

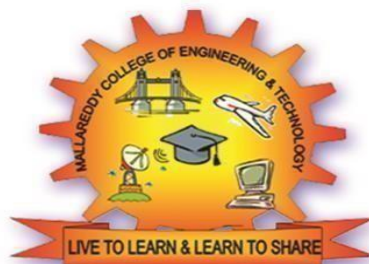
DIGITAL NOTES
ON
FUNDAMENTALS OF CYBER
SECURITY
(R20A6214)

Prepared by

Ms.Anitha Patibandla

Associate Professor, Dept. of ECE

B.TECH III YEAR – II SEM (R20)



(2023-2024)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

(Affiliated to JNTUH, Hyderabad, Approved by AICTE - Accredited by NBA & NAAC – 'A' Grade - ISO 9001:2015 Certified)

Maisammaguda, Dhulapally (Post Via. Hakimpet), Secunderabad – 500100, Telangana State, India

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

B.Tech -III Year-I Sem (ECE & ANE)

L/T/P/C

3/-/3

(R20A6214) FUNDAMENTALS OF CYBER SECURITY

COURSE OBJECTIVES

1. To understand the basic concepts of cyber-Security.
2. To study different attacks in cyber-crimes.
3. To understand different tools and methods used in cyber-crime.
4. To study cyber security challenges and implications.
5. To know about Cyber Security Organizational Issues, Policies.

UNIT I-Introduction to Cyber Security:

Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defense, Security Models, risk management, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy

UNIT II-Cyber Offenses:

How Criminals Plan Them: Introduction, How Criminals plan the Attacks, Social Engineering, Cyber stalking, Cyber cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.

UNIT III-Cybercrime: Mobile and Wireless Devices:

Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

UNIT IV-Types of Attacks and Cybercrime:

Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horse and Backdoors, Steganography, DoS and DDoS attacks, SQL Injection, Buffer Overflow.

UNIT V-Cyber Security Organizational Policies, Risk and Challenges:

Organizational Implications. Introduction, Cost of Cybercrimes and IPR issues, Web threats for Organizations, Security and Privacy Implications, Social media marketing: Security Risks and Perils for Organizations, Social Computing and the associated challenges for Organizations.

TEXT BOOKS:

1. **Cyber Security:** *Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Nina Godbole and Sunil Belapure, Wiley INDIA.

REFERENCE BOOKS:

1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
2. Introduction to Cyber Security , Chwan-Hwa(john) Wu, J. David Irwin. CRC Press T&F Group

COURSE OUTCOMES:

Student will be able to

- Understand basic concepts of Cyber Crimes.
- Ability to identify the attacks in Cyber Crimes
- Able to specify the suitable methods used in Cyber Crime
- Ability to face cyber security challenges
- Understand Cyber Security

UNIT-I

Introduction to Cyber Security

Cyber Security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system.

OR

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.

It is made up of two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.
- Whereas security related to the protection which includes systems security, network security and application and information security.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.
- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.

- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack.

But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Cyber security Fundamentals – Confidentiality:

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

- Backing up data to external drives

- Implementing firewalls
- Having backup power supplies
- Data redundancy

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories:

- 1) **Web-based attacks**
- 2) **System-based attacks**

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

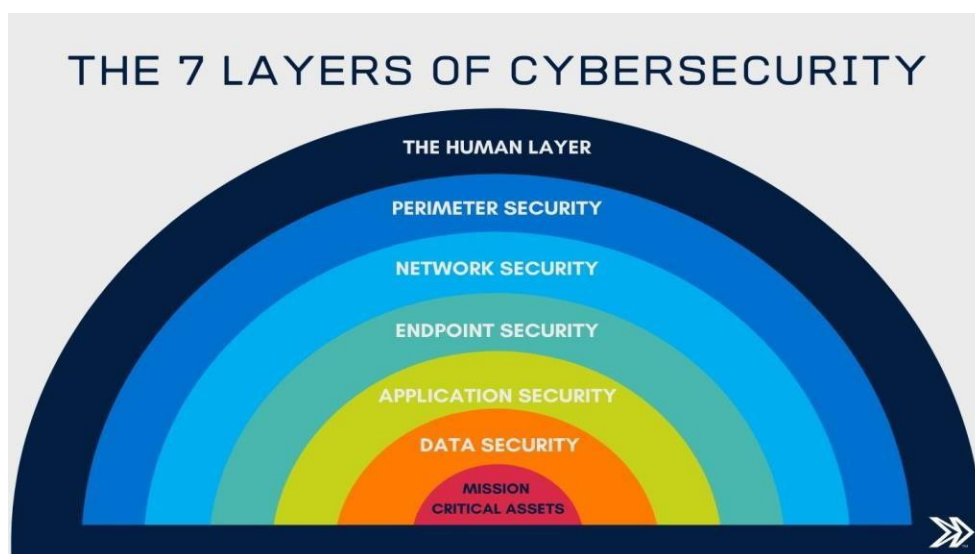
It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receivespecific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.



The 7 layers of cyber security should centre on the mission critical assets you are seeking to protect.

- 1: Mission Critical Assets – This is the data you need to protect
- 2: Data Security – Data security controls protect the storage and transfer of data.
- 3: Application Security – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
- 4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.
- 5: Network Security – Network security controls protect an organization's network and prevent unauthorized access of the network.
- 6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.
- 7: The Human Layer – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Vulnerability, threat, Harmful acts

As the recent epidemic of data breaches illustrates, no system is immune to attacks. Any company that manages, transmits, stores, or otherwise handles data has to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close up security holes as quickly as possible.

Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

Examples of common types of security threats include **phishing attacks** that result in the installation of **malware** that infects your data, failure of a staff member to follow data protection protocols that cause a **data breach**, or even a tornado that takes down your company's data headquarters, disrupting access.

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

Types of vulnerabilities in network security include but are not limited to SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a non-encrypted plain text format.

When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a risk.

SECURITY VULNERABILITIES, THREATS AND ATTACKS –

Categories of vulnerabilities

- Corrupted (Loss of integrity)
- Leaky (Loss of confidentiality)
- Unavailable or very slow (Loss of availability)

– Threats represent potential security harm to an asset when vulnerabilities are exploited

- Attacks are threats that have been carried out

- Passive – Make use of information from the system without affecting system resources
- Active – Alter system resources or affect operation
- Insider – Initiated by an entity inside the organization
- Outsider – Initiated from outside the perimeter

Internet Governance – Challenges and Constraints

- The e-Governance or electronic governance means utilization of ICT (Information and Communications Technology) to carry out the functions and achieve the results of the governance. Governance has become very complex and the increasing expectations from the Government are the reasons for opting for e-governance. Due to changing world and the emergence of digitalization, e-governance has taken the upfront seat. It has become necessary that government initiatives reach the people on time and efficiently through the digitalization of governance.
- People, Process, Technology, and Resources are the four prominent pillars of e-governance. Good governance ensures that all the people can reap the benefits of economic growth. One of the significant steps that the Government took in this regard is to educate the public regarding e-governance initiatives.

Types of Interaction in e-Governance:

There are the following four types of interactions in e-governance.

- **G2G–** (Government to Government) This model aims at sharing the information between Governments like sharing of information between the police departments of various States, Government document exchange, and so on.
- **G2C–** (Government to Citizen) This model aims at sharing the information between the Government and the citizens like online filing of complaints, payment of online bills of electricity, water, and so on.
- **G2B–** (Government to Business) This model aims at sharing information between Government and private sectors like sharing of rules and data, collection of taxes, approval of patents of companies, etc.

- **G2E– (Government to Employees)** This model aims at sharing the information between the Government and employees like employees can fill out all types of forms online.
- Various e-Governance Projects:
- **Smart Gov:** It makes use of e-file instead of paper files. It is implemented in the Andhra Pradesh Secretariat. It is concerned with streamlining operations, knowledge management, and workflow automation.
- **Khajane Project:** It is a project undertaken by the Government of Karnataka. The project resulted in the computerization of the entire treasury data of the Government of the State. Some of the noticeable results are that the number of drawing officers was brought down to around 21,000 from 40,000, nearly 2,000 staff members were trained to handle the software, about 200 posts in the department of treasury have been abolished, and so on.
- **Digital India Programme:** This programme was started by the Department of Electronics and Information Technology. The program aimed at empowering the country by making it digitally developed. The program was implemented in different phases till 2018. The impact of the agenda is that overall 12,000 rural post offices have been linked electronically.
- **e-Kranti Scheme:** It aimed at the expansion of the internet, mobile phones, and computers to rural areas. The scheme includes the starting up of IT-based jobs in rural areas and also the linking of the internet to the remote villages of the country. There are 44 Mission Mode Projects under the e-Kranti program.
- **e-Governance in municipalities:** It is an initiative done under the umbrella of the overall National e-Governance Plan and the Jawaharlal Nehru National Urban Renewal Mission. The program is aimed at increasing the operational working of the Urban Local Bodies. According to NeGP, Government has decided on four infrastructural pillars for the implementation of e-governance- State Wide Area Network, State Data Centre, Common Service Centre, and Service Delivery Gateway.
- **Public Distribution System:** In PDS, there was the computerization of storage and movement of food grains, fair price shop automation, redressal of grievances, etc.
- **e-Panchayats:** The computerization of panchayat is done on a mission mode basis because the e-governance revolution has not touched the Panchayati Raj Institutions significantly. To improve the quality of governance in Panchayati Raj Institutions including 6094 Block Panchayats and 633 Zilla Panchayats, the Ministry of Panchayati Raj, Government of India has initiated the e-governance scheme known as e-panchayats.
- **Digi-Locker:** It is an initiative introduced by the Government of India under the umbrella of Digital India. Important documents such as Aadhaar cards, mark sheets, and certificates can be digitally stored in Digi-locker. Aadhaar number is essentially required for using Digi-Locker. In 2016, there were 20.13 lakh users of the Digi Locker. The main purpose behind the initiative is to go paperless and the security of documents that can be accessed easily from any place and at any time.

Challenges in e-Governance:

- **Trust:** People should trust the Government and they should be comfortable and confident of the tool and technology that they are using. But due to fraudulent transactions and other factors, the trust of the people is compromised which becomes one of the factors responsible for the limited use of e-governance.
- **Digital divide:** It refers to the division between the people who have access to digital technology and the others who don't have access to it. Economic poverty is one of the main causes of the digital divide. People are unable to afford computers.
- **Lack of Awareness:** Due to the use of digital technology also contributes to the limited use of e-governance techniques. People are not aware of the scope of e-governance and depend on intermediaries for its use.
- **Cost:** In a developing country like India, cost plays a major role in regulating the use of e-governance.
- **Privacy and Security:** People are apprehensive about the security and privacy of their personal data. Government should ensure that no compromise should be done at that end.
- **Accessibility:** Due to inadequate infrastructure facilities in rural areas and language barriers people are unable to access e-governance.
- **Low Computer Literacy:** More than 90% of India's population is digitally illiterate. In addition, the illiterate population comprises 25% to 30% which is one of the biggest challenges.
- **Resistance to Change:** Due to the introduction of Information Technology, a lot of changes have taken place but still, there are various officials, citizens, and politicians who are resistant to change and have different opinions regarding e-Governance.

Some of the Advantages of e-Governance:

- Faster communication through the use of phones and the internet, as it decreases the time taken for communication.
- Paper-based communications require heavy expenditure. It needs a lot of stationary, printers, labour, etc. The cost has been reduced with the use of the internet and phones. Moreover, time and environment are also safe due to their use.
- In earlier times, people faced issues due to physical constraints in reaching out to Government officials. Sometimes because of the ignorance of the officials and at other times due to long queues. But now it has become easy. e-Government is convenient as it provides services according to the schedule and venue of the people.
- e-governance has increased the access of information to the people.
- It also results in improved customer service. GDC (Government Data Centers) are the prominent component of ICT infrastructure for supporting e-governance initiatives.

Computer criminals

Computer criminals have access to enormous amounts of hardware, software, and data; they have the potential to cripple much of effective business and government throughout the world. In a sense, the purpose of computer security is to prevent these criminals from doing damage.

We say **computer crime** is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciously.

One approach to prevention or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occurring.

CIA Triad

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

CIA triad broken down:

Confidentiality

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information.

In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

Integrity

Data integrity is what the "I" in CIA Triad stands for.

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability

This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

Understanding the CIA triad

The CIA Triad is all about information. While this is considered the core factor of the majority of IT security, it promotes a limited view of the security that ignores other important factors.

For example, even though availability may serve to make sure you don't lose access to resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

Assets and Threat

What is an Asset: An asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information.

For example: An employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets. An organization's most common assets are information assets. These are things such as databases and physical files – i.e. the sensitive data that you store

What is a threat: A threat is any incident that could negatively affect an asset – for example, if it's lost, knocked offline or accessed by an unauthorized party.

Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.

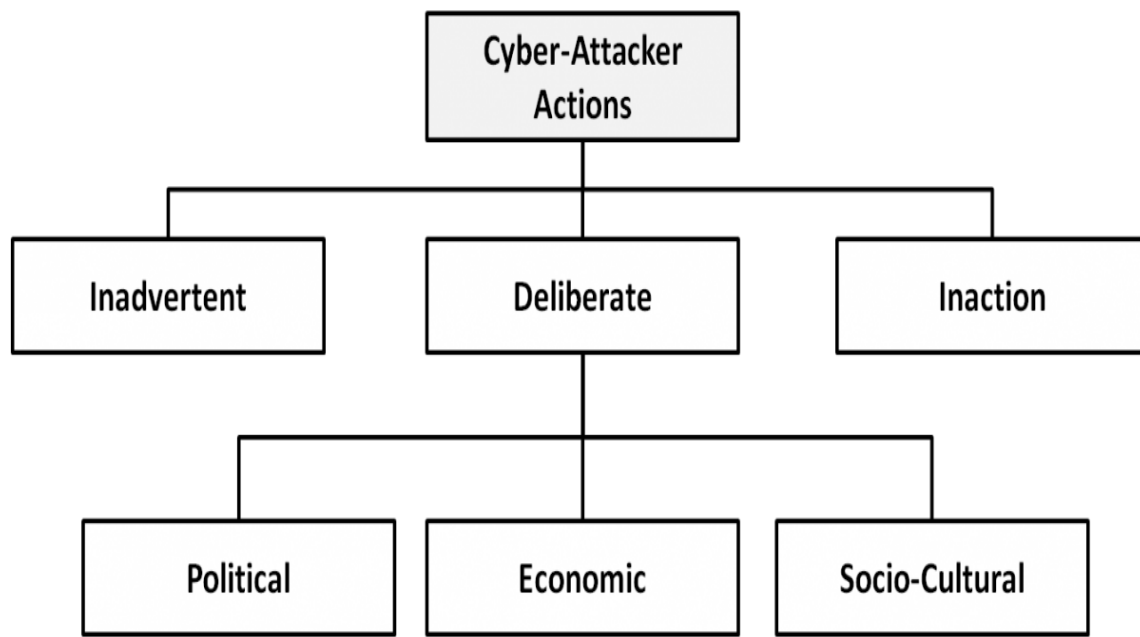
Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

Motive of Attackers

The categories of cyber-attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure, operational cyber security risks arise from three types of actions: i) inadvertent actions (generally by insiders) that are taken without malicious or harmful intent; ii) deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm; and iii) inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action. Of primary concern here are

deliberate actions, of which there are three categories of motivation.

1. **Political motivations:** examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.
2. **Economic motivations:** examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.
3. **Socio-cultural motivations:** examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.



Types of cyber-attacker actions and their motivations when deliberate

Active attacks: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

Types of Active attacks:

Masquerade: in this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

Session replay: In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

Message modification: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

In a **denial of service (DoS)** attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

In a **distributed denial-of-service (DDoS)** exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

Passive Attacks: *Passive attacks* are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted.

Types of Passive attacks:

Eavesdropping (tapping): the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

Traffic analysis: the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

Software Attacks: Malicious code (sometimes called *malware*) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging. Common malware examples are listed in the following table:

Attack	Characteristics
Virus	<p>A <i>virus</i> is a program that attempts to damage a computer system and replicate itself to other computer systems. A virus:</p> <ul style="list-style-type: none">• Requires a host to replicate and usually attaches itself to a host file or a hard drive sector.• Replicates each time the host is used.• Often focuses on destruction or corruption of data.• Usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions.• Often distributes via e-mail. Many viruses can e-mail themselves to everyone in your address book.• Examples: Stoned, Michelangelo, Melissa, I Love You.

Worm	<p>A <i>worm</i> is a self-replicating program that can be designed to do any number of things, such as delete files or send documents via e-mail. A worm can negatively impact network traffic just in the process of replicating itself. A worm:</p> <ul style="list-style-type: none"> • Can install a backdoor in the infected computer. • Is usually introduced into the system through a vulnerability. • Infects one system and spreads to other systems on the network. • Example: Code Red.
Trojan horse	<p>A <i>Trojan horse</i> is a malicious program that is disguised as legitimate software. Discretionary environments are often more vulnerable and susceptible to Trojan horse attacks because security is user focused and user directed. Thus the compromise of a user account could lead to the compromise of the entire environment. A Trojan horse:</p> <ul style="list-style-type: none"> • Cannot replicate itself. • Often contains spying functions (such as a packet sniffer) or backdoor functions that allow a computer to be remotely controlled from the network. • Often is hidden in useful software such as screen savers or games. • Example: Back Orifice, Net Bus, Whack-a-Mole.
Logic Bomb	<p>A <i>Logic Bomb</i> is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack.</p> <ul style="list-style-type: none"> • A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity. • Logic bombs do not self-replicate.

Hardware Attacks:

Common hardware attacks include:

- Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren't limited to software and hardware, but they also affect embedded radio- frequency identification (RFID) chips and memory
- Eavesdropping by gaining access to protected memory without opening other hardware
- Inducing faults, causing the interruption of normal behaviour
- Hardware modification tampering with invasive operations
- Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems
- Counterfeiting product assets that can produce extraordinary operations and those made to gain malicious access to systems.

Cyber Threats-Cyber Warfare: Cyber warfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles.

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Spectrum of Cyber Attacks

Throughout the brief history of cyberwarfare, actors at all levels have performed a wide range of attacks. Despite individual differences, these attacks can be arranged into five categories or levels that build upon one another to form a spectrum: **Network Denial, Enterprise Denial, Enterprise Manipulation, Mission Denial, and Mission Manipulation.**

The "Spectrum of Cyber Attack" incorporates the definition of denial from Joint Publication (JP) 3-12, Cyberspace Operations, "to prevent access to, operation of, or availability of a target function"³ as the foundation for the three levels designated as denial attacks: Network Denial, Enterprise Denial, and Mission Denial. The spectrum builds upon JP 3-12's definition of manipulation, "controls or changes. . . to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification and other similar techniques,"⁴ for the remaining levels designated as manipulation attacks: Enterprise Manipulation and Mission Manipulation. In this definition, physical simply refers to the fact that manipulation effects have an impact outside of cyberspace. This definition not only refers to the physical systems themselves, but also the cognitive layer, or users, of those systems. This describes manipulating a system to in-turn manipulate or drive an effect in the human element. Manipulation attacks require a more complete understanding of the systems involved along with deeper, more intrusive network access. This knowledge and access are required to successfully manipulate, deceive, or otherwise influence the behavior of users within a target organization.

Level 1: Network Denial Definition. A cyber attack that prevents a network from communicating with external networks Description. The first level of attack is the most simple to conduct, difficult to stop, and thus commonly used. Level 1, Network Denial, targets only the transmission of information, not the actual information itself. These attacks may affect only a part of the network or the network in its entirety. They can be accomplished through several different methods, many of which are exceedingly difficult for the victim to stop. Level 1 attacks primarily differ from other levels in that they affect the target's ability to interact with other organizations while internal processes are largely unaffected.

Examples. A simple example of Network Denial is characterized by an attacker that logs into a router at the border of an organization's network and stops it from transferring data. This example results in the blocking of all traffic on a network and isolates the target organization, temporarily preventing it from transmitting any information in or out using computer networks. This type of network isolation degrades the operations of any organization but only as long as the target is unable to restore proper functionality. More advanced level 1 attacks require national-level resources or access to central backbones of the internet. These include Border Gateway Protocol hijacking, Domain Name Server

hijacking, and large-scale Distributed Denial of Service, all of which have been used by either Russia, Iran, or China.⁵ These attacks take advantage of the fundamental trust that the internet is built on, giving them the added benefit that there is very little a victim can do to stop them, and they are always at the disposal of a nation.

Tradeoffs. Network Denial attacks are conceptually simple to execute but only provide temporary paralysis of a target's operations. Fewer moving pieces at the technical level results in the highest chance for success compared to all other levels and requires far less knowledge about the target. New targets can be attacked within hours or days and require little preparation. The trade-off, however, is that level 1 attacks draw significant attention and are quick to diagnose. Overall, level 1 attacks require less time, less funding, and thus less commitment, yet they are only expected to disable an organization for hours to days depending on the sophistication of the target's personnel.

Level 2: Enterprise Denial Definition. A cyber attack that denies an organization's users access to their data Description. The next level of cyber attack also disables an organization, but in a manner that inhibits the daily activities of end-users. The term enterprise is used to describe the systems and applications users rely on to perform day-to-day tasks. Examples of daily activities affected by level 2 attacks include the ability to log into computers, send e-mail, and alter documents. Level 2 attacks differ from level 1, Network Denial, in that they specifically disrupt information that an organization's users interact with directly.

Examples. The most common example of a level 2 attack is ransom malware, or "ransomware," currently in vogue with cybercriminals. Ransomware does not need to know anything about an organization before executing its core objective, to deny users access to their data by encrypting it. The files that become encrypted are critical to the system users as the malicious software attacks all files, historical records, activity records, and any others used to carry out daily tasks and company function. This is precisely why it is so devastating for companies hit by such attacks. The most destructive level 2 attack to date has been the "NotPetya" ransomware that caused an estimated \$10 billion in damages worldwide in 2017. As an example of the financial impact caused by NotPetya, the international shipping company Maersk alone suffered \$300 million in damages and experienced a complete operational shut down for almost a week. This level of disaster is not unique to Maersk,⁶ or even NotPetya itself. "WannaCry," "SamSam," and "Ryuk" are all well-documented ransomware attacks dating back to 2017 that inflicted millions in financial costs and achieved wide-scale operational impacts across numerous organizations.⁷

Tradeoffs. Level 2 attacks are likely to cost more financially than any other cyber attack, purely based on the scope and number of systems they affect. Similar to level 1, level 2 attacks require very little target knowledge, and thus, require less time and monetary investment than other levels. However, the likelihood of success of level 2 attacks is also less than that of level 1 attacks due to the deeper network access required. Additionally, the most damaging level 2 attacks to-date only managed to take organizations offline for a few days despite the severe financial costs, and all operations were restored in a manner of weeks. The Spectrum of Cyber Attack AIR & SPACE POWER JOURNAL → WINTER 2020 95

Level 3: Enterprise Manipulation Definition. A cyber attack that manipulates the decision-making of an organization's users without being detected Description. Enterprise Manipulation is the first level on the spectrum that tailors more toward affecting the behavior of the adversary than removing their ability to operate. These attacks target the same computer systems as level 2, Enterprise Denial, attacks but utilize a deeper understanding of the organization to influence or corrupt, but not deny, common organizational processes. Further, a key objective in executing a level 3 attack is to do so without the user being aware of the attack. This is the key distinction between level 3 and the first two levels. Level 3 attacks must be performed in a manner that is not predictable nor widespread throughout the target organization. Enterprise users have been conditioned over time to be mistrusting of computers and software due to confusing interfaces, technical user manuals, overall complexity, and frequent data loss. By introducing outside gremlins into the systems, end-users can further lose confidence in their ability to effectively perform tasks, thereby leading to loss in productivity and organizational effectiveness.

Examples. Although data manipulation has only started to be openly discussed in the past few years,⁸ it is easy to envision the potential chaos that can result from such attacks and has captured the imagination of television producers in series such as "Mr. Robot."⁹ These attacks can be as simple as removing key e-mails, locking particular user accounts, or corrupting vital user files. More robust and potentially far-reaching attacks can be catastrophic, such as manipulating financial or human resource data. According to Forbes, the manipulation of financial data is already extensively practiced by North Korean hackers. North Korea has stolen a staggering \$2 billion in 35 compromises across 17 nations.¹⁰ For example, North Korea drained \$498K from the city of Tallahassee by manipulating payroll data.¹¹ These attacks were designed to obtain funds rather than impose crippling costs on the underlying organizations, yet the devastating impact to the organizations were the same.

Tradeoffs. Enterprise Manipulation attacks strike at the psyche of an organization with the aim of crippling its effectiveness for a prolonged period of time. Levels 1 and 2 cause overt disruptions resulting in temporary outages, but level 3 attacks can hinder an organization for an indefinite period of time. These attacks require a nearly identical preparation time as level 2 but have a much lower chance of success and less quantifiable results. Level 3 attacks also cost more to execute because they must use more sophisticated tools to remain undetected in the target network. Level 3 attacks will not likely impose costs similar to the other levels, but 96 AIR & SPACE POWER JOURNAL → WINTER 2020 Musielewicz they allow attackers to remain within the network undetected while eroding the productivity of an organization. Level 3 attacks also provide the ability to engage a target without the increased risks of retaliation or escalation because of their inherent stealth and plausible deniability. As long as level 3 attacks remain hidden, they allow the perpetrator to develop level 4 and level 5 attacks, all while the target simultaneously suffers negative impacts on efficiency and productivity.

Level 4: Mission Denial Definition. A cyber attack that specifically prevents the operation of processes or systems critical to an organization's mission Description. The final two

levels of the Spectrum of Cyber Attack focus solely on the chain of systems and processes that are essential to an organization carrying out its core mission. This focus may be the destruction of mission-critical data or even—in very specific scenarios—the physical destruction of hardware through industrial control system manipulation. The precision of these attacks is what specifically distinguishes level 4, Mission Denial, from level 2, Enterprise Denial.

Example. The 2015 Russian attack on the Ukraine power grid is a prime example of a level 4 cyber attack. During this attack, Russia gained critical access to three primary Ukrainian power companies undetected. Once inside the networks, the malicious actors immediately targeted the systems used by internal operators to control the generation of power. The actors surveilled the system operators long enough to learn which interfaces were used to control the power generators. Once known, the attackers systematically shut the generators down and disabled remote access to the controlling computers.¹² By preventing the power generator operators from remotely bringing the systems back online, technicians were required to physically travel and manually restart each generator, a process that took six hours to complete.¹³ What makes this example a level 4 attack instead of a level 2 is that the actors were specifically targeting those systems that were essential to the organization executing its core mission—generating power. If these same actions were conducted against systems not vital to this mission, they would be classified as a level 2 attack.

Tradeoffs. From an attacker's perspective, level 4 attacks are much more predictable than level 2 because of their precise nature. These attacks are far more likely to create the specific effect desired. Reducing the scope of an attack and executing with precision allows the attacker to tailor to specific strategic objectives and execute with a higher level of certainty. In contrast, level 2, Enterprise Denial, has the potential to prevent an organization from accomplishing its primary mission, but only as a byproduct of the primary attack. It is easier for a victim to restore mission-critical functions following a level 2 attack because of the universal aspect of level 2 attacks versus the subtlety required for level 4. Level 2 attacks are far more common and less sophisticated, making them more likely to be anticipated and mitigated by network defenders. Level 4 attacks require notably longer time commitments than levels 1, 2, and 3. This is due to the in-depth understanding required to learn the specifics of how an organization conducts its mission and the time required to maneuver to those systems that enable that mission. These longer time commitments naturally cause the overall cost of operations to go up. The longer an actor must remain in a network, the more sophisticated their tools must be to stay undetected. Once a level 4 attack is executed, it will quickly be discovered by network defenders and the remedy will likely be straightforward. The effective downtime of the organization relies heavily on the extent of any physical damage and is further influenced by the scarcity of any specialized hardware required.

Level 5: Mission Manipulation Definition. A cyber attack that specifically manipulates the systems or processes critical to an organization's mission without being detected. Description. Mission Manipulation is the most sophisticated and strategically complex cyber attack within the spectrum. Mission Manipulation allows for the repeated, sustained disruption of the fundamental mission of an organization.

Level 5 attacks are identical to level 4 except for the critical fact that they are executed

without being detected. This is a small distinction but is exceptionally difficult to achieve.

Example. The destruction of mission-critical systems and the manipulation required to hide those actions has only been demonstrated by one publicly disclosed cyber attack to date: Stuxnet. Extensively documented, Stuxnet is known for the physical destruction it inflicted on Iranian centrifuges from April 2009– June 2010.¹⁴ Yet, the true brilliance of Stuxnet was its skillful deception of the end-users of these systems. Stuxnet systematically destroyed these mission-critical centrifuges while at the same time manipulating the monitoring components to tell the engineers they were functioning properly. Because of the criticality of these centrifuges, the paired destruction and deception of Stuxnet disrupted the organization's ability to perform its primary mission and set back Iran's nuclear program a minimum of two years.¹⁵ The attack exacerbated financial burdens and according to a report by the Center for Security Studies, "likely culminated in an overall feeling of insecurity throughout Iranian society."¹⁶ Even after the discovery of Stuxnet, Iran was not able to fully trust their 98 AIR & SPACE POWER JOURNAL → WINTER 2020 Musielewicz systems—not knowing whether a failure was generated by human error or the actions of malicious code lurking in their systems.

