAttacks

- A passive attack involves gathering informationabout a target without his/her (individual’sorcompany’s)knowledge.
- It can be as simple as watching a building to identify what time employees enter the buildingpremises.
- However,itisusuallydoneusingInternetsearchesorby Googling (i.e.,searching therequired information with the help of search engine Google) an individual orcompany togaininformation.

  1. GoogleorYahoo search:Peoplesearch tolocateinformationaboutemployees.
  2. Surfingonlinecommunity groupslikeOrkut/Facebookwillproveusefultogaintheinformationabout an individual.
  3. Organization’swebsitemayprovideapersonneldirectoryorinformationaboutkeyemployees, for example, contact details, E-Mail address, etc. These can be used in a socialengineeringattack toreach the target(seeSection2.3).
  4. Blogs,newsgroups,pressreleases,etc.aregenerallyusedasthemediumstogaininformationabout the companyoremployees.

5. Going through the job postings in particular job profiles for technical persons can provideinformation about type of technology, that is, servers or infrastructure devices a companymaybeusingon itsnetwork.

2.2.3 ActiveAttacks

- An active attack involves probing the network to discover individual hosts to confirm theinformation (IP addresses, operating system type and version, and services on the network)gatheredin thepassiveattackphase.
- Itinvolvesthe riskofdetectionandisalsocalled"*Rattlingthe doorknobs*" or "*Activereconnaissance*."
- Active reconnaissance can provide confirmation to an attacker about security measures inplace (e.g., whether the front door is locked?), but the process can also increase the chance ofbeingcaught or raise a suspicion.

2.2.4 ScanningandScrutinizingGatheredInformation

- Scanningisakeysteptoexamineintelligentlywhilegatheringinformationaboutthetarget.Theobjectivesofscanningareasfollows:
  1. Portscanning: Identifyopen/closeportsandservices.RefertoBox 2.5.
  2. Networkscanning: UnderstandIPAddressesandrelatedinformationaboutthecomputernetworksystems.
  3. Vulnerabilityscanning: Understandthe existingweaknessesinthesystem.

2.2.5 Attack(GainingandMaintainingtheSystemAccess)

- Afterthescanningandenumeration, theattackislaunchedusingthefollowingsteps:
  1. Crackthepassword.
  2. exploittheprivileges.
  3. executethemaliciouscommands/applications.
  4. hidethefiles(if required).
  5. coverthetracks –deletetheaccesslogs,sothat thereisnotrailillicitactivity.

2.3 SocialEngineering

- Social engineering is the “technique to influence” and “persuasion to deceive” people toobtainthe information orperform someaction.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word,ratherthanexploitingcomputer securityholes.
- It is generally agreed that people are the weak link in security and this principle makes socialengineeringpossible.
- A socialengineerusually usestelecommunication(i.e.,telephoneand/orcellphone) orInternet toget them todo something that is against the security practices and/or policies oftheorganization.
- Social engineering involves gaining sensitive information or unauthorized access privilegesbybuildinginappropriate trust relationships with insiders.
- It is an art of exploiting the trust of people, which is not doubted while speaking in a normalmanner.
- The goal of a socialengineer is to fool someone into providingvaluable information oraccessto that information.
- Social engineer studies the human behavior so that people will help because of the desire tobehelpful, theattitudetotrust people,and the fearof gettingintotrouble.
- The sign of truly successful social engineers is that they receive information without anysuspicion.
- A simple example is calling a user and pretending to be someone from the service deskworkingonanetworkissue;theattackerthenproceedstoaskquestionsaboutwhattheuserisworkingon, what file shares he/sheuses, what his/her password is, and so on…
(seeBox2.6).

Box2.6|SocialEngineeringExample

Mr.Joshi: Hello?

