9. Denning, D.E. (1999) *Information Warfare and Security*, Addison-Wesley.
10. Bologna, G.J. and Shaw, P. (2000) *Avoiding Cyber Fraud in Small Businesses: What Auditors and Owners Need to Know*, Wiley.
11. Mehta, R. and Mehta R. *Credit Cards: A Legal Guide with Special Reference to Credit Card Frauds*, 2nd edn), Universal Law Publishing Company.

Articles and Research Papers

1. Read article *China Mounts Cyber Attacks on Indian Sites* at: http://timesofindia.indiatimes.com/india/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms (29 January 2010).
2. Read article *3,286 Indian Websites Hacked in Five Months* at: http://www.siliconindia.com/shownews/3286_Indian_websites_hacked_in_five_months-nid-63485.html (29 January 2010).
3. Read article *40-50 Indian Sites Hacked by Pak Cyber Criminals Monthly* at: http://archives.info-tech.indiatimes.com/articleshow/35371176.cms (20 January 2010).
4. Read article *Pakistani Cyber criminals Deface 50 to 60 Indian Websites per day* at: http://www.webnewswire.com/node/480067 (15 January 2010).
5. A white paper on Click Frauds can be accessed in the following links:

   http://www.hitslink.com/whitepapers/click-fraud.pdf (24 March 2010).

   Additional links on the topic of "Click Fraud" can be visited at:

   http://www.marketingtilt.com.au/what-is-click-fraud/ (23 March 2010).

   http://en.wikipedia.org/wiki/Click%5Ffraud (24 March 2010).

   http://www.wisegeek.com/what-is-external-click-fraud.htm (24 March 2010).

   http://www.wisegeek.com/what-is-click-fraud.htm (24 March 2010).

   http://www.clickprotector.com/faq.asp (24 March 2010) (FAQ on detecting and stopping Click Frauds).

   http://help.yahoo.com/l/uk/yahoo/ysm/sps/faqs/accclickthru/click_fraud.html (24 March 2010).

   http://www.bukisa.com/articles/186305_what-is-advertising-click-fraud (24 March 2010).
6. A paper on *Anti-Spam Laws and their Effectiveness* can be accessed at:

   http://www-users.rwth-aachen.de/guido.schryen/publications/Schryen%20-%20Anti-spam%20legislation%20-%20ICTL.pdf (8 May 2010).

The appendices that serve as extended material for the topics addressed in this chapter are: A, B, D, E, F, J, K, L, M, O, P, Q, U, V. These are provided in the companion CD.

2 Cyberoffenses: How Criminals Plan Them

Learning Objectives

After reading this chapter, you will be able to:

- Understand different types of cyberattacks.
- Get an overview of the steps involved in planning cybercrime.
- Understand tools used for gathering information about the target.
- Get an overview on social engineering – what and how.
- Learn about the role of cybercafes in cybercrime.
- Understand what cyberstalking is.
- Learn about Botnets and attack vector.
- Get an overview on cloud computing – what and how.

2.1 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 no exceptions; like other tool, they are used as either target of offense or means for committing an offense. In today's world of Internet and computer networks, a criminal activity can be carried out across national borders with "false sense of anonymity"; without realizing, we seem to pass on tremendous amount of information about ourselves. Are we sure this will never be misused? Figure 2.1 gives us an idea about all those agencies that collect information about the individuals (i.e., Personally Identifiable Information such as date of birth, personal E-Mail address, bank account details and/or credit card details, etc. explained in Section 5.3.1, Chapter 5).

Chapter 1 provided an overview of *hacking, industrial espionage, 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).

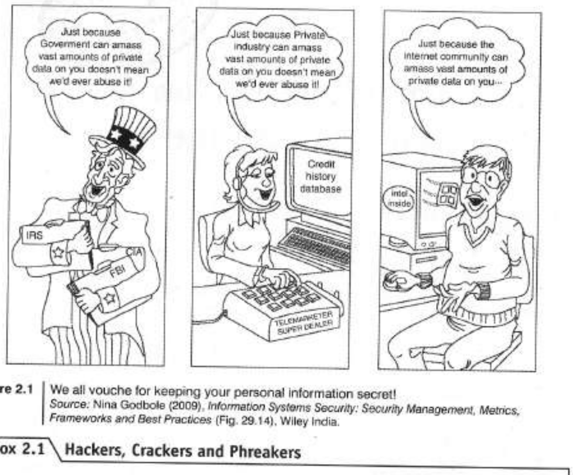

Just because Goverment can amass vast amounts of private data on you doesn't mean we'd ever abuse it!
IRS
FBI
CIA
Just because Private industry can amass vast amounts of private data on you doesn't mean we'd ever abuse it!
Credit history database
TELEMARKETER SUPER DEALER
Just because the internet community can amass vast amounts of private data on you...
intel inside

Figure 2.1 We all vouche for keeping your personal information secret!
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Fig. 29.14), Wiley India.

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 defines 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 files 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.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2), Wiley India.

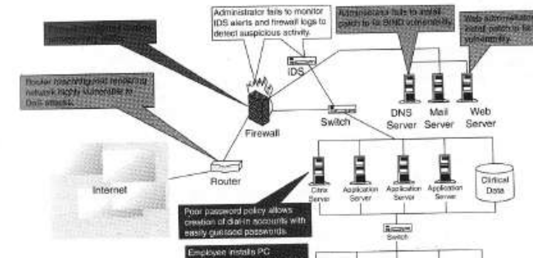

Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.
Administrator fails to install patch to fix BIND vulnerability.
Web administrator fails to install patch to fix IIS Unicode vulnerability.
Router misconfigured rendering network highly vulnerable to DoS attacks.
IDS
Firewall
Switch
DNS Server
Mail Server
Web Server
Internet
Router
Citrix Server
Application Server
Application Server
Application Server
Critical 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.

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.

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

When Edward De Bono wrote his epoch making the book *The Six Thinking Hats* most successful concept that helps people to be more productive, focused, and mindfully involved, little did he know that the hats would follow suit in other domains too!! Just read on to discover about the "hats" in security world. And not only that, but also be conscious to know if any of these hats are around you to jeopardize the security of your information assets on the network.

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 jargon, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

Box 2.2 What Color . . . (*Continued*)

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 *black hat* will wish to secure his/her own machine whereas a white hat might need to break into a black hat's machine in course of an investigation. What exactly differentiates white hats and black hats is open to interpretation; however, white hats tend to cite altruistic motivations. Usually a black hat is a person who uses his knowledge of vulnerabilities and exploits for private gain, rather than revealing them either to the general public or to the manufacturer for correction. Black hats may seek to expand holes in systems; any attempts made to patch software are generally done to prevent others from also compromising a system over which they have already obtained secure control. In the most extreme cases, black hats may work to cause damage maliciously.

Interestingly, this is not all; in the security world, there are hats of other colors too. *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).

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 17.3), Wiley India.

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.

As explained in Section 1.5, Chapter 1, 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).

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

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 (refer to Section 2.4 on "Cyberstalking").

