PVP 20

Code: 20CS4702C

IV B.Tech - I Semester – Regular Examinations - DECEMBER 2023

CYBER SECURITY
(COMPUTER SCIENCE & ENGINEERING)

Scheme of Valuation

UNIT-I

1a) Write a short note on:-

i) Cyber terrorism (3.5 M)

Explanation – 3.5 M

ii) Cyber Squatting (3.5 M)

Explanation – 3.5 M

1 b) Explain different types of Cybercrimes. (7 M)

Explaining any 4 types of cybercrimes – 7 M

OR

2 a) Define Cybercrime. Who are Cyber criminals and explain their types. (7 M)

Definition's : 3 M

Cyber Criminals Definition: 1 M

Cyber Criminals Types: 3 M

2 b) Write a short note on:-

i) Software piracy. (3.5 M)

Explanation – 3.5 M

ii) Password sniffing. (3.5 M)

Explanation – 3.5 M

UNIT-II

3 a) What is Cyber stalking? Discuss. (7 M)

Explanation – 4 M

Types of stalkers – 3 M

3 b) Write about Cyber café and Cybercrimes. (7 M)

Explanation – 7 M

OR

4 a) What are Botnets? Explain. (7 M)

Explanation – 7 M

4 b) How Botnets are involved in Cybercrimes? (7 M)

Explanation – 7 M

UNIT-III

5 a) Discuss about Authentication Service Security. (7 M)

Explanation & Mechanisms – 7 M

5 b) What are different security challenges posed by Mobile devices? (7 M)

Explanation – 7 M

OR

6 a) Explain about the Organizational Security policies for mobile devices. (7 M)

Explanation – 7 M

6 b) What are different Security policies on Laptops and Wireless devices? Explain. (7 M)

Explanation – 7 M

UNIT-IV

7 a) What is Phishing? How it Works. (7 M)

Explanation – 7 M

7 b) Difference between Steganography and Cryptography. (7 M)

Explanation – 7 M

OR

8 a) Discuss in detail about Virus and Worms. (7 M)

Explanation on virus– 3.5 M

Explanation on worms– 3.5 M

8 b) Explain Buffer Overflow. (7 M)

Explanation – 7 M

UNIT-V

9 a) Discuss about Social Computing. (7 M)

Explanation – 7 M

9 b) Discuss about Social media Marketing. (7 M)

Explanation – 7 M

OR

10 a) What are different perils for Organizations on web threats? (7 M)

Explanation – 7 M

10 b) What are different Security Risks for Organizations on social media marketing? (7 M)

Explanation – 7 M

PVP 20

Code: 20CS4702C

IV B.Tech - I Semester – Regular Examinations - DECEMBER 2023

CYBER SECURITY
(COMPUTER SCIENCE & ENGINEERING)

Detailed Solution Set

UNIT-I

1a) Write a short note on:-

i) Cyber terrorism (3.5 M)

This term was coined in 1997 by Barry Collin, a senior research fellow at the institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. The use of information technology and means by terrorist groups & agents is called as Cyberterrorism.
"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."

(or)

Cyberterrorism is defined as "any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism."

ii) Cyber Squatting (3.5 M)

The term is derived from "squatting" which is the act of occupying an abandoned/unoccupied space/ building that the user does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.
Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them. This term is explained here because, in a way, it relates to cybercrime given the intent of cybersquatting.

Cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying "domain names" that have existing businesses names.

In India, Cybersquatting is considered to be an Intellectual Property Right (IPR). In India, Cybersquatting is seen to interfere with "Uniform Dispute Resolution Policy" (a contractual obligation to which all domain name registrants are presently subjected to).

1 b) Explain different types of Cybercrimes. (7 M)

"Crime is defined as an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the off ender liable to punishment by that law". Cybercrimes are classified as follows:

• Cybercrime against individual:
- Electronic mail (E-Mail) Spoofing and other online frauds
- Phishing, Spear Phishing and various forms
- Spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- Password sniffing

• Cybercrime against Property:
- Credit Card Frauds
- Intellectual Property (IP) Crimes
- Internet time theft

• Cybercrime against Organization:
- Unauthorized accessing of Computer
- Password Sniffing
- Denial-of-service Attacks (DoS Attacks)
- Virus attacks/dissemination of Viruses
- E-Mail bombing/Mail bombs
- Salami Attack/Salami technique
- Logic Bomb
- Trojan Horse
- Data Diddling
- Newsgroup Spam/Crimes emanating from Usenet newsgroup
- Industrial spying/Industrial espionage
- Computer network intrusions
- Software piracy

• Cybercrime against Society:
- Forgery
- Cyberterrorism
- Web Jacking

• Crimes emanating from Usenet newsgroup

OR

2 a) Define Cybercrime. Who are Cyber criminals and explain their types. (7 M)

Definition:

"A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime."