The Caller: Hello, Mr. Joshi. This is Geeta Thomas from Tech Support. Due to some disk spaceconstraintsonthefileserver,wewillbemovingfewuser’shomedirectoriestoanotherdisk.This activity will be performed tonight at 8:00 p.m. Your account will be a part of this move andwillbeunavailable temporarily.

Mr.Joshi: Ohh…okay.Iwillbeat myhome bythen,anyway.

Caller: Great!!! Pleaseensuretologoffbeforeyouleave office.We justneedtocheckacoupleofthings. What isyour username?

Mr.Joshi: Username is“pjoshi.”Noneof myfi les willbelost in themove, right?

Caller: No sir.Butwewillhave tocheckyouraccounttoensurethe same.Whatisthepasswordofthat account?

Mr.Joshi: Mypasswordis “ABCD1965,” all charactersinuppercase.

Caller: Ok,Mr.Joshi.Thankyouforyourcooperation.Wewillensurethatallthefilesarethere.

Mr.Joshi: Thankyou. Bye.

Caller: Byeand have aniceday.

2.3.1 ClassificationofSocialEngineering

Human-BasedSocialEngineering

- Human-basedsocialengineeringreferstoperson-to-personinteractiontogettherequired/desiredinformation.
- Anexampleiscallingthehelpdesk and tryingto findout apassword.

1. **Impersonating an employee or validuser:**
   - “Impersonation” is perhaps the greatest technique used by social engineers to deceivepeople.
   - Socialengineers“takeadvantage”ofthefactthatmostpeoplearebasicallyhelpful,so it seems harmless to tell someone who appears to be lost where the computer roomis located, or to let someone into the building who “forgot” his/her badge, etc., orpretendingto be anemployeeor validuser on the system.
2. **Posingasanimportantuser:**
   - The attacker pretends to be an important user– for example, a Chief ExecutiveOfficer (CEO) or high-level manager who needs immediate assistance to gain accesstoasystem.
   - The attacker uses intimidation so that a lower-level employee such as a help-deskworker will help him/her in gaining access to the system. Most of the low-levelemployees will not ask any question to someone who appears to be in a position ofauthority.
3. **Usingathirdperson:**
   - 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 cannotbecontacted forverification.
4. **Callingtechnicalsupport:**
   - Callingthetechnical supportforassistanceis aclassicsocialengineeringexample.
   - Help-desk and technical support personnel are trained to help users, which makesthem goodpreyforsocial engineeringattacks.
5. **Shouldersurfing:**
   - Itisatechniqueofgatheringinformationsuchasusernamesandpasswordsbywatching over a person’s shoulder while he/she logs into the system, thereby helpinganattacker togain accessto thesystem.
6. **Dumpsterdiving:**
   - It involves **looking in the trash for information written on pieces of paper orcomputerprintouts**.
   - ThisisatypicalNorthAmericanterm;itisusedtodescribethepracticeofrummaging through commercial or residential trash to find useful free items that havebeendiscarded.
   - Itisalsocalleddumpstering,binning,trashing,garbingorgarbage gleaning.
   - “Scavenging”isanothertermtodescribethesehabits.
   - In the UK, the practice is referred to as “ binning” or “skipping” and the person doingitis a “binner”ora“skipper.”

Computer-Based SocialEngineering

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

1. **FakeE-Mails:**

- The attacker sends fake E-Mails(seeBox2.7)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-upwindows:**

- 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.

2.4 Cyber stalking

- 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, groupofindividuals, or organization**.
- The behavior includes false accusations, monitoring, transmission of threats, IDtheft, 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 businessplace, 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 TypesofStalkers

Thereareprimarilytwo types ofstalkers.