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. (The custodian of a property can be an individual or an organization; for discussion purpose not mentioned here.) Criminals plan passive and active attacks (see Sections 2.2.2 and 2.2.3 for more details on these topics). 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 breaches of confidentiality.

In addition to the active and passive categories, attacks can be categorized as either inside or outside. An attack originating and/or attempted within the security perimeter of an organization is an inside attack; it is usually attempted by an "insider" who gains access to more resources than expected. An outside attack is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

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

The literal meaning of "Reconnaissance" is *an act of reconnoitering – explore, often with the goal 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 preattack 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 (see Table 2.1).
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.

Box 2.4 Tips for Effective Search with "Google" Search Engine

The Google search engine can be used indigenously to perform "Reconnaissance" phase of an attack. The following commands can be used effectively in the Google search engine.

http://groups.google.com: This site can be used to search the Google newsgroups.

Site: If you include [site:] in your query, Google will restrict the results to those websites in the given domain. For instance, [help site:www.google.com] will find pages about help within www.google.com. [help site:com] will find pages about help within .com URLs (uniform resource locator). Note that, there should be no space between the "site:" and the domain. This feature is also available through advanced search page, under Advanced Web Search > Domains.

Filetype: This will search within the text of a particular type of file. The file type to search must be typed after the colon.

Link: The query [link:] will list the webpages that have links to the specified webpage. For instance, [link: www.google.com] will list webpages that have links pointing to the Google homepage. Note that there can be no space between the "link:" and the webpage URL. This functionality is also accessible from the advanced search page, under Page Specific Search > Links.

Box 2.4 Tips for . . . (*Continued*)

Inurl: If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the URL. For instance, [inurl:google search] will return documents that mention the word "google" in their URL, and mention the word "search" anywhere in the document (URL or no). Note that there should be no space between the "inurl:" and the following word. Putting "inurl:" in front of every word in your query is equivalent to putting "allinurl:" in front of your query: this implies [inurl:google inurl:search] is the same as [allinurl: google search].

Cache: If you include other words in the query, Google will highlight those words within the cached document. For instance, [cache: www.google.com web] will show the cached content with the word "web" highlighted. This feature is also accessible by clicking on the "Cached" link on Google's main results page. The query [cache:] will show the version of the webpage that Google has in its cache. For instance, [cache: www.google.com] will show Google's cache of the Google homepage. Note that there should be no space between the "cache:" and the webpage URL.

Related: The query [related:] will list webpages that are "similar" to a specified webpage. For instance, [related: www.google.com] will list webpages that are similar to the Google homepage. Note that there should be no space between the "related:" and the webpage URL. This feature is also accessible by clicking on the "Similar Pages" link on Google's main results page, and from the advanced search page, under Page Specific Search > Similar.

Info: The query [info:] will present some information that Google has about that webpage. For instance, [info: www.google.com] will show information about the Google homepage. Note that there should be no space between the "info:" and the webpage URL. This feature is also accessible by typing the webpage URL directly into a Google search box.

Define: The query [define:] will provide a definition of the word/phrase you enter after it, gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them).

Stocks: If you begin a query with the [stocks:] operator, Google will treat the rest of the query terms as stock ticker symbols and will link to a page showing stock information for those symbols. For instance, [stocks: intc yhoo] will show information about Intel and Yahoo. (Note that you must type the ticker symbols, not the company name.) This feature is also available if you search just on the stock symbols (e.g., [intc yhoo]) and then click on the "Show stock quotes" link on the results page.

Allintitle: If you start a query with [allintitle:], Google will restrict the results to those with all of the query words in the title. For instance, [allintitle: google search] will return only documents that have both "google" and "search" in the title. This feature is also available through advanced Search page, under Advanced Web Search > Occurrences.

Intitle: If you include [intitle:] in your query, Google will restrict the results to documents containing that word in the title. For instance, [intitle:google search] will return documents that mention the word "google" in their title and the word "search" anywhere in the document (title or no). Note that there should be no space between the "intitle:" and the following word. Putting [intitle:] in front of every word in your query is equivalent to putting [allintitle:] at the front of your query: this implies that [intitle:google intitle:search] is the same as [allintitle: google search].

Allinurl: If you start a query with [allinurl:], Google will restrict the results to those with all of the query words in the URL. For instance, [allinurl: google search] will return only documents that have both "google" and "search" in the URL.

Note that [allinurl:] works on words, not on URL components. In particular, it ignores punctuation. Thus, [allinurl: foo/bar] will restrict the results to page with the words "foo" and "bar" in the URL, but won't require that they be separated by a slash within that URL, that they be adjacent, or that they be in that particular word order. There is currently no way to enforce these constraints.

Source: http://www.google.com.tw/help/operators.html

Network sniffing is another means of passive attack to yield useful information such as Internet Protocol (IP) address ranges, hidden servers or networks, and other available services on the system or network. The network traffic is sniffed for monitoring the traffic on the network – attacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Along with Google search, various other tools are also used for gathering information about the target/victim (Table 2.1).