Alternative definitions of Cybercrime are as follows:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.

2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.
4. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.

Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime. The term "cybercrime" relates to a number of other terms that may sometimes be used to describe crimes committed using computers.

- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms.

Cybercrime specifically can be defined in a number of ways; a few definitions are:

- A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
- Crimes completed either on or with a computer.
- Any illegal activity done through the Internet or on the computer.
- All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.
-

Cybercrime involves such activities as child pornography; credit card fraud; cyberstalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and trademark protection; overriding encryption to make illegal copies; software piracy and stealing another's identity (known as identity theft) co perform criminal acts.

Cybercriminals are those who conduce such acts. They can be categorized into three groups that reflect their motivation:

Type I: Cybercriminals- hungry for recognition

- Hobby hackers;
- IT professionals (social engineering is one of the biggest threat);
- politically motivated hackers;
- terrorist organizations.

Type Il: Cybercriminals - not interested in recognition

- Psychological perverts;
- financially motivated hackers (corporate espionage);
- state-sponsored hacking (national espionage, sabotage);
- organized criminals.

Type III: Cybercriminals - the insiders

- Disgruntled or former employees seeking revenge;
- competing companies using employees to gain economic advantage through damage and/or theft.

2 b) Write a short note on:-

i) Software piracy. (3.5 M)

This is a big challenge area indeed. Cybercrime investigation cell of India defines "software piracy" as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. There are many examples of software piracy:

1. end-user copying: friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
2. hard disk loading with illicit means: hard disk vendors load pirated software;
3. counterfeiting: large-scale duplication and distribution of illegally copied software;
4. Illegal downloads from the Internet: by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose:
   - getting untested software that may have been copied thousands of times over,
   - the software, if pirated, may potentially contain hard-drive-infecting viruses,
   - there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users,
   - there is no warranty protection,
   - there is no legal right to use the product, etc.

ii) Password sniffing. (3.5 M)

Password Sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site. Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents. Laws are not yet set up to adequately prosecute a person for impersonating another person online. Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

It is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.

And yet, password sniffers aren't always used for malicious intent. They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN). IT practitioners know that users download and install risky software at times in their environment, running a passive password sniffer on the network of a business to identify leaky applications is one legitimate use of a password sniffer.

UNIT-II

3 a) What is Cyber stalking? Discuss. (7 M)

The dictionary meaning of "stalking" is an "act or process of following prey stealthily – trying to approach somebody or something.". Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization. The behavior

includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes. Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person. It involves harassing or threatening behavior that an individual will conduct repeatedly, for example, following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

Types of Stalkers : There are primarily two types of stalkers.

1. Online stalkers:
   - They aim to start the interaction with the victim directly with the help of the Internet.
   - E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
   - The stalker makes sure that the victim recognizes the attack attempted on him/her.
   - The stalker can make use of a third party to harass the victim.
2. Offline stalkers:
   - The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
   - Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
   - The victim is not aware that the Internet has been used to perpetuate an attack against them.

3 b) Write about Cyber café and Cybercrimes. (7 M)

In February 2009, Nielsen survey on the profile of cybercafes users in India, it was found that 90% of the audience, across eight cities and 3,500 cafes, were male and in the age group of 15–35 years; 52% were graduates and postgraduates, though almost over 50% were students. Hence, it is extremely important to understand the IT security and governance practiced in the cybercafes. In the past several years, many instances have been reported in India, where cybercafes are known to be used for either real or false terrorist communication. Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes. Cybercafes have also been used regularly for sending obscene mails to harass people. Public computers, usually referred to the systems, available in cybercafes, hold two types of risks.

- First, we do not know what programs are installed on the computer – that is, risk of malicious programs such as keyloggers or Spyware, which maybe running at the background that can capture the keystrokes to know the passwords and other confidential information and/or monitor the browsing behavior.
- Second, over-the-shoulder surfing can enable others to find out your passwords. Therefore, one has to be extremely careful about protecting his/her privacy on such systems, as one does not know who will use the computer after him/her.