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

2.4.3 How StalkingWorks?

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/cellphone. Once the contact is established,the stalker maymakecalls to thevictim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. Th eletters may have the tone of loving, threatening or can be sexually explicit. Th e stalkermayuse multiplenameswhilecontactingthe victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors orthreatenthevictim.
5. The stalker may post the victim's personal information on any website related to illicitservices such as sex-workers' services or dating services, posing as if the victim hasposted 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. Thestalkerwillusebadand/or offensive/attractivelanguagetoinvitethe interestedpersons.
6. Whosoever comes across the information, start calling the victim on the given contactdetails(telephone/cell phonenos), askingforsexual services or relationships.
7. Somestalkerssubscribe/registertheE-Mailaccountofthevictimtoinnumerablepornographic and sex sites, because of which victim will start receiving such kind ofunsolicitedE-Mails.

2.4.4 Real-LifeIncidentofCyberstalking

CaseStudy
The Indian police have registered first case of cyberstalkinginDelhi–thebriefaccountofthecasehasbeenmentionedhere.Tomaintainconfidentialityandprivacyoftheentitiesinvolved,
• Mrs.Joshi received almost 40 calls in 3days 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 to ward another Person using Internet and other forms ofo nline communication channels as medium.

Box2.8 |Cyberbullying

The NationalCrime PreventionCouncildefines*Cyberbullying*as“whentheInternet,cellphones or other devices are used to send or post text or images intended to hurt or embarrassanotherperson.”

www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, andprivacydefinescyberbullyingas“asituationwhenachild,tween,orteenisrepeatedly‘tormented,threatened,harassed,humiliated,embarrassed,orotherwisetargeted’byanotherchild, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digitaltechnology.”

The practice of cyberbullying is not limited to children and, while the behavior is identified bythe same definition in adults, the distinction in age groups is referred to as cyberstalking orcyberharassment when perpetrated byadults toward adults.[4]
*Source:*http://en.wikipedia.org/wiki/Cyber-bullying(2April2009).

2.5 Cyber café andCybercrimes

- In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of15–35 years;52%weregraduatesandpostgraduates,thoughalmostover50%werestudents.
- Hence,itisextremelyimportanttounderstandtheITsecurityandgovernancepracticedinthecybercafes.
- In the past several years, many instances have been reported in India, where cybercafes areknownto beusedfor either real or false terrorist communication.
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal ofmoneyhavealso happened through cybercafes.
- Cybercafeshavealsobeenused regularlyforsendingobscenemailsto harass people.
- Public computers, usually referred to the systems, available in cybercafes, hold two types ofrisks.
- **First**, we do not know what programs are installed on the computer– that is, risk ofmalicious programs such as *keyloggers* or *Spyware*, which maybe running at the backgroundthat can capture the keystrokes to know the passwords and other confidential informationand/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 doesnotknow 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 Section79,which imposedon them a responsibility for“due diligence” failing which they would be liable for theoffenses committed in their network.
- Cyber criminals prefer cyber cafes to carry out their activities.
- Thecriminalstendtoidentifyoneparticularpersonalcomputer(PC)topreparei tfortheiruse.
- Cybercriminalscaneitherinstallmaliciousprogramssuchaskeyloggersand/orSpywareorlaunchan attack on the target.
- Cybercriminalswillvisitthesecafesataparticulartimeandontheprescribedfrequency,maybealternate dayortwiceaweek.
- Arecentsurveyconductedinoneofthemetropolitancitiesin Indiarevealsthefollowingfacts:

  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 anti virus 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 allactivities 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 pickup clues after the Internet 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 loggedfiles.

  4. Annualmaintenancecontract(AMC)foundtobenotinaplaceforservicingthecomputers;hence, harddisksforallthecomputersarenotformattedunlessthecomputeris down. Not having the AMC is a risk from cybercrime perspective because a cybercriminalcan install a Malicious Code on a computer and conduct criminal activities without anyinterruption.