Table 2.1 | Tools used during passive attacks

Name of the Tool	*Brief Description*	*Remarks*
Google Earth	Google Earth is a virtual globe, map, and geographic information program. It maps the Earth by the superimposition of images obtained from satellite imagery and provides aerial photography of the globe. It is available under three different licenses: Google Earth, a free version with limited functionality; Google Earth Plus (discontinued), with additional features; and Google Earth Pro intended for commercial use.	For more details on this tool, visit: http://earth.google.com/ Like "Google Earth," similar details can be obtained from http://www.wikimapia.org/ Indian Space Research Organization (ISRO) unveiled its beta version of Bhuvan (meaning Earth in Sanskrit), a Web-based tool like Google Earth, that promises better 3-D satellite imagery of India than is currently being offered by Google Earth and that too with India-specific features such as weather information and even administrative boundaries of all states and districts, visit: http://bhuvan.nrsc.gov.in/
Internet Archive	The Internet Archive is an Internet library, with the purpose of offering permanent access for researchers, historians and scholars to historical collections that exist in digital format. It includes texts, audio, moving images, and software as well as archived webpages in our collections.	An attacker gets the information about latest update made to the target's website as well as can dig the information which maybe available in the history (e.g., contact list of executives and higher management officials are always updated). For more details on this tool, visit: http://www.archive.org/index.php
Professional Community	LinkedIn is an interconnected network of experienced professionals from around the world, representing 170 industries and 200 countries.	One can find details about qualified professionals. For more details on this tool, visit: http://www.linkedin.com/
People Search	People Search provides details about personal information: date of birth, residential address, contact number, etc.	To name a few, visit: • http://www.whitepagesinc.com • http://www.intelius.com/ • http://www.whitepages.com/
Domain Name Confirmation	To perform searches for domain names (e.g., website names) using multiple keywords. This helps to enable to find every registered domain name in "com," "net," "org," "edu," "biz," etc.	For more details on this tool, visit: • http://www.namedroppers.com/ • http://www.binarypool.com/bytes.html
WHOIS	This is a domain registration lookup tool. This utility is used for communicating with WHOIS servers located around the world to obtain domain registration information. WHOIS supports IP address queries and automatically selects the appropriate WHOIS server for IP addresses. This tool will lookup information on a domain, IP address, or a domain registration information. You can select a specific WHOIS server, or you can use the "Default" option which will select a server for you.	For more details on this tool, visit: • http://whois.domaintools.com/ • http://www.whois.net/ • http://www.samspade.org/ For further details of this lookup utility, visit: • http://resellers.tucows.com/opensrs/whois/ • http://www.nsauditor.com/docs/html/tools/Whois.htm
Nslookup	The name nslookup means "name server lookup." The tool is used on Windows and Unix to query domain name system (DNS) servers to find DNS details, including IP addresses of a particular computer and other technical details such as mail exchanger (MX) records for a domain and name server (NS) servers of a domain.	For more details on this tool, visit: • http://www.kloth.net/services/nslookup.php • http://nslookup.downloadsoftware4free.com/
Dnsstuff	Using this tool, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookup, WHOIS lookups, etc.	For more details on this tool, visit: http://www.dnsstuff.com/
Traceroute	This is the best tool to find the route (i.e., computer network path) to a target system. It determines the route taken by packets across an IP network.	For more details on this tool, visit: http://www.rjsmith.com/tracerte.html
VisualRoute Trace	This is a graphical tool which determines where and how virtual traffic on the computer network is flowing between source and target destination.	For more details on this tool, visit: http://www.visualware.com/
eMailTrackerPro	eMailTrackerPro analyzes the E-Mail header and provides the IP address of the system that sent the mail.	For more details on this tool, visit: http://www.emailtrackerpro.com/
HTTrack	This tool acts like an offline browser. It can mirror the entire website to a desktop. One can analyze the entire website by being offline.	For more details on this tool, visit: http://www.httrack.com/
Website Watcher	The tool can be used to keep the track of favorite websites for an update. When the website undergoes an update/change, this tool automatically detects it and saves the last two versions onto the desktop.	For more details on this tool, visit: http://www.aignes.com/
Competitive Intelligence	Competitive intelligence can provide information related to almost any product, information on recent industry trends, or information about geopolitical indications. Effective use of competitive intelligence can reveal attack against the website or an industrial espionage.	To name a few, visit: • http://bigital.com/ • http://www.amity.edu/aici/

(Continued)

Table 2.1 | *(Continued)*

Note: IP is Internet Protocol here.

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.

Table 2.2 gives the list of tools used for active attacks – some of the tools are also used during "vulnerability assessment" and/or "penetration testing." Refer to Appendix E in CD.

Table 2.2 | Tools used during active attacks

Name of the Tool	*Brief Description*	*Remarks*
Arphound	This is a tool that listens to all traffic on an Ethernet network interface. It reports IP/media access control (MAC) address pairs as well as events, such as IP conflicts, IP changes and IP addresses with no reverse DNS, various Address Resolution Protocol (ARP) Spoofing and packets not using the expected gateway.	This is open-source software. For more details on this tool and download, visit: http://www.nottale.net/index.php?project=arphound
Arping	This is a network tool that broadcasts ARP packets and receives replies similar to "ping." It is good for mapping a local network and finding used IP space. It broadcasts a "who-has ARP packet" on the network and prints answers. It is very useful when trying to pick an unused IP for a Net to which routing does not exist as yet.	This is open-source software. For more details on this tool and download,visit: http://www.habets.pp.se/synscan/programs.php?prog=arping
Bing	This is used for Bandwidth Ping. It is a point-to-point bandwidth measurement tool based on ping. It can measure raw throughput between any two network links. Bing determines the real (raw as opposed to available or average) throughput on a link by measuring Internet Control Message Protocol (ICMP) echo requests roundtrip times for different packet sizes for each end of the link.	This is open-source software. For installation and usage information, visit: http://ai3.asti.dost.gov.ph/sat/bing.html
Bugtraq	This is a database of known vulnerabilities and exploits providing a large quantity of technical information and resources.	This software is for free usage. Visit the following site for more details: http://www.securityfocus.com/bid
Dig	This is used to perform detailed queries about DNS records and zones, extracting configuration, and administrative information about a network or domain.	This is open-source software. For additional technical details, visit: http://www.isc.org/index.pl?/sw/bind/
DNStracer	This is a tool to determine the data source for a given DNS server and follow the chain of DNS servers back to the authoritative sources.	This is also open-source software. For additional technical details, visit: http://www.mavetju.org/unix/dnstracer.php

(*Continued*)

Table 2.2 | (*Continued*)

Name of the Tool	*Brief Description*	*Remarks*
Dsniff	This is a network auditing tool to capture username, password, and authentication information on a local subnet.	This is open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
Filesnarf	This is a network auditing tool to capture file transfers and file sharing traffic on a local subnet.	This is also open-source software. For additional technical details, visit: http://monkey.org/~dugsong/dsniff/
FindSMB	This is used to find and describe server message block (SMB) servers on the local network.	It is open-source software; visit the following site for downloads: http://us3.samba.org/samba/
Fping	This is a utility similar to ping used to perform parallel network discovery.	For this open-source software, visit: http://www.fping.com/
Fragroute	This intercepts, modifies and rewrites egress traffic destined for a specified host, implementing several intrusion detection system (IDS) evasion techniques.	This is another open-source material; visit: http://www.monkey.org/~dugsong/fragroute/
Fragtest	This tests the IP fragment reassembly behavior of the Transmission Control Protocol (TCP) stack on a target. It intercepts, modifies and rewrites egress traffic destined for a specified host, implementing most of the attacks.	For more details on this open-source software, visit: http://www.monkey.org/~dugsong/fragroute/
Hackbot	This is a host exploration tool, simple vulnerability scanner and banner logger.	Another open-source software, whose details can be found at: http://freshmeat.net/projects/hackbot/
Hmap	This is used to obtain detailed fingerprinting of web servers to identify vendor, version, patch level, including modules and much more. *Hmap* is a web server fingerprinting tool.	Details of this open-source software can be found at: http://ujeni.murkyroc.com/hmap/
Hping	This is a TCP/IP packet assembler and analyzer. It can perform firewall ruleset testing, port scanning, network type of service/quality-of-service (TOS/QOS) testing, maximum transmission unit (MTU) discovery, alternate-protocol traceroute, TCP stack auditing, and much more. Using *hping* you can do the following: • Firewall testing; • advanced port scanning; • network testing, using different protocols, TOS, fragmentation; • manual path MTU discovery; • advanced traceroute, under all the supported protocols; • remote OS fingerprinting; • remote uptime guessing; • TCP/IP stacks auditing; • hping can also be useful to students that are learning TCP/IP.	This is open-source software. For additional technical details, visit: http://www.hping.org/

(*Continued*)

Table 2.2 | (Continued)