Indian Information Technology Act (ITA) 2000, does not define cybercafes and interprets cybercafes as "network service providers" referred to under the Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network. Cybercriminals prefer cybercafes to carry out their activities. The criminals tend to identify one particular personal computer (PC) to prepare it for their use. Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target. Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week. A recent survey conducted in one of the metropolitan cities in India reveals the following facts:

1. Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
2. Antivirus software is found to be not updated to the latest patch and/or antivirus signature.
3. Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks. Deep Freeze can wipe out the details of all activities carried out on the computer when one clicks on the "restart" button. Such practices present challenges to the police or crime investigators when they visit the cybercafes to pick up clues after the Interet Service Provider (ISP) points to a particular IP address from where a threat mail was probably sent or an online Phishing attack was carried out, to retrieve logged files.
4. Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down. Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.
5. Pornographic websites and other similar websites with indecent contents are not blocked.
6. Cybercafe owners have very less awareness about IT Security and IT Governance.
7. Government/ISPs/State Police (cyber cell wing) do not seem to provide IT Governance guidelines to cybercafe owners.
8. Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes – one of the cybercafe owners whom we interviewed expressed a view that the police will not visit a cybercafe unless criminal activity is registered by filing an First Information Report (FIR). Cybercafe owners feel that police either have a very little knowledge about the technical aspects involved in cybercrimes and/or about conceptual understanding of IT security. There are thousands of cybercafes across India.

In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe. Here are a few tips for safety and security while using the computer in a cybercafe:

- Always logout
- Stay with the computer
- Clear history and temporary files
- Be alert
- Avoid online financial transactions
- Change passwords
- Use Virtual keyboard
- Security warnings

OR

4 a) What are Botnets? Explain. (7 M)

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.

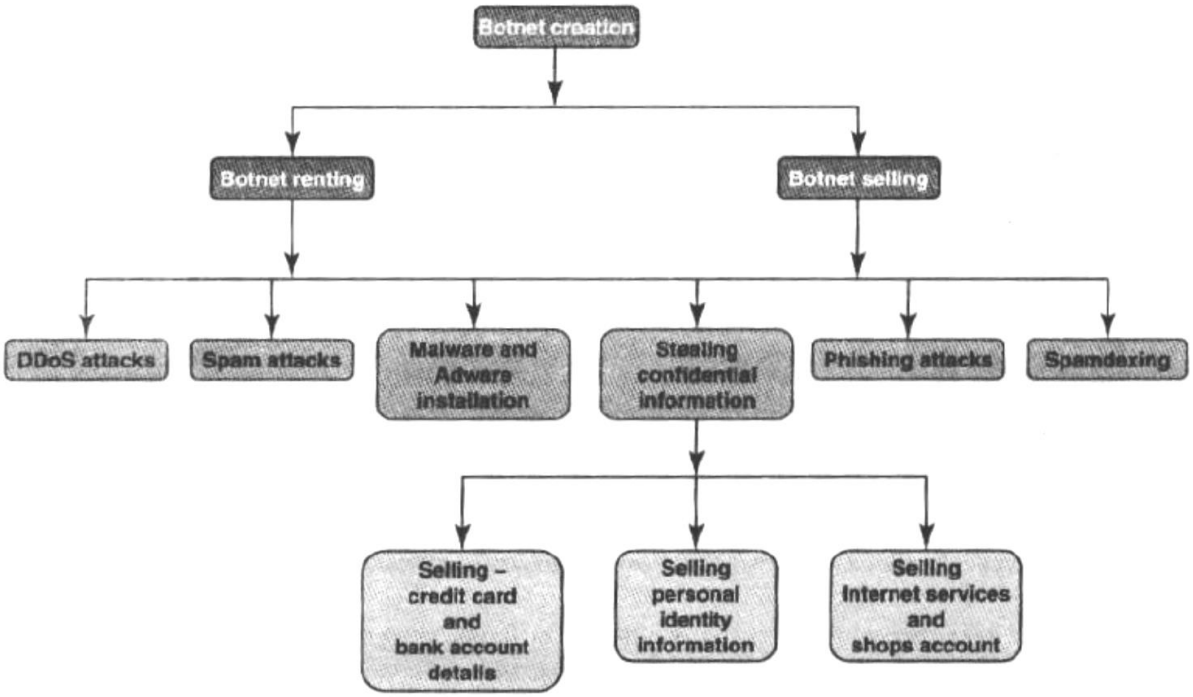
One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date
2. Set the OS to download and install security patches automatically
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet: A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.
4. Disconnect from the Internet when you are away from your computer
5. Downloading the freeware only from websites that are known and trustworthy
6. Check regularly the folders in the mail box – "sent items" or "outgoing" – for those messages you did not send
7. Take an immediate action if your system is infected

4 b) How Botnets are involved in Cybercrimes? (7 M)

In simple terms, a Bot is simply an automated computer program, one can gain the control of computer by infecting them with a virus or other Malicious Code that gives the access. Computer system maybe a part of a Botnet even though it appears to be operating normally.

- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "Zombie networks" have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge required to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.
- If someone wants to start a "business" and has no programming skills, there are plenty of "Bot for sale" offers on forums.
- 'encryption of these programs' code can also be ordered in the same way to protect them from detection by antivirus tools.
- Another option is to steal an existing Botnet. Figure explains how Botnets create business.
- One can reduce the chances of becoming part of a Bot by limiting access into the system.
- Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.



UNIT-III

5 a) Discuss about Authentication Service Security. (7 M)

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves mutual 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 (imitate) 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.

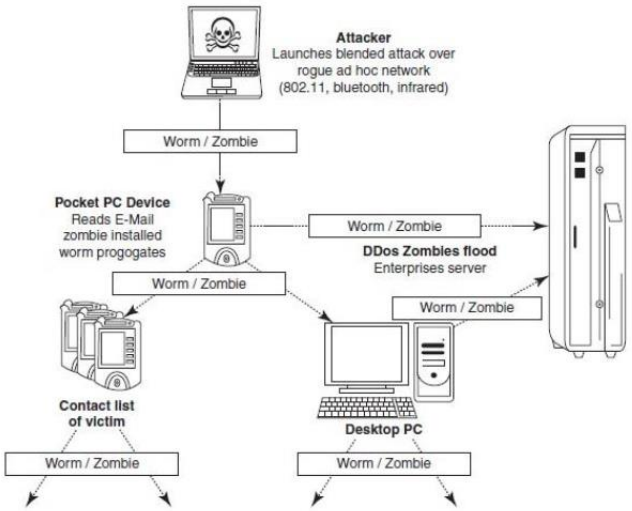


Figure: Push attack on mobile devices. DDoS implies distributed denial-of-service attack

