Chapter 3: Tools and Methods used in Cybercrime

Tools and Methods used in Cybercrime: Introduction, Proxy Servers, Anonymizers, Phishing, Password Cracking, Key Loggers and Spy wares, Virus and Worms, Trozen Horses and Backdoors, Steganography, DoS and DDOS Attacks, Attacks on Wireless networks. Textbook:1 Chapter 4 (4.1 to 4.9, 4.12)

3.1. Introduction

1). Discuss the different forms of attacks through which attacker target the computer system. (08M)

Different forms of attacks through which attacker target the computer systems are as follows. Initial uncovering, Network probe (Investigation), Crossing the line toward E-crime, Capturing the network, Grab the data, and Covering tracks:

1. Initial uncovering:

Two steps involved: step1) Reconnaissance- attackers gathers the information about the target on the Internet websites in a legitimate way.

Searching information about target on internet by googling as by surfing public websites/searching news article

step2) Attacker finds information about company's internal network such as Internet domain, machine names and the company's Internet Protocol (IP) address ranges to steal data.

2. Network probe (Investigation). At the network probe stage, the attacker uses more invasive techniques to scan the information Usually "ping sweep of the network IP addresses.

And then a port scanning tool 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 E-crime (refer Table 3.1)

Crossing the line toward electronic crime (E-crime) He/she does this by exploiting possible holes on the target system.
Once the attackers are able to access a user account, then they will attempt further exploits to get an administrator "root access"

Root access is a Unix term and is associated with the system privileges required to run all services and access all files on the system.

Root is a 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 the internal network quickly and easily by target system.

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 and services that have a backdoor password.
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 potentially expensive and embarrassing situation for an individual and/or for an organization.
6. Covering tracks: (refer Table 3.2) 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.
During this entire process, the attacker takes optimum care to hide his/her identity (ID) from the first step itself.

2). Explain the following

i) Scareware, ii) Malvertising, iii). Clickjacking, iv). Ransomware (08M)

- Various tools and techniques used to launch attacks against the targets
- **Scareware:** It comprises several classes of scam software with malicious payloads or of limits or no benefit, which are sold to consumers via certain unethical marketing practices.
- It uses social engineering approach for selling. It causes anxiety or the perception of a threat.
- Some form of Spyware and adware uses scareware tactics.
- Pop messages in websites such as "your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click yes below"→ is an example of
- **Malvertising:** It is a malicious advertising → malware+ advertising→ an online criminal methodology that appears focused on the installation of unwanted media networks.
- Criminals attempts to distribute malware through advertising. Malware may be hidden in advertising or embedded into a webpage or within software, which is available to download.
- **Clickjacking-** It is a malicious techniques of tricking netizens into revealing confidential information and/or taking control of their system by clicking on seemingly innocuous webpages.
- **Clickjacking takes** embedded code executed without netizen's knowledge. It is also called as user interface redressing.

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 propagates as a conventional computer worm entering system through email attachment, or vulnerability in a network.

Then ransomware disable the essential system service and encrypt some of the personal files.

Table 3.1 List of websites commonly browsed by attackers to obtain the information on the vulnerabilities

1. http://www.us-cert.giov/ **US-CERT** is the operational arm of the National Cyber Security Division (NCSD) at the department of Homeland Security (DHS). US Government.
2. http://cve.mitre.org/ **common vulnerabilities and Exposures (CVE)** is a dictionary of publicly known information security vulnerabilities and exposures and free for public use.
3. http://www.secunia.com/ -- **Secunia:** It has thousands of vulnerability lists that updated periodically.
4. http://www.hackerstorm.com/ **--Hackstorm:** This website was created for open source vulnerability database (OVSDB).
5. http://www.hackerwatch.org/ -- **hackerwatch:** It is an online community where Internet users can report and share information to block and Identify security.
6. http://www.zone-h.org/ -- **zone-h:** It reports on recent web attacks and cybercrimes and lists them on the website. We can see defaced webpages and details about them.
7. http://www.milworm.com/ --- **milworm**: It gives Day wise information about the exploits.
8. https://www.osvdb.org/ -- **OSVDB—**Open-source vulnerabilities database providing large quantity of technical information.
9. https://www.metasploit.com/ **--Metasploit** is an open source computer security project that provides information about security vulnerabilities and aids in penetration testing
10. https://www.w00w00.org/files/LibExploit-- **LibExploit** is a generic exploit creation library helps cyber security community when writing exploits to test vulnerability.

11. **https://www.immunitysec.com/products-canvas-shtml --** **Canvas** is commercia vulnerability exploitation tool from Dave Aitel's ImmunitySec**.**

12. **https://www.coresecurity.com/content/core-impact-overview --Core impact exploitation tool**

Table 3.2. Tools used to cover tracks

1. http://www.ibt.ku.dk/jesper/ELSave: **ELSave:** It is a tool to save and/or clear an NT (New Technology) event log.
2. http://ntsecurity.nu/toolbox/winzapper/ -- **WinZappep :** This tools enables to erase event records selectively from the security logs 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/ --- **Evidence eliminato**r: It is simple and one of the top-quality professional PC cleaning program that is capable of defeating known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis De impossible.
4. http://www.traceless.com/computer-forensics/ --**Traceless:** It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc.