Name of the Tool	*Brief Description*	*Remarks*
	Hping works on the following Unix-like systems: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.	
Httping	This is similar to "ping," that is, hping, but for HTTP requests. It shows how long a URL will take to connect, send a request, and receive a reply.	This is open-source software. For additional technical details, visit: http://www.vanheusden.com/httping/
Hunt	This is a tool for exploiting well-known weaknesses in the TCP/IP protocol suite.	This is also open-source software. For additional technical details, visit: http://lin.fsid.cvut.cz/~kra/index.html
Libwhisker	This is an application library designed to assist in scannabilities.	Details of this open-source software can be found at: http://www.wiretrip.net/rfp/lw.asp
Mailsnarf	This is a network auditing tool to capture SMTing for CGI/web vulnerP and POP3 E-Mail traffic (including message headers, bodies, and attachments) on a local subnet.	For this open-source software, you can visit: http://monkey.org/~dugsong/dsniff/
Msgsnarf	This is a network auditing tool to capture instant message (Yahoo, MSN, ICQ, iChat, AIM, and many more) traffic on a local subnet.	Same as above
NBTScan	This is a utility for scanning networks for NetBIOS information. It reports IP address, NetBIOS name, logged-in username, and MAC address.	Details of this open-source material can be found at: http://www.inetcat.org/software/nbtscan.html
Nessus	This is a powerful, fast, and modular security scanner that tests for many thousands of vulnerabilities. ControlScans' system can also be used to create custom Nessus reports.	To know more about this open-source utility, visit: http://www.nessus.org/
Netcat	This is a utility to read and write custom TCP/User Datagram Protocol (UDP) data packets across a network connection for network debugging or exploration.	Explore more details of this open-source utility at: http://www.atstake.com/research/tools/network_utilities/
Nikto	This is a web server vulnerability scanner that tests over 2,600 potentially dangerous files/CGIs on over 625 types of servers. This tool also performs comprehensive tests against web servers for multiple items and version-specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).	Nikto is an open-source web server scanner; visit the following site for more detail: http://www.cirt.net/code/nikto.shtml
Nmap	This is a port scanner, operating system fingerprinter, service/version identifier, and much more. Nmap is designed to rapidly scan large networks.	For details of this open-source software, visit: http://insecure.org/nmap/

(Continued)

Table 2.2 | (Continued)

Name of the Tool	*Brief Description*	*Remarks*
Pathchar	This is a network tool for inferring the characteristics of Internet paths, including Layer 3 hops, bandwidth capacity, and autonomous system information.	For further details, visit: http://ee.lbl.gov/
Ping	This is a standard network utility to send ICMP packets to a target host.	For further details, visit: http://www.controlscan.com/auditingtools.html#
ScanSSH	This supports scanning a list of addresses and networks for open proxies, SSH Protocol servers, and Web and SMTP servers. Where possible, it displays the version number of the running services. ScanSSH supports the following features: • Variable scanning speed: per default, ScanSSH sends out 100 probes per second; • open proxy detection; • random sampling: it is possible to randomly sample hosts on the Internet.	The first version of the ScanSSH Protocol scanner was released in September 2000. For further details and downloading the current version, visit: http://www.monkey.org/~provos/scanssh/
SMBclient	This helps a client to talk to an SMB (Samba, Windows File Sharing) server. Operations include getting files from the server, putting files on the server, retrieving directory information, and much more. It is an open-source/free software suite that has, since 1992, provided file and print services to all types of SMB/common Internet file system (CIFS) clients, including the numerous versions of Microsoft Windows operating systems. Samba is freely available under the GNU General Public License.	
SMTPscan	This is a tool to determine the type and version of a remote Simple Mail Transfer Protocol (SMTP) mail server based on active probing and analyzing error codes of the target SMTP server.	For further details, visit: http://www.greyhats.org/outils/smtpscan/
TCPdump	It is a network tool for the protocol packet capture and dumper program.	For further details, visit: http://ee.lbl.gov/
TCPreplay	This is a utility to read captured TCPdump/pcap data and "replay" it back onto the network at arbitrary speeds. TCPreplay is a suite of licensed tools written by Aaron Turner for Unix operating systems. It gives you the ability to use previously captured traffic to test a variety of network devices. It allows you to classify traffic as client or server; rewrite open system interconnection (OSI) Layers 2, 3 and 4 headers; and finally replay the traffic back onto the network and through other	TCPreplay suite includes the following tools: • TCPprep: It is a multi-pass packet capture (pcap) file preprocessor which determines packets as client or server and creates cache files used by TCPreplay and TCPrewrite. • TCPrewrite: It is a pcap file editor which rewrites TCP/IP and Layer 2 packet headers.

(Continued)

Table 2.2 | *(Continued)*

Name of the Tool	*Brief Description*	*Remarks*
	devices such as switches, routers, firewalls, network-based intrusion detection system (NIDS), and intrusion prevention system (IPS). TCPreplay supports both single and dual NIC modes for testing both sniffing and inline devices. TCPreplay is used by numerous firewalls, IDS, IPS, and other networking vendors, enterprises, universities, laboratories, and open-source projects.	• TCPreplay: It replays pcap files at arbitrary speeds onto the network. • TCPreplay-edit: It replays and edits pcap files at arbitrary speeds onto the network. • TCPbridge: It bridges two network segments with the power of TCPrewrite. For further details, visit: http://tcpreplay.synfin.net/trac/
THC-Amap	This is a scanner to remotely fingerprint and identify network applications and services.	For further details, visit: http://freeworld.thc.org/releases.php
Traceroute	This is a standard network utility to trace the logical path to a target host by sending ICMP or UDP packets with incrementing tunneled transport layer security (TTLs).	For further details, visit: http://ee.lbl.gov/
URLsnarf	This is a network auditing tool to capture HTTP traffic on a local subnet.	For further details, visit: http://monkey.org/~dugsong/dsniff/
XProbe2	This is a tool employing several techniques to actively fingerprint the operating system of a target host.	For further details, visit: http://www.sys-security.com/html/projects/X.html

Note: IP is Internet Protocol here.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Table 35.2), Wiley India.

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.

Box 2.5 Ports and Ports Scanning

A port is an interface on a computer to which one can connect a device. TCP/IP Protocol suite made out of the two protocols, TCP and UDP, is used universally to communicate on the Internet. Each of these has ports 0 through 65536 (i.e., the range is from 2^0 to 2^{16} for binary address calculation). The port numbers are divided into three ranges:

Box 2.5 Ports and Ports . . . (*Continued*)

1. Well-known ports (from 0 to 1023);
2. registered ports;
3. dynamic and/or private ports.

The list of well-known port numbers and short description about the services offered by each of these are provided in Table 2.3.