5. Pornographicwebsitesandothersimilarwebsiteswithindecentcontentsarenotblocked.

6. Cybercafeownershaveverylessawareness aboutITSecurityandITGovernance.

7. Government/ISPs/StatePolice(cybercellwing)donotseemtoprovideITGovernanceguidelines to cybercafeowners.

8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodicvisits to cybercafes – one of the cybercafe owners whom we interviewed expressed a viewthat the police will not visit a cybercafe unless criminal activity is registered by filing an FirstInformationReport(FIR).Cybercafeownersfeelthatpoliceeitherhaveaverylittleknowledge aboutthe technicalaspectsinvolvedincybercrimes and/oraboutconceptualunderstandingofIT security. Therearethousandsofcybercafes across India.

In the event that a central agency takes up the responsibility for monitoring cybercafes, anindividualshould takecarewhile visitingand/or operatingfromcybercafe.

Hereare afewtips forsafetyand securitywhileusingthe computer inacybercafe:

1. Always logout:
2. Staywiththecomputer:
3. Clearhistoryand temporaryfiles:
4. Bealert:
5. Avoidonlinefinancialtransactions:
6. Changepasswords:
7. UseVirtualkeyboard:
8. Securitywarnings:

2.6 Botnets:TheFuelforCybercrime

2.6.1 Botnet

- Thedictionarymeaning ofBot is

“(*computing*)*an automatedprogram for doing someparticular task,often overa network.*”

- Botnetisatermusedforcollectionofsoftwarerobots,orBots,thatrunautonomouslyandautomatically.
- Thetermisoftenassociatedwithmalicioussoftwarebutcanalsorefertothenetworkofcomputersusingdistributed computingsoftware.
- Insimpleterms,aBotissimplyanautomatedcomputerprogramOnecangainthecontrolofcomputerbyinfectingthem with avirus orotherMalicious Codethatgives the access.
- Computersystemmaybe apart of aBotneteventhoughitappearstobeoperatingnormally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses toconductingdenial-of-service(DoS) attacks
- ABotnet(alsocalledaszombienetwork)isanetworkofcomputersinfectedwithamalicious program that allows cybercriminals to control the infected machines remotelywithoutthe users’knowledge.
- “*Zombienetworks*”have become asourceof incomeforentire groupsofcybercriminals.

- TheinvariablylowcostofmaintainingaBotnetandtheeverdiminishingdegreeofknowledgerequiredtomanageoneareconducivetothegrowthinpopularityand,consequently,the number ofBotnets.
- Ifsomeonewantstostarta“business”andhasnoprogrammingskills,thereareplentyof “Botforsale”offers onforums.
- ‘encryptionoftheseprograms’codecanalsobeorderedinthesamewaytoprotectthemfrom detection byantivirus tools.
- AnotheroptionistostealanexistingBotnet.Figure2.8explainshowBotnetscreatebusiness.
- Onecanreducethechances of becomingpartofaBotbylimitingaccess intothesystem.
- LeavingyourInternetconnectionONandunprotectedisjustlikeleavingthefrontdoorofthe housewideopen.

Onecanensurefollowingtosecurethesystem:

1. Useantivirusand anti-Spywaresoftware andkeep itup-to-date:
2. SettheOS todownload andinstallsecuritypatchesautomatically:
3. UseafirewalltoprotectthesystemfromhackingattackswhileitisconnectedontheInternet: Afirewallisasoftwareand/orhardwarethatisdesignedtoblockunauthorizedaccesswhilepermittingauthorized communications.
4. DisconnectfromtheInternetwhenyou areawayfromyour computer:
5. Downloadingthefreewareonlyfrom websitesthatareknownandtrustworthy:
6. Checkregularlythefoldersinthemailbox–“sentitems”or“outgoing”–forthosemessagesyou did not send:
7. Takeanimmediate actionif yoursystemisinfected:

Box2.9|TechnicalTerms

Malware: Itismalicious *software*,designedtodamageacomputersystem withouttheowner’s informedconsent.Viruses andworms arethe examplesof malware.

Adware: It is *advertising-supported software*, which automatically plays, displays, or downloadsadvertisements to a computer after the software is installed on it or while the application is beingused.Few Spywaresare classifi ed as Adware.