5. https://www.acesoft.net/ -- Tracks Eraser Pro: It deletes following history data:

- 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 autocomplete.
- Delete IE plugins (selectable).
- Delete index.dat file.
- Delete history of start menu run box.
- Delete history of start menu search box.
- Delete windows temp files.
- Delete history of open/save dialog box.
- Empty recycle bin.

3. Discuss the proxy server and Anonymizers in the cyber security (08M)

4. List the difference between proxy server and anonymizer? (08M)

3.2 Proxy Servers and Anonymizers

- **Proxy server** is computer on a network which acts a s an intermediary for connections with other computers in that network.
- 1st attacker connects to proxy server
- Proxy server can allow an attacker to hide ID
- Purpose of proxy server

    1. Keep the system behind the curtain
    2. Speed up access to resource. It is used to cache the webpages from a web server.
    3. Specialized proxy servers are used to filter unwanted content such as advertisement
    4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the internet, whichever has only one IP address.

Advantages of Proxy server is that its cache memory can serve all users.

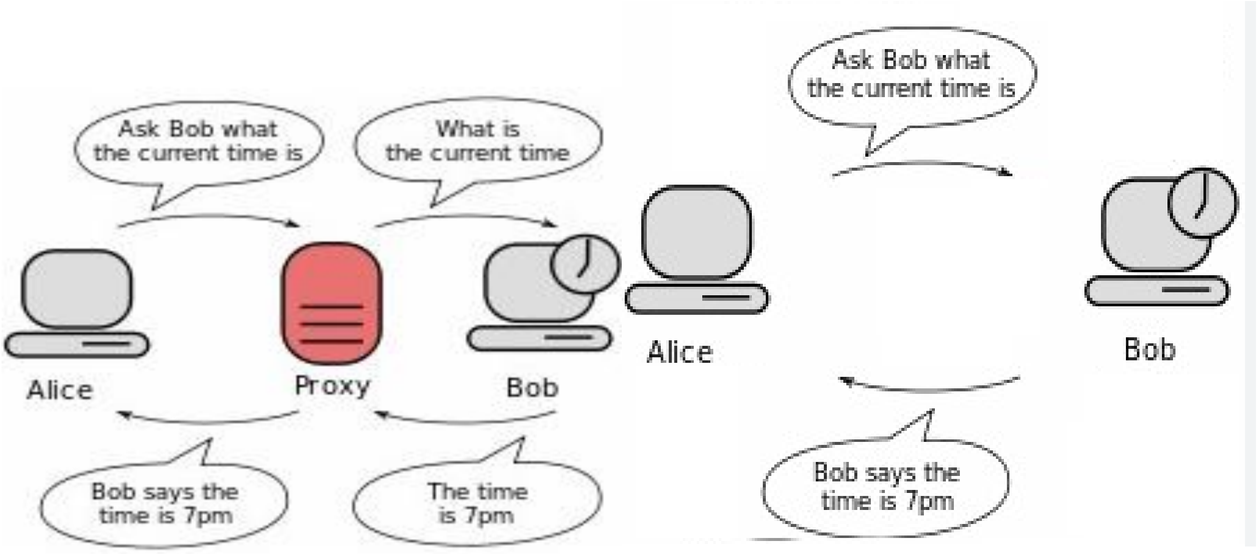


Fig. Proxy server and Normal server

List of website for free proxy servers

1. http://www.proxy4free.com
2. http://www.publicproxyservers.com
3. http://www.proxz.com
4. http://www.anonymitychecker.com
5. http://www.surf24h.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 user's behalf, protecting personal information by hiding the source computer's identifying information.
- An Anonymizer Web site which allows you to use the facilities of the Web without disclosing your identity.
- Such sites are employed by users who do not wish to leave information about their identity on the Internet.
- This prevents spammers sending unsolicited email to you or cyberstalkers contacting you.

List of 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

5.Discuss the following: Google Cookie, Cookie, DoubleClick and G-Zapper. (08M)

Being Anonymous while searching on Google

Google Cookie

Google was the first search engine to use a cookie. 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 d Use deletes before its expiry.)

Cookie (http cookie/browser 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 mechanism of setting and reading cookies invites attackers to use these cookies as "Spyware."
There are two types of cookies:

1. Persistent cookie (It 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 web browser. and
2. session cookie It is temporary cookie and does not reside on the PC once the browser is closed

DoubleClick

is a subsidiary of Google and provides Internet ad-serving services and paid search Network (DART Search ") and utilize the cookies, which are called DART cookie.
Double Click was first online media representative business, that is, representing websites to sell advertising space to marketers.

G-zapper

G-Zapper 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 ls 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' D and search history.