Table 2.3 | Well-known port numbers

Port Number	*Port Description*	*Port Number*	*Port Description*
1	TCP port service multiplexer (TCPMUX)	118	Structured query language (SQL) services
5	Remote job entry (RJE)	119	NNTP (Newsgroup)
7	ECHO	137	NetBIOS name service
18	Message Send Protocol (MSP)	139	NetBIOS datagram service
20	FTP – Data	143	Internet Message Access Protocol (IMAP)
21	FTP – Control	150	NetBIOS session service
22	Secure shell (SSH) remote log-in protocol	156	SQL server
23	Telnet	161	Simple Network Management Protocol (SNMP)
25	Simple Mail Transfer Protocol (SMTP)	179	Border Gateway Protocol (BGP)
29	MSG ICP	190	Gateway Access Control Protocol (GACP)
37	Time	194	Internet relay chat (IRC)
42	Nameserv (host name server)	197	Directory location service (DLS)
43	WHOIS	389	Lightweight Directory Access Protocol (LDAP)
49	Log-in (log-in host protocol)	396	Novell netware over IP
53	Domain name system (DNS)	443	Secure Hypertext Transfer Protocol (S-HTTP)
69	Trivial File Transfer Protocol (TFTP)	444	Simple Network Paging Protocol (SNPP)
70	Gopher services	445	Microsoft-DS
79	Finger	458	Apple quick time
80	HTTP	546	DHCP client
103	X.400 Standard	547	DHCP server
108	SNA gateway access server	563	SNEWS
109	POP2	569	MSN
110	POP3	1080	Socks
115	Simple File Transfer Protocol (SFTP)		

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Chapter 35, p. 774), Wiley India.

Box 2.5 Ports and Ports . . . (*Continued*)

There are some well-known IP ports (0–999) that require scanning owing to vulnerabilities known about them. In TCP/IP and UDP networks, a port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are preassigned to them by the Internet Assigned Numbers Authority (IANA), an organization working under the auspices of the Internet Architecture Board (IAB), responsible for assigning new Internet-wide IP addresses.

Table 2.3 lists the well-known ports along with the services run on them. Although public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws, and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Port Scanning

A "port" is a place where information goes into and out of a computer and so, with port scanning, one can identify open doors to a computer. Ports are basically entry/exit points that any computer has, to be able to communicate with external machines. Each computer is enabled with three or more external ports. These are the ports used by the computer to communicate with the other computers, printer, modem, mouse, video game, scanner, and other peripherals. The important characteristic about these "external ports" is that they are indeed external and visible to the naked eye. Port scanning is often one of the first things an attacker will do when attempting to penetrate a particular computer. Tools such as Nmap (Table 2.2 lists a few vulnerability assessment tools) offer an automated mechanism for an attacker to not only scan the system to find out what ports are "open" (meaning being used), but also help to identify what operating system (OS) is being used by the system.

Port scanning is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked. Port scanning is an act of systematically scanning a computer's ports. In technological terms, "port scanning" refers to the act of using various open-ended technologies, tools, and commands to be able to communicate with another remote computer system or network, in a stealth mode, without being apparent, and be able to obtain certain sensitive information about the functions of system and the properties of the hardware and the software being used by the remote systems.

In "portscan," a host scans for listening ports on a single target host. In "portsweep," a host scans multiple hosts for a specific listening port. The result of a scan on a port is usually generalized into one of the following three categories:

1. **Open or accepted:** The host sent a reply indicating that a service is listening on the port.
2. **Closed or not listening:** The host sent a reply indicating that connections will be denied to the port.
3. **Filtered or blocked:** There was no reply from the host.

TCP/IP suite of protocols is used to communicate with other computers for specific message formats. Most of these protocols are tied to specific port numbers that are used to transfer particular message formats as data. Security administrators as well as attackers have a special eye on few well-known ports and protocols associated with it.

1. Ports 20 and 21 – File Transfer Protocols (FTP) – are used for uploading and downloading of information.
2. Port 25 – Simple Mail Transfer Protocol (SMTP) – is used for sending/receiving E-Mails.
3. Port 23 – Telnet Protocol – is used to connect directly to a remote host and Internet control message.
4. Port 80 – It is used for Hypertext Transfer Protocol (HTTP).
5. Internet Control Message Protocol (ICMP) – It does not have a port abstraction and is used for checking network errors, for example, ping.

Box 2.5 Ports and Ports . . . (*Continued*)

Open ports present two vulnerabilities of which administrators must be wary:

1. Vulnerabilities associated with the program that is delivering the service.
2. Vulnerabilities associated with the OS that is running on the host.

Closed ports present only the latter of the two vulnerabilities that open ports do. Blocked ports do not present any reasonable vulnerabilities. There is also the possibility that there are no known vulnerabilities in either the software (program) or the OS at the given time.[2]

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step is to identify:

1. The valid user accounts or groups;
2. network resources and/or shared resources;
3. OS and different applications that are running on the OS.

Most of the tools listed in Table 2.2 are used for computer network scanning as well.

Usually, most of the attackers consume 90% of the time in scanning, scrutinizing and gathering information on a target and 10% of the time in launching the attack.

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 (we will address it in Chapter 4);
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.

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

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 office. We just need to check a couple of things. What is your username?

Mr. Joshi: Username is "pjoshi." None of my files 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 files are there.

Mr. Joshi: Thank you. Bye.

Caller: Bye and have a nice day.

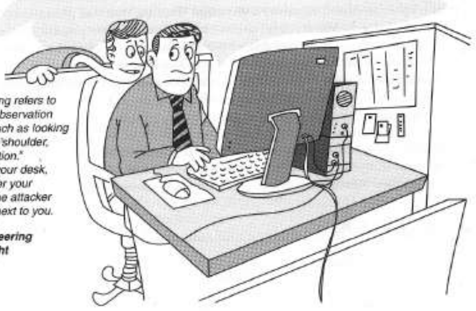
people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble. The sign of truly successful social engineers is that they receive information without any suspicion. A simple example is calling a user and pretending to be someone from the service 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).

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" (e.g., posing oneself as an employee of the same organization) 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.



Shoulder surfing refers to "using direct observation techniques, such as looking over someone'shoulder, to get information." Look around your desk, when you enter your passwords. The attacker may be right next to you.

Social Engineering may start right at work!!!

Figure 2.3 | Social engineering – shoulder surfing.

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 (Fig. 2.3).
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."

In practice, *dumpstering* is more like fishing around than diving in. Usually, people dumpster dive to search the items, to reclaim those, which have been disposed of but can still be put to further use, for example, E-Waste, furniture, clothes, etc. The term "dumpster diving" may have originated from the notional image of someone leaping into large rubbish bins, the best known of which are produced under the name "dumpster." "Scavenging" is equivalent of "dumpster diving," in the digital world. It is a form in which discarded articles and information are scavenged in an attempt to obtain/recover advantageous data, if it is possible to do so. Consider, for example, going through someone's trash to recover documentation of his/her critical data [e.g., social security number (SSN) in the US, PAN number in India, credit card identity (ID) numbers, etc.]. According to a definition in the glossary of terms for the convoluted terminology of information warfare, "scavenging" means "searching through object residue (e.g., discarded disks, tapes, or paper) to acquire sensitive data without authorization."