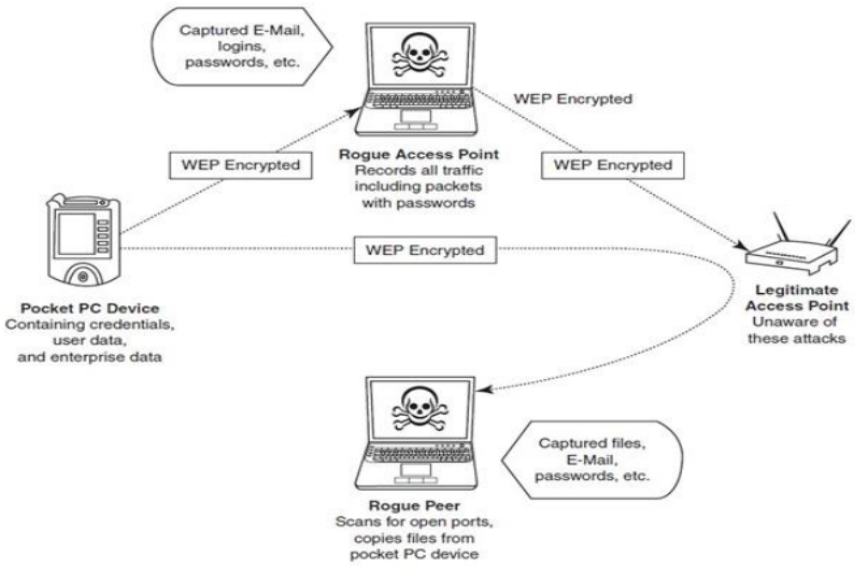


Figure: Pull attack on mobile devices

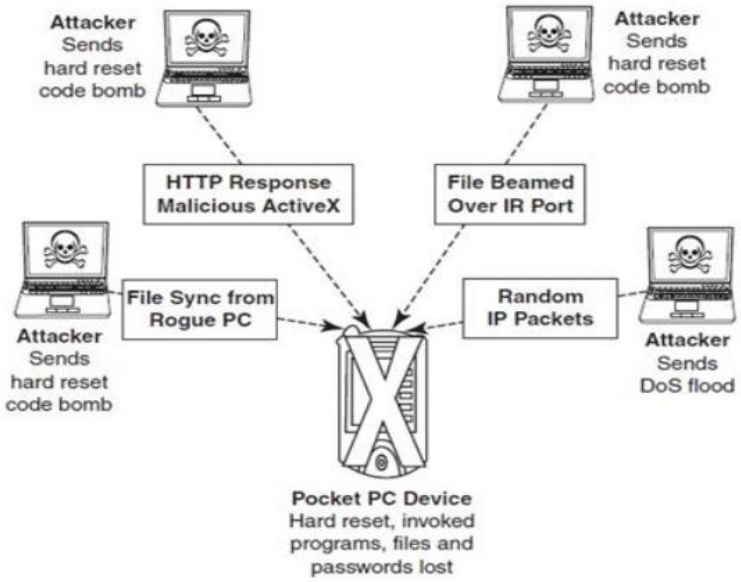


Figure: Crash attack on mobile devices. DoS- Denial-of-service attack

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.

5 b) What are different security challenges posed by Mobile devices? (7 M)

Mobility brings two main challenges to cybersecurity:

- on the hand-held devices, information is being taken outside the physically controlled environment and 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.

As the number of mobile device users increases, two challenges are presented:

- at the device level called “microchallenges” and
- at the organizational level called “macrochallenges”

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.

OR

6 a) Explain about the Organizational Security policies for mobile devices. (7 M)

Importance of Security Policies relating to Mobile Computing Devices:

- Growth of mobile devices used makes the cybersecurity issue harder than what we would tend to think.
- People (especially, the youth) have grown so used to their mobiles that 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 & 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 the sensitive customer data such as credit reports, Social Security Numbers (SSNs) & contact information.
- This not only the Public Relations (PR) disaster, but it could also violate laws & regulations.
- When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure.

Operating Guidelines for Implementing Mobile Device Security Policies:

- By using the following steps we can reduce the risk when mobile device lost or stolen
- Determine whether the employees in the organization need to use mobile computing devices or not.
- Implement additional security technologies like strong encryption, device passwords and physical locks.
- Standardize the mobile computing devices and the associated security tools being used with them.
- Develop a specific framework for using mobile computing devices.
- Maintain an inventory so that you know who is using what kinds of devices.
- Establish patching procedures for software on mobile devices.
- Label the devices and register them with a suitable service.
- Establish procedures to disable remote access for any mobile.
- Remove data from computing devices that are not in use
- Provide education and awareness training to personnel using mobile devices.

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 a distinct mobile computing policy.
- Another way is including such devices under existing policy.

There are also approaches in between, where mobile devices fall under both existing general policies and a new one. There may not be a need for separate policies for wireless, LAN, WAN etc because a properly written network policy can cover all connections to the company data, including mobiles & wireless.

6 b) What are different Security policies on Laptops and Wireless devices? Explain. (7 M)

Laptops, like other mobile devices, enhance the business functions. 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 cybersecurity 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. Most laptops contain personal and corporate information that could be sensitive. Such information can be misused if found by a malicious user.

Physical Security Countermeasures:

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.
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
3. Motion sensors and alarms: Alarms and motion sensors are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device & the key ring device crosses the specified range.
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 universal database for verification, which in turn makes the resale of stolen laptops a difficult process.
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
    - Creating the awareness among the employees about the sensitive information contained in the laptop
    - Making a copy of the purchase receipt of laptop, serial number & description of 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

- Disabling IR ports and wireless cards when not in use
- Choosing a secure OS
- Registering the laptop with the laptop manufacturer to track down the laptop in case of theft
- Disabling unnecessary user accounts and renaming the administrator account
- Backing up data on a regular basis

A few logical access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering
2. Avoiding weak passwords/open access
3. Monitoring application security and scanning for vulnerabilities
4. Ensuring that unencrypted data/unprotected fi le 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
11. Other countermeasures:
    - Choosing a secure OS that has been tested & has high security incorporated into it
    - Registering the laptop with the laptop manufacturer to track down the laptop in case of theft
    - Disabling unnecessary user accounts & renaming the administrator account
    - Disabling display of the last logged in username in the login dialog box
    - Backing up data on a regular basis

UNIT-IV

7 a) What is Phishing? How it Works. (7 M)

"Phishing" refers to an attack using mail programs to deceive Internet users into disclosing confidential information that can be then exploited for illegal purposes. While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening 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. 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.