G-Zapper reads the Google cookie installed on users PC, displays thee 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

3.3 Phishing

6. Explain the Phishing, with examples and discuss the step how it works?

Phishing is introduced in 1996. Phishing refers to an attack using mail programs to deceive internet users into disclosing confidential information that can be then exploited for illegal purpose.

- 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.
- **Examples**: stealing personal and financial data - and can infect systems with viruses and also a method of online ID theft in various cases.
- Fake email using other reputed companies or individual identity
- People associate phishing with E-mail message that spoof or mimic banks credit card companies or other business such as Amazon, and eBay

- **Phishers works as follows**

1. **Planning:** Criminals called as phisher, decide the target & determine how to get E-mail address
2. **Setup:** Once phishers know which business/business house to spoof and who their victims are, they create methods for delivering the message & to collect the data about the target.
3. **Attack:** Phisher sends a phony message that appears to be from a reputed source
4. **Collection:** Phisher record the information of victims entering into web pages or pop-up window
5. **Identity theft and fraud:** Phisher use Information that they have gathered to make illegal purchases and commit fraud.

Recently more and more organisation/Institute provides greater online access for their customers and hence criminals are successfully using phishing techniques to steal personal information and conduct ID theft at global level.

7.What are the different ways of password cracking?

3.4 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 from data that have been stored in or transmitted by a computer system.
- Attacker follow common approach of guessing of passwords.
- The purpose of password cracking is as follows:
  - To recover a forgotten password.
  - As a preventive measure by system administrators to check for easily crackable passwords
  - To gain unauthorized access to a system.

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

- Find a valid user account such as an Administrator or Guest;
- Create a list of possible passwords;
- Rank the passwords from high to low probability;
- 4 Key-in each password
- Try again until a successful password is found.

Password Cracking Tool

Default password(s)	Cain & Abel	John the Ripper	THC-Hydra
Aircrack-ng	LOphtCrack	AirSnort	Solar Winds
Pwdump	RainbowCrack	Brutus	

Passwords can be guessed sometimes with knowledge of the user's personal information

- 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. Users name or login name;
- 5. Name of user's friend/relative/pet;
- 6. User's birthplace or date of birch, 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, actress, spiritual gurus) by the user.

- 9. Simple modification of one of the preceding, such as suffixing a digit, particularly, or reversing the order of letters.
- Password cracking attacks can be classified under three categories as follows
- 1. Online attacks;
- 2. Offline attacks;
- 3. non-electronic attacks (e.g., social engineering, shoulder surfing and dumpster diving

- **3.4.1 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.
- Popular Online attack is **Man-in-the-middle (MITM) attack/ "bucket-brigade attack"/Janus attack.**
- It is **form of eavesdropping**, here attacker establishes connection between a victim and the server to which the 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.
- It is used to **obtain the passwords for E-mail accounts** on public websites such as Yahoo, Hotmail and Gmail.
- It is also used to get the **password for financial websites**, to gain the access to banking websites.
- **3.4.2 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 require physical access** to the computer and copying the password file from the system onto removable media.

These are **used to get the password** in the clear text format.

Type of attack	**Description**	**Example of a password**
Dictionary attack	Attempts to match all the words from the dictionary to get the password	Administrator
Hybrid attack	Substitutes numbers and symbols to get the password	Adm1n1strator
Brute Force attack	Attempts all possible permutation-combination of letter numbers and special characters	Adm!n@09

- **3.4.3. 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@S$V/ord: 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.
- **Strong password:**
- A **strong password is long enough**, random or otherwise difficult to guess - producible only by the user who choose it.
- The length of time deemed to be too long will vary with the attacker, the attacker's resources, the ease in 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 banks electronic money transfer system might be worth many weeks of computer time for trying a crack it..
- **There are some examples of strong passwords:**
- 1. **Coon vert £100 to Euros!:** Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.
- 2. **465304H:** It is mix of numbers and a letter at the end, usually used on mass user accounts and 3 passwords can be generated randomly, for example, in schools and business.
- 3**. PIeai@3:** It is not a dictionary word: however it has cases of alpha along with numeric and punctuation characters.
- 4. **MoOoOfln245679:** It is long with both alphabets and numerals.
- 5**. t3wahSetyeT4:** It is not a dictionary word; however, it has both alphabets and numerals

3.4.4. Random Passwords

- Password is stronger if it includes a mix of **upper and lower case** letters, **numbers and other symbols**, when allowed, for the same umber 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**.

- **The general guidelines applicable to the password policies, which can be implemented organization-wide will are as follows:**
- **Passwords and user logon identities (IDs) should be unique to each authorized user.**
- Passwords should consist of a **minimum of eight alphanumeric characters** (no common names or phrases).
- There should be **computer-controlled lists of prescribed password rules and periodic testing** (eg., letter and number sequences, character repetition, initials, common words and standard names) to identify any password weaknesses.
- Passwords **should be kept private,** that is, not shared with friends, colleagues, etc. They shall not be coded into programs or noted down anywhere.
- Passwords shall be changed **every 30/45 days or less**. Most operating systems (OS) can enforce a password with an automatic expiration and prevent repeated or reused passwords.
- User accounts **should be frozen after five failed logon attempts.** All erroneous password entries should be recorded **in an audit log for later inspection and action, as necessary.**
- Sessions **should be suspended after 15 minutes** (or other specified period) of inactivity and require the passwords to be re-entered.
- **Successful logons should display the date and time of the last logon and logoff.**
- **Logon IDs and passwords should be suspended after a specified period** of non-use.
- 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.
- **Similarly, netizens 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 and banking/financial user accounts (e.g. online (Yahoo/Hotmail/Gmail) banking/securities trading accounts) **should be kept separate.**
- 2. Passwords should be **of minimum eight alphanumeric characters** (common names or phrases should 2.
- 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 has 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**
- 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.