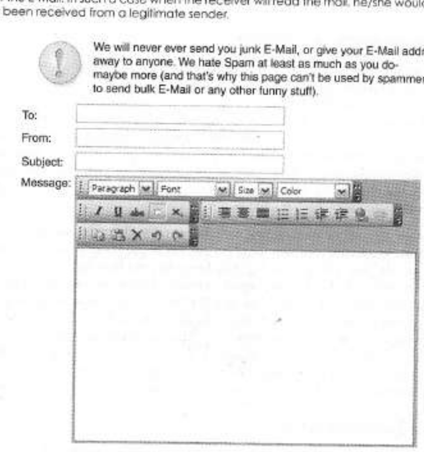
Computer-Based Social Engineering

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 numerous users in such that the user finds it as a legitimate mail. This activity is also called "Phishing" (we shall address it in Chapter 5). It is an attempt to entice the Internet users (netizens) to reveal their sensitive personal information, such as usernames, passwords and credit card details by impersonating as a trustworthy and legitimate organization and/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 lures 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.

Box 2.7 Fake E-Mails

Free websites are available to send fake E-Mails. From Fig. 2.4, one can notice that "To" in the text box is a blank space. Hence, anyone can fill any E-Mail address with the intention of fooling the receiver of the E-Mail. In such a case when the receiver will read the mail, he/she would think that the E-Mail has been received from a legitimate sender.



We will never ever send you junk E-Mail, or give your E-Mail address away to anyone. We hate Spam at least as much as you do-maybe more (and that's why this page can't be used by spammers to send bulk E-Mail or any other funny stuff).

To:

From:

Subject:

Message:

Figure 2.4 Sending fake E-Mails.
Source: http://deadfake.com/Send.aspx (2 April 2009).

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. We will address keylogger, viruses, Trojans, and worms in Chapter 4.
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.

Social engineering indeed is a serious concern as revealed by the following past statistics on numbers:

1. As per Microsoft Corporation recent (October 2007) research, there is an increase in the number of security attacks designed to steal personal information (PI) or the instances of tricking people to provide it through social engineering. According to an FBI survey, on average 41% of security-related losses are the direct result of employees stealing information from their companies. The average cost per internal incident was US$ 1.8 million.
2. The Federal Trade Commission (FTC) report of 2005 shows that "more than one million consumer fraud and ID theft complaints have been filed with federal, state, and local law enforcement agencies and private organizations" (2005, Consumer Fraud and Identity Theft section, para 1; we will discuss ID Theft in Chapter 5).
3. According to a 2003 survey [released on 2 April 2006 by the United States Department of Justice (Identity Theft Hits Three Percent, para 1)], "An estimated 3.6 million – or 3.1% – of American households became victims of ID theft in 2004." This means that now, more than ever, individuals are at a high risk of having their PI stolen and used by criminals for their own personal gain.

Typically, many organizations have information valuable enough to justify expensive protection mechanisms/security mechanisms. Critical information may include patient records in the medical and healthcare domain [known as protected health information (PHI)], corporate financial data, electronic funds transfers, access to financial assets in the financial services domain, and PI about clients or employees. Compromising critical information can have serious consequences, including the loss of customers, criminal actions being brought against corporate executives, civil law cases against the organization, loss of funds, loss of trust in the organization, and collapse of the organization. To respond to the threats, organizations implement InfoSec plans to establish control of information assets. However, "social engineers" try to device a way to work their way around this to obtain the valuable information, an illicit act on ethical grounds.

Social engineering succeeds by exploiting the trust of the victim. Hence, continuous training/awareness sessions about such attacks are one of the effective countermeasures. Strict policies about service desk staff never asking for personally identifying information, such as username and passwords, over the phone or in person can also educate potential victims and recognize a social engineering attempt.

Social engineering and dumpster diving are also considered passive information-gathering methods.

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.[3]

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 (see Table 2.1). 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.

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. The letters may have the tone of loving, threatening or can be sexually explicit. The 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.

Box 2.8 Cyberbullying

The National Crime Prevention Council defines 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 defines 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).

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 (refer to Chapter 5).

2.4.4 Real-Life Incident of Cyberstalking

Case Study

The Indian police have registered first case of cyberstalking in Delhi[5] – 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.

2.5 Cybercafe and Cybercrimes

In February 2009, Nielsen survey[6] 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*, (we will discuss it in Chapter 4) 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 peeping (i.e., 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[7] (it is discussed in great detail in Chapter 6) does not define cybercafes and interprets cybercafes as "network service providers" referred to under the erstwhile Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network. The concept of "due diligence" was interpreted from the various provisions in cybercafe regulations where available or normal responsibilities were expected from network service providers.

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 – techniques used for this are discussed in Chapter 4. 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 (this is an eye-opener after going through the following observations:

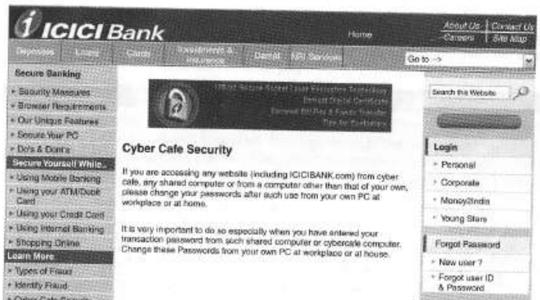
1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Although such intent is noble, this software happens to help cybercriminals hoodwink the investigating agencies. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button.[8] 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 (Phishing attacks are explained in Chapter 5) 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 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.

> There is an expectation that the Indian Computer Emergency Team referred to under Section 70B of ITA 2008 may itself be designated as the agency of the Central Government with a national jurisdiction and (Computer Emergency Response Team) CERT, and may itself be stepping into the shoes of the Indian Computer Emergency Team.[7,8]

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

1. **Always logout:** While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or "sign out" before leaving the system. Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. However, do not save your login information through options that allow automatic login. Disable such options before logon.
2. **Stay with the computer:** While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.
3. **Clear history and temporary files:** Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files. Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used. Therefore, before you begin browsing, do the following in case of the browser Internet Explorer:
   - Go to *Tools* → *Internet options* → click the *Content* tab → click *AutoComplete*. If the checkboxes for passwords are selected, deselect them. Click *OK* twice.
   - After you have finished browsing, you should clear the history and temporary Internet files folders. For this, go to *Tools* → *Internet options* again → click the *General* tab → go to *Temporary Internet Files* → click *Delete Files* and then click *Delete Cookies*.
   - Then, under history, click clear history. Wait for the process to finish before leaving the computer.
4. **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.
5. **Avoid online financial transactions:** Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.
6. **Change passwords:** The screenshot displayed in Fig. 2.5 by ICICI Bank about changing the bank account/transaction passwords is the best practice to be followed.[9]
7. **Virtual keyboard:** Nowadays almost every bank has provided the virtual keyboard on their website. The advantages of utilizing virtual keyboard and its functions are displayed in the screenshot shown in Fig. 2.6.[10]
8. **Security warnings:** One should take utmost care while accessing the websites of any banks/financial institution. The screenshot in Fig. 2.7 displays security warnings very clearly (marked in bold rectangle), and should be followed while accessing these financial accounts from cybercafe.

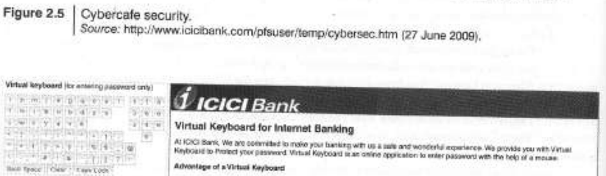


Cyber Cafe Security

If you are accessing any website (including ICICIBANK.com) from cyber cafe, any shared computer or from a computer other than that of your own, please change your passwords after such use from your own PC at workplace or at home.