Tradeoffs. Level 5 attacks require substantially more resources than any other level, both in time and human capital. Mission Manipulation is expected to require a combination of customized tools, in-depth knowledge, sophisticated cyber expertise, specialized engineering knowledge, and significant amounts of time. It requires time to gain network access, time to harvest information, time to develop tools, time to maneuver within the network, and time to execute. It was speculated that Stuxnet required the combined efforts of Israel and the United States¹⁷—two of the most technologically sophisticated nations in the world—a minimum of three years of preparation, a year of continuous execution, and an estimated \$100 million dollars.¹⁸ The target knowledge, commitment, and technical expertise required to execute attacks at level 5 demands real-time development as the exact configurations and nuances of mission systems are almost impossible to know before accessing them. The skills and tools for such specialized or indigenous mission systems may be extremely hard to find, or may not exist, requiring them to be built from the ground up. In spite of these heavy constraints, a level 5 attack has the ability to cause massive high-level impacts that rival the sophistication of any operation in the other warfare domains. It can single-handedly achieve strategic objectives through nonkinetic means, and importantly, allow for plausible deniability that reduces the risk of retaliation and conflict escalation. As seen in the Stuxnet example, the culmination of such high levels of investment can produce powerful effects that last for years.

Cyber Crime:

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

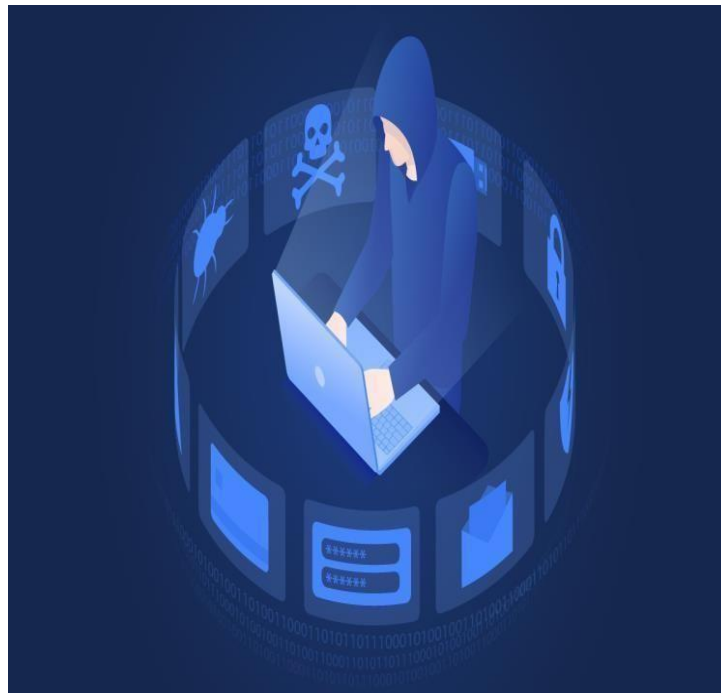
Cyber Terrorism:

Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication.

Cyber Espionage:

Cyber spying, or cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet.



Security Policies:

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.

A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment.

Need of Security policies-

- 1) It increases efficiency.
- 2) It upholds discipline and accountability
- 3) It can make or break a business deal
- 4) It helps to educate employees on security literacy

There are some important cyber security policies recommendations describe below-

Virus and Spyware Protection policy:

- It helps to detect threats in files, to detect applications that exhibits suspicious behavior.
- Removes, and repairs the side effects of viruses and security risks by using signatures.

Firewall Policy:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

Application and Device Control:

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

CYBERSPACE

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

REGULATIONS

There are five predominant laws to cover when it comes to cybersecurity:

Information Technology Act, 2000 The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.

But with the cyber attackers getting sneakier, topped by the human tendency to misuse technology, a series of amendments followed.

The ITA, enacted by the Parliament of India, highlights the grievous punishments and penalties safeguarding the e-governance, e-banking, and e-commerce sectors. Now, the scope of ITA has been enhanced to encompass all the latest communication devices.

The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously:

Section 43 - Applicable to people who damage the computer systems without permission from the owner. The owner can fully claim compensation for the entire damage in such cases.

Section 66 - Applicable in case a person is found to dishonestly or fraudulently committing any act referred to in section 43. The imprisonment term in such instances can mount up to three years or a fine of up to Rs. 5 lakh.

Section 66B - Incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years imprisonment. This term can also be topped by Rs. 1 lakh fine, depending upon the severity.

Section 66C - This section scrutinizes the identity thefts related to imposter digital signatures, hacking passwords, or other distinctive identification features. If proven guilty, imprisonment of three years might also be backed by Rs. 1 lakh fine.

Section 66 D - This section was inserted on-demand, focusing on punishing cheaters doing impersonation using computer resources.

Indian Penal Code (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860

- invoked along with the Information Technology

Act of 2000. The primary relevant section of the IPC

covers cyber frauds:

Forgery (Section 464)

Forgery pre-planned for cheating

(Section 468) False

documentation (Section 465)

Presenting a forged document as

genuine (Section 471) Reputation

damage (Section 469)

Companies Act of 2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cement all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs have become even more proactive and stern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014 prescribe strict guidelines confirming the cybersecurity obligations and responsibilities upon the company directors and leaders.

NIST Compliance

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body.

NIST Cybersecurity Framework encompasses all required guidelines, standards,

and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness.

It promotes the resilience and protection of critical infrastructure by: Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs
Determining the most important activities and critical operations - to focus on securing them
Demonstrates the trust-worthiness of organizations who secure critical assets
Helps to prioritize investments to maximize the cybersecurity ROI
Addresses regulatory and contractual obligations
Supports the wider information security program
By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST.

Final Thoughts As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security. Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent.

Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyberland - can bring about online safety and resilience.

ROLE OF INTERNATIONAL LAWS

In various countries, areas of the computing and communication industries are regulated by governmental bodies. There are specific rules on the uses to which computers and computer networks may be put, in particular there are rules on unauthorized access, data privacy and spamming. There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes. There are laws governing trade on the Internet, taxation, consumer protection, and advertising. There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies. Some states limit access to the Internet, by law as well as by technical means.

INTERNATIONAL LAW FOR CYBER CRIME

Cybercrime is "international" that there are 'no cyber-borders between countries'. The complexity in types and forms of cybercrime increases the difficulty to fight back. Fighting cybercrime calls for international cooperation. Various organizations and governments have already made joint efforts in establishing global standards of legislation and law enforcement both on a

regional and on an international scale

THE INDIAN CYBERSPACE

Indian cyberspace was born in 1975 with the establishment of National Informatics Centre (NIC) with an aim to provide govt with IT solutions. Three networks (NWs) were set up between 1986 and 1988 to connect various agencies of govt. These NWs were, INDONET which connected the IBM mainframe installations that made up India's computer infrastructure, NICNET (the NIC NW) a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central govt with the state govts and district administrations, the third NW setup was ERNET (the Education and Research Network), to serve the academic and research communities.

New Internet Policy of 1998 paved the way for services from multiple Internet service providers (ISPs) and gave boost to the Internet user base grow from 1.4 million in 1999 to over 150 million by Dec 2012. Exponential growth rate is attributed to increasing Internet access through mobile phones and tablets. Govt is making a determined push to increase broadband penetration from its present level of about 6%¹. The target for broadband is 160 million households by 2016 under the National Broadband Plan.

NATIONAL CYBER SECURITY POLICY

National Cyber Security Policy is a policy framework by Department of Electronics and Information Technology. It aims at protecting the public and private infrastructure from cyberattacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyberspace as a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

VISION

To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

MISSION

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and

minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

OBJECTIVE

Ministry of Communications and Information Technology (India) define objectives as follows

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

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 vectors.
 - 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 tools, 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. Cybercriminals use the World Wide Web and Internet to an optimum level for all illegal activities to score 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).

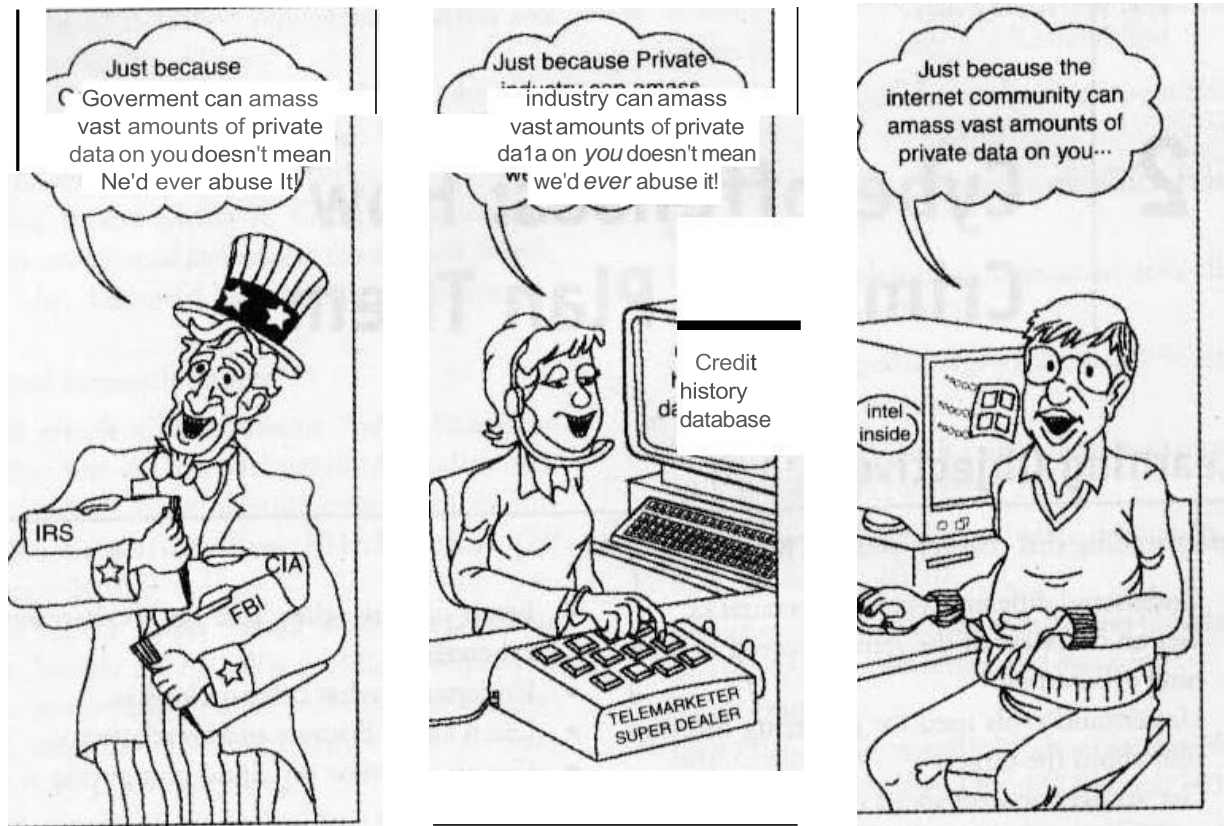


Figure 2.1 We all vouch for keeping your personal information secret!

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 hockerisa 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 crocker 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 hocking 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 "crocker" 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 a 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: Nino Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2), Wiley India.

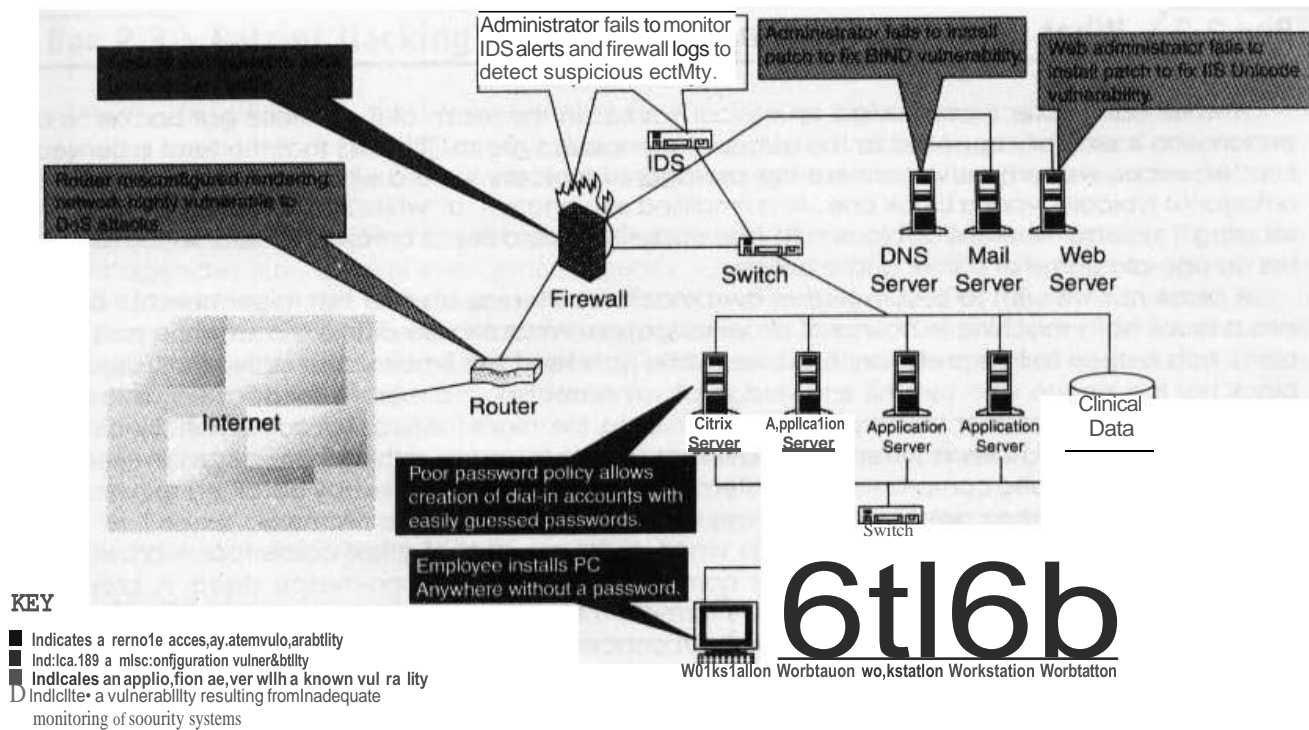


Figure 2.2 Network vulnerabilities - sample network.

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 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 "crocker" 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: Nino 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 it difficult to trace and apprehend the criminals.
2. Crimes targeted at property: This includes stealing mobile devices such as cell phone, laptops, personal digital assistants (PDAs), and removable media (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 scaling 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 Hack:ng

Patriot hacking¹¹¹ also known as *Digital Warfare*, is a form of vigilante computer systems' crocking 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 hocking 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 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 chat 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 airer 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 pre-attack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment. Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security characteristics 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, hardware, 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 r;ps 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 "[inurl:]" in front of your query; this implies [inurl:google inurl:search] is the same as [inurl: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 yaho) 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 yaho)) 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 J Tools used during passive attacks

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
Google Earth	<p>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.</p> <p>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.</p>	<p>For more details on this tool, visit: http://earth.google.com/</p> <p>Like "Google Earth," similar details can be obtained from http://www.wikimapia.org/</p> <p>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 comes with India-specific features such as weather information and even administrative boundaries of all states and districts, visit: http://bhuvan.nrsc.gov.in/</p>
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 text, 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.	<p>To name a few, visit:</p> <ul style="list-style-type: none"> • http://www.whicpagesinc.com • http://www.incdius.com/ • http://www.whirepages.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.	<p>For more details on this tool, visit:</p> <ul style="list-style-type: none"> • http://www.namedroppers.com/ • http://www.binarypool.com/byces.hunt

Table 2.11 (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
WHOIS	<p>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.</p> <p>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.</p>	<p>For more details on this tool, visit:</p> <ul style="list-style-type: none"> • http://whois.domaintools.com/ • http://www.whois.net/ • http://www.samspace.org/ <p>For further details of this lookup utility, visit:</p> <ul style="list-style-type: none"> • http://resellers.rucows.com/opensrs/whois/ • http://www.nsauditor.com/docs/html/roots/vhois.htm
Nslookup	<p>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.</p>	<p>For more details on this tool, visit:</p> <ul style="list-style-type: none"> • http://www.klochee.com/services/nslookup.php • http://nslookup.downloadsoftware4free.com/
Dnssniff	<p>Using this tool, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookup, WHOIS lookups, etc.</p>	<p>For more details on this tool, visit:</p> <p>http://www.dnssniff.com/</p>
Traceroute	<p>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.</p>	<p>For more details on this tool, visit:</p> <p>http://www.rjsmich.com/tracenet.html</p>
VisualRoute Trace	<p>This is a graphical tool which determines where and how virtual traffic on the computer network is flowing between source and target destination.</p>	<p>For more details on this tool, visit:</p> <p>http://www.visualware.com/</p>
eMailTrackerPro	<p>eMailTrackerPro analyzes the E-Mail header and provides the IP address of the system that sent the mail.</p>	<p>For more details on this tool, visit:</p> <p>http://www.emailtrackerpro.com/</p>
HTTrack	<p>"[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.</p>	<p>For more details on this tool, visit:</p> <p>http://www.hrcrack.com/</p>
Website Watcher	<p>The tool can be used to keep 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.</p>	<p>For more details on this tool, visit:</p> <p>http://www.aignes.com/</p>
Competitive Intelligence	<p>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.</p>	<p>To name a few, visit</p> <ul style="list-style-type: none"> • http://bigira.com/ • http://www.amiry.edu/aici/

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 for CD.

Table 2.2 | Tools used during active attacks

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
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 request 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.dosc.gov.ph/sar/bing.html
Bugmap	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.sccurifyfocus.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/
DNSuacrr	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.maverju.org/unix/dnsracer.php

Table 2.2 (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
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 rescues 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. <i>Hmap</i> 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 <i>hping</i> you can do the following: <ul style="list-style-type: none"> • 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; • <i>hping</i> 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.	
Huping	This is similar to "ping," 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/hrrping/
Hunc	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/1-kra/index.html
Libwhisker	This is an application library designed to assist in scanabilities.	Details of this open-source software can be found at: http://www.wirctrip.net/rfp/lw.asp
Mailsnarf	This is a network auditing tool to capture SMTP for CCI/web vulnerability 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.inercat.org/software/nbtscan.html
Nessus	This is a powerful, fast, and modular security scanner that tests for many thousands of vulnerabilities. ControlScan system can also be used to create custom Nessus reports.	To know more about this open-source utility, visit: http://www.w.nessus.org/
Ncccr	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.acsrakc.com/research/cool/network_utilitie/
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 server 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 details: http://www.clrc.net/codc/nikro.shtml
Nmap	This is a port scanner, operating TCP fingerprint, 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/

Table 2.2 (Continued)

<i>Name of the Tool</i>	<i>Brief Description</i>	<i>Remarks</i>
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: <ul style="list-style-type: none"> • 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/oultis/smrpscan/
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: <ul style="list-style-type: none"> • 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.

Table 2.2 (Continued)

Name of the Tool	Brief Description	Remarks
	<p>devices such as switches, routers, firewalls, network-based intrusion detection system (NIDS), and intrusion prevention system (IPS).</p> <p>TCPReplay supports both single and dual NIC modes for testing both sniffing and inline devices.</p> <p>TCPReplay is used by numerous firewalls, IDS, IPS, and other networking vendors, enterprises, universities, laboratories, and open-source projects.</p>	<ul style="list-style-type: none"> • 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 TCPReplay. <p>For further details, visit: http://tcpreplay.synfin.net/uac/</p>
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/hrml/projects/X.html

Note: IP is Internet Protocol here.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Incident Response* (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/closed 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-Daca	143	Internet Message Access Protocol (IMAP)
21	FTP - Control	150	NetBIOS session service
22	Secure shell (SSH) remote log-in protocol	156	SQLserver
23	Telnet	161	Simple Network Management Protocol (SNMP)
25	Simple Mail Transfer Protocol (SMTP)	179	Border Gateway Protocol (BGP)
29	MSGICP	190	Gateway Access Control Protocol (GACP)
37	Time	194	Internet relay chat (IRC)
42	Namcserv (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 network 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-OS
79	Finger	458	Apple quick time
80	HTTP	546	DHCP client
103	X.400 Standard	547	OHCP server
108	SNA gateway access server	563	SNEWS
109	POP2	569	MSN
110	POP3	1080	Socks
115	Simple File Transfer Protocol (SFTP)		

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.

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 of 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 constraint on the file server, we will be moving a 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's 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:** TC 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, crashing, garbing or garbage gleanng. "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, *dumpstming* 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-\v'aste, 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: If an attacker sends fake E-Mails (see Box 2.7) to numerous users in such a way 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 user (netizens) to reveal their sensitive personal information, such as; user-names, 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 *ji-hack* 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).

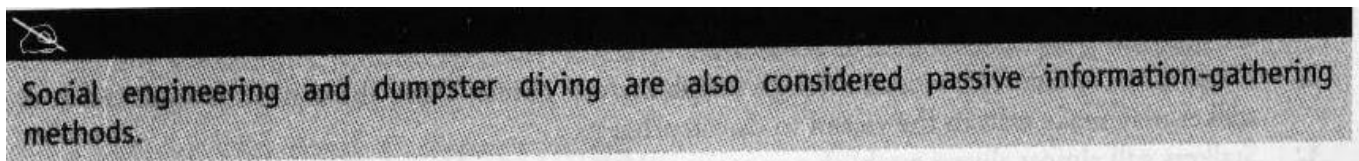
2. **E-Mail attachments:** E-Mail attachments are used to *send* malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed. Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment. 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 unthinkingly 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 devise 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, theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.¹³¹

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 in which they 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.❖❖

Source: <http://en.wikipedia.org/wiki/Cyber-bullying> (2 April 2009).

5. The stalker may pose 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 Delhi¹⁵¹ 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 harassment, 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 survey¹⁶¹ 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 as terminals, 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 may be running in 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.

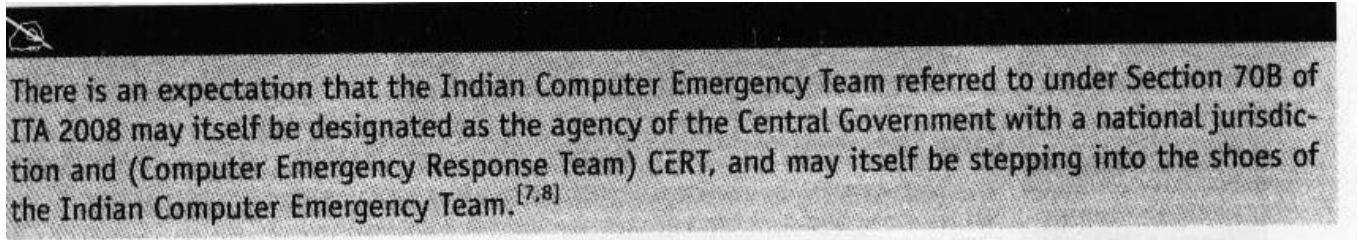
Indian Information Technology Act (ITA) 2000¹⁷¹ (as discussed in great detail in Chapter 6) does not define cybercafes and interprets cybercafes as "network service providers" referred to under the erstwhile Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network. The concept of "due diligence" was interpreted from the various provisions in cyber-cafe 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.¹⁸¹ Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Internet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack (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/TSPs/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:

- I. Always logout: While checking E-Mails or logging into chatting services such as instant messaging or using any other service which 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 login.
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.¹⁹¹
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. 2.6.¹¹¹
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.

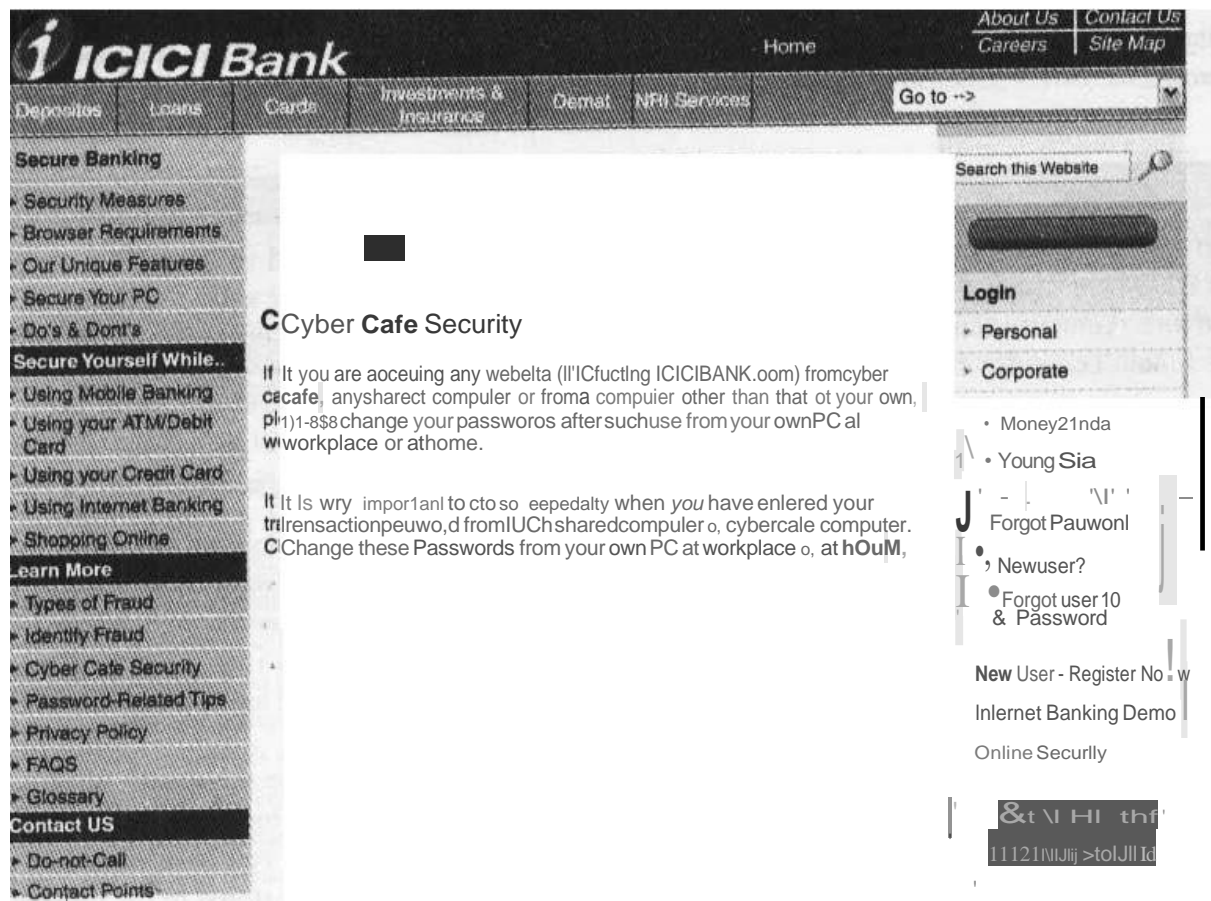


Figure 2.5 Cybercafe security.

Source: <http://www.icicibank.com/pfsuser/temp/cybersec.htm> (27 June 2009).

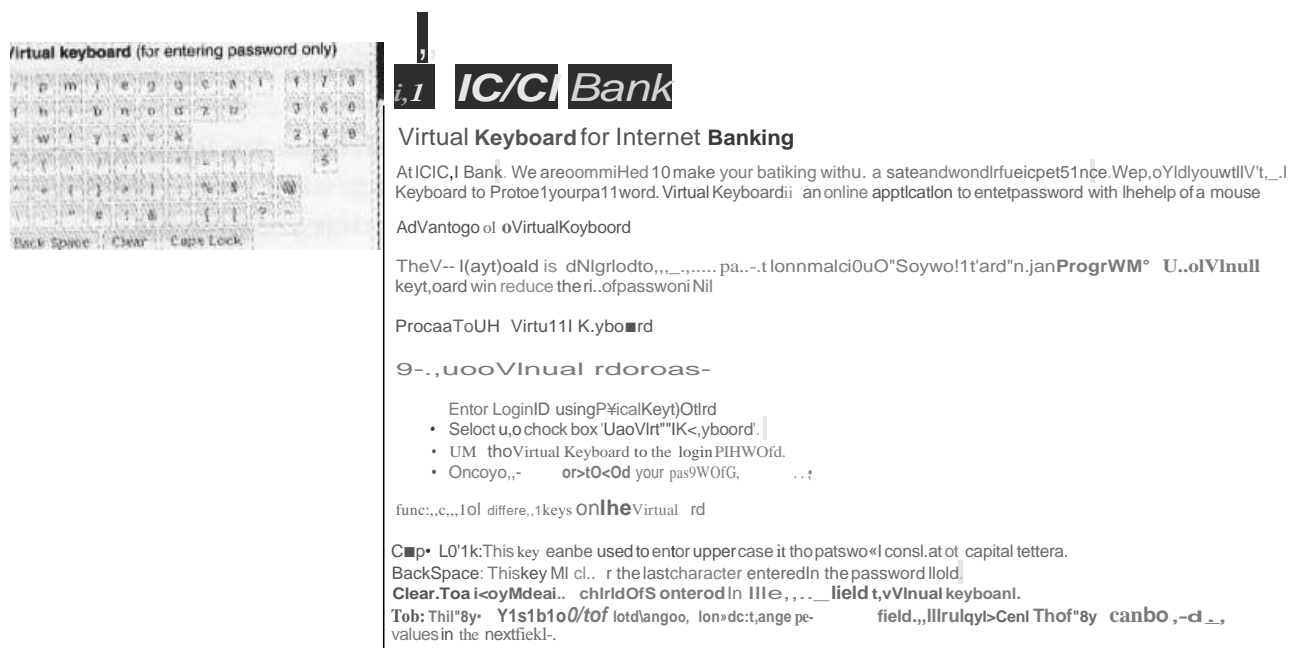


Figure 2.6 Virtual keyboard.