How Phishing Works?

Phishers work in the following ways:

1. Planning: Criminals, usually called as phishers, decide the target.
2. Setup: Once phishers know which business/business house to spoof and who their victims.
3. Attack: 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 popup windows.
5. Identity theft and fraud: Phishers use the information that they have gathered to make illegal purchases or commit fraud.

Nowadays, more and more organizations/institutes 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.

7 b) Difference between Steganography and Cryptography. (7 M)

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, of the message itself is not disguised, but the content is obscured. It is said that terrorists use where the existence 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.

The difference between Steganography and Cryptography:

Steganography	**Cryptography**
Steganography means covered writing.	Cryptography means secret writing.
Steganography is less popular than Cryptography.	While cryptography is more popular than Steganography.
Attack's name in Steganography is Steganalysis.	While in cryptography, Attack's name is Cryptanalysis.
In steganography, structure of data is not usually altered.	While in cryptography, structure of data is altered.
Steganography supports Confidentiality and Authentication se curity principles.	While cryptography supports Confidentiality and Authentication se curity principles as well as Data integrity and Non-repudiation.
In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only secret message is hidden.
In steganography, not much mathematical transformations are involved.	Cryptography involves the use of number theory, mathematics etc. to modify data
In Steganography the information is hidden.	In cryptography the information is

Steganography	Cryptography
	transformed.
Hidden information is not visible.	Transformed information is visible.
Steganography Provides Confidentiality only.	Cryptography Provides Confidentiality, Integrity, Non-repudiation.
Steganography doesn't have specific algorithms.	Cryptography have Various recognized and approved algorithms.
The goal of steganography is to make the information invisible to anyone who doesn't know where to look or what to look for	The main goal of cryptography is to keep the contents of the message secret from unauthorized access.

OR

8 a) Discuss in detail about Virus and Worms. (7 M)

Computer Virus:

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:

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

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 sent 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. 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.

Types of Viruses

1. Boot sector viruses: It infects the storage media on which OS is stored (e.g., hard drives) and which is used to start the computer system.
2. Program viruses: These viruses become active when the program file (usually with extensions .bin, .com,.exe, .ovl, .drv) is excuted
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.
4. Stealth viruses: It hides itself and so detecting this type of virus is very difficult. It canhiding itself such a way that antivirus software also cannot detect it. Example for Stealth virus is "Brain Virus".
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 with the help of an antivirus program.
6. Macro viruses: 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 macrovirus gets onto a victim's computer then every document he/she produces will become infected.
7. Active X and Java Control: All the web browsers have settings about Active X and Java Controls.

Computer Worm:

A computer worm is self-replicating malware computer program. 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 co 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. 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.

8 b) Explain Buffer Overflow. (7 M)

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. This may result unreliable 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 that data written to an array. Buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. 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. 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.

Types of Buffer Overflow

1. Stack-Based Buffer Overflow:

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

- "Stack" is a memory space in which automatic variables (and often function parameters) are allocated.
- Function parameters are allocated on the stack and are not automatically initialized by the system, so they usually have garbage in them until they are initialized.
- Once a function has completed its cycle, the reference to the variable in the stack is removed.

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

- 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.
- 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.
- A function pointer, or exception handler, which is subsequently executed.

The factors that contribute to overcome the exploits are

- Null bytes in addresses;
- Variability in the location of shell code;
- Differences between environments.

2. 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. The characteristics of stack based and heap-based programming are as follows:

- "Heap" is a "free store" that is a memory space, where dynamic objects are allocated.
- The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions; it is different from the memory space allocated for stack and code.

- Dynamically created variables (i.e., declared variables) are created on the heap before the execution program is initialized to zero.

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.

How to Minimize Buffer Overflow

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

- Assessment of secure code manually: Buffer overflow occurs when a program or process tries to store more data in a buffer than it was intended to hold. Developers should be educated about minimizing the use of functions like strcpy(), strcat(), sprintf() and vsprintf() in C Language.
- 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.
- 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 restructure the programming code if such warnings are displayed.
- 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 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.

UNIT-V

9 a) Discuss about Social Computing. (7 M)

Social computing is also known as "Web 2.0" - it empowers people to use Web-based public products and services. Social computing is much more than just individual networking and entertainment. It helps thousands of people across the globe to support their work, health, learning, getting entertained and citizenship tasks in a number of innovative ways.