It is very important to do so especially when you have entered your transaction password from such shared computer or cybercafe computer. Change these Passwords from your own PC at workplace or at house.

Figure 2.5 | Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).



Virtual Keyboard for Internet Banking

At ICICI Bank, We are committed to make your banking with us a safe and wonderful experience. We provide you with Virtual Keyboard to Protect your password. Virtual Keyboard is an online application to enter password with the help of a mouse.

Advantage of a Virtual Keyboard

The Virtual Keyboard is designed to protect your password form malicious "Spyware" and "Trojan Programs". Use of Virtual keyboard will reduce the risk of password theft.

Process To Use Virtual Keyboard

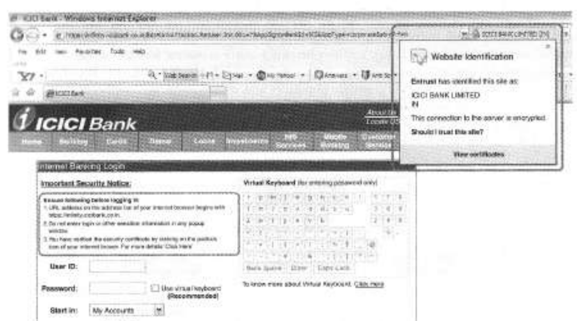
Steps to use Virtual keyboard are as follows:

Enter Login ID using Physical Keyboard.
- Select the check box 'Use Virtual Keyboard'.
- Use the Virtual Keyboard to the login password.
- Once you have entered your password, click"Log-in".
-

Functions of different keys on the Virtual Keyboard

Caps Lock: This key can be used to enter upper case if the password consist of capital letters.
Back Space: This key will clear the last character entered in the password field.
Clear: This key will clear all characters entered in the password field by Virtual keyboard.
Tab: This key is visible only for change or forced change password. field by Virtual keyboard.This key can be used to enter values in the next field.

Figure 2.6 | Virtual keyboard.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).



Website Identification

Entrust has identified this site as:
ICICI BANK LIMITED
IN

This connection to the server is encrypted.

Should I trust this site?

View certificates

Important Security Notice:

Ensure following before logging in
1. URL address on the address bar of your internet browser begins with https://infinity.icicibank.co.in.
2. Do not enter login or other sensitive information in any popup window.
3. You have verified the security certificate by clicking on the padlock icon of your internet browser. For more details 'Click Here'

User ID:

Password: □ Use virtual keyboard (Recommended)

Start in: My Accounts

Log-in

To know more about Virtual Keyboard. Click Here

New users? Register here.
Report a suspicious E-Mail
Forgot password?
Cyber Cafe Security
Trouble logging in?
About E-Mail fraud

DIGITAL SECURITY: infinity.icicibank.co.in has been verified by Entrust. The communication of your private information from any address beginning with "https" is encrypted and secured using SSL.

Customer Service | Internet Banking FAQ'S | Internet Banking Demo | Privacy | Online Security | Terms and Conditions | Disclaimer

Figure 2.7 | Security warnings.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Individual should take care while accessing computers in public places, that is, accessing the Internet in public places such as hotels, libraries and holiday resorts. Moreover, one should not forget that whatever is applicable for cybercafes (i.e., from information security perspective) is also true in the case of all other public places where the Internet is made available (refer to Appendix J in CD). Hence, one should follow all tips about safety and security while operating the systems from these facilities.

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.[11]

In simple terms, a Bot is simply an automated computer program (explained in Box 1.2, Chapter 1). One can gain the control of your computer by infecting them with a virus or other Malicious Code that gives the access. Your 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 (the term is discussed in detail in Chapter 4).

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*" (explained in Chapter 1, Fig. 1.3) have become a source of income for entire groups of cybercriminals. 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. Obfuscation and 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.

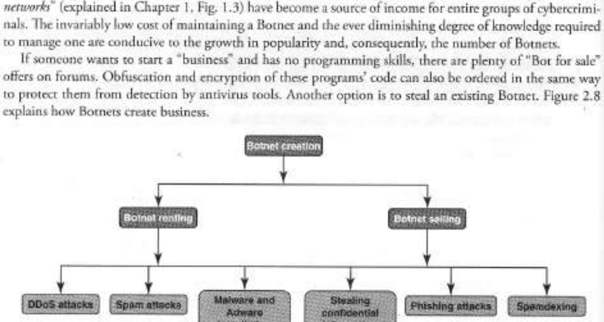

Botnet creation
Botnet renting
Botnet selling
DDoS attacks
Spam attacks
Malware and Adware installation
Stealing confidential information
Phishing attacks
Spamdexing
Selling – credit card and bank account details
Selling personal identity information
Selling Internet services and shops account

Figure 2.8 | Botnets are used for gainful purposes.

Box 2.9 Explanation for Technical Terms used in Fig. 2.8

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 classified as Adware.

Spam: It means unsolicited or undesired E-Mail messages (this is discussed in detail in Chapter 5).

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 (this is discussed in details in Chapter 4).

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: [12,13]

1. **Use antivirus and anti-Spyware software and keep it up-to-date:** It is important to remove and/or quarantine the viruses. The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.
2. **Set the OS to download and install security patches automatically:** OS companies issue the security patches for flaws that are found in these systems.
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. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria. A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-à-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.
4. **Disconnect from the Internet when you are away from your computer:** Attackers cannot get into the system when the system is disconnected from the Internet. Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.
5. **Downloading the freeware only from websites that are known and trustworthy:** It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars, etc. However, one should remember that many free software(s) contain other software, which may include Spyware.
6. **Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send:** If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet. This is not foolproof; many spammers have learned to hide their unauthorized access.
7. **Take an immediate action if your system is infected:** If your system is found to be infected by a virus, disconnect it from the Internet immediately. Then scan the entire system with fully updated antivirus and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities. There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

2.7 Attack Vector

An "attack vector" is a path or means by 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.[14]

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.

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 fix) 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 fix to users of such software. If the vulnerability is not particularly dangerous, software vendors prefer to hold until multiple updates (i.e., security fixes 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.

Source: http://en.wikipedia.org/wiki/Zero_day_attack (9 October 2009).

The most common malicious payloads are viruses (which can function as their own attack vectors), Trojan Horses, worms, and Spyware (refer to Chapter 4). 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. However, in more general usage, the payload is the bits that get delivered to the end-user at the destination.[15,16]

The attack vectors described here are how most of them are launched.[16,18]

1. **Attack by E-Mail**: The hostile 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, hoaxes, 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 and hoaxes 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, 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.
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. Next they begin scanning the Internet from the computer they have just infected, and start looking for other computers to infect. If the worm is successful, it propagates rapidly. The worm owner soon has thousands of "zombie" computers to use for more mischief.
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 file-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 on the sly. Spyware is the most common form of foistware. Foistware is quasi-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.

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 makes it easier for cybercriminals to attack these systems.