Source: <http://www.icicibank.com/pfsuser/Webnews/Virtualkeyboad.htm> (27 June 2009).

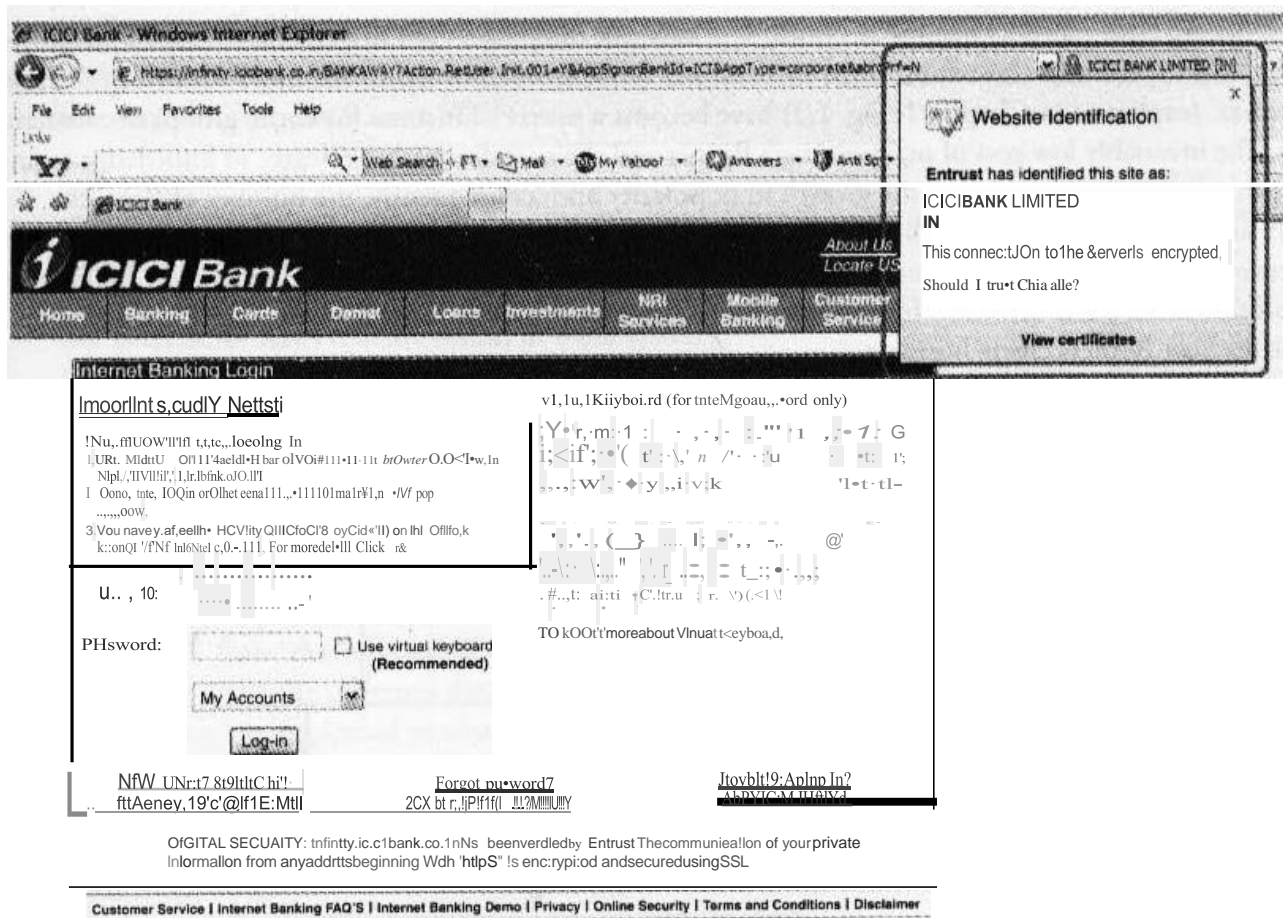


Figure 2.7 Security warnings.

Source: <http://www.icicibank.com/pfsuser/webnews/virtualkeyboard.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.¹¹¹⁾

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 them access. Your computer system may be a part of a Botnet even though it appears to be operating normally. Bots 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 z.ombic network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge. "Zombinetworks" (explained in Chapter I, 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.

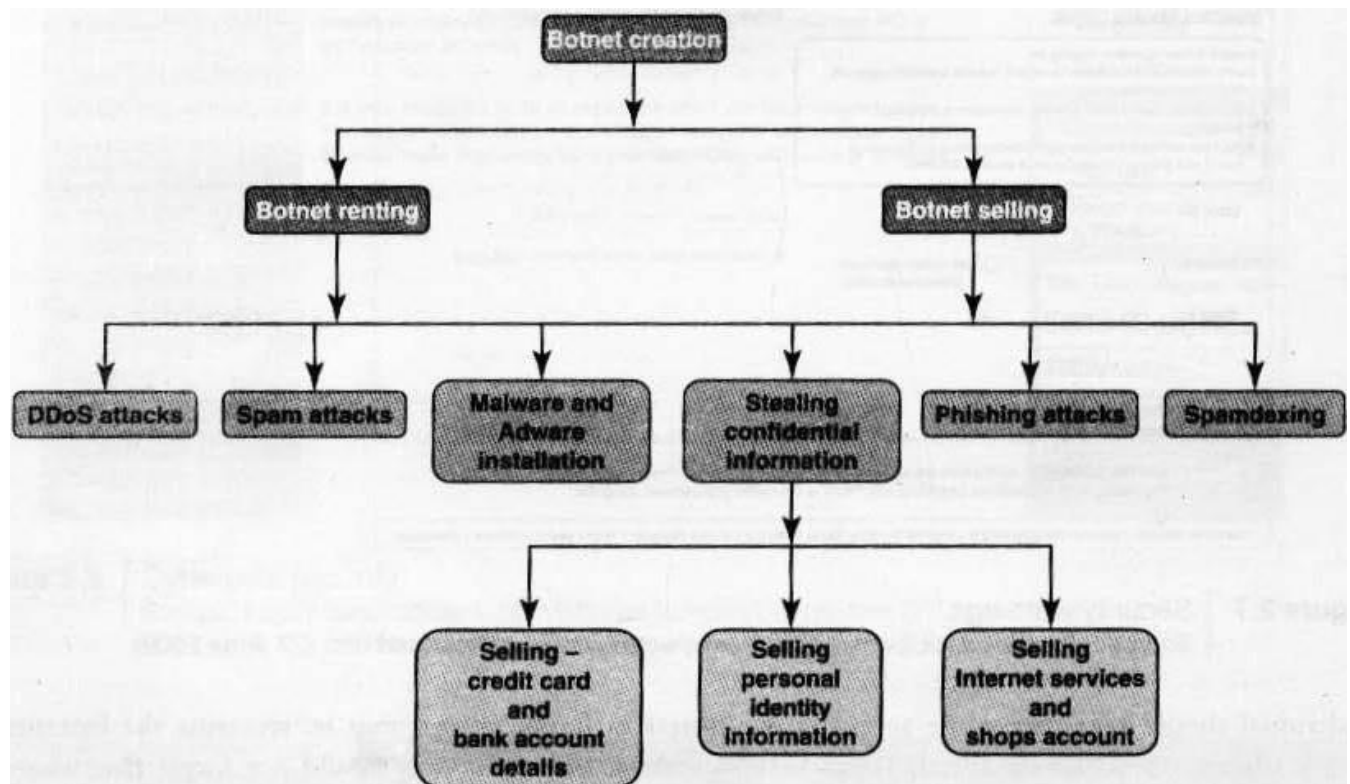


Figure 2.8 | Botnets are used for gainful purposes.

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 cloaked 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:^{112,n.1}

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-a-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 mailbox, 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 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.¹¹⁴¹

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) attack¹¹⁷¹ 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.^{1171, 161}

The attack vectors described here are how most of them are launched.^{1171, 181}

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 rouse 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 Chat (IRC), and P2P file-sharing networks rely on cozy connections between the computer and 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").

¹⁹¹ 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 advantages¹²⁰¹:

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.3cera.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.	Appiscri-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.appiscri.com/
5.	Microsoft Live Mesh: This cloud setup synchronizes the files with 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/

(Continued)

Table 2.4 | (Continued)

Sr. No.	Service Providers	Weblink
	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/inrl/cn/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/thecenterprisecloud.aspx

Source: <http://blog.taragana.com/index.php/archive/top-10-cloud-computing-service-providers/> (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 follows¹¹⁹¹:

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 Lasc.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 shared 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.
	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 system, it becomes difficult to trace inappropriate and/or illegal activity.	Organization should enforce the contractual liability toward providing security violation log 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.

Sourre: <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 induced 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 example.
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 tool 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.merineews.com/catFull.jsp?articleID::J55371> (25 June 2009).
- [8] To know more on cybercafe, visit: <http://punekar.in/sire/2009/02/04/city-cyber-cafes-in-scall-deep-freeze-software-for-security/> (27 June 2009).

- [9] To know more on cybercafe, visit: <http://www.icicibank.com/pfsuser/comp/cybersec.htm> (27 June 2009).
- [10] To know more on cybercafe, visit: <http://www.icicibank.com/ptsuser/webnews/virtualkey-board.htm> (27 June 2009).
- [11] To know more on Botnet, visit: <http://en.wikipedia.org/wiki/Botnet> (19 March 2009).
- [12] To know more on Bomer, visit: <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/ale132.shtm> (30 March 2009).
- [13] To know more on Bornet, visit: <http://www.viruslist.com/en/analysis?pubid=204792068> (30 March 2009).
- [14] To know more on arrack vector, visit: <http://searchsecurity.techtarget.com/dictionary/definition/1005812/anack-vector.html#> (17 July 2009).
- [15] To know more on attack vector, visit: http://searchsecurity.techtarget.com/solution/0,,sid14_gci214475,00.html (17 July 2009).
- [16] To know more on arrack vector, visit: <http://www.nec-security.org/article.php?id=949> (17 July 2009).
- [17] To know more on zero-day arrack, visit: http://en.wikipedia.org/wiki/Zero_day_arrack (9 October 2009).
- [18] To know more on attack vector, visit: <http://cybercoyore.org/security/vectors.shtml> (17 July 2009).
- [19] To know more on cloud computing, visit: http://en.wikipedia.org/wiki/Cloud_computing (9 October 2009).
- [20] To know more on cloud computing, visit: <http://communication.howsruffworks.com/cloud-computing2.htm> (9 October 2009).

FURTHER READING

Books

1. Godbole, N. (2009) *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. Graves, K. (2007) *CEH - Official Certified Ethical Hacker Review Guide*, Wiley Publishing Inc., IN, USA.
3. Milhorn, H.T. (2007) *Cybercrime: How to Avoid Becoming a Victim*, Universal Publishers, USA.

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, C, D, E, F, J, L. These are provided in the companion CD.

Unit III

CYBERCRIMES: MOBILE AND WIRELESS DEVICES

INTRODUCTION. Why should *mobile devices* be protected? Every day, *mobile devices* are lost, stolen, and infected. *Mobile devices* can store important business and personal *information*, and are often be used to access University systems, email, banking

Proliferation of mobile and wireless devices:

- people hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.

They might even access corporate networks and pull up a document or two on their mobile gadgets

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure below helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

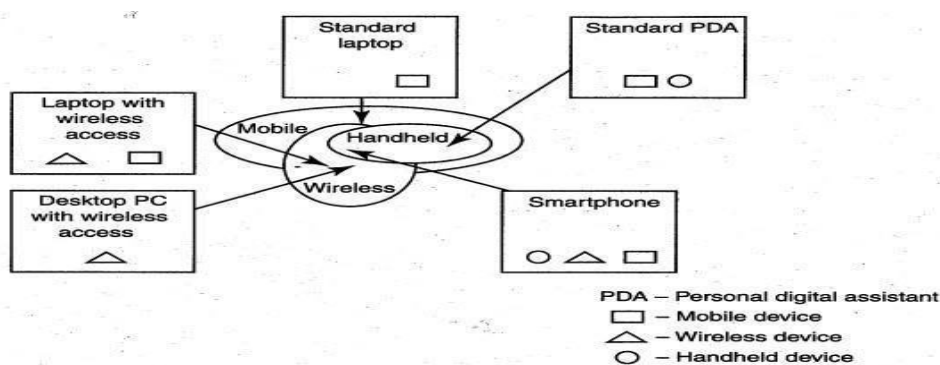


Figure : Mobile, Wireless and hand-held Devices

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

1. Portable computer: It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.

2. Tablet PC: It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

3. Internet tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

4. Personal digital assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

5. Ultramobile (PC): It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

6. Smartphone: It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.

8. Fly Fusion Pentop computer: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Trends in Mobility:

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure below shows the different types of mobility and their implications.

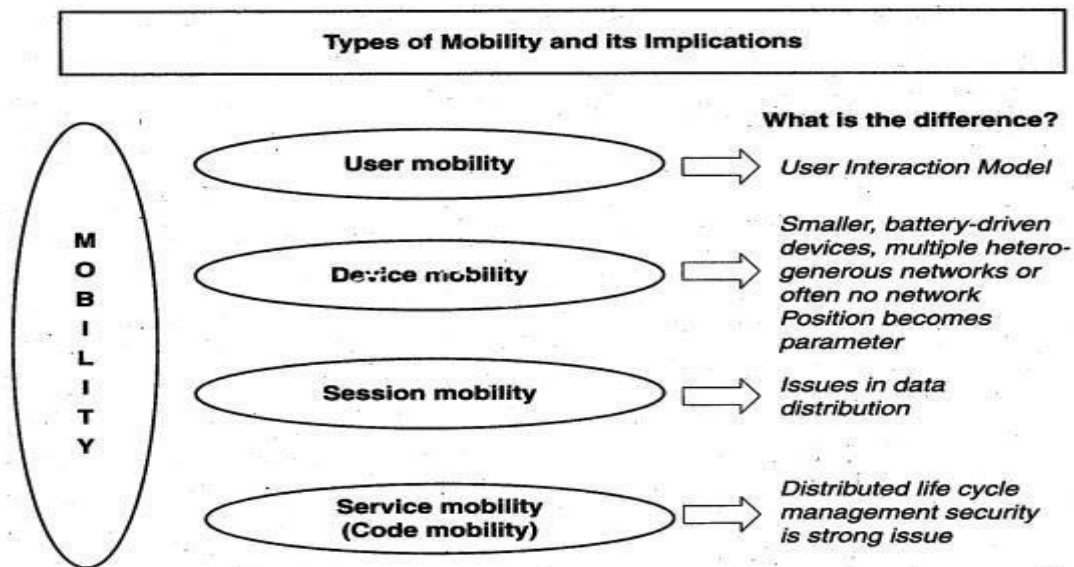


Figure: Mobility types and implications

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks- that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Popular types of attacks against 3G mobile networks are as follows:

1. Malwares, viruses and worms: Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- **Skull Trojan:** It targets Series 60 phones equipped with the Symbian mobile OS.
- **Cabir Worm:** It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
- **Mosquito Trojan:** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
- **Brador Trojan:** It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conducive to traditional worm propagation vector such as E-Mail file attachments.
- **Lasco Worm:** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

2. Denial-of-service (DoS): The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber security threats to wired Internet service providers (ISPs) is a distributed denial-of-service (DDoS) attack. DDoS

attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

3. Overbilling attack: Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.

4. Spoofed policy development process (PDP): These attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].

5. Signaling-level attacks: The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Today belongs to "mobile computing," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment

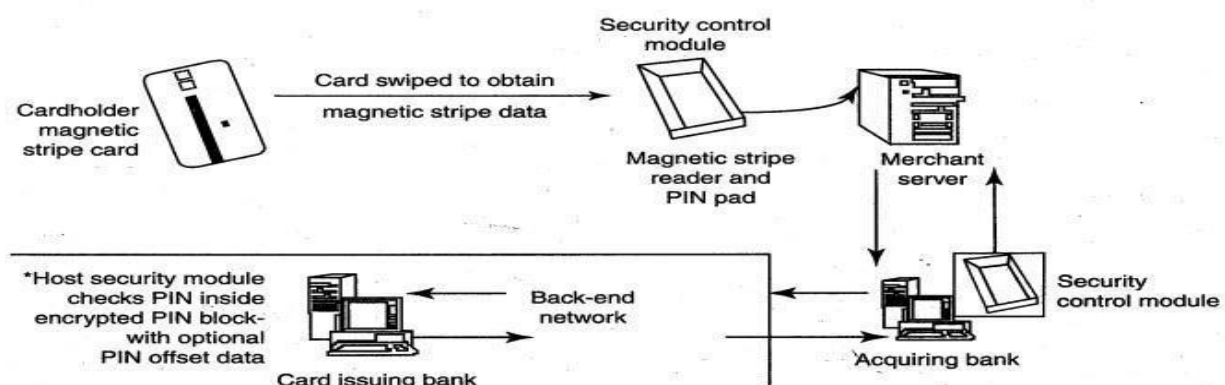


Figure : Online environment for credit card transactions

There is a system available from an Australian company "Alacrity" called closed-loop environment for for wireless (CLEW). Figure above shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in Figure, the basic flow is as follows:

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)

4. The bank/merchant is notified
5. The credit card transaction is completed.

Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in below figure. As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macro- challenges."

Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API), security etc.

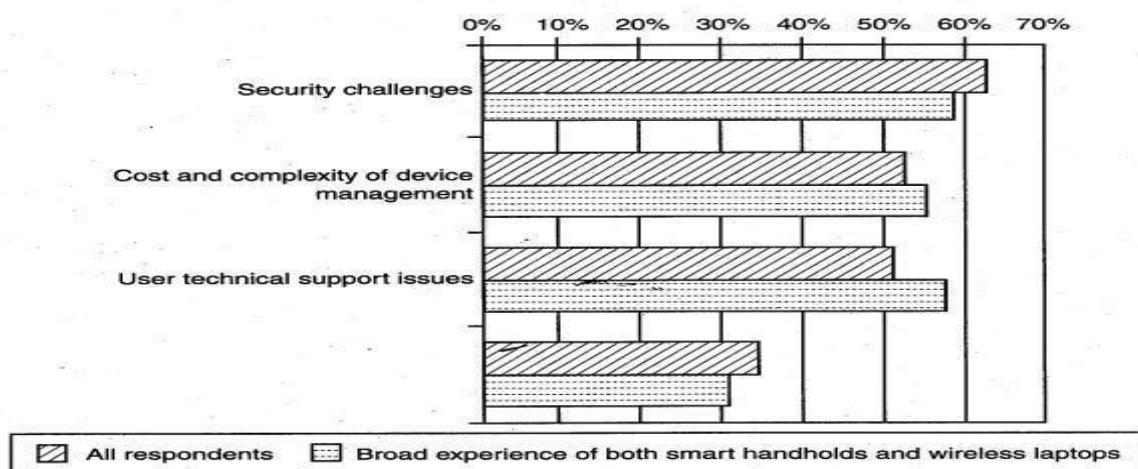


Figure: Important issues for managing mobile devices

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the "gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.

In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Authentication Service Security:

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves authentication between the device and the

base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.

Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.

Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

- **Mobile Phone Theft:**

Mobile phones have become an integral part of everybody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also led to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.

The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.

2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

- [Mobile - Viruses](#)
- [Concept of Mishing](#)
- [Concept of Vishing](#)
- [Concept of Smishing](#)
- [Hacking - Bluetooth](#)

Organizational security Policies and Measures in Mobile Computing Era:

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile

computing devices than their employers or they themselves know; they listen to music using their hand-held devices. One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.,
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized
7. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Organizational Policies for the Use of Mobile Hand-Held Devices

There are many ways to handle the matter of creating policy for mobile devices. One way is creating distinct mobile computing policy. Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one. In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time that they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless. Also, employees who use mobile devices more than 20% of

the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs .

Concept of Laptops:

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable. Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive..

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees' laptops and to reduce the likelihood that employees will lose laptops.

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

2. Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.

3. Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn

makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or key employees of the organizations.

5. Other measures for protecting laptops are as follows:

- Engraving the laptop with personal details
- Keeping the laptop close to oneself wherever possible
- Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves
- Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop
- Making a copy of the purchase receipt, laptop serial number and the description of the laptop
- Installing encryption software to protect information stored on the laptop
- Using personal firewall software to block unwanted access and intrusion
- Updating the antivirus software regularly
- Tight office security using security guards and securing the laptop by locking it down in lockers when not in use
- Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an anti theft device;
- Disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

Information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical or access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/ access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handling of removable drives/storage mediums /unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls / intrusion detection system (IDSs).
10. Encrypting critical file systems.

4 Tools and Methods Used in Cybercrime

Learning Objectives

After reading this chapter, you will be able to:

- Understand about proxy servers and anonymizers.
 - Learn about password cracking.
 - Learn what keyloggers and Spywares do.
 - Get an overview of virus and worms.
 - Learn about Trojan Horses and backdoors.
 - Understand what steganography is.
 - Learn about DoS and DDoS attacks.
 - Learn about SQL injection.
 - Understand buffer overflow.
 - Get an overview of wireless network hacking.
-

4.1 Introduction

In Chapter 2, we have learnt about how criminals/attackers plan cyberoffenses against an individual and/or against an organization. In Chapter 3, we have learnt how mobile technology plays an important role to launch cyberattacks. With this background, in this chapter, we will focus upon different forms of attacks through which attackers target the computer systems. There are various tools and techniques (see Box 4.1) and complex methodologies used to launch attacks against the target. Although discussing all of them is virtually impossible in a single chapter, yet still, we have provided an insight toward these techniques to enable the reader to understand how the computer is an indispensable tool for almost all cybercrimes. As the Internet and computer networks are integral parts of information systems, attackers have in-depth knowledge about the technology and/or they gain thorough knowledge about it. (See Section 10.4.2, Chapter 10 in CD.)

Network attack incidents reveal that attackers are often very systematic in launching their attacks (see Section 7.13, Chapter 7). The basic stages of an attack are described here to understand how an attacker can compromise a network here:

1. **Initial uncovering:** We have explained this in Chapter 2. Two steps are involved here. In the first step called as *reconnaissance*, the attacker gathers information, as much as possible, about the target by legitimate means - searching the information about the target on the Internet by Googling social networking websites and people finder websites. The information can also be gathered by surfing the public websites/searching news articles/press releases if the target is an organization/institute. In the second step, the attacker uncovers as much information as possible on the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges. From prevention perspective, at this stage, it is really not possible to detect the attackers because they have done nothing illegal as yet and so their information requests are considered legitimate.

Box 4.1 Scareware, Malvertising, Clickjacking and Ransomware

1. **Scareware:** It comprises several classes of scare software with malicious payloads (explained in chapter 1), or of limited or no benefit, which are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat, generally directed at an unsuspecting user. Some forms of Spyware and Adware also use scareware tactics. Some websites display pop-up advertisement windows or banners with text such as: "Your computer may be infected with harmful Spyware programs. Immediate removal may be required. To scan, click 'Yes' below." These websites can go as far as saying that a user's job, career or marriage would be at risk. Websites displaying such advertisements for such products are often considered as scareware. Serious scareware applications qualify as rogue software.
2. **Malvertising:** It is a malicious advertising - malware + advertising - an online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space. Cybercriminals attempt to distribute malware through advertising. Possible vectors of attack include Malicious Code hidden within an advertisement, embedded into a webpage or within software which is available for download.
3. **Clickjacking:** It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages. Clickjacking takes the form of embedded code and/or script which is executed without netizens' knowledge. Cybercriminals take the advantage of vulnerability across a variety of browsers and platforms to launch this type of attack. For example, clicking on a button that appears to perform another function. The term "clickjacking" was coined by Jeremiah Grossman and Robert Hosen in 2008. The exploit is also known as User-Interface (UI) redressing.
4. **Ransomware:** It is computer malware that holds a computer system, or the data it contains, hostage against its user by demanding a ransom for its restoration. It typically propagates as a conventional computer worm, entering a system through, for example, vulnerability in a network service or an E-Mail attachment. It may then
 - disable an essential system service or block the display at system start-up and
 - encrypt some of the user's personal files.

In both cases, the malware may extort by

- prompting the user to enter a code obtainable only after wiring payment to the attacker or sending an SMS message and accruing a charge;
- urging the user to buy a decryption or removal tool.

Sources: <http://en.wikipedia.org/wiki/Scareware> (10 January 10); <http://www.anti-malvertising.com/> [10 January 10]; <http://en.wikipedia.org/wiki/Clickjacking> (10 February 10); [http://en.wikipedia.org/wiki/Ransomware_\(malware\)](http://en.wikipedia.org/wiki/Ransomware_(malware)) (10 January 10)

2. **Network probe:** At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool (see Table 2.2) is used to discover exactly which services are running on the target system. At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.
3. **Crossing the line toward electronic crime (crime):** Now the attacker is considering what is technically a "computer crime." He/she does this by exploiting possible holes on the target system. The attacker usually goes through several stages of exploits to gain access to the system. Certain programming errors can be used by attackers to compromise a system and are quite common in practice (see Table 4.1 for list of website... commonly browsed by attackers to obtain the information on the vulnerabilities). Exploits usually include vulnerabilities in common gateway interface (CGI) scripts or well-known buffer-overflow holes, but the easiest way to gain an entry is by checking for default login accounts with easily guessable (or empty) passwords. Once the attackers are able to access a user account without many privileges, they will attempt further exploits to get an administrator or "root" access. Root access is a Unix term

Table 4.1 Websites and tools used to find the common vulnerabilities

Website	Brief Description
http://www.us-cert.gov/	US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (OHS). US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the US government about cybersecurity. US-CERT publishes information about a variety of vulnerabilities under "US-CERT Vulnerabilities Notes."
http://eve.mitre.org/	Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures and free for public use. CVE's common Identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
http://secunia.com/	It has thousands of vulnerability lists that are updated periodically. It has a vulnerability database and provides in-depth analysis about virus, worm alerts and software vulnerability.
http://www.hackmorm.com/	This website was created for open-source vulnerability database (OSVDB) tool. Since then it has grown in popularity and provides additional information about penetration testing. The site is updated with whole bunch of news and alerts about vulnerability research.
http://www.hackerwatch.org/	It is an online community where Internet users can report and share information to block and identify security threats and unwanted traffic.
http://www.wne-h.org/	It reports on recent web attacks and cybercrimes and lists them on the website. One can view numerous defaced webpages and details about them.
http://www.milworm.com/	It contains day-wise information about exploits.
http://www.osvdb.org/	OSVDB: This is an open-source vulnerability database providing a large quantity of technical information and resources about thousands of vulnerabilities.
http://www.metasploit.com/	Metasploit is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing. Its most well-known subproject is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. The Metasploit Project is also well-known for antiforensic and evasion tools, some of which are built into the Metasploit Framework.
http://www.w00w00.org/files/ LibExploit	LibExploit is a generic exploit creation library. It helps cybersecurity community when writing exploits to test vulnerability.
http://www.immunitysec.com/products-canvas.shtml	Canvas is a commercial vulnerability exploitation tool from Dave Aitd's ImmunitySec. It includes more than 150 exploits and also available are VisualSploit Plugio for drag and drop CUI exploit creation (optional).
http://www.coresecurity.com/concent/core-impact-overview	Core Impact is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits and can do neat tricks such as exploiting one system and then establishing an encrypted tunnel through that system to reach and exploit other systems.

and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems). "Root" is basically an administrator or super-user access and grants them the privileges to do anything on the system.