In the modern era, we are "constantly connected," business is "24 x7" - the business where world never sleeps. People carry anxieties in a competitive business world. In such a milieu, people and organizations are appreciating the "power of social media." Business is taken forward based on how connections are made through social networks.

In this process, a lot of information gets exchanged and some of that could be confidential, Personally Identifiable Information (PIl)/SPI, etc. There is a new genre of challenges, though they come with rising use of social computing and organizations need to watch for these challenges. For example, social computing poses the risk of "digital divide." Getting too used to readily available information, people may get into the mode of not questioning the accuracy and reliability of information that they readily get on the Internet.

With social computing, there are new threats emerging; those threats relate to security, safety and privacy. How to protect one's online privacy is in fact a major preoccupation for people all over the world; particularly in European countries where there is a very high consciousness about privacy loss.

Impersonation and identity, Cyber bullying and online grooming are new emerging threats. Data ownership and lack of controls in users hand for guarding their data are resulting in privacy invasion. Care should be taken while using social media when communicating with internal or external stake holders.

9 b) Discuss about Social media Marketing. (7 M)

Of late, social media marketing has become dominant in the industry. 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. MySpace is used by 6% of the organizations.

The Internet has penetrated India in a big way and due to this security breach incidences are on the rise. Hackers use a number of Internet channels such as the Web, E-Mail, instant messaging, Voice over Internet Protocol (VoIP), etc. to launch sophisticated and targeted attack to steal information from which they can benefit financially.

Although the euphoria about social media marketing practice is high (seems mainly due to competitive pressures), organizations must protect their data. 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.".

"Social media marketing" is an approach that makes use of social media sites to enhance the visibility on the Internet so as to promote products and services. People find that social media sites are useful for building social (and business) networks and for exchanging ideas and knowledge. 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, etc. Following are the most typical reasons why organizations use social media marketing to promote their products and services:

- To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
- 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.
- To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
- To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
- 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.

In addition to the social media online tools mentioned in, there are other tools too that organizations use; industry practices indicate the following:

- Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
- Professional networking tool Linkedin is used to connect with and create a community of top executives from the Fortune 500.
- Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
- 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.
- Wikipedia is also used for brand building and driving traffic.

OR

10 a) What are different perils for Organizations on web threats? (7 M)

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. There are web portals too in the E-Commerce model of doing business. Video and audio contents are delivered from the Web; software and infrastructure get delivered from the cloud! There is an inevitable dependence on the Internet. Therefore, cybercriminals find it convenient to use the Net for committing crimes. Employees expect to have Internet access at work just like they do at home. Mobility is picking up in India too though at a much limited pace compared to other countries. Mobile workforce has various categories. Workforce mobility poses challenges for IT managers whose agenda is to protect the business and business assets against malware. Protection of information assets is important; especially protection of removable/detachable media. Other concerns are about keeping Internet bandwidth available for legitimate business needs and ensuring uptime of applications and business websites. IT Managers should find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

From an organizational perspective, web threats can be classified into two broad categories.

1. First, employees do a number of activities online such as visiting infected websites, accessing pornographic sites, responding to Spam mails and attempting to hack sites (for legitimate and illegitimate reasons) to name a few.
2. Second, there are many challenges and difficulties IT managers face when it comes to managing web use in a secure and efficient way and when it comes to handle an "incident" alert received.

IT management is preoccupied with some of the top issues - they are described below:

- Employees wasting time on social networking and similar sites (such as Facebook, Twitter, etc.) and its impact on employee productivity. With rise in workforce mobility, this is likely to affect even more as it is very difficult to monitor remote employee.
- Enforcing "Acceptable Use Policies" is a challenge, especially, in very large, multi-location and3.matrix-structured organizations where getting the leaders to agree are a big challenge.

- The difficulty in monitoring employees' web usage - there are tethered as well as remote employees; keeping them under watch constantly is next to impossible. Also, people are becoming increasingly aware about their "privacy rights.“
- Keeping security systems up to date with patches and signatures is a challenge; this includes the challenge of operating system (OS) patches as well. We often hear about Microsoft vulnerability attacks. Most of us are busy installing one patch or the other on our laptops or desktops - it is the a necessary evil in Windows world.
- Legal and regulatory compliance risks (such as employees visiting inappropriate websites and the accidental disclosure of confidential information online). Laws are getting tough and regulatory compliance pressures are high especially in data breaches and employee privacy matters.
- Keeping the Internet bandwidth free for legitimate business use - there are bandwidth-hungry applications such as live video conferencing, YouTube, online training modules, as class room-based faculty delivered face-to-face training is the thing of the past, etc.
- Protecting remote workers and homeworkers (workforce mobility) - mobility of white collar workers is on the rise as mentioned.
- Employees using unauthorized Web-based applications - this is indeed a challenge in a virtual team environment with employees spread across locations. Protecting the organization against Spyware and malware.
- Remote filtering capabilities are incorporated into the newest versions of Websense. Web filtering and web security software restrict the use of Internet.
- Protecting multiple offices and locations - these are effects of globalization and the emerging "follow-the-sun-model" wherein business never sleeps and customers' insistence on business continuity means that there are alternate locations acting as shadow sites.