- 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**
- 10. In case **E-Mail accounts/user accounts have been hacked**, respective **agencies/institutes** should be contacted immediately

8.How can keyloggers can be used to commit a cybercrime?

OR

Explain the following i) Software keyloggers, ii) Hardware keyloggers, iii) Antikeylogger and Spywares

3.5 Key Loggers and Spy wares

- 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.
- 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

- **3.5.1 Software Keylogger**
- Software keyloggers are software programs 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 without the knowledge of the user.
- Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafes, library) 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. DLL does all the recording of keystrokes

Some important Keylogger as follows

All in one Keylogger	Stealth Keylogger	Perfect Keylogger	KGB spy	Spy Buddy
Elite Keylogger	Cyberspy	Powered Keylogger	XPC Spy	Spytech spyagent stealth

3.5.2 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:**
- http://www.keyghost.com
- http://www.keelog.com
- http://www.keydevil.com
- http://www.keykatcher.com

3.5.3 Antikeylogger

- Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.
- Advantages of using antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeylogger 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
5. It secures E-Mail and instant messaging/chatting **Note:** Visit http://www.anti-keyloggers.com for more information)

3.5.4 Spywares

- Spyware is a type of malware 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.
- Spyware is secretly monitoring the user. Spywares programs collect personal information about the victim, such as Internet surfing habits/ patterns and websites visited.
- These program changes the internet settings then the user start complaining about the speed issues to ISP. Various Spywares are available in the market.
- Anti Spyware software's are available in the market. These have become a common element now days from computer security practices perspective.

Spywares examples

007 Spy	Spector Pro	eBlaster
Remotespy:	Stealth Recorder Pro	Stealth Website Logger
Flexispy	Wiretap Professional	PC PhoneHome
SpyArsenal Print Monitor Pro:		

3.6 Virus and Worms

9. Discuss about Virus and worms
OR
Discuss the concept of Virus and worms. How criminals use these tools for the attack.

- 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 users
- Virus contains malicious instructions that may cause damage or annoyance; the combination of possibly malicious code with the ability to spread is what that makes viruses a considerable concern.
- A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person.
- 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 random.

Viruses can take some typical actions:

1. Displays a message to prompt an action which may set of the virus
2. Delete files inside the system into which Viruses enter
3. Scramble data on hard disk
4. Cause erratic screen behaviour
5. Halt the system (PC)
6. Replicate themselves to propagate further harm

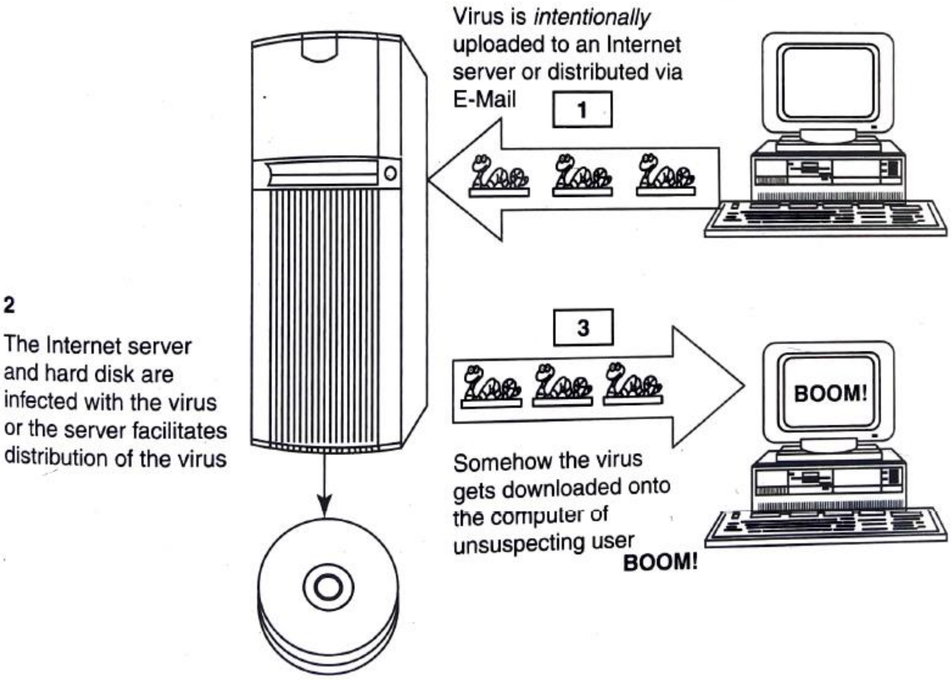

Virus is *intentionally* uploaded to an Internet server or distributed via E-Mail
1
2
The Internet server and hard disk are infected with the virus or the server facilitates distribution of the virus
3
BOOM!
Somehow the virus gets downloaded onto the computer of unsuspecting user
BOOM!