4. **Capturing the network:** At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack. "The attacker will usually install a set of tools that replace existing files and services with Trojan files (*Trojan Horse* is further discussed in detail in this chapter) and service... which have a backdoor password. There are a number of "hacking tools" which can clean up log files and remove any trace of an intrusion; most of the time, they are individual programs written by hackers. Such tools provide copies of system files that look and act like real things, but in fact they provide the attacker a backdoor entry into the system and hide processes he/she might be running on the system and his/her user information. This allows the attacker to return to the system at will, which means that the attacker has "captured" the network. Once the attacker has gained access to one system, he/she will then repeat the process by using the system as a stepping stone to access other systems deeper within the network, as most networks have fewer defenses against attacks from internal sources.
5. **Grab the data:** Now that the attacker has "captured the network," he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface webpages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.
6. **Covering tracks:** This is the last step in any cyberattack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected. The attacker can remain undetected for long periods or use this phase either to start a fresh reconnaissance to a related target system or continued use of resources, removing evidence of hacking, avoiding legal action, etc. (See table 4.210 for tools used to cover tracks.)

During the entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself. How it is possible is described in the next section.

Table 4.2 | Tools used to cover tracks

Sr. No.	Website	Brief Description
	http://www.ibr.ku.dk/jesper/ELSave/	ELSave: It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. Its executable is available on the weblink, but source code is not available.
2	http://nccsecurity.ru/toolbox/winzipper/	WinZipper: This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely.
3	http://www.evidence-eliminator.com/ http://www.traceless.com/computer-forensics/	Evidence eliminator: It is simple and one of the top-quality professional PC cleaning programs that is capable of defeating a known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible. Traceless: It is a privacy cleaner for Internet Explorer (IE) that can delete common Internet tracks, including history, cache, saved URLs, cookies, etc.

(Continued)

Table 4.2 | (Continued)

Sr. No.	Website	Brief Description
5	http://www.acesofr.net/	<p>Tracks Eraser Pro: It deletes following history data:</p> <ul style="list-style-type: none"> • Delete address bar history of IE, Netscape, AOL, Opera. • Delete cookies of IE, Netscape, AOL, Opera. • Delete Internet cache (temporary Internet files). • Delete Internet history files. • Delete Internet search history. • Delete history of auto complete. • Delete IE plugins (selectable). • Delete index.dat file. • Delete history of start menu run box. • Delete history of scan menu search box. • Delete windows temp files. • Delete history of open/save dialog box. • Empty recycle bin.

4.2 Proxy Servers and Anonymizers

Proxy server is a computer on a network which acts as an intermediary for connections with other computers on that network.

The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy. This enables an attacker to surf on the Web anonymously and/or hide the attack. A client connects to the proxy server and requests some services (such as a file, webpage, connection or other resource) available from a different server. The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client. Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

A proxy server has following purposes:

1. Keep the systems behind the curtain (mainly for security reasons).
2. Speed up access to a resource (through "caching"). It is usually used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the internet, whenever one has only one IP address (visit <http://www.multiproxy.org/multiproxy.htm> for more information).

One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy's cache memory, which will improve user response time. In fact there are special servers available known as *cache servers*. A proxy can also do logging.

Listed are few websites where free proxy servers can be found:

1. <http://www.proxy4free.com>
2. <http://www.publicproxyservers.com>

3. <http://www.proxz.com>
4. <http://www.anonymitychecker.com>
5. <http://www.surf14h.com>
6. <http://www.hidemyass.com>

An *anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.¹ Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client. In 1997 the first anonymizer software tool was created by Lance Cottrell, developed by Anonymizer.com. The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the Internet, which ensures the privacy of the user. (See Section 9.7, Chapter 9.)

Listed are few websites where more information about anonymizers can be found:

1. <http://www.anonymizer.com>
2. <http://www.browzar.com>
3. <http://www.anonymize.net>
4. <http://www.anonymouse.ws>
5. <http://www.anonymousindex.com>

Box 4.2 Being Anonymous While Searching on Google!

Google Cookie

Google was the first search engine to use a cookie.² Google set the standard and nowadays cookies are commonplace among search engines. This cookie places a unique ID number on your hard disk. Anytime you visit Google, user gets a Google cookie if a user doesn't already have one. If a user has one then it will read and record the unique ID number. Google can build a detailed list of your search terms over many years. (Google's cookies are set to expire by the year 2038, unless a user deletes before its expiry.)

Cookie

Cookie (also known as HTTP cookie/browser cookie) is a small text file that contains a string of alphanumeric characters and is used for storing netizen's website preferences/authentication while visiting the same webpage again and again or also acts as identifier for server-based session - such browser mechanism of setting and reading cookies invites attackers to use these cookies as "Spyware." There are two types of cookies:

1. Persistent cookie and
2. session cookie.

Persistent cookie is stored by the web browser into the cookie folder on the PC's hard disk. It remains under the cookie folder, which is maintained by the web browser. Session cookie is a temporary cookie and does not reside on the PC once the browser is closed (see Boxes 9.2, 9.3 and 9.4, Chapter 9).

DoubleClick

It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing (DART Search³) and utilize the cookies, which are called DART cookie. Internet Advertising Network was started by Kevin O'Connor and Dwight Merriman in 1995. IAN and the DoubleClick division of Poppe.Tyson were merged into a new corporation named DoubleClick in 1996. DoubleClick was first in the online media representative business, that is, representing websites to sell advertising space to marketers. In 1997 it began offering the online ad serving and management technology they had

Box 4.2 Being Anonymous ... (Continued)

developed to other publishers as the DART services. The DART cookie is a persistent cookie, which consists of the name of the domain that has set the cookie, the lifetime of the cookie and a "value." DoubleClick's DART mechanism generates a unique series of characters for the "value" portion of the cookie. These DoubleClick DART cookies help marketers learn how well their Internet advertising campaigns or paid search listings perform. Many marketers and Internet websites use DoubleClick's DART technology to deliver and serve their advertisements or manage their paid search listings. DoubleClick's DART products set or recognize a unique, persistent cookie when an ad is displayed or a paid listing is selected. The information that the DART cookie helps to give marketers includes the number of unique users their advertisements displayed to, how many users clicked on their Internet ads or paid listings and which ads or paid listings they clicked on.

G-Zapper


G-Zapper¹⁴¹ utility helps to stay anonymous while searching Google. Google stores a unique identifier in a cookie on the computer (i.e., on the hard disk) which allows to track keywords that are searched for. This information is used to compile reports, track user habits and test features. In the future, it would be possible that this information is sold and/or shared with others.

G-Zapper helps to protect users' ID and search history. G-Zapper reads the Google cookie installed on users' PC, displays the date it was installed, determines how long user searches have been tracked and displays Google searches. G-Zapper allows user to automatically delete or entirely block the Google search cookie from future installation.

This utility can be downloaded from <http://www.dummysoftware.com/gzopper.html>

4.3 Phishing

While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail. This message and other such messages are examples of Phishing - in addition to stealing personal and financial data - and can infect systems with viruses and also a method of online ID theft in various cases. Most people associate Phishing with E-Mail messages that spoof or mimic banks, credit card companies or other business such as Amazon and eBay. These messages look authentic and attempt to get users to reveal their personal information.

 It is believed that *Phishing* is an alternative spelling of "fishing," as in "to fish for information." The first documented use of the word "Phishing" was in 1996.

4.3.1 How Phishing Works?

Phishers work in the following ways[S]:

1. **Planning:** Criminals, usually called as phishers, decide the target (i.e., specific business/business house/an individual) and determine how to get E-Mail address of that target or customers of that business. Phishers often use mass mailing and address collection techniques as spammers.
2. **Setup:** Once phishers know which business/business house to spoof and who their victims are, they will create methods for delivering the message and to collect the data about the target. Most often this involves E-Mail addresses and a webpage.

3. **Attack:** This is the step people are most familiar with - the phisher sends a phony message that appears to be from a reputable source.
4. **Collection:** Phishers record the information of victims entering into webpages or pop-up windows.
5. **Identity theft and fraud:** Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Phishing started off as being part of popular hacking culture. Nowadays, more and more organizations/institutions provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level. We have explained Phishing and Identity Theft in detail in Chapter 5.

4.4 Password Cracking

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords and data that have been stored in or transmitted by a computer system.¹⁶¹ Usually, an attacker follows a common approach - repeatedly making guesses for the password. The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to log on with different passwords. The attacker follows the following steps:

1. Find a valid user account such as an Administrator or Guest;
2. create a list of possible passwords;
3. rank the passwords from high to low probability;
4. key-in each password;
5. try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information (explained in Chapter 5). Examples of guessable passwords include:

1. Blank (none);
2. the words like "password," "passcode" and "admin";
3. series of letters from the "QWERTY" keyboard, for example, qwerty, asdf or qwertyuiop;
4. user's name or login name;
5. name of user's friend/relative/parent;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actresses, spiritual gurus) by the user;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list. This is still considered manual cracking, is time-consuming and not usually effective.

Passwords are stored in a database and password verification process is established into the system when a user attempts to login or access a restricted resource. To ensure confidentiality of passwords, the

password verification data is usually not stored in a clear text format. For example, one-way function (which may be either an encryption function or a cryptographic hash) is applied to the password, possibly in combination with other data, and the resulting value is stored. When a user attempts to login to the system by entering the password, the same function is applied to the entered value and the result is compared with the stored value. If they match, user gains the access; this process is called *authentication*.

Even though these functions create hashed passwords, which may be cryptographically secure, an attacker attempts to get possession of the hashed password, which will help to provide a quick way to test guesses for the password by applying the one-way function to each guess and comparing the result to the verification data. The most commonly used hash functions can be computed rapidly and the attacker can test these hashes with the help of passwords cracking tools (see Table 4.3) to get the plain text password.

Table 4.3 Password cracking tools

Website	Brief Description
www.defaultpassword.com	Default password(s): Network devices such as switches, hubs and routers are equipped with "default passwords" and usually these passwords are not changed after commissioning these devices into the network (i.e., into LAN). The intruders can gain the access using these default passwords by visiting the said website.
http://www.oxid.ir/cain.html	Cain & Abel: This password recovery tool is typically used for Microsoft Operating Systems (OSs). It allows to crack the passwords by sniffing the network, cracking encrypted passwords using dictionary, brute force attacks, decoding scrambled passwords and recovering wireless network keys.
http://www.openwall.com/john	John the Ripper: This is a free and open-source software - a password cracker, compatible with many OSs like different flavors of Unix, Windows, DOS, BeOS and OpenVMS. Its primary purpose is to detect weak Unix passwords.
http://frecworld.tbc.org/thc-hydra	THC-Hydra: It is a very fast network logon cracker which supports many different services.
http://www.aircrack-ng.org	Aircrack-ng: It is a set of tools used for wireless networks. This tool is used for 802.11a/b/g wired equivalent privacy (WEP) and Wi-Fi Protected Access (WPA) cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force.
http://www.l0phtcrack.com	L0phtCrack: It is used to crack Windows passwords from hashes which it can obtain from stand-alone Windows workstations, networked servers, primary domain controllers or Active Directory. It also has numerous methods of generating password guesses (dictionary, brute force, etc.).
http://airsnort.shmoo.com	AirSnort: It is a wireless LAN (WLAN) tool which recovers WEP encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. It requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. It runs under Windows or Linux.

(Continued)

Table 4.3 (Continued)

Website	Brief Description
http://www.solarwinds.com	SolarWinds: It is a plethora of network discovery/monitoring/attack tools and has created dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, a Simple Network Management Protocol (SNMP) brute force cracker, router password decryption and more.
http://www.foofus.net/figig/pwdump	Pwdump: It is a Windows password recovery tool. Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is <i>also</i> capable of displaying password histories if they are available.
http://projecr-rainbowcrack.com	RainbowCrack: It is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plain texts one by one, which can be time-consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called "rainbow tables." It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.
http://www.hoobie.net/brutus	Brutus: It is one of the fastest, most flexible remote password crackers available for free. It is available for Windows 9x, NT and 2000. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP and more.

Password cracking attacks can be classified under three categories as follows:

1. Online attack ;
2. offline attacks;
3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving are explained in Chapter 2).

4.4.1 Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack." It is a form of active eavesdropping^[71] in which the attacker establishes a connection between a victim and the server to which a victim is connected. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password and passes the connection to the victim server (e.g., an attacker within reception range of an unencrypted Wi-Fi wireless access point can insert himself as a man-in-the-middle). This type of attack is used to obtain the passwords for E-Mail accounts on public websites such as Yahoo, Hotmail and Gmail and can also be used to get the passwords for financial websites that would like to gain the access to banking websites.

4.4.2 Offline Attacks

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used. Offline attacks usually require physical

Table 4.4 | Types of password cracking attacks

<i>Type of Attack</i>	<i>Description</i>	<i>Example of a Password</i>
Dictionary attack	Attempts to match all the words from the dictionary to get the password	Adminiscracor
Hybrid attack	Substitutes numbers and symbols to get the password	Adm In lscrator
Brute force attack	Attempts all possible permutation-combinations of letters, numbers and special characters	Adm!n@09

access to the computer and copying the password file from the system onto removable media. Different types of offline password attacks are described in Table 4.4. Few tools listed in Table 4.2 also use these techniques to get the password in the clear text format.

4.4.3 Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found by executing a brute force attack and by using a subset of all possible passwords, such as words in the dictionary, proper names and words based on the username or common variations on these themes. Passwords that can be easily guessed by acquaintances of the netizens (such as date of birth, pet's name and spouses' name) are considered to be very weak. Here are some of the examples of "weak passwords":

1. Susan: Common personal name;
2. aaaa: repeated letters, can be guessed;
3. rover: common name for a pet, also a dictionary word;
4. abc123: can be easily guessed;
5. admin: can be easily guessed;
6. 1234: can be easily guessed;
7. QWERTY: a sequence of adjacent letters on many keyboards;
8. 12/3/75: date, possibly of personal importance;
9. nbusr123: probably a username, and if so, can be very easily guessed;
10. p@\$\$Word: simple letter substitutions are preprogrammed into password cracking tools;
11. password: used very often - trivially guessed;
12. December12: using the date of a forced password change is very common.

A strong password is long enough, random or otherwise difficult to guess - producible only by the user who chooses it. The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease with which a password can be tried and the value of the password to the attacker. A student's password might not be worth more than a few seconds of computer time, while a password controlling access to a large bank's electronic money transfer system might be worth many weeks of computer time for trying to crack it. Here are some examples of strong passwords:

1. Convert_£100 to Euros!: Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
2. 382465304H: It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly, for example, in schools and business.
3. 4pRte!ai@3: It is not a dictionary word: however it has cases of alpha along with numeric and punctuation characters.

4. MoOoOAn245679: It is long with both alphabets and numerals.
5. t3wabSetyeT4: It is not a dictionary word; however, it has both alphabets and numerals.

Visit <http://www.microsoft.com/protect/fraud/p-words/checker.aspx> to check the strength of your password.¹⁸¹

4.4.4 Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper and lower case letters, numbers and other symbols, when allowed, for the same number of characters. The difficulty in remembering such a password increases the chance that the user *will* write down the password, which makes it more vulnerable to a different attack (in this case, the paper being lost or stolen and the password discovered). Whether this represents a net reduction in security depends on whether the primary threat to security is internal (e.g., social engineering) or external. A password can, at first sight, be random, but if you really examine it, it is just a pattern. One of these types of passwords is 26845. Although short, it is not easily guessed. However, the person who created the password is able to remember it because it is just the four direction keys on the square number board (found at the right of most keyboards) plus a five in the middle. If you practice it, it is just one swift motion of moving two fingers around the board (which is very *easy* to use). Forcing users to use system-created random passwords ensures that the password will have no connection with each user and should not be found in any dictionary. Several OSs have included such a feature. Almost all the OSs also include password aging; the users are required to choose new passwords regularly, usually after 30 or 45 days. Many users dislike these measures, particularly when they have not been taken through security awareness training. The imposition of strong random passwords may encourage the users to write down passwords, store them in personal digital assistants (PDAs) or cell phones and share them with others against memory failure, increasing the risk of disclosure.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user login identifiers (IDs) should be unique to each authorized user.
2. Passwords should consist of a minimum of eight alphanumeric characters (no common names or phrases).
3. There should be computer-controlled lists of prescribed password rules and periodic testing (e.g., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
4. Passwords should be kept private, that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
5. Passwords shall be changed every 30/45 days or less. Most operating systems (OSs) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
6. User accounts should be frozen after five failed login attempts. All erroneous password entries should be recorded in an audit log for later inspection and action, as necessary.
7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.
8. Successful logons should display the date and time of the last login and logoff.
9. Login IDs and passwords should be suspended after a specified period of non-use.
10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user (to keep this user connected while personnel attempt to investigate the incoming connection).

Similarly, citizens should practice password guidelines to avoid being victim of getting their personal E-Mail accounts hacked/attacked by the attackers.

1. Passwords used for business E-Mail accounts, personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be kept separate.
2. Passwords should be of minimum eight alphanumeric characters (common names or phrases should be phrased).
3. Passwords should be changed every 30/45 days.
4. Passwords should not be shared with relatives and/or friends.
5. Password *used* previously should not be used while renewing the password.
6. Passwords of personal E-Mail accounts (Yahoo/Hotmail/Gmail) and banking/financial user accounts (e.g., online banking/securities trading accounts) should be changed from a secured system, within couple of days, if these E-Mail accounts have been accessed from public Internet facilities such as cybercafes/hotels/libraries.
7. Passwords should not be stored under mobile phones/PDAs, as these devices are also prone to cyber-attacks (explained in Section 3.8, Chapter 3).
8. In the case of receipt of an E-Mail from banking/financial institutions, instructing to change the passwords, before clicking the weblinks displayed in the E-Mail, legitimacy of the E-Mail should be ensured to avoid being a victim of Phishing attacks (we will explain Phishing attack in detail in Chapter 5).
9. Similarly, in case of receipt of SMS from banking/financial institutions, instructing to change the passwords, legitimacy of the E-Mail should be ensured to avoid being a victim of Smishing attacks (explained in detail in Chapter 3).
10. In case E-Mail accounts/user accounts have been hacked, respective agencies/institutes should be contacted immediately.

4.5 Keyloggers and Spywares

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.¹⁹¹

Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

4.5.1 Software Keyloggers

Software keyloggers are software programs (see Table 4.5) installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruses (will discuss more on this in subsequent sections of this chapter) without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafes, library - we have already discussed this in Chapter 2) and can obtain the required information about the victim very easily. A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. It does all the recording of keystrokes.¹⁹¹

Table 4.5 Software keyloggers

Website	Brief Description
http://www.soft-cencral.net	SC-KeyLog PRO: It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected logfile. SC-KeyLog PRO also captures Windows user login passwords. The captured information is completely hidden from the user and allows to remotely install the monitoring system through an E-Mail attachment without the user recognizing the installation at all.
http://www.spytech-web.com	Spytech SpyAgent Stealth: It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.
http://www.relytec.com	All In One Keylogger: It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs. This keylogger allows secretly tracking of all activities from all computer users and automatically receiving logs to a desired E-Mail/FTP account. With this keylogger, one can read chat conversations, look at the E-Mails as well as watch the sites that have been surfed.
http://www.stealthkeylogger.org	Stealth Keylogger: It is a computer monitoring software that enables an invisible log report where the entire PC keyboard activities are recorded daily on a specific time or hourly on daily basis. The entire log reports are generated either in text or HTML file format as defined by the user. The keylogger facilitates mailing of log report at the specified E-Mail address.
http://www.blainetools.com	Perfect Keylogger: It has its advanced keyword detection and notification. User can create a list of "on alert" words or phrases and keylogger will continually monitor keyboard typing, URLs and webpages for these words or phrases - for example, "bomb," "sex," "visiting places around Mumbai" and "Windows vulnerabilities." When a keyword is detected, perfect keylogger makes screenshot and sends E-Mail notification to the user.
http://kgb-spy-software.en.softonic.com	KGB Spy: It is a multifunctional keyboard tracking software, widely used by both regular users and IT security specialists. This program does not just record keystrokes but is also capable of recording language-specific characters. It records all typed data/all keyboard activity. It can be used to monitor children's activity at home or to ensure employees do not use company's computers inappropriately. Visit www.refog.com to find more on this product.
http://www.spy-guide.net/spybuddy-spy-software.htm	Spy Buddy: This, along with keylogger, has following features: <ul style="list-style-type: none"> • Internet conversation logging; • disk activity logging; • Window activity logging; • application activity logging; • clipboard activity logging; • AOL/Internet explorer history; • printed documents logging; • keylogger keystroke monitoring; • websites activity logging; • screenshot capturing; • WebWarch keyword alerting

Table 4.5 | (Continued)

<i>Website</i>	<i>Brief Description</i>
http://www.elire-keylogger.com	Elite Keylogger: It captures ever)' keystroke typed, all passwords (including Windows logon passwords), chats, instant messages, E-Mails, websites visited, all program launched, usernames and time they worked on the computer, desktop activity, clipboard, etc.
http://www.cyberspysoftware.com	CyberSpy: It provides an array of features and easy-to-use graphical interface along with computer monitoring capabilities such as keep tabs on the employees and keeps track of what children are viewing on the Internet. CyberSpy can be used as complete PC monitoring solution for any home or office. CyberSpy records all websites visited, instant message conversations, passwords, E-Mails and all keystrokes pressed. It also has the ability to provide screenshots at set intervals.
http://www.mykeylogger.com	<p>Powered Keylogger: Powered keylogger can be used for the following:</p> <ul style="list-style-type: none"> • <i>Surveillance</i>: It is for anyone to control what happens on the computer while the computer's owner is away. • <i>Network administration</i>: It is for network administrators to control outgoing traffic and sites visited. • <i>Shared PC activity tracking</i>: It is to analyze the usage of shared PC. • <i>Parental control</i>: It helps parents to monitor their children's computer and Internet activity. • <i>Employee productivity monitoring</i>: It helps managers to check and increase productivity of their staff or just to prevent the leak of important information.
http://www.x-pcsoft.com	<p>XPC Spy: XPC Spy is one of the powerful keylogger spy software, runs stealthy under MS Windows and has the following features:</p> <ul style="list-style-type: none"> • Records all keystrokes typed; • records all websites visited; • records all programs executed, folders explored, files opened or edited, documents printed, etc.; • records all windows opened; • records all clipboard text content; • records all system activities; • records webmails sent (database update online, more and more webmail servers are supported); • records all ICQ Messenger chat conversations; • records all MSN Messenger chat conversations; • records all AOL/AIM Messenger chat conversations; • records all Yahoo! Messenger chat conversations; • runs invisible in the background and is protected by password; • is built-in screenshot pictures viewer; • schedules monitor process, users time to start or stop monitoring; • sends logs report via E-Mail.

4.5.2 Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs. Each keypress on the keyboard of the ATM gets registered by these keyloggers. These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

Listed are few websites where more information about hardware keyloggers can be found:

1. <http://www.keyghosr.com>
2. <http://www.keelog.com>
3. <http://www.keydevil.com>
4. <http://www.keykarcher.com>

4.5.3 Antikeylogger

Antikeylogger¹¹¹ is a tool that can detect the keylogger installed on the computer system and also can remove the tool. Visit <http://www.anti-keyloggers.com> for more information.

Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk.
3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
4. It prevents ID theft (we will discuss it more in Chapter 5).
5. It secures E-Mail and instant messaging/chating.

4.5.4 Spywares

Spyware is a type of malware (i.e., malicious software - see Box 4.3 to know about different types of malwares) that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden from the user; it is secretly installed on the user's personal computer. Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.¹¹¹

It is clearly understood from the term *Spyware* that it secretly monitors the user. The features and functions of spyware are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect Internet surfing activities by installing another stealth utility on the users' computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Provider (ISP). Various Spywares are available in the market and the ones that are popular are listed in Table 4.6.

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares (refer to Appendix 8: List of Useful Software Utilities and Websites in CO) are available in the market. Installation of anti-Spyware software has become a common element nowadays from computer security practices perspective.

Box 4.3 Malwares

Malware, short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent (see Box 9.8. Chapter 9). The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive or annoying software or program code.¹¹³¹ Malware can be classified as follows:

1. **Viruses and worms:** These are known as *infectious malware*. They spread from one computer system to another with a particular behavior (will discuss more on this in Section 4.6).
2. **Trojan Horses:** A Trojan Horse,¹¹⁴¹ Trojan for short, is a term used to describe malware that appears to the user to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system (will discuss more on this in Section 4.7).
3. **Rootkits:** Rootkits¹¹⁵¹ is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised. For further details refer to Section 7.12.1, Chapter 7.
4. **Backdoors:** Backdoor¹¹⁶¹ in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected.
5. **Spyware:** For further details see Section 4.5.
6. **Botnets:** For further details see Section 2.6 in Chapter 2.
7. **Keystroke loggers:** For further details see Section 4.5.

Table 4.6 | Spywares

Website	Brief Description
http://www.e-spy-software.com	007 Spy: It has following key features: <ul style="list-style-type: none"> • Capability of overriding "antispy" programs like "Ad-aware"; • record all websites URL visited in Internet; • powerful keylogger engine to capture all passwords; • view logs remotely from anywhere at anytime; • export log report in HTML format to view it in the browser; • automatically clean-up on outdated logs; • password protection.
http://www.spectrsoft.com	Spector Pro: It has following key features: <ul style="list-style-type: none"> • Captures and reviews all chats and instant messages; • captures E-Mails (read, sent and received); • captures websites visited; • captures activities performed on social networking sites such as MySpace and Facebook; • enables to block any particular website and/or chatting with anyone; • acts as a keylogger to capture every single keystroke (including usernames and passwords).
http://www.speccorsoft.com	eBlaster: Besides keylogger and website watcher, it also records E-Mail sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording MySpace and Facebook activities and any other program activity.
http://www.rcmorspy.com	Remotespy: Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

(Continued)

Table 4.6 | (Continued)

<i>Website</i>	<i>Brief Description</i>
http://www.copofbesrsoft.com	<p>Stealth Recorder Pro: It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features:</p> <ul style="list-style-type: none"> • Real-time MP3 recording via microphone, CD, line-in and stereo mixer as MP3, WMA or WAV formatted files; • transferring via E-Mail or FTP, the recorded files to a user-defined E-Mail address or FTP automatically; • controlling from a remote location; • voice mail, records and sends the voice messages.
http://www.amplusnet.com	<p>Stealth Website Logger: It records all accessed websites and a detailed report can be available on a specified E-Mail address. It has following key features:</p> <ul style="list-style-type: none"> • Monitor visited websites; • reports sent to an E-Mail address; • daily log; • global log for a specified period; • log deletion after a specified period; • honey and password protection; • not visible in add/remove programs or task manager.
http://www.flexispy.com	<p>Flexispy: It is a cool char can be installed on a cell/mobile phone. After installation, Flexispy secretly records conversation that happens on the phone and sends this information to a specified E-Mail address.</p>
http://www.wiretappro.com	<p>Wiretap Professional: It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. This spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.</p>
http://www.pcphonehome.com	<p>PC PhoneHome: It is a software that cracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC PhoneHome has been installed, connected to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user's choice and to PC PhoneHome Producer Company.</p>
http://www.spyarsenal.com	<p>SpyArsenal Print Monitor Pro: It has following features:</p> <ul style="list-style-type: none"> • Keep track on a printer/plotter usage; • record every document printed; • find out who and when certain paper printed with your hardware.

4.6 Virus and Worms

Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. A virus can start on event-driven effects (e.g., triggered after a specific number of executions), time-driven effects (e.g., triggered on a specific date, such as Friday the 13th) or can occur at random. Viruses can take some typical actions:

1. Display a message to prompt an action which may set off the virus;
2. delete files inside the system into which viruses enter;
3. scramble data on a hard disk;
4. cause erratic screen behavior;
5. halt the system (PC);
6. just replicate themselves to propagate further harm.

figures 4.1-4.3 explain how viruses spread (a) through the Internet, (b) through a stand-alone computer system and (c) through local networks.

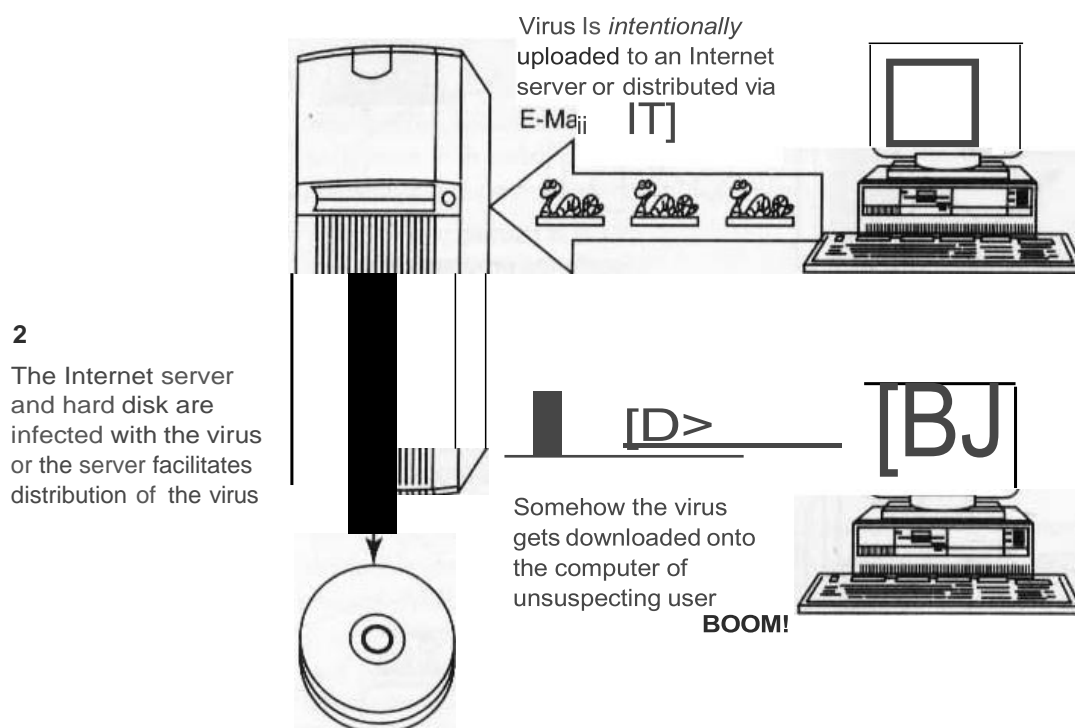


Figure 4.1 | Virus spreads through the Internet.