Cloud computing is Internet ("cloud")-based development and use of computer technology ("computing").[19] 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[20]:

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. A public cloud sells services to anyone on the Internet (see Table 2.4 for cloud computing service providers). A private cloud is like a proprietary network or a data center that supplies the hosted services to a limited number of people. When a service provider uses public cloud resources to create a private cloud, the result is called a "virtual private cloud." The goal of cloud computing is to provide easy, scalable access to the computing resources and IT services.

Table 2.4 | Cloud computing service providers

Sr. No.	*Service Providers*	*Weblink*
1.	**Amazon:** It offers flexible, simple, and easy computing environment in the cloud that allows development of applications.	http://aws.amazon.com/ec2/
2.	**3Tera:** It offers AppLogic grid OS that enables infrastructure solutions according to the changing needs of business.	http://www.3tera.com/
3.	**Force.com:** It allows building of core business applications like enterprise resource planning (ERP), human resource management (HRM), and supply chain management (SCM).	http://www.salesforce.com/platform/
4.	**Appistry-Cloud Computing Middleware:** It allows easily scalable cloud computing for a wide variety of applications and services for both public and private clouds.	http://www.appistry.com/
5.	**Microsoft Live Mesh:** This cloud setup synchronizes the files with the all users' devices like laptop, Mac, mobile phone, or others and allows to access the files from any device as well as enables sharing of files.	https://www.mesh.com/Welcome/default.aspx
6.	**AppNexus:** This helps a user to launch several operating systems, run a variety of applications, load balance these applications, and store huge amount of secure data.	http://www.appnexus.com/
7.	**Flexiscale:** It is self-service through control panel or API – features full self-service – start/stop/delete, change memory/CPU/storage/IPs of virtual dedicated servers.	http://www.flexiscale.com/
8.	**GoogleApp Engine:** This is a free setup that allows the users to run their web application on Google infrastructure.	http://www.google.com/apps/intl/en/business/index.html
9.	**GoGrid:** It offers unique multiserver control panel that enables the user to deploy and manage load-balanced cloud servers.	http://www.gogrid.com/
10.	**Terremark Enterprise Cloud:** It provides the power to the user for computing resources for user's mission-critical applications.	http://www.terremark.com/services/cloudcomputing/theenterprisecloud.aspx

(Continued)

Source: http://blog.taragana.com/index.php/archive/top-10-cloud-computing-service-provider/ (9 October 2009).

Although cloud computing is an emerging field, the idea has been evolved over few years. It is called cloud computing because the data and applications exist on a "cloud" of Web servers.

2.8.2 Types of Services

Services provided by cloud computing are as follows[19]:

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.
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. See Table 2.5 to understand major areas of concerns in cloud computing domain.

Table 2.5 | Risks associated with cloud computing environment

Sr. No.	*Area*	*What is the Risk?*	*How to Remediate the Risk?*
1.	Elevated user access	Any data processed outside the organization brings with it an inherent level of risk, as outsourced services may bypass the physical, logical, and personnel controls and will have elevated user access to such data.	Customer should obtain as much information as he/she can about the service provider who will be managing the data and scrutinizing vendor's monitoring mechanism about hiring and oversight of privileged administrators, and IT controls over the access privileges.
2.	Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments. This can result into non-compliance with various standards/laws like the US government's Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley; the European Union's Data Protection Directive or the credit card industry's Payment Card Industry Data Security Standard (PCI DSS).	The organization is entirely responsible for the security and integrity of their own data, even when it is held by a service provider. Hence, organization should force cloud computing service providers to undergo external audits and/or security certifications and submit the report on periodic basis.
3.	Location of the data	The organizations that are obtaining cloud computing services may not be aware about where the data is hosted and may not even know in which country it is hosted.	Organizations should ensure that the service provider is committed to obey local privacy requirements on behalf of the organization to store and process the data in the specific jurisdictions.
4.	Segregation of data	As the data will be stored under stored environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data are also stored under the same server.	Organization should be aware of the arrangements made by the service provider about segregation of the data. In case of encryption mechanism, the service provider should display encryption schemes and testing of the mechanism by the experts.
5.	Recovery of the data	Business continuity in case of any disaster – availability of the services and data without any disruption. Application environment and IT infrastructure across multiple sites are vulnerable to a total failure.	Organization should ensure the enforcement of contractual liability over the service provider about complete restoration of data within stipulated timeframe. Organization should also be aware of Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) established by the service provider.
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.	Organization should enforce the contractual liability toward providing security violation logs at frequent intervals.
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.	Organization should ensure getting their data in case of such major events.

Source: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 (9 October 2009).

The risk areas identified in Table 2.5 are considered to be key obstacles to adoption of cloud computing and making it an area of active research across the globe.

Summary

In this chapter we have discussed how technology is used in a different way for conducting illegal activities against a person, property, and/or organizations including governments. Considerable amount of time is spent in gathering information about a target. Therefore, one should have adequate knowledge about the technology to use, the different tools and techniques. Public networks and cybercafes are used to hide the ID for information gathering as well as launching attacks and hence it becomes important to take utmost care while operating/surfing through such facilities. People are the weakest link in the security domain and, hence, they get either exploited/deceived to obtain the required information; thus, this is called social engineering. Cyberstalking is another way through which criminals interact with victims directly, avoiding face-to-face conversation. Criminals do this either for harassing and/or threatening behavior or to get the information from the victim. The Internet has become an integral part of the lifestyle nowadays and IT is found to be pervasive – the result is cloud computing; however, we should also be aware of threats inducing from such technologies like Botnets and attack vectors. Every technology has some limitations and attackers having good amount of knowledge will always try to exploit it.

Review Questions

1. How are cybercrimes classified? Explain with examples.
2. Explain the difference between passive and active attacks. Provide examples.
3. What is social engineering?
4. What is cyberstalking? As per your understanding is it a crime under the Indian IT Act?
5. Explain how Botnets can be used as a fuel to cybercrime.
6. What are the different attacks launched with attack vector. Explain.
7. Explain cloud computing and cybercrime.

References

[1] To know more on patriot hacking, visit: http://en.wikipedia.org/wiki/Patriot_hacking (25 June 2009).

[2] To know more on port scanner, visit: http://en.wikipedia.org/wiki/Port_scanner (10 February 2010).

[3] To know more on cyberstalking, visit: http://en.wikipedia.org/wiki/Cyberstalking (2 April 2009).

[4] To know more on cyberbullying, visit: http://en.wikipedia.org/wiki/Cyber-bullying (2 April 2009).

[5] To know more on cyberstalking, visit: http://cyberlaws.net/cyberindia/2CYBER27.htm (2 April 2009).

[6] To know more on cybercafe, visit: http://www.business-standard.com/india/news/cyber-cafe-audience-captive-power/351936/ (25 June 2009).

[7] To know more on cybercafe, visit: http://www.merinews.com/catFull.jsp?articleID=155371 (25 June 2009).

[8] To know more on cybercafe, visit: http://punekar.in/site/2009/02/04/city-cyber-cafes-install-deep-freeze-software-for-security/ (27 June 2009).