Fig 3.1. Virus spreads through the Internet

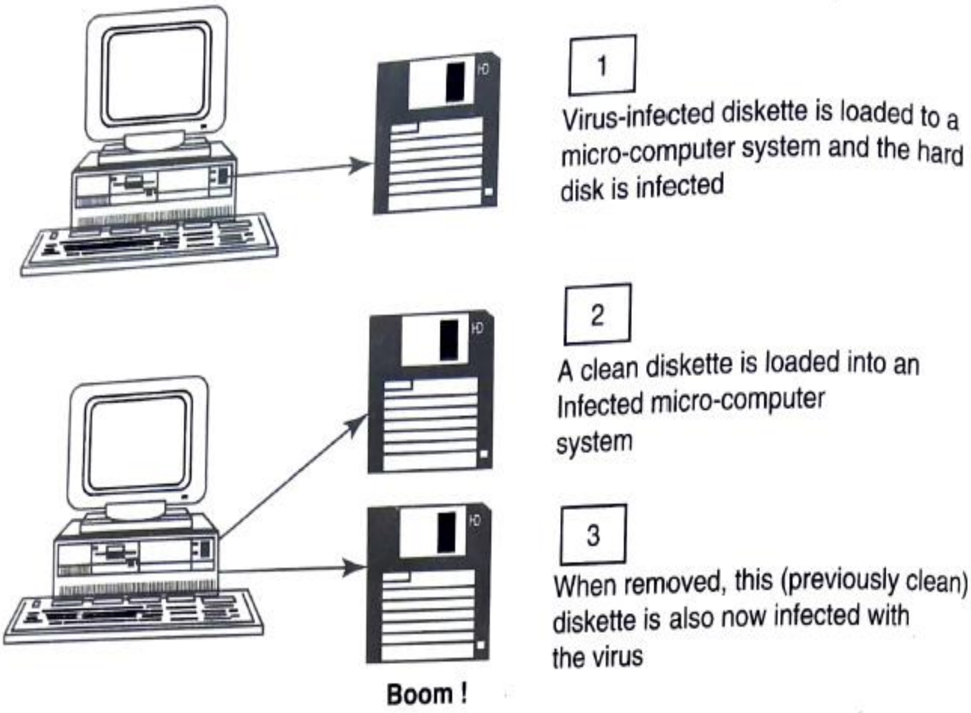

1
Virus-infected diskette is loaded to a micro-computer system and the hard disk is infected
2
A clean diskette is loaded into an Infected micro-computer system
3
When removed, this (previously clean) diskette is also now infected with the virus
Boom !

Fig 3.2: Virus spreads through stand-alone system

Figure 3.1 shows the virus spread through internet. Figure 3.2 shows the Virus spreads through stand-alone system. And Figure 3.3 shows the 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 malwares, 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.

Malware includes viruses, worms, Trojans, most Rootkits, Spyware, dishonest Adware, Crimeware and other malicious and unwanted software as well as true viruses.