Spam: ItmeansunsolicitedorundesiredE-Mail messages

Spamdexing: It is also known as search Spam or search engine Spam. It involves a number ofmethods, such as repeating unrelated phrases, to manipulate the relevancy or prominence ofresources indexed by a search engine in a manner inconsistent with the purpose of the indexingsystem.

DDoS: Distributed denial-of-service attack (DDoS) occurs when multiple systems flood thebandwidth or resources of a targeted system, usually one or more web servers. These systems arecompromised byattackers usingavarietyof methods

2.7 AttackVector

- **An "attack vector" is a path**, which an attacker can gain access to a computer or to anetworkserver to deliverapayload ormalicious outcome.
- **Attackvectors**enableattackerstoexploitsystemvulnerabilities,includingthehumanelement.
- **Attack vectors** include viruses, E-Mail attachments, webpages, pop-up windows, instantmessages, chat rooms, and deception. All of these methods involve programming (or, inafew cases,hardware), exceptdeception, inwhich a human operator isfooled into removingorweakeningsystem defenses.
- Tosomeextent,firewallsandantivirussoftwarecanblockattackvectors.
- However,noprotectionmethod is totallyattack-proof.
- A defense method that is effective today may not remain so for long because attackers areconstantly updating attack vectors, and seeking new ones, in their quest to gain unauthorizedaccessto computers andservers. Refer to Box2.10.
- The most common malicious payloads are viruses (which can function as their own attackvectors),Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to thewarheadin thetip of the missile.
- In the technical terms, *payload* is the necessary data being carried within a packet or othertransmission unit – in this scenario (i.e., attack vector) payload means the malicious activitythatthe attack performs.
- From the technical perspective, payload does not include the "overhead" data required to getthe packet to its destination. Payload may depend on the following point of view: "Whatconstitutes 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 layerhandles.

Theattack vectorsdescribed herearehow mostofthemarelaunched.

1. Attack by E-Mail: The content is either embedded in the message or linked to by themessage. Sometimes attacks combine thetwo vectors, so that ifthe message doesnotgetyou,the attachment will. Spam is almost always carrier for scams, fraud, dirty tricks, or maliciousactionofsomekind. Anylink that offers something"free"ortemptingis asuspect.

2. Attachments (and other files): Malicious attachments install malicious computer code. Thecode couldbe a virus, Trojan Horse, Spyware,or any other kindof malware. Attachmentsattemptto install theirpayloadas soonasyou open them.

3. Attack by deception: Deception is aimed at the user/operator as a vulnerable entry point. It isnot just malicious computer code that one needs to monitor. Fraud, scams, and to some extentSpam,nottomentionviruses,wormsandsuchrequiretheunwittingcooperationofthecomputer's operator to succeed. Social engineering are other forms of deception that are often anattackvector too.

4. Hackers: Hackers/crackers are a formidable attack vector because, unlike ordinary MaliciousCode,peopleareflexibleandtheycanimprovise.Hackers/crackersuseavarietyofhackingtools, heuristics, Cyberoffenses: How and social engineering to gain access to computers andonline accounts. They often install a Trojan Horse to commandeer the computer for their ownuse.

5. Heedless guests (attack by webpage): Counterfeit websites are used to extract personalinformation. Such websites lookvery much likethe genuine websites they imitate.One maythink he/she is doing business with someone you trust. However, he/she is really giving theirpersonal information, like address, credit card number, and expiration date. They are often usedin conjunction with Spam, which gets you there in the first place. Pop-up webpages may installSpyware,Adwareor Trojans.

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

7. Malicious macros: Microsoft Word and Microsoft Excel are some of the examples that allowmacros. A macro does something like automating a spreadsheet, for example. Macros can also beused for malicious purposes. All Internet services like instant messaging, Internet Relay Chart(IRC), and P2P file-sharing networks rely on cozy connections between the computer and theother computers on theInternet.If one isusing P2P software then his/her system is morevulnerableto hostileexploits.