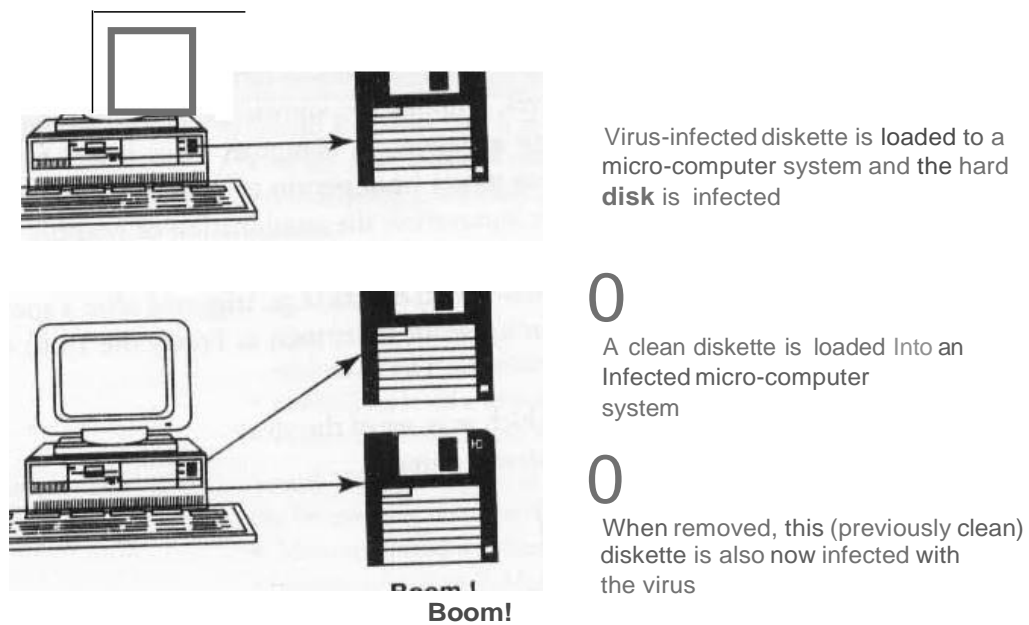


Figure 4.2 | Virus spreads through stand-alone system.

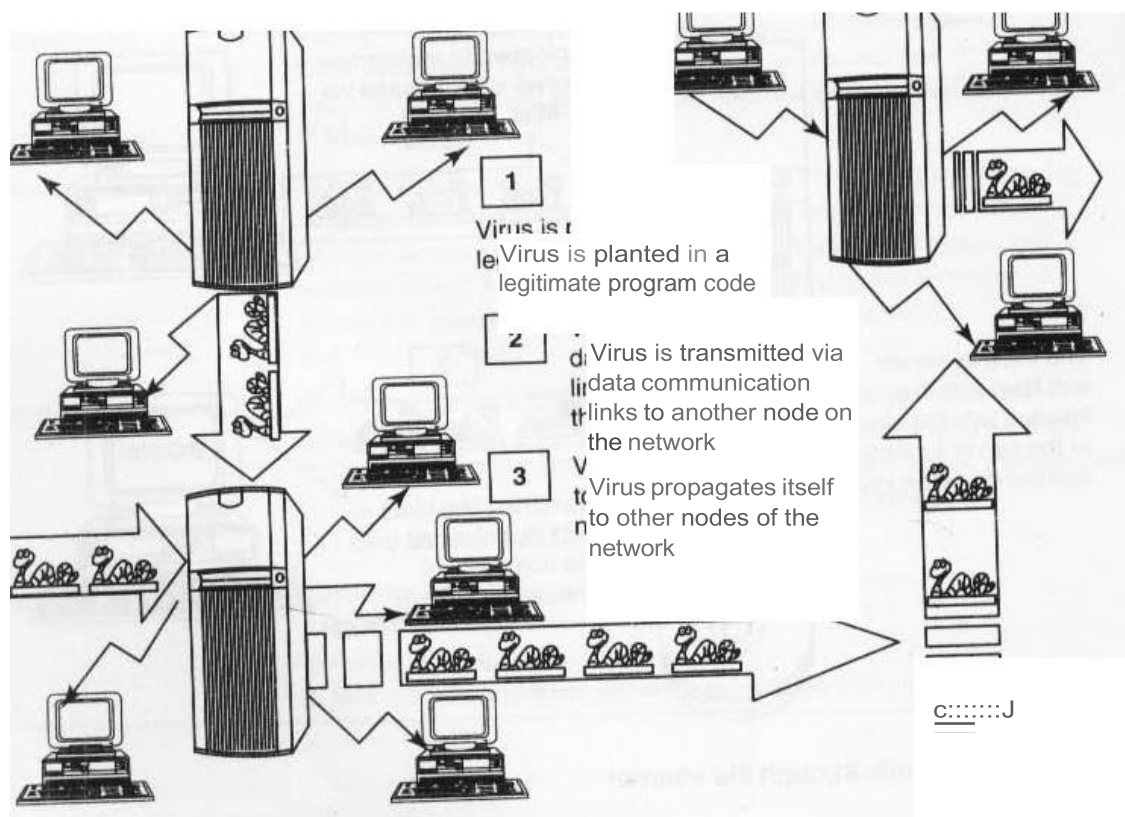


Figure 4.3 | Virus spreads through local networks.

Computer virus has the ability to copy itself and infect the system. The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability. A true virus can only spread from *one* system to another (in some form of executable code) when its host is taken to the target computer; for instance, when a user sends it over the Internet or a network, or carried it on a removable media such as CD, DVD or USB drives. Viruses can increase their chances of spreading to other systems by infecting files on a network file system or a file system that is accessed by another system.¹¹⁷¹

As explained in earlier sections, the term *computer virus* is sometimes used as a *catch-all phrase* to include all types of malware, Adware and Spyware programs that do not have reproductive ability. Malware includes computer viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, crimeware and other malicious and unwanted software as well as true viruses. Viruses are sometimes confused with computer worms and Trojan Horses, which are technically different (see Table 4.7 to understand the difference between computer virus and worm). A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions. Worms and Trojans, such as viruses, may harm the system's data or performance. Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them. Some virus do nothing beyond reproducing themselves.¹¹⁷¹

Table 4.7 | Difference between computer virus and worm

Sr. No.	Facet	Virus	Worm
	Different types	Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic code virus	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing worms, worms
2	Spread mode	Needs a host program to spread	Self, without user intervention
3	What is it?	A computer virus is a software program that can copy itself and infect the data or information, without the users' knowledge. However, to spread to another computer, it needs a host program that carries the virus	A computer worm is a software program, self-replicating in nature, which spreads through a network. It can send copies through the network with or without user intervention
4	Inception	The creeper virus was considered as the first known virus. It was spread through ARPANET in the early 1970s. It spreads through the TENEX OS and uses connected modem to dial out to a remote computer and infect it.	The name worm originated from the Shockwave Rider, a science fiction novel published in 1975 by John Brunner. Later researchers John F. Shock and Jon A. Hupp at Xerox PARC published a paper in 1982, <i>The Worm Programs</i> and after that the name was adopted
5	Prevalence	Over 100,000 known computer viruses have been there though not all have attacked computers (till 2005)	Prevalence for virus is very high as against moderate prevalence for a worm.

Source: See [18] in References section.

4.6.1 Types of Viruses

Computer viruses can be categorized¹¹⁹¹ based on attacks on various elements of the system and can put the system and personal data on the system in danger.

1. **Boot sector viruses:** It infects the storage media on which OS is stored (e.g., floppy diskettes and hard drives) and which is used to start the computer system. The entire data/programs are stored on the floppy disks and hard drives in smaller sections called sectors. The first sector is called the BOOT and it carries the master boot record (MBR). MBR's function is to read and load OS, that is, it enables computer system to start through OS. Hence, if a virus attacks an MBR or infects the boot record of a disk, such floppy disk infects victim's hard drive when he/she reboots the system while the infected disk is in the drive. Once the victim's hard drive is infected all the floppy diskettes that are being used in the system will be infected. Boot sector viruses often spread to other systems when shared infected disks and pirated software(s) are used.
2. **Program viruses:** These viruses become active when a program file (usually with extensions .bin, .com, .exe, .ovl, .drv) is executed (i.e., opened - program is started). Once these program files get infected, the virus makes copies of itself and infects the other programs on the computer system.
3. **Multipartite viruses:** It is a hybrid of a boot sector and program viruses. It infects program files along with the boot record when the infected program is active. When the victim starts the computer system next time, it will infect the local drive and other programs on the victim's computer system.
4. **Stealth viruses:** It camouflages and/or masks itself and so detecting this type of virus is very difficult. It can disguise itself such a way that antivirus software also cannot detect it thereby preventing spreading into the computer system. It alters its file size and conceals itself in the computer memory to remain in the system undetected. The first computer virus, named as Brain, was a stealth virus. A good antivirus detects a stealth virus lurking on the victim's system by checking the areas the virus must have infected by leaving evidence in memory.
5. **Polymorphic viruses:** It acts like a "chameleon" that changes its virus signature (i.e., binary pattern) every time it spreads through the system (i.e., multiplies and infects a new file). Hence, it is always difficult to detect polymorphic virus without the help of an antivirus program. *Polymorphic generators* are the routines (i.e., small programs) that can be linked with the existing viruses. These generators are not viruses but the purpose of these generators is to hide actual viruses under the cloak of polymorphism. The first all-purpose polymorphic generator was the mutation engine (MtE) published in 1991. Other known polymorphic generators are Dark Angel's Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns'n'Roses Polymorphic Engine (GPE) and Dark Slayer Confusion Engine (DSCE).
6. **Macroviruses:** Many applications, such as Microsoft Word and Microsoft Excel, support MACROS (i.e., macrolanguages). These macros are programmed as a macro embedded in a document. Once a macrovirus gets onto a victim's computer then every document he/she produces will become infected. This type of virus is relatively new and may get slipped by the antivirus software if the user does not have the most recent version installed on his/her system.
7. **Active X and Java Control:** All the web browsers have settings about Active X and Java Controls. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work - such as enabling or disabling pop-ups, downloading files and sound - which invites the threats for the computer system being targeted by unwanted software(s) floating in cyberspace.

To know more on viruses see Box 4.4 and to know more on the world's worst virus attacks see Table 4.8. As Windows OS is the most used OS across the globe, the lists of viruses displayed in Table 4.8 are the attacks on Windows OS. The terms "Virus" and "Worm" are used interchangeably and hence readers may find that the viruses listed under Table 4.8 may be referred as worms on some websites and/or in some books.

Box 4.4 More about Viruses!

1. The early "hacking" sites that have allowed to download favorite virus are as follows:
 - www.2600.com
 - www.LOpht.com
2. The exhaustive list of viruses can be found at:
[http://en.wikipedia.org/wiki/List_of_computer_viruses_\(all\)](http://en.wikipedia.org/wiki/List_of_computer_viruses_(all))
3. The viruses can attack a system 365 days a year. However, on the designated payload dates, the viruses may do more than just infect the system. Virus calendar can be found at:
<http://home.mcofee.com/virusInfo/VirusCalendar.aspx>
4. **Computer virus hoax:** It is a message warning the recipient of a non-existent computer virus threat. The message is usually a chain E-Mail that tells the recipient to forward it to everyone they know. They often include announcements claimed to be from reputable organizations such as Microsoft, IBM or news sources such as CNN and include emotive language and encouragement to forward the message. These sources are quoted to add credibility to the hoax. The list of virus hoax can be found at:
http://en.wikipedia.org/wiki/Virus_hoax
5. **Unix and Linux OS are immune from computer viruses:** This is a myth that Unix/Linux systems are as susceptible to hostile software attacks as any other systems. However, such systems usually found to be well-protected compared with Microsoft Windows because fast updates are available to most Unix/Linux vulnerabilities. The list of virus/worms found on Unix/Linux systems can be found at:
http://en.wikipedia.org/wiki/Linux_malware

Table 4.8 | The world's worst virus attacks!!!

Sr. No.	Virus	Brief Description
	Conficker	It is also known as Downup, Downadup and Kido. It targets Microsoft Windows OS and was first detected in November 2008. It uses flaws in Windows software and dictionary attacks on administrator passwords to compromise machines and link them into a virtual computer that can be commanded remotely by its authors. The name Conficker is blended from an English term "configure" and the German word " ficken," which means "to have sex with" or "to mess with" in colloquial German.
2	IN.F/AutoRun	AutoRun and the companion feature AutoPlay are components of the Microsoft Windows OS that dictate what actions the system takes when a drive is mounted. This is the most common threat that infects a PC by creating an "autorun.inf" file. The file contains information about programs meant to run automatically when removable devices are connected to the computer. End-users must disable the AutoRun feature enabled by default in Windows. AutoRun functionality is used in attack vector attacks.

(Continued)

Table 4.8 (Continued)

No.	Virus	Brief Description
3	Win32 PSW. OnLineGames	This is a dangerous virus that replicates itself as other viruses and spreads from one computer system to another carrying a payload of destruction. It can infect several computers within few minutes. It is more concerned with gamers around the world, stealing confidential and other financial credentials as well as gaining access to the victim's accounts. This virus is also termed as Trojan.
4	Win32/Agent	This virus is also termed as Trojan. It copies itself into temporary locations and steals information from the infected system. It adds entries into the registry, creating several files at different places in the system folder, allowing it to run on every start-up, which enables it to gather complete information about the infected system and then transfer it to the intruder's system.
5	Win32/FlyStudio	It is known as Trojan with characteristics of backdoor. This virus does not replicate itself, but spreads only when the circumstances are beneficial. It is called as backdoors because the information stolen from a system is sent back to the intruder.
6	Win32/Paceic.Gen	This threat designates a wide range of malwares that makes use of an obfuscation layer to steal passwords and other information from the infected system.
7	Win32/Qhoxr	This virus copies itself to the System32 folder of the Windows directory giving control of the computer to the attacker. The attacker then modifies the Domain Name Server/System (DNS) settings redirecting the computer to other domains. This is done to compromise the infected machine from downloading any updates and redirect any programs made to a website that downloads other malicious files on the victim's computer.
8	WMA/ TrojanDownloader. GetCodec	This threat as the suffix .GcrCodec modifies the audio files present on the system to ".wma" format and adds a URL header that points to the location of the new codec. In this manner, the host computer is forced to download the new codec and along with the new codec several other Malicious Codes are also downloaded. This means that the end-user will download the new codec believing that something new might happen, whereas the Malicious Code runs in the background causing harm to the host computer. At present, there is no way to verify the authenticity of the codec being downloaded as a new enhancement or a Trojan Horse; therefore, users must avoid unnecessary downloading of new codecs unless they are downloaded from a trusted website. Unnecessary downloading of codecs should also be avoided.

Source: <http://www.brighthub.com/computing/smb-m:url/andc/44811..l:px>

A computer worm is a self-replicating malware computer program.¹²⁰¹ It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.¹¹⁸¹ See Table 4.9 to know more on World's worst worm attacks.

Table 4.9 | The world's worst virus and worm attacks!!!

Sr. No.	Worm	Brief Description
	Morris Worm	It is also known as "Gear Worm" or Internet Worm. It was written by a student, Robert Tappan Morris, at Cornell University and launched on 2 November 1988 from MIT. It was reported that around 6,000 major Unix machines were infected by the Morris worm and the total cost of the damage calculated was US\$ 10-100 millions.
2	LOVEYOU	It is also known as VBS/Loveletter or Love Bug Worm. It successfully attacked tens of millions of Windows computers in 2000. The E-Mail was sent with the subject line as "ILOVEYOU" and an attachment "LOVE-LETTER-FOR-YOU.TXT vbs." The file extension "vbs" was hidden, hence the receiver downloads the attachment and opens it to see the contents.
3	Nimda	It is the most widespread computer worm and a file infector. It can affect Internet's within 22 minutes. Nimda affected both user workstations (i.e., clients) running on Windows 95, 98, Me, NT, 2000 or XP and Servers running on Windows NT and 2000. It is "admin" when this worm's name is spelled backward.
4	Code Red	<p>This computer worm was observed on the Internet on 13 July 2001. It attacked computers running on Microsoft's IIS web server.</p> <p>The Code Red worm was first discovered and researched by eEye Digital Security employees, Marc Maiffret and Ryan Permeh. They named the worm Code Red because they were drinking Pepsi's "Mountain Dew Code Red" over the weekend. They analyzed it because of the phrase "Hacked by Chinese!" with which the worm defaced websites.</p> <p>On 4 August 2001 "Code Red II" appeared on the Internet and was found to be a variant of the original Code Red worm.</p>
5	Melissa	It is also known as "Melissa," "Simpsons," "Kwajibo" or "Kwejeebo." It is a mass-mailing macro worm. Melissa was written by David L. Smith in Aberdeen Township, New Jersey, who named it after a lap dancer he met in Florida. The worm was in a file called "Lise.DOC" which had passwords that allow the access into 80 pornographic websites. This worm in the original form was sent through an E-Mail to many Internet users. Melissa spread on Microsoft Word 97, Word 2000 and also on Microsoft Excel 97, 2000 and 2003. It can mass-mail itself from E-Mail client Microsoft Outlook 97 or Outlook 98.
6	MSBlast	The Blaster (Vonn): It is also known as Lovsan or Lovesan, found during August 2003, which spread across the systems running on Microsoft Windows XP and Windows 2000. The worm also creates an entry under OS registry to launch the worm every time Windows starts. This worm contains two messages hidden in strings. The first, "I just want to say LOVE YOU SAN!!" and so the worm sometimes was called "Lovesan worm." The second message, "Billy gives why do you make this possible? Stop making money and fix your software!!" This message was for Bill Gates, the co-founder of Microsoft and target of the worm.
7	Sobig	<p>This worm, found during August 2003, infected millions of Internet-connected computers that were running on Microsoft Windows. It was written in Microsoft Visual C++ and compressed using a data compression tool, "brotli" (lzma). It is not only replicates by itself but also a Trojan Horse as it masquerades as something other than malware. It will appear as an E-Mail with one of the following subjects:</p> <ul style="list-style-type: none"> • Re: Approved • Re: Details

Table 4.9 | (Continued)

Sr. No.	Worm	Brkj'Dncryptunt
		<ul style="list-style-type: none"> • Re: Re: <i>My</i> details • Re: Thank you! • Re: That movie • Re: Wicked scrensaver • Re: Your application • Thank you! • Your details <p>le will contain the text as "See the attached file for details" or "Please see the attached file for derails." The E-Mail will also contain an attachment by one of the names mentioned below:</p> <ul style="list-style-type: none"> • applkarion.pif • details.pif • documcnr_9446.pif • documem_all.pif • movie0045.pif • thank_you.pif • your_details.pif • your_docurnem.pif • wicked_scr.scr
8	Storm Worm	<p>This worm, found on 17 January 2007, is also known as a backdoor Trojan Horse that affects the systems running on Microsoft OSs. The Storm worm infected thousands of computer systems in Europe and in the US on Friday, 19 January 2007, through an E-Mail with a subject line about a recent weather disaster, "230 dead as storm batters Europe."</p> <p>The worm is also known as:</p> <ul style="list-style-type: none"> • Small.dam or Trojan-Downloader.Win32.Small.dam • CME-71 I • W32/Nuwar@MM and Oownloader-BAI • Troj/Dorf and Mal/Dorf • Trojan.DL.Tibs.Gcn!Pac13 • Trojan.Oownloader-647 • Trojan.Peacomm • TROJ_SMALL.EDW • Win32/Nuwar • Win32/Nuwar.N@MM!CME-71 I • W32/Zhelatin • Trojan.Peet, Trojan.Tabs
9	Michelangelo	<p>It is a worm discovered in April 1991 in New Zealand. This worm was designed primarily to infect the systems that were running on disk operating system (DOS) systems. Like other boot sector viruses, Michelangelo operated at the BIOS level and remained dormant until 6 March, the birthday of an artist "Michelangelo di Lodovico Buonarroti Simoni" - an Italian Renaissance painter, sculptor, architect and poet.</p>

(Continued)

Table 4.9 (Continued)

Sr. No.	Worm	Brief Description
10	Jerusalem	This worm is also known as "BlackBox." Jerusalem infected the files residing on DOS. It was first detected in Jerusalem, Israel, in October 1987. It has become memory resident (using 2 KB of memory). Once the system gets infected then it infects every executable file, except "COMMAND.COM." ".COM" files grow by 1,813 bytes when infected by Jerusalem and are not reinfected. Similarly ".EXE" files grow from 1,808 to 1,823 bytes each time they get infected. Jerusalem reinfests ".EXE" files each time the file is loaded until their size is increased that is found to be "too large to load into memory."

Almost every day new viruses/worms are created and they become new threat to citizens. (See Box 4.4 to know more about viruses.) In summary, in spite of different platforms (i.e., OS and/or applications), a typical definition of computer virus/worms might have various aspects¹²¹¹ such as:

1. A virus attacks specific file types (or files).
2. A virus manipulates a program to execute tasks unintentionally.
3. An infected program produces more viruses.
4. An infected program may run without error for a long time.
5. Viruses can modify themselves and may possibly escape detection this way.

4.7 Trojan Horses and Backdoors.

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the file allocation table on the hard disk. A Trojan Horse may get widely redistributed as part of a computer virus.²¹ The term Trojan Horse comes from Greek mythology about the Trojan War (see Box 4.5).

Box 4.5 Trojan War

The Trojan Horse is a tale from the Trojan War, as told in Virgil's Latin epic poem *The Aeneid* Quintus of Smyrna. The events in this story from the Bronze Age took place after Homer's *Iliad* and before his *Odyssey*. It was the stratagem that allowed the Greeks finally to enter the city of Troy and end the conflict. In the best-known version, after a fruitless 10-year siege, the Greeks construct a huge wooden horse in an attempt to once and for all destroy Troy from the inside. According to Quintus, it was Odysseus who came up with the idea of building a great wooden horse in which 30 men could hide to be wheeled into the city without the Trojans knowing. The Greeks build a huge, magnificent wooden horse in 3 days under the leadership of Epeios. Odysseus' plan also calls for one man to remain outside the horse. This man will act as though the Greeks abandoned him, leaving the horse as a gift for the Trojans. The Greeks chose their soldier Sinon to play this role, as he is the only volunteer. Virgil describes the actual encounter between Sinon and the Trojans; Sinon successfully convinces the Trojans that he has been left behind and the Greeks are gone, and the horse is wheeled inside the city walls as a victory trophy. That night, the Greek soldiers hidden inside the horse emerged and opened the city gates for the rest of the Greek army. They raided and destroyed the city of Troy, finally ending the Trojan War.

Source: http://en.wikipedia.org/wiki/Trojan_Horse (11 January 10).

Like Spyware and Adware, Trojans can get into the system in a number of ways, including from a web browser, via E-Mail or in a bundle with other software downloaded from the Internet. It is also possible to inadvertently transfer malware through a USB flash drive or other portable media. It is possible that one could be forced to reformat USB flash drive or other portable device to eliminate infection and avoid transferring it to other machines. (Users would not know that these could infect their network while bringing some music along with them to be downloaded.)

Unlike viruses or worms, Trojans do not replicate themselves but they can be equally destructive. On the surface, Trojans appear benign and harmless, but once the infected code is executed, Trojans kick in and perform malicious functions to harm the computer system without the user's knowledge.

For example, `waterfalls.scr` is a waterfall screen saver as originally claimed by the author; however, it can be associated with malware and become a Trojan to unload hidden programs and allow unauthorized access to the user's PC.

Visit http://en.wikipedia.org/wiki/List_of_trojan_horses to get the list of noteworthy Trojan Horses. Some typical examples of threats by Trojans are as follows:

1. They erase, overwrite or corrupt data on a computer.
2. They help to spread other malware such as viruses (by a dropper Trojan).
3. They deactivate or interfere with antivirus and firewall programs.
4. They allow remote access to your computer (by a remote access Trojan).
5. They upload and download file without your knowledge.
6. They gather E-Mail addresses and use them for Spam.
7. They log keystrokes to steal information such as passwords and credit card numbers.
8. They copy fake links to false websites, display porn sites, play sounds/videos and display images.
9. They slow down, rearrange or shut down the system.
10. They reinstall themselves after being disabled.
11. They disable the task manager.
12. They disable the control panel.

4.7.1 Backdoor

A backdoor is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes. However, attackers often use backdoors that they develop or install themselves as part of an exploit. In some instances, a worm is designed to take advantage of a backdoor created by an earlier attack.¹²⁴¹

A backdoor works in background and hides from the user. It is very similar to a virus and, therefore, is difficult to detect and completely disable. A backdoor is one of the most dangerous parasite, as it allows the malicious person to perform any possible action on a compromised system. Most backdoors are autonomous malicious programs that must be somehow installed on a computer. Some parasites do not require installation as their parents are already integrated into particular software running on a remote host. Programmers, of course, leave such backdoors in their software for diagnostics and troubleshooting purposes. Attackers often discover these undocumented features and use them to intrude into the system.

What a Backdoor Does?

Following are some functions of backdoor¹²⁵¹:

1. It allows an attacker to create, delete, rename, copy or edit any file, execute various commands; change any system settings; alter the Windows registry; run, control and terminate applications; install arbitrary software and parasites.

2. Jr allows an attacker to control computer hardware devices, modify related settings, shutdown or restart a computer without asking for user permission (see Section 7.13.7, Chapter 7).
3. It steals sensitive personal information, valuable documents, passwords, login names, ID details; logs user activity and cracks web browsing habits.
4. It records keystrokes that a user types on a computer's keyboard and captures screenshots.
5. It sends all gathered data to a predefined E-Mail address, uploads it to a predetermined FTP server or transfers it through a background Internet connection to a remote host.
6. It infects files, corrupts installed applications and damages the entire system.
7. Jr distributes infected files to remote computers with certain security vulnerabilities and performs attacks against hacker-defined remote hosts.
8. It installs hidden FTP server that can be used by malicious persons for various illegal purposes.
9. It degrades Internet connection speed and overall system performance, decreases system security and causes software instability. Some parasites are badly programmed as they waste too many computer resources and conflict with installed applications.
10. It provides no uninstall feature, and hides processes, files and other objects to complicate its removal as much as possible.

Following are a few examples of backdoor Trojans:

1. **Back Orifice:** It is a well-known example of backdoor Trojan designed for remote system administration. It enables a user to control a computer running the Microsoft Windows OS from a remote location. The name is a word play on Microsoft BackOffice Server software. Readers may visit <http://www.culdeadcow.com/rools/bo.html> to know more about backdoor.
2. **Bifrost:** It is another backdoor Trojan that can infect Windows 95 through Vista. It uses the typical server-client backdoor program configuration to allow a remote attacker, who uses client, to execute arbitrary code on the compromised machine.
3. **SAP backdoors**¹²⁶¹: SAP is an Enterprise Resource Planning (ERP) *system* and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning. Backdoors can present in SAP User Master that supports an authentication mechanism when a user connects to access SAP and ASAP Program Modules which support SAP Business Objects.
4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests. Readers may visit <http://www.onapsis.com/research.html> to know more about this tool.

4.7.2 How to Protect from Trojan Horses and Backdoors

Follow the following steps to protect your systems from Trojan Horses and backdoors:

1. **Stay away from suspect websites/webBnks:** Avoid downloading free/pirated softwares that often get infected by Trojans, worms, viruses and other things. We have addressed "how to determine a legitimate website" in Chapter 5.
2. **Surf on the Web cautiously:** Avoid connecting with and/or downloading any information from peer-to-peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search engines are used while surfing the information on the Web.

(See Box 4.6 to know more on P2P networks.) It may be experienced that, after downloading the file, it never works and here is a chance that - although the file has not worked, something must have happened to the system - the malicious software deploys its gizmos and the system is at serious health risk. Enabling Spam filter "ON" is a good practice but is not 100% foolproof. Spammers are constantly developing new ways to go through such filters.

3. **Install antivirus/Trojan remover software:** Nowadays antivirus software(s) have built-in feature for protecting the system not only from viruses and worms but also from malware such as Trojan Horses. Free Trojan remover programs are also available on the Web and some of them are really good.