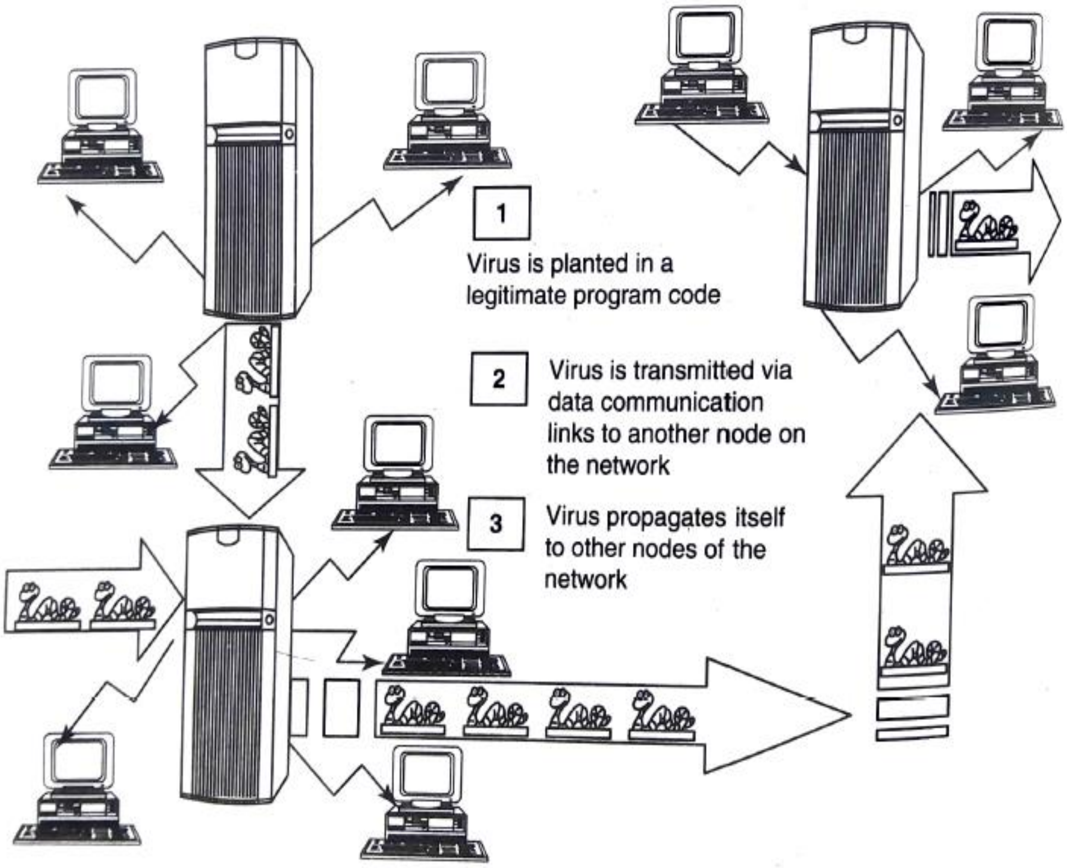

1
Virus is planted in a legitimate program code
2
Virus is transmitted via data communication links to another node on the network
3
Virus propagates itself to other nodes of the network

Fig. 3.3. Virus spreads through local networks

10. Discuss the difference between Virus and Worms

SL. No	Facet	Virus	Worm
1	Different types	Stealth virus, self-modified virus, encryption with variable key virus,	E-Mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing, networks worms

		polymorphic code virus, metamorphic code virus	
2	Spread mode	Needs a host program to spread	Self-spreading, without user intervention
3	What is it?	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.	The name worm originated from Inception. The Shockwave Rider, a science fiction novel published in 1975 by John Brunner.
5	Prevalence	Prevalence for virus is very high.	Moderate prevalence for a worm.

3.6.1 Types of Viruses:

Categorized based on attacks on various elements of the system

1. **Boot sector viruses:** It Infects the storage media on which OS is stored and which is used to start the computer system. Spread to other systems when shared infected disks and pirated software's are used.
2. **Program viruses:** These viruses becom Active when the programs files (usually with extension .bin, .com, .exe,. ovl, .drv) is executed. Makes copy of itself.
3. **Multipartite viruses:** It is hybrid of a boot sector and program viruses. It infects program files along with the record when the infected program is active.
4. **Stealth viruses:** It camouflages and/or Masks (hides) itself so detecting this virus is difficult. It can hide itself such a way that anti-virus software also cannot detect it. Memory to remind in the system and detected. Example of 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 spread through the system (i.e., multiplies and infects a new file). Polymorphic generators are routines (small programs) that can be linked with the existing viruses.

   Generators are not viruses but purpose to hide actual viruses under the cloak of polymorphism. It is difficult to detect polymorphic virus with the help of an antivirus program.First Polymorphic generator was the Mutation Engine (MtE). Other Polymorphic generators are Dark Angel’s Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns’nRoses Polymorphic Engine (GPE), and Dark Slayer Confusion Engine (DSME)

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 macro virus gets onto a victim's computer then every document he/she produces will become Infected.
7. **Active X Java control:** All the web browsers have settings about Active X and Java Commands. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work.
8. Which invites the threats for the computer system being targeted by unwanted software

Examples of The World's Virus attacks !!!

Conficker	INF/AutoRun	Win32 PSW. OnLineGames	Win32/Agent (Trojan)
Win32/FlyStudio (Trojan with characteristic of backdoor)	Win32/Pacex.Gen	Win32/ Qhost	WMATrojanDownloader.GerCodec

<u>Worms:</u>

- It is self-replicating malware computer program.
- It uses a computer network to send copies of itself to other nodes and it can transmit without any intervention
- This is due to security shortcomings on the target computer
- Unlike Virus, it does not need to attach itself to an existing program
- It will 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.
- See table 3.3 to know more on World's worst worm attacks.
- The world's worst virus and worm attacks!

Morris Worm	ILOVEYOU	Nimda	Code Red	Melissa
MSBlast	Sobig	Storm Worm	Michelangelo	Jerusalemn

Everyday new virus albums are created day be coming you trade to netizens. In spite of different platforms OS and or applications a typical definition of computer virus or warm white have the various aspects such as

- A virus attacks specific file types (or files).
- Virus manipulates a program to execute tasks and unintentionally.
- An infected program produces more viruses.
- An infected program may Run without error for a long time

Viruses can modify themselves and may possibly escape detection this way

****

Explain Malware and its classification

Malware

- Malware, Short for malicious software, is a software designed to infiltrate a computer system without the owner's informed consent.
- The represents a variety of forms of hostile, intrusive or annoying software or program code.
- It can be classified as follows
  - 1. Viruses and worms
  - 2. Trojan Horses
  - 3. Rootkits
  - 4.Backdoors
  - 5. Spyware
  - 6.Botnets
  - Keystroke loggers
- **Viruses and worms:** These are known as infectious malware. They spread from one computer system to another with a particular behavior
- 2. **Trojan Horses:** A Trojan Horse, Trojan for short, is a term used to describe malware that appears, t the User, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system
- 3. **Rootkits:** Rootkits is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised.
- 4.**Backdoors:** Backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access for plain text and so on while attempting to remain undetected

- 5. **Spyware:** Spyware is a type of malware 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.