8. Foistware (sneakware): Foistware is the software that **adds hidden components** to thesystem withcunning nature. Spyware is the most common form of foistware.Foistware ispartial- legal software bundled with some attractive software. Sneak software often hijacks yourbrowser and divertsyou tosome “revenueopportunity”thatthefoistwarehas setup.

9. Viruses: Thesearemaliciouscomputercodesthathitcharideandmakethepayload.Nowadays,virus vectorsincludeE-Mailattachments, downloaded files, worms, etc.

Box2.10 |Zero-Day Attack

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

Sometimes software vendors discover the vulnerability but developing a patch can take time.Alternatively,software vendorscanalsoholdreleasingthe patchreasontoavoidtheflooding thecustomerswithnumerousindividualupdates.A“zero-day”attackislaunchedjustonorbeforethefirstor“zeroth”dayofvendorawareness,reasonbeingthevendorshouldnotgetanyopportunitytocommunicate/distributeasecurityfixtousersofsuchsoftware.Ifthevulnerabilityisnotparticularlydangerous,softwarevendorsprefertoholduntilmultipleupdates(i.e.,securityfixescommonlyknownaspatches)arecollectedandthenreleasethemtogetherasapackage.Malwarewritersareabletoexploitzero-dayvulnerabilitiesthroughseveraldifferentattackvectors.

Zero-day emergency response team (ZERT): This is a group of software engineers who workto release non-vendor patches for zero-day exploits. Nevada is attempting to providesupportwith the Zeroday Project at www.zerodayproject.com, which purports to provide information onupcomingattacksandprovidesupporttovulnerablesystems.Alsovisittheweblinkhttp://www.isotf.org/zerttoget moreinformation about it.

2.8 Cloud Computing

- The growing popularity of cloud computing and virtualization among organizations have made it possible, the next target of cybercriminals.
- Cloudcomputingservices,whileofferingconsiderablebenefitsandcostsavings,moveservers outside the organizations security perimeter, which make it easier for cyber criminals toattack these systems.
- Cloud computing is Internet (“cloud”)-based development and use of computer technology(“computing”).
- The term cloud isused as a metaphor fo r 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.

Acloudservicehasthreedistinctcharacteristicswhichdifferentiateitfromtraditionalhosting:
1. Itis sold on demand –typicallybythe minuteorthehour;
2. It is elastic in terms of usage – a user can have as much or as little of a service as he/she wantsat anygiventime;
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 accessspeedoverthe Internet havegenerated agreat demandforcloud computing.

2.8.1 Why CloudComputing?

The cloud computing has following advantages.
1. Applications and data can be accessed from anywhere at any time. Data may not be held on aharddrive on oneuser’s computer.
2. It could bring hardware costs down. One would need the Internet connection.
3. Organizations donothavetobuyasetofsoftwareorsoftwarelicensesforeveryemployeeandtheorganizations could payametered feetoacloud computingcompany.
4. Organizations do not have to rent a physical space to store servers and databases. Servers anddigital storage devices take up space. Cloud computing gives the option of storing data onsomeoneelse’s hardware, therebyremovingthe need forphysical spaceonthefront end.
5. Organizations would be able to save money on IT support because organizations will have toensure about the desktop (i.e., a client) and continuous Internet connectivity instead of serversandotherhardware. The cloud computingservicescanbeeither privateorpublic.

2.8.2 Typesof Services

Services provided by cloud computing areas 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 theprovider’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.

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 asTwitteror Last.fm.

2.8.3 Cyber crime 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.
- Risksassociatedwithcloud computingenvironmentareasfollows

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 notable 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.Segregationofdata	Data of one organization is scattered in different locations
5.Recovery of the data	Incase 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-termviability	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.