10 b) What are different Security Risks for Organizations on social media marketing?

(7 M)

First and foremost, it is essential to establish a "social media policy." Use of personal blogging for work-related matters should be monitored and minimized. "Employee Time Wasted on Internet Surfing" about employees endlessly surfing on the Internet during the work hours.
"Enforcing Policy Usage in the Organization". Once the policy is created, employers should communicate it to employees and should enforce its implementation through continuous monitoring. Increasing employee awareness is an ongoing activity. There is no go without it. This is because people can change their way of behaving in social networks only if they are aware of the security risks; sometimes they are genuinely not aware of those risks. There is a strong need to establish firm processes that are systematically linked to daily workflows. Such processes should be easy to implement and audit. For example, administrators should ensure that the latest security updates are downloaded. Although it seems to be mundane and boring activity, it is crucial. Organizations must enable their IT administrators to identify network attacks in time or to avoid them altogether. IDS and firewalls play a crucial role here. “Need-based access policy", with this it becomes possible to control and monitor access to critical data, and to track such access at any time. Doing this reduces the risk of information falling into wrong hands through unauthorized channels. Blocking the infected websites is another necessary activity. Access blocking can also be applied to any other suspicious site on the Internet. The filter function should be kept continuously up to date by maintaining so-called black- and white-listed websites. Using next-generation firewalls helps organizations keep their security technology up

to date. Some firewalls provide a comprehensive analysis of all data traffic. Deep inspection of network traffic makes it possible to monitor the type of data traffic, the websites from which it is coming, to know the web browsing patterns and peer-to-peer applications to encrypted data traffic in SSL tunnel. Protection against vulnerability is possible by carefully planning vulnerability scanning and penetration testing. An intrusion prevention system (IPS) serves as a protective barrier to the corporate network. Having identified an attack, the IPS immediately stops it and prevents it from spreading in the network. The IPS also enables patching of servers and services by securing servers under security threat, which will then be patched during the next maintenance window. Within this group, the use of social media can be monitored only on a very limited basis or not at all. This makes it even more important to assign the rights for defining all network access centrally, for example, using an SSL VPN portal - VPN is virtual private network, a tunnel within the Internet. The user level a strong authentication via single sign-on makes the administrator's work easier. Even the Intranets are not spared by cyber attackers. Therefore, securing the Intranets should also be included in the protector activities. The Intranet of every company contains highly sensitive information pertaining to the business areas involved These areas need to be isolated from the rest of the internal network by using the firewalls to segment the Intranet. This enables segregation of departmental Intranets; for example, a company can separate departments such as finance or accounting from the rest of the Intranet and thereby prevent infections from penetrating these critical segments of the corporate network.
If there is a need to use an existing multiple network segments then you can deploy multiple DMZ with differing security policies (levels). For example, you may need to deploy the applications for Extranets, Intranets, web server hosting and remote access gateways. The corporate security department, therefore, needs to include mobile devices in the security policies. This can be done, for example, with the assessment function by checking the login device for the required security settings and for the presence of security-relevant software packages. Through this function, it can be checked whether the proper and latest host firewall is installed and whether both the OS and antivirus software as well as all patches are up to date. On the basis of necessity warranted by a situation, mobile devices can be forwarded directly to a website containing the required updates. With the use of centralized management, administrators can manage, monitor and configure the entire network and all devices using a single management console. They can also monitor user activities on the network by viewing reports. For example, system administers will be able to know who has accessed which data at what time. This allows preventing attacks more effectively and provides more efficient protection for corporate applications at risk. A central management console also makes it possible to roll out and maintain standard security guidelines for the entire corporate network. Given these issues, risks and challenges involved with the use of social media marketing tools, indeed the involvement of the senior employees of the organization is critical to the success of the social media marketing initiative.