Box 4.6 Peer-to-Peer (P2P) Networks

Peer-to-peer, commonly abbreviated as P2P, is any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or slave hosts). Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model where only servers supply and clients consume.²⁷¹ There are different levels of P2P networking¹²⁸¹:

1. **Hybrid P2P:** There is a central server that keeps information about the network. The peers are responsible for storing the information. If they want to contact another peer, they query the server for the address.
2. **Pure P2P:** There is absolutely no central server or router. Each peer acts as both client and server at the same time. This is also sometimes referred to as "serverless" P2P.
3. **Mixed P2P:** It is between "hybrid" and "pure" P2P networks. An example of such a network is Gnutella that has no central server but clusters its nodes around so-called "supernodes."

Advantages of P2P Networks

1. It enables faster delivery of information from one computer to another by bypassing a central server.
2. It increases personal efficiency and personal empowerment. Users will no longer have to wait in queues to perform essential tasks, as all activities take place at the user's discretion.
3. It represents significant cost savings over client/server models. As resources and computing power are distributed across the entire network, there is no need for expensive centralized servers; this will reduce the need for centralized management, storage and other related resources.
4. It offers easy scalability and all that is necessary for a network to grow is add more peers.
5. It increases a network's fault tolerance. As no part of the system is essential to its operation, you can take down a few nodes and the network remains functional.
6. It leverages previously unused resources found on hundreds of millions of computers (and other services) that are connected to the "edges" of the Internet.
7. It frees up bandwidth on the Internet (or on a private network). In traditional client-server model, the server is the bottleneck and often cannot handle everything the client requests.
8. It requires no centralized management, oversight or control.
9. It offers increased privacy, as all data and messages are directly exchanged between two computers.
10. It results in networks that are more flexible and adoptable compared with traditional client-server networks.

Besides all these advantages, there are still many reasons why P2P might not be the right model and is used only for specific sets of activities.

Box 4.6 Peer-to-Peer ... (Continued)**Drawbacks of P2P Networks**

1. It propagates all sorts of undesirable items and activities including misinformation.
2. It increases network's. on individual system's. exposure to network attacks, viruses and other malicious damage.
3. It makes no guarantee that content/resources will always be available - any peer can go "dark" if he/she shuts down his/her computer.
4. It does not enforce content ownership (copyright).
5. It cannot enforce standards (either technological or ethical/moral/social).
6. It can be overwhelmed by increased traffic when it is unprepared (Napster uses many clogged university networks).
7. It is plagued by lack of standards, infrastructure and support. It is a kind of "Wild West" of the Internet.
8. Its transactions are difficult to translate into revenue streams and this lack of revenue generation could hinder its future development.

Ares, BitTorrent, LimeWire and Kazaa are a few examples of popular P2P file-sharing programs. Readers may visit <http://www.bestsecuritytips.com/xfsection+article.articleid+49.htm> to know more on these popular P2P file-sharing programs.

Source: www.bus.ucf.edu/leigh/isrn5937/linked/Ledesrno_J.doc (17 May 2010).

4.8 Steganography

Steganography is a Greek word that means "secret writing." It is a method that attempts to hide the existence of a message or communication. The word "steganography" comes from the two Greek words: steganos meaning "covered" and graphos meaning "to write" that means "concealed writing." This idea of secret hiding is not a novelty; it has been used for centuries all across the world under different regimes. The practice dates back to ancient Rome and Greece where the messages were etched into wooden tablets and then covered with wax or when messages were passed by shaving a messenger's head and then carving a secret message on it, letting his hair grow back and then shaving it again after he arrived at the receiving party to reveal the message.

Given the sheer volume of data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved. One better known but rapidly growing method is steganography, the art and science of hiding information so that it does not even appear to exist! Steganography is always misunderstood with cryptography (see Box 4.7 to know difference between these two techniques). The different names for steganography are data hiding, information hiding (explained in Section 7.12.2, Chapter 7) and digital watermarking.

For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any noticeable change in the image. Steganography can be used to make a digital watermark to detect illegal copying of digital images. Thus, it aids confidentiality and integrity of the data. *Digital watermarking* is the process of possibly irreversibly embedding information into a digital signal. The signal may be, for example, audio, pictures or video. If the signal is copied then the information is also carried in the copy.

Box 4.7 Difference between Steganography and Cryptography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message: this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. It is said that terrorists use steganography techniques to hide their communication in images on the Internet; most popular images are used such as those of film actresses or other celebrities. In its basic form, steganography is simple. For example, every fourth letter of a memo could hide a message. This simple technique has an added advantage over encryption that it does not arouse suspicion, that is, there is not much scope for getting started on investigation! Presence of an encryption could set off an investigation, but a message hidden in plain sight would get ignored (see Box 7.13, Chapter 7).

In October 2001, the New York Times published an article claiming that al-Qaeda had used steganographic techniques to encode messages into images, and then transported these via E-Mail and possibly via Usenet to prepare and execute the 11 September 2001 Terrorist Attack.¹³⁰¹

The term "cover" or "cover medium" is used to describe the original, innocent message, data, audio, video and so on. It is the medium that hides the secret message (see Fig. 4.4). It must have parameters that can be altered or used without damaging or noticeably changing the cover media. If the cover media are digital, these alterable parts are called "redundant bits." These bits or a subset can be replaced with the message that is intended to be hidden. Interestingly, steganography in digital media is very similar to "digital watermarking." In other words, when steganography is used to place a hidden "trademark" in images, music and software, the result is a technique referred to as "watermarking" (see Table 4.10 to know more about steganography tools).

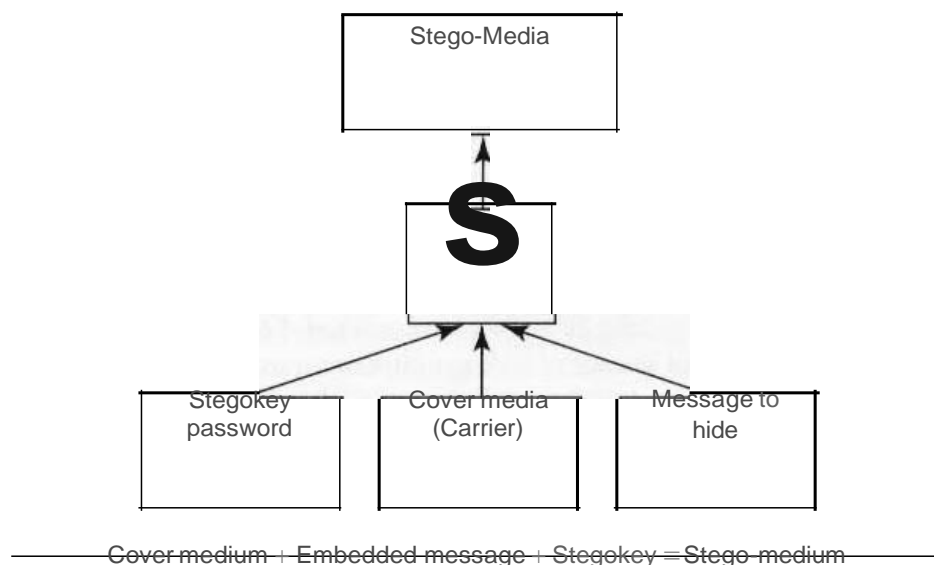


Figure 4.4 How steganography works.

Source: <http://www.cosc.iup.edu/sezekiel/Seminar/steg.ppt#452,15,Steganography%20of%20today's%20talk> (11 May 10).

Table 4.10 Steganography tools

Website	Description
http://www.securifyfocus.com	DiSi-Steganograph: It is a very small, DOS-based steganographic program that embeds data in PCX images.
http://www.brothersoft.com/invisible-foldm-54597.html	Invisible Folders: It has the ability to make any file or folder invisible to anyone using your PC even on a network.
http://www.invisibbcrecs.com	Invisible Secrets: It not only encrypts the data and files for safe-keeping or for secure transfer across the Net but also hides them in places such as picture or sound files or webpages. These types of files are a perfect disguise for sensitive information.
http://www.programurl.com/sscalth-files.lam	Stealth Files: It hides any type of file in almost any other type of file. Using steganography technique, Stealth Files compresses, encrypts and then hides any type of file inside various types of files (including EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI, WAV, DOC, BMP) and other types of video, image and executable files.
http://www.programurl.com/hermeric-stcgo.hun	Hermeric Scego: It is a steganography program that allows to encrypt and hide contents of any data file in another file so that the addition of the data. The container file will not noticeably change the appearance of the file. This program allows, hiding a file of any size in one or more BMP image files with or without the use of a user-specified stego/encryption key so that (a) the presence of the hidden file is undetectable (even by forensic software using statistical method) and (b) if a user-specified stego key is used then the hidden file can be extracted only by someone, using the software, who knows the stego key.
http://www.scurstar.com/producers_drivecryptpp.php	DriveCrypt Plus (DCPP): It has following features: <ul style="list-style-type: none"> • It allows secure hiding of an entire OS inside the free space of another OS. • Full-disk encryption (encrypts parts or 100% of your hard disk including the OS). • Preboot authentication (before the machine boots, a password is requested to decrypt the disk and start your machine).
http://www.petircola.net/fubicn/steganography/mp3stego	MP3Scego: It hides information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
http://compression.ru/video/srcgo_vidco/index_cn.html	MSU StegoVideo: It allows, hiding any file in a video, equipment. Main features are as follows: <ul style="list-style-type: none"> • Small video distortions after hiding information. • It is possible to extract information after video compression. • Information is protected with the password.

Steganography, Sudoku and SMS: It is a revised version of information hiding (i.e., steganography) with a twist. This methodology was proposed by Chang et al. during 2008, which was inspired by Zhong and Wong's method and Sudoku solutions. Sudoku game has gained popularity recently and SMS is a popular medium of communication nowadays - messages are concealed into Sudoku puzzle, which are then communicated to intended recipient through SMS. As soon as recipient solves the puzzle, he/she can extract the data hidden into Sudoku puzzle image.

4.8.1 Steganalysis

Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography. The goal of steganalysis is to identify suspected packages and to determine whether or not they have a payload encoded into them, and if possible recover it. Automated tools are used to detect such steganographed data/information hidden in the image and audio and/or video files (see Table 4.11 for more details).

4.9 DoS and DDoS Attacks

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users.

4.9.1 DoS Attacks

In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam *mail* depriving him of the services he is entitled to access or provide. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent the Internet site or service from functioning efficiently or at all, temporarily or indefinitely. The attackers typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, mobile phone networks and even root name servers (i.e., domain name

Table 4.11 | Steganalysis tools

Website	Brief Description
http://www.vw.sarc-wv.com/producers/stegalyzer.aspx	StegAlyzerAS: It is a digital Forensic analysis tool designed to scan "suspect media" or "forensic images" of suspect media for known artifacts of steganography applications.
http://www.sarc-wv.com/stegalyzers.aspx	StegAlyzerSS: It is a digital forensic analysis tool designed to scan "suspect media" or "forensic images" of suspect media for uniquely identifiable hexadecimal byte patterns, or known signatures. It can detect when particular steganography applications are used to embed hidden information within them.
http://www.spy-hunter.com/stegspy/download.htm	StegSpy: It is a program that is always in progress and the latest version includes identification of a "steganized" file. It detects steganography and the program used to hide the message. The latest version also identifies the location of the hidden content as well. StegSpy identifies programs such as Hiderman, JPHideandSeek, Masker, JPegX and Invisible Secret.
http://www.outguess.org/detection.php	Stegdetect: It is an automated tool for detecting steganographic content in the images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images.
http://stegsecret.sourceforge.net	Stegsecret: It is a steganalysis open-source project that makes detection of hidden information possible in different digital media. It is a JAVA-based multiplatform steganalysis tool that allows the detection of hidden information by analyzing the most known steganographic methods.
http://sourceforge.net/projects/vsl	Virtual Steganographic Laboratory (VSL): It is a graphical block diagramming tool that allows complex using, testing and adjusting of methods both for image steganography and steganalysis.

servers). Buffer overflow technique is employed to commit such kind of criminal attack known as *Spoofing*. The term IP address Spoofing refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the IP of the sender or impersonating another computing system. A packet is a formatted unit of data carried by a packet mode computer network. The attacker spoofs the IP address and floods the network of the victim with repeated requests. As the IP address is fake, the victim machine keeps waiting for response from the attacker's machine for each request. This consumes the bandwidth of the network which then fails to serve the legitimate requests and ultimately breaks down.

The United States Computer Emergency Response Team defines symptoms of DoS attack, to include:

1. Unusually slow network performance (opening files or accessing websites);
2. unavailability of a particular website;
3. inability to access any website;
4. dramatic increase in the number of Spam E-Mails received (this type of DoS attack is termed as an E-Mail bomb).

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic.
2. Disrupt connections between two systems, thereby preventing access to a service.
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

4.9.2 Classification of DoS Attacks

See Table 4.12 for classification of DoS attacks.

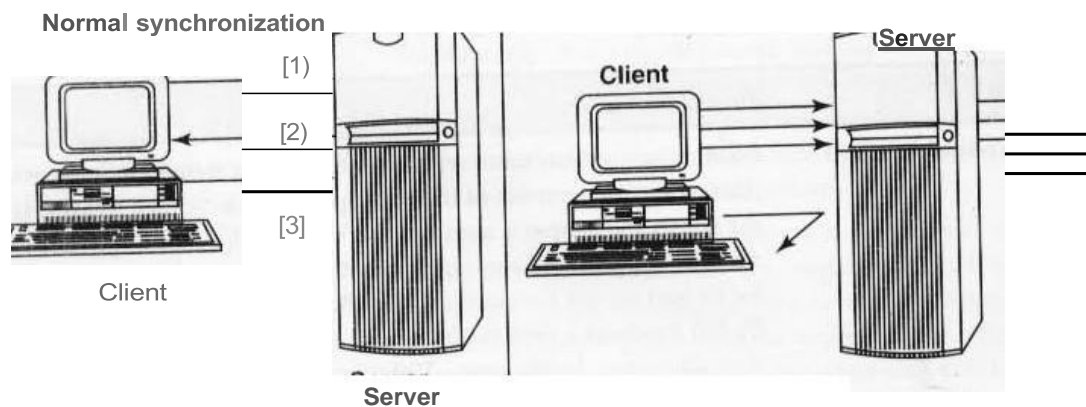
Table 4.12 Classification of DoS attacks

Sr. No.	DoS Attacks	Brief Description
	Bandwidth attacks	Loading any website takes certain time. Loading means complete webpage (i.e., with entire content of the webpage - text along with images) appearing on the screen and system is awaiting user's input. This "loading" consumes some amount of memory. Every site is given with a particular amount of bandwidth for its hosting, say for example, 50 GB. Now if more visitors connect, use all 50 GB bandwidth then the hosting of the site can ban this site. The attacker does the same - he/she opens 100 pages of a site and keeps on refreshing and consuming all the bandwidth, thus, the site becomes out of service.
2	Logic attacks	These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.
3	Protocol attacks	Protocols here are rules that are to be followed to send data over network. These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amounts of its resources.
4	Unintentional DoS attack	This is a scenario where a website ends up denied not due to a deliberate attack by a single individual or group of individuals, but simply due to a sudden enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less well-prepared site, for example, as part of a news story. The result is that a significant proportion of the primary site's regular users, potentially hundreds of thousands of people, click that link within a few hours and have the same effect on the target website as a DDoS attack.

4.9.3 Types or Levels of DoS Attacks

There are several types or levels of DoS attacks as follows:

1. **Flood attack:** This is the earliest form of DoS attack and is also known as *ping flood*. It is based on an attacker simply sending the victim overwhelming number of ping packets, usually by using the "ping" command, which results in more traffic than the victim can handle. This requires the attacker to have a faster network connection than the victim (i.e., access to greater bandwidth than the victim). It is very simple to launch, but to prevent it completely is the most difficult.
2. **Ping of death attack:** The ping of death attack sends oversized Internet Control Message Protocol (ICMP) packets, and it is one of the core protocols of the IP Suite. It is mainly used by networked computers' OSs to send error messages indicating (e.g., that a requested service is not available or that a host or router could not be reached) datagrams (encapsulated in IP packets) to the victim. The maximum packet size allowed is of 65,536 octets. Some systems, upon receiving the oversized packet, will crash, freeze or reboot, resulting in DoS (e.g., the ping of death attack relied on a bug in the Berkeley TCP/IP stack, which also existed on most systems that copied the Berkeley network code).
3. **SYN attack:** It is also termed as *TCP SYN Flooding*. In the Transmission Control Protocol (TCP), handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with a SYN (using a legitimate or spoofed source address). The server replies with a SYN-ACK. The client then does not send back an ACK, causing the server (i.e., target system) to allocate memory for the pending connection and wait. This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system. Figure 4.5 explains how the DoS attack takes place.



3-way Handshake

- Client sends synchronize (syn) pkt to web server
- Server sends synchronize acknowledgment (syn-ack)
- Client replies with an acknowledgment pkt, the connect is established

Chaotic Handshake

- Client sends multiple synchronize (syn) pkts to web server - all with bad addresses
- Server sends synchronize acknowledgments to incorrect addresses leaving half open connections and flooded queue
- Legitimate user is denied access because queue is full and additional connections cannot be accepted

Figure 4.5 | Denial-of-service (DoS) attack.

4. **Teardrop attack:** The teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them. IP's packet fragmentation algorithm is used to send corrupted packets to confuse the victim and may hang the system. This attack can exist in various OSs due to a bug in their TCP/IP fragmentation reassembly code. Windows 3.1x, Windows 95 and Windows NT OSs as well as versions of Linux (i.e., prior to versions 2.0.32 and 2.1.63) are vulnerable to this attack.¹³¹¹
5. **Smurf attack:** It is a way of generating significant computer network traffic on a victim network. This is a type of DoS attack that floods a target system via spoofed broadcast ping messages. This attack consists of a host sending an ICMP echo request (ping) to a network broadcast address (e.g., network addresses with the host portion of the address having all 1s). Every host on the network receives the ICMP echo request and sends back an ICMP echo response inundating the initiator with network traffic. On a multi-access broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim. Internet relay chat (IRC) servers are the primary victim of smurf attacks on the Internet [(IRC is a form of real-time Internet text messaging (chat) or synchronous conferencing)].
6. **Nuke:** Nuke¹³²¹ is an old DoS attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target. It is achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop. A specific example of a nuke attack that gained some prominence is the WinNuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A series of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death (BSOD).

4.9.4 Tools Used to Launch DoS Attack

Various tools (see table 4.13) use different types of traffic to flood a victim, but the objective behind the attack and the result is the same: A service on the system or the entire system (i.e., application/website/network) is unavailable to a user because it is kept busy trying to respond to an exorbitant number of requests. A DoS attack is usually an attack of last resort because it is considered to be an unsophisticated attack as the attacker does not gain access to any information but rather annoys the target and interrupts the service. (See Box 4.8 to know more about blended threats and Box 4.9 for PDoS attacks.)

Table 4.13 Tools used to launch DoS attack

Sr. No.	Tool	Brief Description
	J0112	A major vulnerability has been discovered in Windows' networking code. The vulnerability allows remote attackers to cause a DoS attack against Windows-based machines - the attack causes the target machine to consume 100% of the CPU time on processing of illegal packets.
1.	Ncmesg	This program generates random packets of spoofed source IP to enable the attacker to launch DoS attack.
3	T:irg;i	It is a program that can be used to run eight different DoS attacks. The attacker has the option to launch either individual attacks or try all the attacks until one is successful.
4	Crazy Pinger	This tool could send large packets of ICMP to a remote target network.
5	SomeTrouble	It is a remote hoocher and bomber. It is developed in Delphi.

Box 4.8 Blended Threat

Blended threat is a more sophisticated attack that bundles some or the worst aspects of viruses, worms, Trojan Horses and Malicious Code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, transmit and thereafter spread an attack. Characteristics of blended threats are that

1. They cause harm to the infected system or network.
2. They propagate using multiple methods as attack may come from multiple points.
3. They also exploit vulnerabilities.

To be considered a blended threat, the attack would normally serve to transport multiple payloads in one payload. For example, it would not only just launch a DoS attack but it would also, for example, install a backdoor and maybe even damage a local system in one shot. Additionally, blended threats are designed to use multiple modes of transport. Therefore, while a worm may travel and spread through E-Mail, a single blended threat could use multiple routes including E-Mail, IRC and file-sharing networks.

Finally, rather than a specific attack on predetermined ".exe" files, a blended threat could do multiple malicious acts, such as modify your ".exe" files, HTML files and registry keys at the same time - basically it can cause damage to several areas of your network at one time.

Blended threats are considered to be the worst risk to security since the inception of viruses, as most blended threats require no human intervention to propagate.

Source: <http://www.webopedia.com/didyouknow/internet/2004/virvs.asp> (11 January 2010).

Box 4.9 Permanent Denial-of-Service (PDoS) Attack

A PDoS attack damages a system so badly that it requires replacement or reinstallation of hardware. Unlike DDoS attack - which is used to sabotage a service or website or as a cover for malware delivery - PDoS is a pure hardware sabotage. It exploits security flaws that allow remote administration on the management interfaces of the victim's hardware, such as routers, printers or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt or defective firmware image - a process which when done legitimately is known as *flashing*. Owing to these features, and the potential and high probability of security exploits on network-enabled devices (NEEDs), this technique has come to the attention of numerous hacker communities. Phlashed is a tool created by Rich Smith (an employee of Hewlett-Packard's Systems Security Lab) who detected and demonstrated PDoS vulnerabilities at the 2008 EU SecWest Applied Security Conference in London.

Source: http://en.wikipedia.org/wiki/Denial-of-service_attack (11 May 2010).

4.9.5 DDoS Attacks

In a DDoS attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the DoS attack.

A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems (as explained in Chapter 1) are called "secondary victims" and the main target is called "primary victim."

Table 4.14 | Tools used to launch DDoS attack

<i>Sr. No.</i>	<i>Tool</i>	<i>Brief Description</i>
	Trinoo	It is a set of computer programs to conduct a DDoS attack. It is believed that Trinoo networks have been set up on thousands of systems on the Internet that have been compromised by remote buffer overrun exploit.
2	Tribe Flood Network (TFN)	It is a set of computer programs to conduct various DDoS attacks such as ICMP flood, SYN Flood, UDP Flood and Smurf attack.
3	Stachddrahc	It is written by Random for Linux and Solaris systems, which acts as a DDoS agent. It combines features of Trinoo with TFN and adds encryption.
4	Shafte	This network looks conceptually similar to a Trinoo; it is a packet flooding attack and the client controls the size of the flooding packets and duration of the attack.
5	MStream	It uses spoofed TCP packets with the ACK flag set to attack the target. Communication is not encrypted and is performed through TCP and UDP packet. Access to the handler is password protected. This program has a feature not found in other DDoS tools. It informs all connected users of access, successful or not, to the handler(s) by connecting parties.

Malware can carry DDoS attack mechanisms - one of the better-known examples of this is MyDoom. Typically, DoS mechanism triggered on a specific date and time. This type of DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack. A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent. Nowadays, Bomber (as explained in Chapter 2) is the popular tool to launch DoS/DDoS attacks. Attackers can also break into systems using automated tools (see Table 4.14) that exploit flaws in programs that listen for connections from remote hosts.

4.9.6 How to Protect from DoS/DDoS Attacks

Computer Emergency Response Team Coordination Center (CERT/CC) offers many preventive measures from being a victim of DoS attack.¹³³¹

1. Implement router filters. This will lessen your exposure to certain DoS attacks.
2. If such filters are available for your system, install patches to guard against SYN flooding.
3. Disable any unused or inessential network service. This can limit the ability of an attacker to take advantage of these services to execute a DoS attack.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, central processing unit (CPU) usage or network traffic.
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files (see Table 4.15).
8. Invest in and maintain "hot spares" - machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

Table 4.15 Tools for detecting DoS/DDoS attacks

No.	Tool	Brief Description
1	Zombie Zapper	It is a free, open-source tool that can tell a zombie system flooding packets to stop flooding. It works against Trinoo, TFN and Srscheldrahr. It assumes various defaults are still in place used by these attack tools, however, it allows you to put the zombies to sleep.
2	Remote Intrusion Detector (RID)	It is a tool developed in "C" computer language, which is a highly configurable packet snooper and generator. It works by sending out packets defined in the config.txt file, then listening for appropriate replies. It detects the presence of Trinoo, TFN or Srscheldrahr clients.
3	Security Auditor's Research Assistant (SARA)	It gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws such as incorrectly set up or configured network services, well-known bugs in the system or network utilities, system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database and weak policy decisions.
4	Find_DDoS	It is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.
5	ODoSPing	It is a remote network scanner for the most common DDoS programs. It can detect Trinoo, Srscheldrahr and Tribe Flood Network programs running with their default settings.

Computer Emergency Response Team Coordination Center (CERT/CC) was started in December 1988 by the Defense Advanced Research Projects Agency, which was part of the US Department of Defense, after the Morris Worm disabled about 10% of all computers connected to the Internet. It is located at the Software Engineering Institute, a federally funded research center operated by Carnegie Mellon University. It studies Internet security vulnerabilities and provides services to websites that have been attacked. It also publishes security alerts.

Source: <http://WWW.WeQopedki.com/TERM/C/CERTCC.html> 131 May 2010).

4.10 SQL Injection

Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS). SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

Attackers target the SQL servers - common database servers used by many organizations to store confidential data. The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card numbers, social security numbers or passwords. During an SQL injection attack, Malicious Code is inserted into a web form

field or the website's code to make a system execute a command shell or other arbitrary commands. Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field. For example, an arbitrary command from an attacker might open a command prompt or display a table from the database. This makes an SQL server a high-value target and therefore a system seems to be very attractive to attackers.

The attacker determines whether a database and the cables residing into it are vulnerable, before launching an attack. Many webpages take parameters from web user and make SQL query to the database. For example, when a user logs in with username and password, an SQL query is sent to the database to check if a user has valid name and password. With SQL injection, it is possible for an attacker to send crafted username and/or password field that will change the SQL query.

4.10.1 Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, such as, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
2. To check the source code of any website, right click on the webpage and click on "view source" (if you are using IE - [Internet Explorer] - source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the `<FORM>` and `</FORM>` have potential parameters that might be useful to find the vulnerabilities.


```
<FORM action=Sear-ctrlsearch.{LSp method=post}>
<input type=hidden name=A value=C>
</FORM>
```
3. The attacker inputs a *single quote* under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as *use 'a' = '11'* (or something similar) then the website is found to be susceptible to an SQL injection attack.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

Here are few examples of variable field which the attacker uses on a webpage to test for SQL vulnerabilities:

1. `Bfah'orl=l--`
2. `LtJgin:bl'ah' or l=l--`
3. `/password:bl'il/ or 1=1-`
4. `http://search/index.asp?id=blah'or 1=1-`

Similar SQL commands may allow bypassing of a login and may return many rows in a table or even an entire database table because the SQL server is interpreting the terms literally. The double dashes near the end of the command tell SQL to ignore the rest of the command as a comment.

Blind SQL Injection

Blind SQL injection¹⁴ is used when a web application is vulnerable to SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be the one that displays data; however, it will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack can become time-intensive because a new statement must be crafted for each bit recovered. There are several tools that can automate these attacks once the location

of the vulnerability and the range of information have been established. Readers may refer to Ref. #7, Additional Useful Web References, Further Reading to know about white paper.

In summary, using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance
 - To get a directory listing: Blah' ;exec masrer..xp_cmdshell "dfr c:\.*Is>c:\direccory.txt";
 - To ping an IP address: Blah' ;exec mascer..xp_cmdshell "ping 192.168.1.1".
2. May gain access to the database by obtaining username and their password
 - To get a user listing: SELECT ' FROM users WHERE name= "OR '1' = '1'."
3. Add new data to the database
 - Execute the INSERT command: This may enable selling politically incorrect items on an E-Commerce website.
4. Modify data currently in the database
 - Execute the UPDATE command: May be used to have an expensive item suddenly be deeply "discounted."

mySQLenum: It is a command line automatic blind SQL injection tool for web application that uses MySQL server as its back-end. The main objective of this tool is to provide an easy-to-use command line interface. Readers may visit <http://pentestit.com/2010/01/15/mysqlenum-automatic-blind-sql-injection-tool/> to know more on this tool.

See Table 4.16 to know some automated tools that are used either to find database vulnerabilities and/or to protect the database applications.

Table 4.16 | Tools used for SQL Server penetration

Sr. No.	Tool	Brief Description
	http://www.appsecinc.com	AppDetectivePro: It is a network-based, discovery and vulnerability assessment scanner that discovers database applications within the infrastructure and assesses security strength. It locates, examines, reports and finds security holes and misconfigurations as well as identifies user rights and privilege levels based on its security methodology and extensive knowledge based on application-level vulnerabilities. Thus, organizations can harden their database applications.
2	http://www.appsecinc.com	DbProtect: It enables organizations with complex, heterogeneous environments to optimize database security, manage risk and bolster regulatory compliance. It integrates database asset management, vulnerability management, audit and threat management, policy management, and reporting and analytics for a complete enterprise solution.
3	http://www.iss.net	DatabaseScanner: It is an integrated part of Internet Security Systems' (ISS) Dynamic Threat Protection platform that assesses online business risks by identifying security exposures in the database applications. Database scanner offers security policy generation and reporting functionality, which instantly measures policy compliance and automates the process of securing critical online business data. Database scanner runs independently of the database and quickly generates detailed reports with all the information needed to correctly configure and secure databases.