- 6.**Botnets:** These refers to network of hijacked internet connected devices that are installed with malicious code known s malware. The infected devices are called as bots. Hackers remotely controls the

- 7. **Keystroke loggers:** 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.
- 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

Explain the concept of Computer 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

3.7 Trozen Horses and Backdoors

Discuss the difference between Trozen Horses and Backdoors? Explain the concept of Trozen Horses and Backdoors?	05M

- 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.
- Get into system from number of ways, including web browser, via E-mail, or with software download from the Internet.
- Trojan do not replicate themselves but they can be equally destructive
- Examples of threats by Trojans
- Erase, overwrite or corrupt data on computer
- Help to spread other malware
- Deactivate or interface with antivirus and firewall
- Allow to remote access to your computer
- Upload and download files without user knowledge
- Gather E-Mail address and use them for spam
- Slow down, restart or shutdown the system
- Reinstall themselves after being disable
- Disable task manager or control panel
- Copy fake links to false websites, display porno sites, play sounds/videos and display images
- Log keystrokes to steal info such as password or credit card number.

3.7.1 Backdoors

- It means of access to a computer program that bypass security mechanisms
- Programmer use it for troubleshooting
- Attackers often use backdoors that they detect or install themselves as part of an exploit
- Works in background and hides from user
- Most dangerous parasite, as it allows a malicious person to perform any possible action

- Programmer sometimes leave such backdoor in their software for diagnostic and troubleshooting purpose. Attacker discover these undocumented features and use them.

What a backdoor does?

1. It allows an attacker to create, delete, rename, copy or edit any file; change any system setting, alter window registry; run control and terminate application; instal arbitrary software
2. The control computer hardware devices, modify related setting, shutdown or restart a computer without asking for user permission
3. Steals sensitive personal information, logs user activity, tracks web browsing habits
4. Record Keystrokes that a user types on a computer's keyboard and captures screenshots
5. Sends all gathered data to predefined E-Mail address
6. It infects files, corrupts installed app and damage entire system
7. It distributes infected files to remote computers and perform attack against hacker-defined remote hosts.
8. It installed hidden FTP server that can be used by malicious person
9. It degrades Internet connection speed and overall system performance
10. It provides uninstall features and hides processes, files and other objects to complicate its removal as much as possible.

Examples of Backdoor Trojans

1. **Back office:** Enable user to control a computer running the Microsoft windows OS from remote location
2. **Bifrost**: Infect Windows 95 through Vista
3. **SAP backdoors:** 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.

1. **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.

3.7.2 How to protect from Trojan Horses and Backdoors

1. **Stay away from suspect websites/web links:**

   Avoid downloading free/pirated softwares that often Ca by Trojans, worms, viruses and other things.

2. **Surf on the web cautiously:**

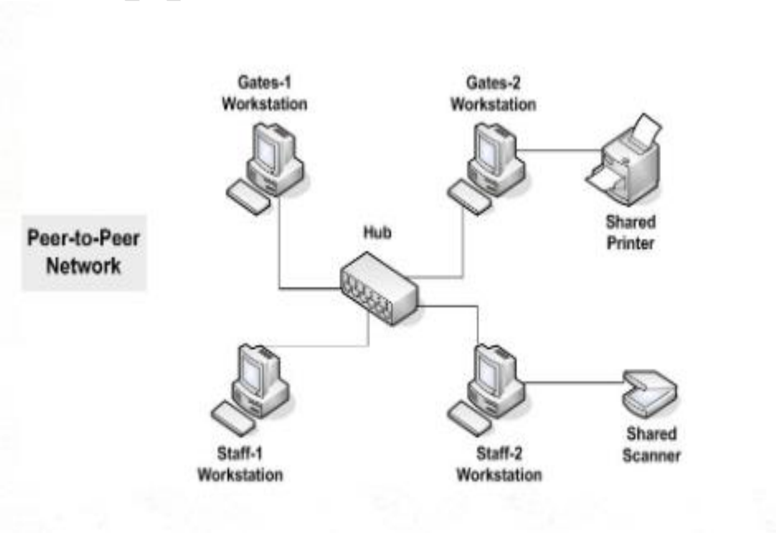
Avoid connecting with and/or downloading any information from peer (P2P) networks, which are most dangerous networks to spread Trojan Horses and other threats. P2P networks create files packed with malicious software, and then rename them to files with the criteria of common search that are used while surfing the information on the web.