(Continued)

Table 4.16 j (Continued)

<i>Sr. No.</i>	<i>Tool</i>	<i>Brief Description</i>
4	http://www.ca.com/us/securityadvisor	SQLPoke: IL is an NT-based tool that locates Microsoft SQL (MSSQL) servers and tries to connect with the default System Administrator (SA) account. A list of SQL commands are executed if the connection is successful.
5	http://www.vngssoftwue.com:0111/	NGSSQLCrack: It can guard against weak passwords that make the network susceptible to attack. This is a password cracking utility for Microsoft SQL server 7 and 2000 and identifies user accounts with weak passwords so that they can be reset with stronger ones, thereby protecting the overall integrity of the system.
6	http://www.security-database.com/toolswatch	Microsoft SQL Server Fingerprint (MSSQLFP) Tool: This is a tool that performs fingerprinting version of Microsoft SQL Server 2000, 2005 and 2008, using well-known techniques based on several public works that identifies the SQL version and also can be used to identify vulnerable versions of Microsoft SQL Server.

4.10.2 How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. Input validation

- Replace all single quotes (escape quotes) to two single quotes.
- Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as `is ; , -`, `select`, `insert` and `xp_` can be used to perform an SQL injection attack.
- Numeric values should be checked while accepting a query string value. Function - `IsNumeric()` for Active Server Pages (ASP) should be used to check these numeric values.
- Keep alert boxes and form fields as short as possible to limit the length of user input.

2. Modify error reports: SQL errors should not be displayed to outside users and to avoid this, the developer should handle or configure the error report very carefully. These errors sometimes display full query pointing to the syntax error involved and the attacker can use it for further attacks.

3. Other preventions

- The default system accounts for SQL server 2000 should never be used.
- Isolate database server and web server. Both should reside on different machines.
- Most often attackers may make use of several extended stored procedures such as `xp_cmdshell` and `xp_grantlogin` in SQL injection attacks. In case such extended stored procedures are not used or have unused triggers, stored procedures, user-defined functions, etc., then these should be moved to an isolated server.

These are the minimum countermeasures that can be implemented to prevent SQL injection attack. Technocrats may want to know more on this topic and can go through Refs. #8 and #9, Additional Useful Web References.

SQLBlot is an open data base connectivity (ODBC) driver that acts as an SQL injection protection feature. It attempts to detect and block malicious SQL statements, It, V"Prks as an ordinary ODB .data. source and monitor every S(II statements being executed.

4.11 Buffer Overflow

Buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it. The extra data overwrites adjacent memory, which may contain other data, including program variables and program flow control data. This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash) or a breach of system security.

Buffer overflows can be triggered by inputs that are designed to execute code or alter the way the program operates. They are, thus, the basis of many software vulnerabilities and can be maliciously exploited. Bounds checking can prevent buffer overflows.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check data written to an array (the built-in buffer type), which is within the boundaries of that array.¹¹⁵

Buffer overflow occurs when a program or process stores more data in a buffer (temporary data storage area) than it was intended to hold. As buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

The knowledge of C, C++ or any other high-level computer language (i.e., assembly language) is essential to understand buffer overflow, as basic knowledge of process memory layout is very important. A buffer is a contiguous allocated chunk of memory such as an array or a pointer in C. In C and C++, there are no automatic bounds checking on the buffer - which means a user can write past a buffer. For example,

```
int main () {
    int buffer[10];
    buffer[20] = 10;
}
```

This C program is a valid program and every compiler can compile it without any errors. However, the program attempts to write beyond the allocated memory for the buffer, which might result in an unexpected behavior.

4.11.1 Types of Buffer Overflow

Stack-Based Buffer Overflow

Stack buffer overflow occurs when a program writes to a memory address on the program's stack outside the intended data structure - usually a fixed length buffer. Here are the characteristics of stack-based programming:

1. "Stack" is a memory space in which automatic variables (and often function parameters) are allocated.
2. function parameters are allocated on the stack (i.e., local variables that are declared on the stack - unless they are also declared as "static" or "register") and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.

3. Once a function has completed its cycle, the reference to the variable in the stack is removed. (Therefore, if a function is called multiple times, its local variables and parameters are recreated and destroyed each time the function is called and exited.)

U1c arcacker may exploit stack-based buffer overflows to manipulate the program in various ways by overwriting:

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

Three factors that contribute to overcome the exploits are

1. Null bytes in addresses;
2. variability in the location of shellcode;
3. differences between environments.



A shellcode is a small piece of code used as a payload in the exploitation of software vulnerability. It is called "shellcode" because it starts with command shell from which the attacker can control the compromised machine.

NOPs

NOP or NOOP (short form of no operation or no operation performed) is an assembly language instruction/command that effectively does nothing at all. The explicit purpose of this command is not to change the status of status flags or memory locations in the code. This means NOP enables the developer to force memory alignment to act as a placeholder to be replaced by active instructions later on in program development.

NOP opcode can be used to form a NOP slide, which allows code to execute when the exact value of the instruction pointer is indeterminate (e.g., when a buffer overflow causes a function's return address on the stack to be overwritten). It is the oldest and most widely used technique for successfully exploiting a stack buffer overflow. It helps to know/locate the exact address of the buffer by effectively increasing the size of the larger stack buffer area. The attacker can increase the odds of finding the right memory address by padding his/her code with NOP operation. To do this, much larger sections of the stack are corrupted with the NOOP machine instruction. At the end of the attacker-supplied data, after the NOOP instructions, an instruction is placed to perform a relative jump to the top of the buffer where the shellcode is located. This collection of NOOP is referred to as the "NOP sled" because if the return address is overwritten with any address within the NOOP region of the buffer then it will "slide" down the NOOP until it is redirected to the actual Malicious Code by the jump at the end. This technique requires the attacker to guess where in the stack the NOP sled is compared with small shellcode.

Owing to the popularity of this technique, many vendors of intrusion prevention systems will search for this pattern of NOOP machine instructions in an attempt to detect shellcode in use. It is important to note that a NOP sled does not necessarily contain only traditional NOOP machine instructions but also any instruction that does not corrupt the state of machine to a point where the shellcode will not run and can be used in place of the hardware-assisted NOOP. As a result, it has become common practice for exploit writers to compose a NOP sled with randomly chosen instructions that will have no real effect on the shellcode execution.¹³⁵¹

Heap Buffer Overflow

Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit. In either case, the overflow occurs when an application copies more data into a buffer than the buffer was designed to contain. A routine is vulnerable to exploitation if it copies data to a buffer without first verifying that the source will fit into the destination. The characteristics of stack-based and heap-based programming are as follows:

1. "Heap" is a "free store" that is a memory space, where dynamic objects are allocated.
2. The heap is the memory space that is dynamically allocated by `new()`, `malloc()` and `calloc()` functions; it is different from the memory space allocated for stack and code.
3. Dynamically created variables (i.e., declared variables) are created on the heap before the execution program is initialized to zero and are stored in the memory until the life cycle of the object has completed.

Memory on the heap is dynamically allocated by the application at run-time and normally contains program data. Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as `malloc` metadata) and uses the resulting pointer exchange to overwrite a program function pointer.

4.11.2 How to Minimize Buffer Overflow

Although it is difficult to prevent all possible attacks, the following methods will definitely help to minimize such attacks:

1. **Assessment of secure code manually:** Buffer overflow occurs when a program or process writes more data in a buffer than it was intended to hold. Developers should be educated about minimizing the use of vulnerable functions available in C library, such as `strcpy()`, `strcat()`, `sprintf()` and `vsprintf()`, which operate on null-terminated strings and perform no bounds checking. The input validation `scanf()` function that reads user input into a buffer is very essential.
2. **Disable stack execution:** Malicious code causes input argument to the program, and it resides in the stack and not in the code segment. Any code that attempts to execute any other code residing in the stack will cause a segmentation violation. Therefore, the simplest solution is to invalidate the stack to execute any instructions. However, this solution is not easy to implement. Although possible in Linux, some compilers (including GNU Compiler Collection (GCC)) use trampoline functions to implement taking the address of a nested function that works on the system stack being executable. A trampoline is a small piece of code created at run-time when the address of a nested function is taken. It normally resides in the stack and in the stack frame of the calling function and thus requires the stack to be executable. However, a version of the Linux kernel enforces the non-executable stack is freely available.
3. **Compiler tools:** Over the years, compilers have become more and more aggressive in optimizations, and the checks they perform. Various compiler tools already offer warnings on the use of unsafe constructs such as `gets()`, `strcpy()`, etc. Developers should be educated to recognize the programming code if such warnings are displayed.
4. **Dynamic run-time checks:** In this scheme, an application has restricted access to prevent attacks. This method primarily relies on the safety code being preloaded before an application is executed. This preloaded component can either provide safer versions of the standard unsafe functions or

Table 4.17 | Tools used to defend/protect buffer overflow

Sr. No.	Tool	Brief Description
	StackGuard	It was released for GCC in 1997 and published at USENIX Security 1998. It is an extension to GCC that provides buffer overflow protection. It was invented by Crispin Cowan. It is a compiler approach for defending programs and systems against "stack-smashing" attacks. These attacks are the most common form of security vulnerability. Programs that have been compiled with StackGuard are largely immune to stack-smashing attack. Whenever vulnerability is exploited, it detects the attack in progress, raises an intrusion alert and halts the victim program.
2	ProPolice	The "stack-smashing protector" or SSP, also known as PmPolice, is an enhancement of the StackGuard concept written and maintained by Hiroaki Ech of IBM. Its name derives from the word propolis. The stack protection provided by ProPolice is specifically for the C and C++ languages. It is also optionally available in Gentoo Linux with the hardened USE flag.
3	LibSafe	It was released in April 2000 and gained popularity in the Linux community. It does not need access to the source code of the program to be protected. Libsafe protection is system wide and automatically gets attached to the applications. It is based on a middleware software layer that intercepts all function calls made to library functions known to be vulnerable. A substitute version of the corresponding function implements the original function in a way that ensures that any buffer overflows are contained within the current stack frame, which prevents attackers from overwriting the return address and hijacking the control flow of a running program. The real benefit of using libsafe is protection against future attacks on programs not yet known to be vulnerable.

it can ensure that return addresses are not overwritten. One example of such a tool is libsafe. The libsafe library provides a way to secure calls to these functions, even if the function is not available. It makes use of the fact that stack frames are linked together by frame pointers. When a buffer is passed as an argument to any of the unsafe functions, libsafe follows the frame pointers to the correct stack frame. It then checks the distance to the nearest return address and when the function executes, it makes sure that address is not overwritten.

5. Various tools are used to detect/defend buffer overflow: See Table 4.17 to know about few such tools.

4.12 Attacks on Wireless Networks

Even when people travel, they still need to work. Thus, work *seems* to be moving out of the traditional offices into homes, hotels, airport lounges and taxis. The employee is no longer tied to an office location and is, in effect, "boundaryless." When one talks to the young generation about their lifestyles, one realizes that gone are those days when an "office" conjured up the image of the four walls, set in the formal setting, typical office decor and with all the formality that one can imagine, which may perhaps be difficult for our new generation to appreciate. In the yesteryears, "working" meant leaving home, commuting to the workplace, spending those typical 9 a.m.-6 p.m. in the office and then shutting down the work and commuting back home or wherever back one wished to be after office hours. The "working" and "away from work" were clearly delineated distinct states that one could be in. Gone are those days and now we are in the era of computing anywhere, anytime! There is no doubt that workforce "mobility" is on the rise (see Box 9.1, Chapter 9).

The following are different types of "mobile workers":

1. **Tethered/remote worker:** This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, tele-cottagers and, in some cases, branch workers.
2. **Roaming user:** This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
3. **Nomad:** This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels. This type includes the sales and field forces.

Wireless technologies have become increasingly popular in day-to-day business and personal lives. Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs. Wireless networks are generally composed of two basic elements: (a) access points (APs) and (b) other wireless-enabled devices, such as laptops, radio transmitters and receivers to communicate or "connect" with each other (see Fig. 4.6). APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.

Wireless access to networks has become very common by now in India - for organizations and for individuals. Many laptop computers have wireless cards preinstalled for the buyer, for example, in India, such cards are provided by 1ATA Indicom, Reliance and Airtel. There are many hotels and equivalent establishments all over the world (including India) where the rooms are "Wi-Fi enabled." There is no denying that the ability to enter a network while on the move (working away from home or in other locations that are not routine office locations, working while in hotels, etc.) has great benefits (see Box 4.10 for some interesting facts).

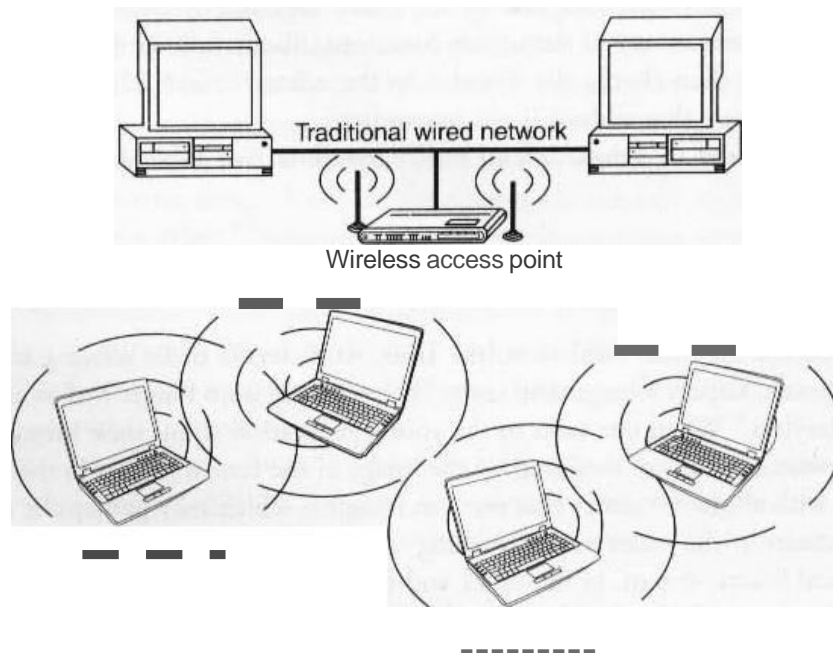


Figure 4.6 | Wireless networks.

Box 4.10 Going Wi-Fi

Start with a laptop computer or other portable device that could benefit from Internet access. Make sure it is wireless. Look for Intel's Centrino sticker or any sign that Wi-Fi is built into the device. If not, you need an external Wi-Fi Personal Computer Memory Card International Association (PCMCIA)-compliant card. Find a public hotspot by searching store windows for stickers that say Wi-Fi Zone, T-Mobile HotSpot or anything indicating a wireless service. Boot up your laptop and login, at home or at a hotel, or get a Wi-Fi router and plug one end into your cable or digital subscriber line (DSL) modem. The router will broadcast the wireless Internet signal in your house and you can sit on the couch and surf the Internet.

Although wireless technology is not new, it is now being used by families who need an easy way to share a fast Internet connection with two or more computers at home. It is helping almost anybody, including even the "non-techies," to get Internet access while they buy their daily cup of coffee at a Wi-Fi coffeehouse. This kind of scene is now very common in most Indian metros, including some small cities too.

Cell phones have become indispensable for many who use them to keep track of family members or to call for help in an emergency. Wi-Fi is not there yet, however, the idea of wireless Internet access on every corner is becoming a 24/7 possibility as more companies set up public hotspots. Like cell phones, Wi-Fi is not something you will use every minute, but it can be convenient when you need to check for an E-Mail message or compare the price of an online gift.



Readers may like to visit <http://computer.howstuffworks.com/wifi-quiz.htm> to test fundamental knowledge about wireless networks before going through this section.

Wireless technology is no more a buzzword in today's world. Let us understand important components of a wireless network, apart from components such as modem, routers, hubs and firewall, which are integral parts of any wired network as well as wireless network.

- J. 802.11 networking standards: Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication in the 2.4, 3.6 and 5 GHz frequency bands.
- 802.11: It is applicable to WLANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency-hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
 - 802.11n: It provides 54 Mbps transmission in the 5 GHz band and uses orthogonal frequency-division multiplexing (OFDM) which is more efficient coding technique compared with FHSS and DSSS.
 - 802.11b: It provides 11 Mbps transmission in the 2.4 GHz band and uses complementary codec: coding (CCK) modulation to improve speeds. In 1999, ratification was made to the original 802.11 standard, and was termed as 802.11b, which allowed wireless functionality comparable to Ethernet. Although it was being a slowest standard, at the same time being the least expensive, the evolution led to the rapid acceptance of 802.11b across the world as the definitive WLAN technology and known as "Wi-Fi standard."
 - 802.11g: It provides 54 Mbps transmission in the 2.4 GHz band and the same OFDM coding as 802.11a, hence it is a lot faster than 802.11a and 802.11b.
 - 802.11n: It is the newest standard available widely and uses multiple-input multiple-output (MIMO) that enabled to improve the speed and range significantly. For example, although

802.11g provides 54 Mbps transmission theoretically, however, it can only achieve 24 Mbps of speed because of network traffic congestion. However, 802.11n can achieve speeds as high as 140 Mbps.

The other important 802 family members are as follows:

- **802.15:** This standard is used for *personal WLANs* and covers a very short range. Hence, it is used for *Bluetooth Technology*.
 - **802.16:** It is also known as *WiMAX*. It combines the benefits of broadband and wireless, hence it provides high-speed wireless Internet over very long distances and provides access to large areas such as cities. This standard is developed by IEEE working group established in 1999 to develop the standards for *Wide Area Metropolitan Area Networks*.
2. **Access points:** It is also termed as AP. It is a hardware device and/or a software characterised as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.
 3. **Wi-Fi hotspots:** A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.
 - **Free Wi-Fi hotspots:** Wireless Internet service is offered in public areas, free of cost and that too without any authentication. The users will have to enable the wireless on their devices, search for such hotspots and will have to *click* connect. The Internet facility is made available to the user. As the authentication mechanism on the router is disabled, user gets connected to WLAN and cybercriminals get their prey. As, access to free hotspots cannot be controlled, cybersecurity is always questioned. Readers may visit www.hotspot-locations.com to find wireless hotspots in their area. Hotspot locations is the free global hotspot database of wireless access points made available to the general public.
 - **Commercial hotspots:** The users are redirected to authentication and online payment to avail the wireless Internet service in public areas. The payment can be made using credit/debit card through payment gateways such as PayPal. Major airports and business hotels are usually charged to avail wireless Internet service. Some Internet service providers offer virtual private network (VPN) as a security feature but found to be an expensive option.

Although the user has been authenticated while connecting to a hotspot, it does not mean that he/she is on the secured communication channel. A "poisoned/rogue hotspot" is termed to be a free public hotspot set up by the cybercriminals, with the objective of sniffing the data sent by the user. They can easily obtain the User IDs (i.e., login names), decipher the passwords and/or other sensitive information by examining packets sent by the user (see Section 7.9, Chapter 7).
 4. **Service set identifier (SSID):** It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID, which results in the detected network displaying as an unnamed network and the user would need to manually enter the correct SSID to connect to the network. Hence, it is also advised to set the SSID manually rather than leaving it blank. Moreover, it is important to note that turning off the broadcast of the SSID discourages casual wireless snooping, however, it does not stop an attacker from trying to attack the network.
 5. **Wired equivalence privacy (WEP):** Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is

always termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.

6. **Wi-Fi protected access (WPA and WPA2):** During 2001, serious weakness in WEP was identified that resulted WEP cracking software(s) being made available to enable cybercriminals to intrude into WLANs. WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WPA2 is the approved Wi-Fi alliance (www.wi-fi.org) interoperable implementation of 802.11i. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government agencies.
7. **Media access control (MAC):** It is a unique identifier of each node (i.e., each network interfaces) of the network and it is assigned by the manufacturer of a network interface card (NIC) stored in its hardware. MAC address filtering allows only the devices with specific MAC addresses to access the network. The router should be configured so that only those addresses are allowed. Although this method appears to be very secure, the attacker can spoof a MAC address, that is, copy the known MAC address to entice the network that the device he/she is using belongs to the network, at the same time it is important to note that, in case you purchase a new device or if any visitors would like to connect to the network, you will need to add the MAC addresses of these new devices to the list of approved addresses.

How to find MAC Address?

Readers may visit www.dcn.fnl.gov/DCG-Docs/mac/ OR www.coffer.com/mac_info/ to know the steps to find the MAC address on the systems running on various operating systems (OS) as well as in case if no OS is installed.

While all this sounds very exciting, it is important to understand that wireless networking has many security issues. Crackers have found wireless networks relatively easy to break into. They are known to use wireless technology to crack into non-wireless networks. Network administrators must be aware of these risks and should stay up to date on any new risks that arise. Users of wireless equipment must be aware of these risks so as to take personal protective measures. As the wireless service technology is getting improved and falling within an easy reach of information technology (IT) as well as non-IT workers, the risks to users of wireless technology have increased exponentially (see Section 9.3.1, Chapter 9).

There were relatively few dangers when wireless technology was first introduced. Although the attackers have no time to latch on to the new technology as wireless was not commonly found in the workplace, however, there are a great number of security risks associated with wireless technology. Some issues are obvious and some are not. At a corporate level, it is the responsibility of the IT department to keep up to date with the types of threats and appropriate countermeasures to deploy. Security threats are growing in the wireless arena. The attackers have learnt that there is much vulnerability in the current wireless protocols, encryption methods and the carelessness and ignorance that exist at the user and corporate IT levels. Cracking methods have become much more sophisticated and innovative with the availability of different tools used to search and hack wireless networks. Cracking has become much easier and more accessible with easy-to-use Windows- and Linux-based tools being made available on the Web at no charge (see Table 4.18).

The overall philosophy behind wired networks vs. wireless networks is "trust." On a wired network, the hardware is under the direct control of the network administrator, and therefore, the overall attitude toward

Table 4.18 Tools used for hacking wireless networks

Website	Brief Description
http://www.nemumbier.com/	NecSrumbler: This tool is based on Windows OS and easily identifies wireless signals being broadcast within range. It also has ability to determine signal/noise char can be used for site surveys.
http://www.kismetwireless.net/	Kismet: This tool detects and displays SSIDs that are not being broadcast which is very critical in finding wireless networks. NecSrumbler does have this key functional element - ability to display wireless networks that are not broadcasting their SSID.
http://sourceforge.net/projects/airsnort/files/	Airsnort: This tool is very easy and is usually used to sniff and crack WEP keys (http://airsnort.shmoo.com/).
http://wirelessdefence.org/Contents/coXIPAttyMain.htm	CowPatty: This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the "New WEP" for home wireless security. This program simply tries a bunch of different options from a dictionary file to see if one ends up matching what is defined as the preshared key.
http://www.wireshark.org/	Wireshark (formerly ethtereal): Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs.

Source: <http://www.ethicalhackers.net/conlem/view/16/24/> (10 May 10).

the workstations tends to be one of course. With a wireless network, it is possible that someone could sit in the parking lot with a laptop and access your wireless network. Therefore, the general attitude toward wireless workstations tends to be one of extreme distrust. However, this difference in attitude of fear causes the same administrators to take extreme positions when it comes to guarding network security. Although they tend to go to extreme lengths at securing a wireless network, at times they almost neglect wired network security. Things to watch out for are the following: Are there any unused network jacks or unused switch ports in the office? This is important because if someone was able to sneak into the office and plug a laptop into one of these unused jacks, you may no longer have the same level of trust in the hardware on your wired network.

4.12.1 Traditional Techniques of Attacks on Wireless Networks

In security breaches, penetration of a wireless network through unauthorized access, is termed as *Wireless Cracking*. There are various methods that demand high level of technological skill and knowledge, and availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

- I. **Sniffing:** It is eavesdropping on the network and is the simplest of all attacks. Sniffing is the simple process of intercepting wireless data that is being broadcasted on an unsecured network. Also termed as reconnaissance technique, it gathers the required information about the active/available Wi-Fi networks. The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as
 - Passive scanning of wireless network;
 - detection of SSID;
 - collating the MAC address;
 - collecting the names to crack WEP

2. **Spoofing:** The primary objective of this attack is to successfully masquerade the identity by falsifying data and thereby gaining an illegitimate advantage. The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a legitimate network. It causes unsuspecting computers to automatically connect to the spoofed network instead of the real one. The attacker can conduct this activity easily because while setting up a wireless network, the computers no longer need to be informed to access the network; rather they access it automatically as soon as they move within the signal range. This convenient feature is always exploited by the attacker.
 - **MAC address Spoofing:** It is a technique of changing an assigned media access control (MAC) address of a networked device to a different one. This allows the attacker to bypass the access control lists on servers or routers by either hiding a computer on a network or allowing it to impersonate another network device.
 - **IP Spoofing:** It is a process of creating IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. To engage in IP Spoofing, the attacker uses a variety of techniques to find an IP address of a trusted host(s) and then modifies the packet headers so that it appears that the packets are coming from that host, that is, legitimate sender.
 - **Frame Spoofing:** The attacker injects the frames whose content is carefully spoofed and which are valid as per 802.11 specifications. Frames themselves are not authenticated in 802.11 networks and hence when a frame has a spoofed source address, it cannot be detected unless the address is entirely faked/bogus.
3. **Denial of service (DoS):** We have explained this attack in detail in Section 4.9.
4. **Man-in-the-middle attack (MITM):** It refers to the scenario wherein an attacker on host A inserts A between all communications between hosts X and Y without knowledge of X and Y. All messages sent by X do reach Y but through A and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.
5. **Encryption cracking:** It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

4.12.2 Theft of Internet Hours and Wi-Fi-based Frauds and Misuses

Information communication technology (ICT) is within reach of people nowadays and most of the new systems (i.e., computers) are equipped for wireless Internet access as more and more people are opting for Wi-Fi in their homes. Wireless network into homes is becoming common necessity because of lifestyle and availability of inexpensive broadband routers that can be configured easily and/or there is no need to configure these devices at all because of plug-and-play feature. This enables the Internet on the finger tip of home users and in case, unfortunately, he/she visits a malicious webpage, the router is exposed for an attack. Thus, as the networks become stronger and more prevalent, more of the signals are available outside the home of the subscriber, spilling over into neighbor's apartments, hallways and the street. In today's era of high dependency on the Internet for many aspects of our life and given that predators are lurking around as potential cybercriminals, they (criminals) often wonder how they can find out who they are stealing from so that they can get an idea if their information is safe. According to a study by Jupiter Research, 14% of wireless

network owners have accessed their neighbor's connection.³⁶¹ It appears that more and more people are logging on for free.

Cybercriminals know that they should not steal Internet hours purchased by others but somehow they want to get their work done without paying for the Internet connection and they also want to know if anyone knows how to find out who they are stealing it from. Here is what they are mostly likely to do: (a) they find out the IP address of the router that you are using, (b) open up a command prompt (go to Start > click on Run > type cmd and press Enter) at the command prompt and (c) type this command `ipconfig /all` and press Enter. Look for the default gateway (this is the router); once you see the IP address type the router's IP address into your browser and you can find out some information about who you are seeing Internet from.

An interesting question is whether "stealing" wireless Internet is illegal. We have discussed it under a mini-case in Chapter 11 (in CD) and readers may visit the URL provided in Ref. #13, Additional Useful Web References, Further Reading. Here is one scenario, given that use of laptops is now common place. Suppose you figure out how to connect the laptop to one of the many wireless networks detected on your laptop. Is this illegal? As we shall learn in Chapter 6 the laws vary around the world. However, for the most part, logging and collecting information, such as surfing the Web or checking E-Mail, from wireless networks that are accessible to anyone with a receiver is OK. The act of wardriving is searching for wireless networks by a moving vehicle using a portable computer or PDA.⁷¹ Readers may visit the URL mentioned in Ref. #3, Video Clips, Further Reading to watch a small video clip on how wardriving is conducted.

Software for wardriving is freely available and can be downloaded from the Internet - to name a few NetStumbler for Windows, Kismet or SWScanner for Linux, and FrecBSD, NecBSD, OpenBSD, DragonFly BSD, Solaris and KisMac for Macintosh. Wardrivers log and collect information from the wireless access points (WAP) they find while driving (see Box 4.11). Think about radio airwaves: as long as you have a radio, listening to a radio station broadcasting where you are driving is free (at least in the US).

Box 4.11 The New "Wars" in the Internet Era!

Basically, the term "wardriving" was derived from the term wardialing from the 1983 film *WarGames*, which involved searching for computer systems to connect to, using software that dialed numbers sequentially, to see which ones were connected to a fax machine or computer. Subsequently, many related terms come up:

1. **Warwalking:** It is also known as "warjogging" and is similar in nature to wardriving, except that it is done on foot rather than conducted from a moving vehicle. The disadvantages of this approach consist in slower speed of travel (resulting in fewer and more infrequently discovered networks) and the absence of a convenient computing environment. Consequently, hand-held devices, such as Pocket PCs that can perform tasks while one is walking or standing, have predominated in this area. The inclusion of integrated Wi-Fi (rather than a CompactFlash, i.e., CF is a mass storage device format used in portable electronic devices or PCMCIA add-in card) in Dell Axim, Compaq iPAQ and Toshiba pocket PCs in 2002 - and, more recently, on active Nintendo DS and Sony PSP enthusiast community possessing Wi-Fi capabilities on these devices - has expanded the extent of this practice as the newer Smartphones have also integrated Global Positioning System (GPS). Of recent note, the Nokia N770, N800 and N810 Internet Tablets have very good antennas and will pick up nearly anything in the area, even blocks away from the unit.
2. **Warbiking:** Although warbiking is some as wardriving, it involves searching for wireless networks while on a moving bicycle or motorcycle. This activity is facilitated by the mounting of a Wi-Fi-capable device on the vehicle itself.

Box 4.11 The New "Wars" ... (Continued)

3. **Warkitting:** Workkilling was identified by Tsow, Jakobsson, Yong and Wetzel In 2006. This is a combination of wordriving and rootkitting - an ollock in which the wireless access point's cong. uration or firmware is modiOed over the wireless connection. This allows lhe attacker to control all traffic for the victim and may even permit fo disable Secure Sockef Loyer (SSL) by replacing HTML content. when it is being downloaded. The allacker first discovers vulnerable wireless routers through wardriving and/or by retrieving thenecessary data from existing Wi-A access point data• bases such as WiGLE (www.wigle.net) or WiFiMaps (www.wlfimaps.com) to carry out a work1tting attack
4. **WAPKitting:** In this attack, external software clutches the control of router's nrmworo that can be easily accomplished by exploi1ing open administrative access. WAPldtting con theoretically proceed by more traditional means such as buffer overflow. The ability to install arbitrary control sof1wa1e on a wireless rouser opens unlimited possibilities to on attacker.
5. **WAPJacking:** This type of attack is very similar to DNS poisoning allacks. It changes the settings of existing firmware that helps on attacker to engage in malicious configura1ion of,firmware settings; however, it makes no modification to the firmware itself, that is. allow connections to be hijacked and/or rerouted without lhe user's knowledge. WAPjocking is less powerful attack compared to WAPkitting.

WAPkitting and WAPjocking ore independent ot the means of infection, and specify the relative modifications done to a WAP upon corruption. Warkitting, on the other hand, does not specify the type of WAP alferation, but it does relate to how infection occurs.

Sovrce: <http://on.w,lc.1ped10.org/wik1/Wordriving> (31 Moy 2010J).

Be careful with use of WAPs; when you are usiog a WAP ro gain access co computer on _a nccwork, be aw.tre of the local laws/legislarions where you are doing it because rhings can become dangerous from securiry and privacy as well legal perspective. Maybe if corporations were nor in such a hurry to rele:i e chis rechnology an<l thought about it more thoroughly, they would not have LO deal wich securiry breaches and crealing uperior protection for their own systems. The moral c>f the story is that you must secure your network.

4.12.3 How to Secure the Wireless Networks

Nowadays, security fearures of Wi-Fi networking producers are not rhar time-consuming and non-intuitive: however, they are still ignored, cspecially, by home users. Although following ummarizcJ Hep will help to improve :rnd strengthen rhe security of wireless network. see Table 4.19 co know the available cools ro monitor and protccr lhe wireless nenetworks:

1. ChNge the default setrings of all the equipmenrs/componcms of wireless network (e.g., [P address/ user 10s/administraror passwords, ere.).
2. Enable WPA/\QEP encryption.
3. Change the default SSID.
4. Enable MAC address filtering.
5. Disable remote login.
6. Disable SSID broadcast.
7. Disable the fearurcs lhat arc nor used in the AP (e.g., printing/music support).
8. Avoid providing rhe network a name which can be easily identified (e.g., My_Home_Wili).
9. Connect only LO ccured wireless network (i.e., do nor autoconnect ro open Wi-Fi horspor,).
10. Upgrade router's firmware perioruc. lly.

Table 4.19 | Tools to protect wireless network

Website	Brief Description
http://www.zamzom.com/	Zamzom Wireless Network Tool: New freeware tool helps to protect wireless networks and maintain computer security, detects all computer names, Mac and IP addresses utilizing a single wireless network, reveals all computers - both authorized and unauthorized - who have access to any given wireless network. Thus, it helps users to take vital steps toward securing their wireless networks and acts as a measure that should not be overlooked or skipped.
http://www.airdefense.net/	AirDefense Guard: It provides advanced intrusion detection for wireless LANs and is based on signature analysis, policy deviation, protocol assessment, policy deviation and statistically anomalous behavior. AirDefense detects and responds to: <ul style="list-style-type: none"> • Denial-of-service (DoS) attacks; • man-in-the-middle attacks; • identity theft.
http://www.loud-fa1-blokc.co.uk/tools.html	Wireless Intrusion Detection System (WIDZ): This is an intrusion detection for wireless LANs for 802.11. It guards APs and monitors local frequencies for potentially malevolent activity. It can detect scans, association floods and bogus APs, and it can easily be integrated with other products such as SNORT or Rfsecure.
http://www.dachb0den.com/projects/bsd-airtools.html	BSD-Airtools: This tool provides a complete toolset for wireless auditing (802.11b). It contains AP detection application, Dsrumbler - similar to Netsmblcr. It can be used to detect wireless access points and connected nodes, view signal-to-noise graphs, and interactively scroll through scanned APs and view statistics for each. It also contains a BSD-based WEP cracking application (called as Dweepucils).
http://wifi.google.com/	Google Secure Access: Google Wi-Fi is a free wireless Internet service offered to the city of Mountain View (California, USA). With your Wi-Fi-enabled device and a Google Account, one can go online for free by accessing the network name "GoogleWi-Fi," which is secured by Google's virtual private network (VPN). Google Secure Access encrypts the Internet traffic and sends it through Google's servers on the Internet.

11. Assign static IP addresses to devices.
12. Enable firewalls on each computer and the router.
13. Position the router or AP safely.
14. Turn off the network during extended periods when not in use.
15. Periodic and regular monitor wireless network security.

SUMMARY

When information systems are the target of offense, the criminal's goal is to steal information from, or cause damage to, a computer, computer system or computer network. The perpetrators range from teenagers (script kiddies/cyberjoyriders) to organized crime operators and international terrorists.

A computer can be the target of offense; tools may be used in an offense, or may contain evidence of an offense. An understanding of different uses of a computer will provide foundation of the application of the criminal statutes.

UNIT V

Cyber Security Organizational Policies, Risk and Challenges

Cybersecurity: Organizational Implications

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups.

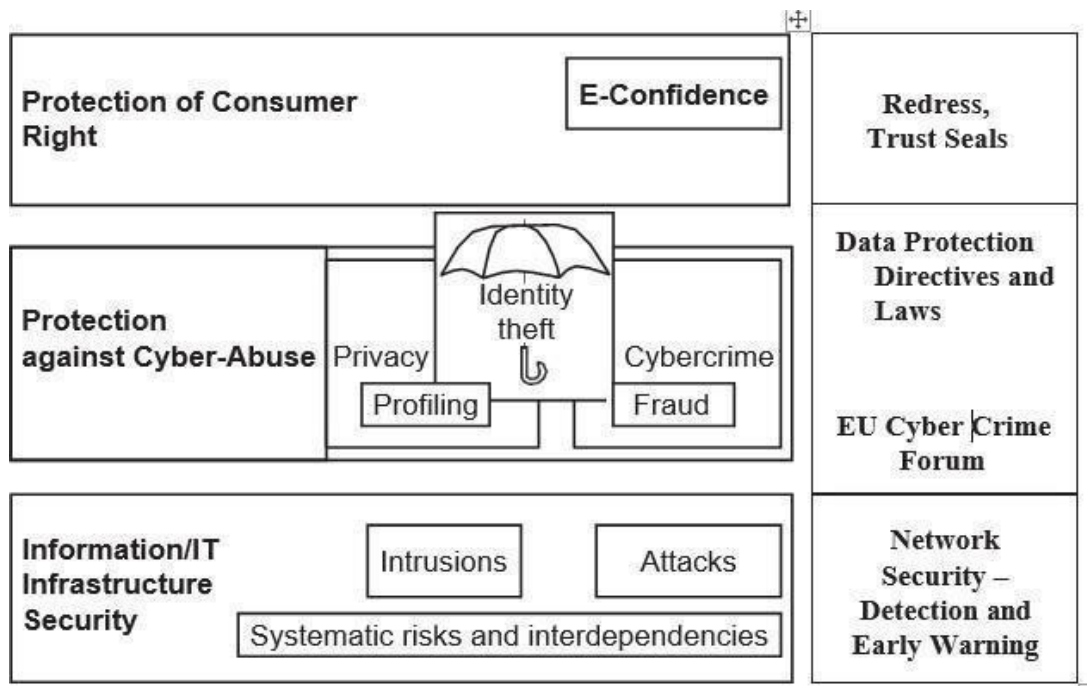


Fig: A cybersecurity perspective. EU is the European Union.

PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Most information the organization collects about an individual is likely to come under “PI” category if it can be attributed to an individual. For an example, PI is an individual’s first name or first initial and last name in combination with any of the following data:

1. Social security number (SSN)/social insurance number.
2. Driver’s license number or identification card number.
3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual’s financial account.
4. Home address or E-Mail address.
5. Medical or health information.

An insider threat is defined as “the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other ‘trusted’ individuals.”

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of “insiders” such as:

1. A malicious insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability.
2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
3. A tricked insider is a person who is “tricked” into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via “pretexting” (known as social engineering).

- **Insider Attack Example 1: Heartland Payment System Fraud**

A case in point is the infamous “Heartland Payment System Fraud” that was uncovered in January 2010. This incident brings out the glaring point about seriousness of “insider attacks. In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is transmitted through a payment network.

- **Insider Attack Example 2: Blue Shield Blue Cross (BCBS)**

Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states.

The two lessons to be learnt from this are:

1. Physical security is very important.
2. Insider threats cannot be ignored.

What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked. There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

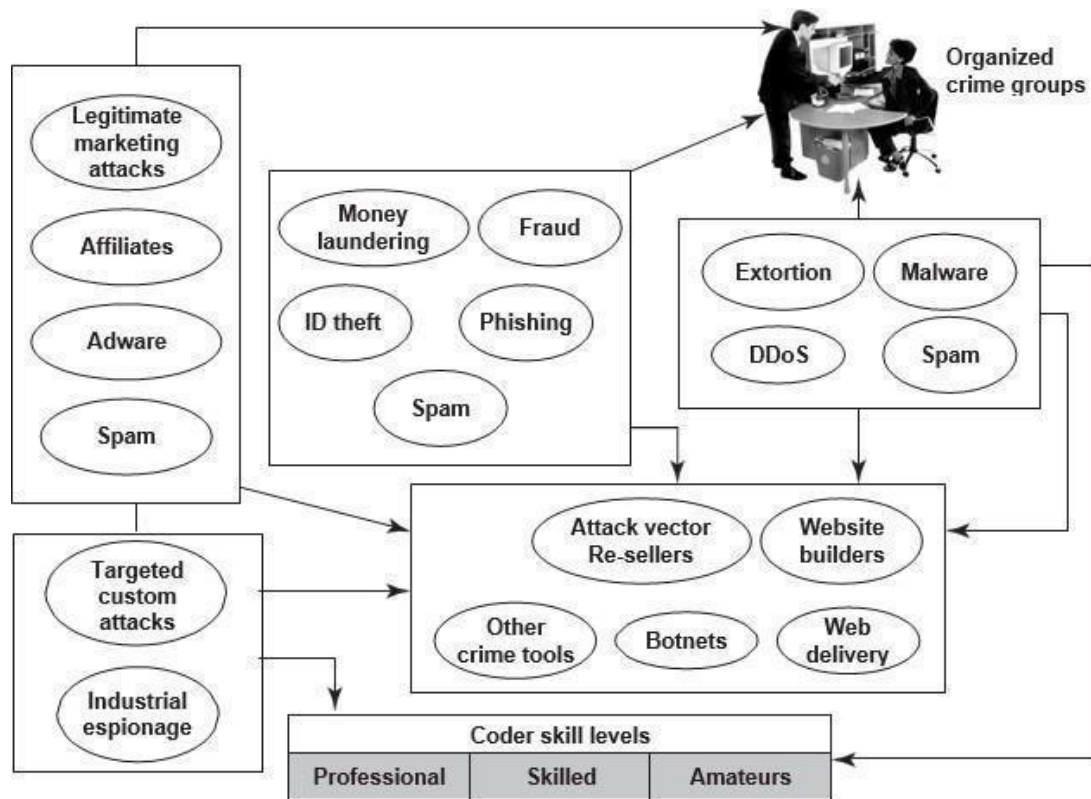


Fig: Cybercrimes – the flow and connections.

A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and “privacy” which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the users’ rights to determine how, when and to what extent information about them is communicated to other parties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
4. **Territorial privacy:** It is about protecting users’ property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are described here.

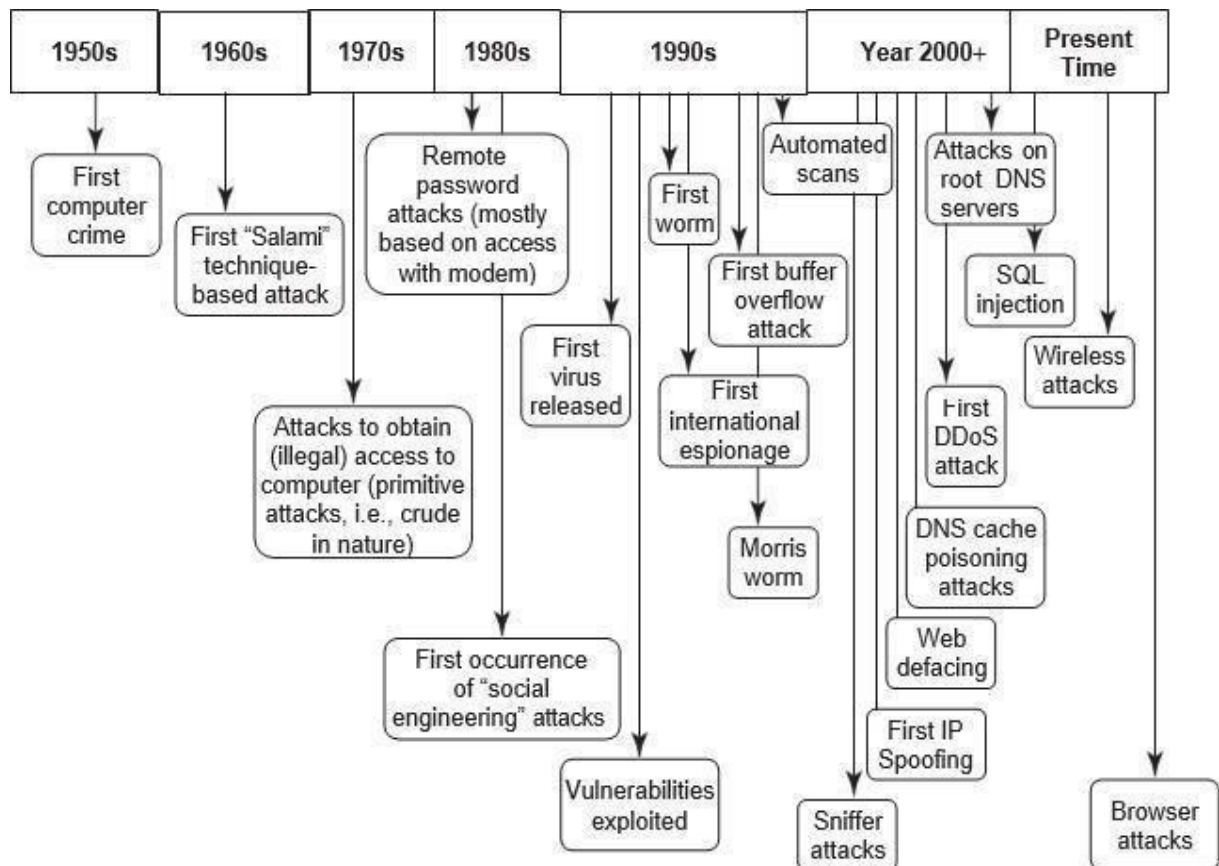


Fig: Security threats – paradigm shift.

The key challenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website.
5. **Confidential information leakage:** "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions.

➔ Cost of Cybercrimes and IPR Issues: Lessons for Organizations

Reflecting on the discussion in the previous sections brings us to the point that cybercrimes cost a lot to organizations.

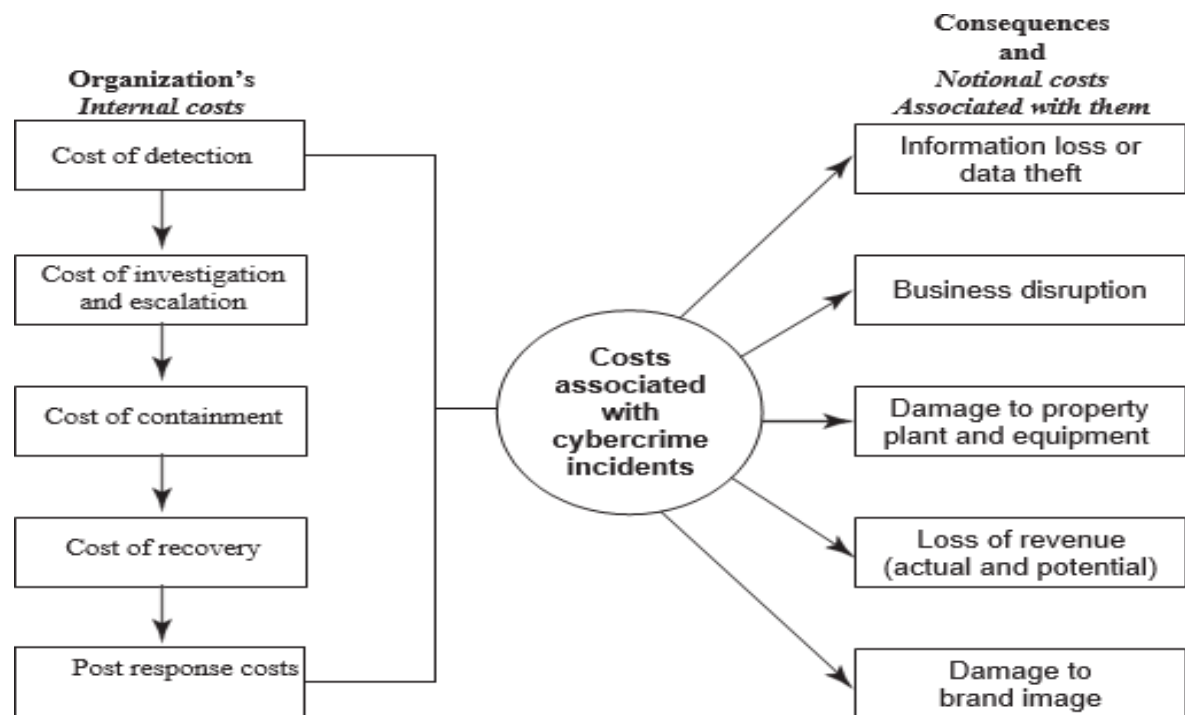


Fig: Cost of cybercrimes.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

Detection and recovery constitute a very large percentage of internal costs. This is supported by a benchmark study conducted by Ponemon Institute USA carried out with the sample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees.

- **Organizations have Internal Costs Associated with Cybersecurity Incidents**

The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark study mentioned:

1. Detection costs.
2. Recovery costs.
3. Post response costs.
4. Investigation costs.
5. Costs of escalation and incident management.
6. Cost of containment.

- **The consequences of cybercrimes and their associated costs, mentioned**

1. Information loss/data theft.
2. Business disruption.

3. Damages to equipment, plant and property.
 4. Loss of revenue and brand tarnishing.
 5. Other costs.
- **There are many new endpoints in today's complex networks; they include hand-held devices.**

Again, there are lessons to learn:

1. **Endpoint protection:** It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of the endpoints.
 2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from "Malicious Code" inside business applications.
 3. **HR checks:** These are important prior to employment as well as after employment.
 4. **Access controls:** These are always important, for example, shared IDs and shared laptops are dangerous.
 5. **Importance of security governance:** It cannot be ignored policies, procedures and their effective implementation cannot be over-emphasized.
- **Organizational Implications of Software Piracy**

Use of pirated software is a major risk area for organizations.

From a legal standpoint, software piracy is an IPR violation crime. Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability.

The most often quoted reasons by employees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readily available.
2. Many others use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

→ **Web Threats for Organizations: The Evils and Perils**

Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing.

- **Overview of Web Threats to Organizations**

The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like they do at home.

IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

- **Employee Time Wasted on Internet Surfing**

This is a very sensitive topic indeed, especially in organizations that claim to have a “liberal culture.” Some managers believe that it is crucial in today’s business world to have the finger on the pulse of your employees.

People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

- **Enforcing Policy Usage in the Organization**

An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization.



Fig: Policy hierarchy chart.

- **Monitoring and Controlling Employees’ Internet Surfing**

A powerful deterrent can be created through effective monitoring and reporting of employees’ Internet surfing.

Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours.

- **Keeping Security Patches and Virus Signatures Up to Date**

Updating security patches and virus signatures have now become a reality of life, a necessary activity for safety in the cyberworld! Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.

- **Surviving in the Era of Legal Risks**

As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection.

Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

- **Bandwidth Wastage Issues**

Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.

There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

- **Mobile Workers Pose Security Challenges**

Use of mobile handset devices in cybercrimes. Most mobile communication devices for example, the personal digital assistant

- **Challenges in Controlling Access to Web Applications**

Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications.

- **The Bane of Malware**

Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyber attackers, too, are learning. Criminals change their techniques rapidly to avoid detection.

- **The Need for Protecting Multiple Offices and Locations**

Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations.

→ **Social Media Marketing: Security Risks and Perils for Organizations**

Social media marketing has become dominant in the industry.

According to fall 2009 survey by marketing professionals, usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. My Space is used by 6% of the organizations.

Although the use of social media marketing site is rampant, there is a problem related to “social computing” or “social media marketing” – the problem of privacy threats.

Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of “social media marketing.”

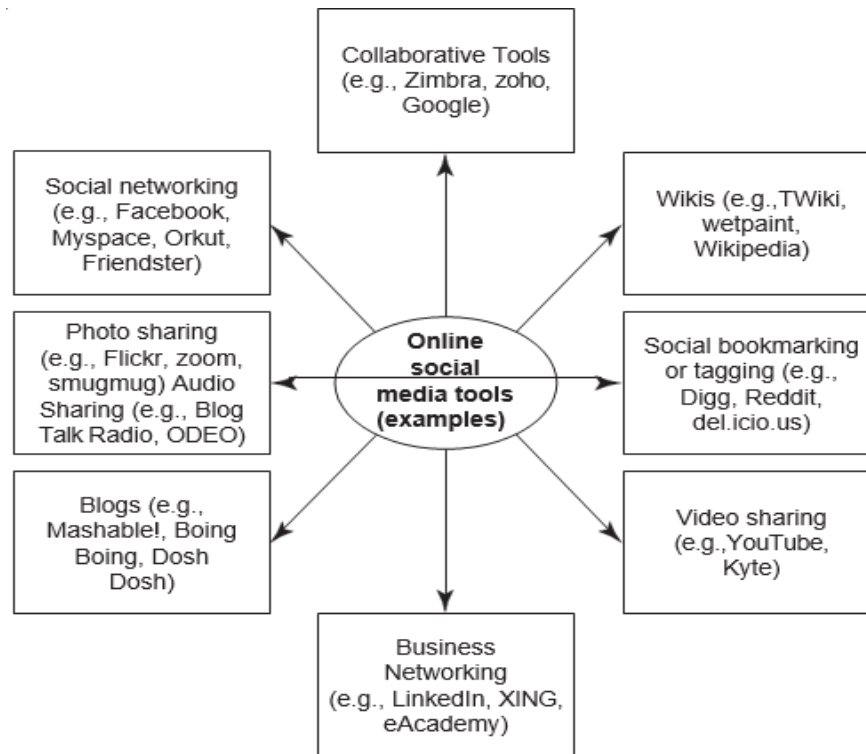


Fig: Social media - online tools.

- **Understanding Social Media Marketing**

Most professionals today use social technologies for business purposes. Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.

Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
2. To increase traffic to their website coming from other social media websites by using Blogs and social and business-networking. Companies believe that this, in turn, may increase their “page rank” resulting in increased traffic from leading search engines.
3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
4. To build credibility by participating in relevant product promotion forums and responding to potential customers’ questions immediately.

5. To collect potential customer profiles. Social media sites have information such as user profile data, which can be used to target a specific set of users for advertising

There are other tools too that organizations use; industry practices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a community of top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

WHAT IS SOCIAL COMPUTING?

The social and interactive aspect of online activity is known as social computing. The phrase may be interpreted in contrast to personal computing, which refers to the activities of single users.

Blogs, wikis, Twitter, RSS, instant messaging, multi-gaming, and open source development are just a few examples of social computing. It also includes social networking and social bookmarking sites. The concept of Web 2.0 can be interpreted as the architecture for applications that support its processes. The term “social computing” is somewhat of a misnomer. It should not be implied that social computer applications are the same as artificial intelligence programs such as socially intelligent computing. The computer is required to exhibit social capabilities and make the person using it feel more socially engaged when they are not.

BENEFITS OF SOCIAL COMPUTING

Social networking allows organizations to do many things, including disseminating information among its various users, keeping them up to date on new knowledge and experience, reducing interruptions, and connecting them with the best experts for particular needs.

The notion of “social computing” refers to increasing knowledge access speed. In addition, it allows for a wide range of information to be shared through interactions with numerous people. By connecting people and thus lowering the cost of communication, computer technology improves communication among many users. The methodology improves user performance and efficiency, increasing access to specialists. Users obtain a better performance and greater efficiency due to this method.

Social computing reduces traveling expenses since it is linked to the internet process, lowering labor and travel costs. As employee satisfaction rises, so does its role in improving performance and quality of service.

EXAMPLES OF SOCIAL COMPUTING

Social computing uses computers and software to create communities around shared interests. All of these examples and blogs, wikis, Twitter, RSS, instant messaging, multiplayer gaming, open-source development, and social networking and social bookmarking sites are all forms. Web 2.0 is closely linked to the notion of social computing.

Many less obvious kinds of social computing are accessible to us today. Consider eBay, where buyers can leave user reviews of sellers and their responses. Look to Amazon, where you may now rate the reviewer rather than only the product.

Security and Privacy Implications from Cloud Computing

There are data privacy risks associated with cloud computing. Basically, putting data in the cloud may impact privacy rights, obligations and status. There is much legal uncertainty about privacy rights in the cloud. Organizations should think about the privacy scenarios in terms of “user spheres.”

There are three kinds of spheres and their characteristics are as follows:

1. **User sphere:** Here data is stored on users’ desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization’s responsibility is to provide access to users and monitor that access to ensure misuse does not happen.
2. **Recipient sphere:** Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data.
3. **Joint sphere:** Here data lies with web service provider’s servers and databases. This is the in between sphere where it is not clear to whom does the data belong.

→ Protecting People’s Privacy in the Organization

The costs associated with cybercrimes. A key point in that discussion is that people perceive their PI/SPI to be very sensitive. From privacy perspective, people would hate to be monitored in terms of what they are doing, where they are moving.

In the US, Social Security Number is a well-established system/mechanism for uniquely identifying all American citizens; however, similar thoughts are now emerging in India. The UID Project was started by Government of India and is running through an agency called Unique Identification Authority of India (UIDAI) based on the similar concept.

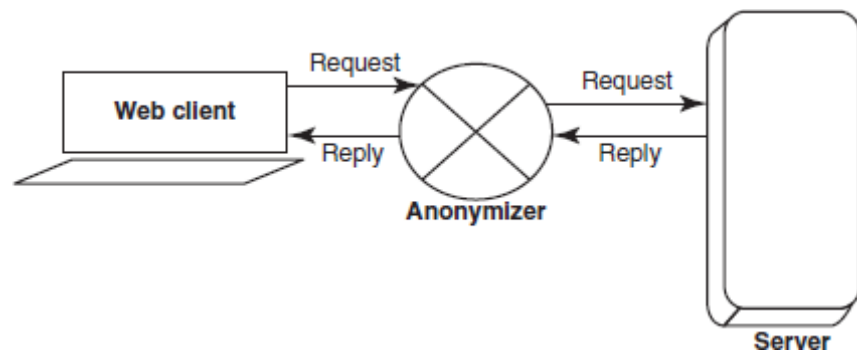


Fig: Anonymity by web proxy.