3. **Install antivirus/Trojan remover Software**

Nowadays antivirus software(s) have built-in features for protecting the system not only from viruses and worms but also from malware such as Trojan hoses. Free Trojan remover programs.

Peer-to-Peer (P2P) Networks

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



- **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.
- **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.
- **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 "super nodes."

3.8 Stganography

Elaborate the steganography and Steganalysis? How criminals use these methods?	06M
Discuss the steganography and Cryptography.	04M

- Greek word that means "Sheltered writing". It is a method that attempts to hide the existence of a message or communication. It comes from 2 Greek words:
- Steganos means "Covered" and graphein means "to write" or "concealed writing"
- Steganalysis: Detecting messages that are hidden in images, audio/video files using steganography.
- For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image.
- It is used to make a digital watermark to detect illegal copying of digital image.
- The Cover medium is used to describe the original, innocent message, data audio, still, video and so on. It is the medium that hides the secret message as shown in figure 3.4. A stegokey password is required in the process.
- Steganography is used to place a hidden "trademark" in images, music and software, the result is a technique referred to as watermarking.

Steganography tools

- http://www.securityfocus.com: DiSi-Steganograph:
- http://www.brothersoft.com/invisible-: Invisible Folders
- http://www.programurl.com/stealth-files.htm Invisible Secrets:
- http://www.programurl.com/hermetic-stego.htm Stealth Files:
- http://www.petitcolas.net/fabien/steganography/mp3stego Hermetic Stego:
- http://compression.ru/video/stego_video/index_en.html DriveCrypt Plus (DCPP):
- http://www.petitcolas.net/fabien/steganography/mp3stego MP3Stego

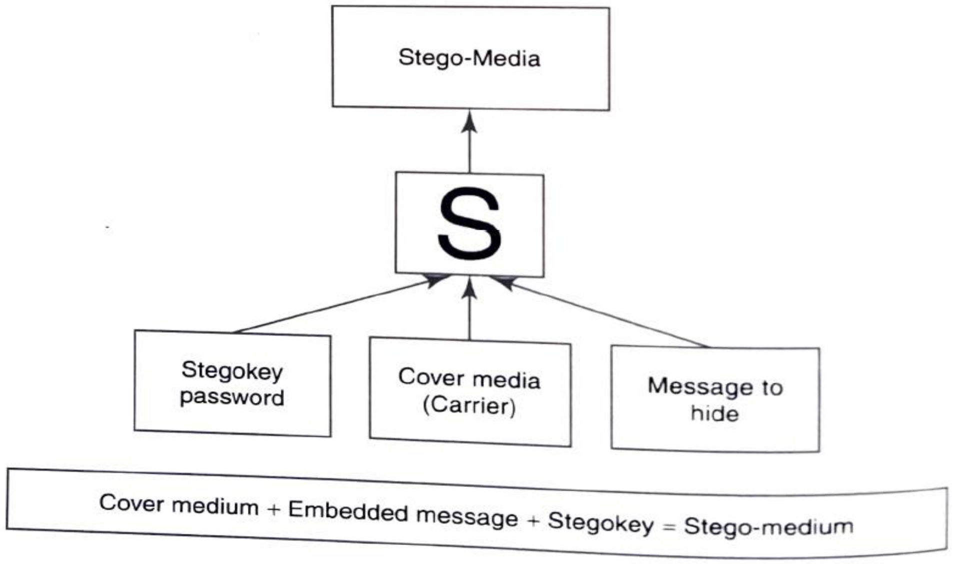


Fig. 3.4 How steganography works.

3.8.1. Steganalysis

Sreganalysis 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 nor they have a payload encoded into them, and if possible recover it.

Automated tools are used to detect such steangraphed data/information hidden in the image and audio and/or video files.

Steganoraphy, Suduko Puzel and SMS:

- It is a revised version of information hiding (i.e., steganography) using Sudoku puzzle.
- 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.

3.9. DoS and DDOS Attacks

Discuss the difference between DoS and DDoS attack.	06M
Explain and list the classification of DoS attacks	07M
Discuss Types or levels of DoS attacks	08M
Discuss the tools used to launch DoS attack.	05M

3.9.1 DoS Attack

- In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Maill box with spam mail depriving him of the services he if entitled to access or provide.
- The attacker typically sites or services hosted on high profile web servers such as bank credit card payment gateways mobile phone networks and even root name servers.
- Buffer overflow techniques is employed to commit such kind of criminal attack

- Attacker spoofs the IP address and floods the network of victim with repeated request
- 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 server the legitimate responses and ultimately breaks down.

Symptoms of DoS attack

- US Computer Emergency Response Team defines symptoms of DoS attack:

1. Unusually slow network performance (Opening file 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 [E-mail Bomb].

What DoS attack does?

- Goal of DoS is not to gain unauthorized access to systems or data, but to prevents intended users of a service from using it. The DoS attack do the following

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

3.9.2 Classification of DoS attacks

- **1. Bandwidth attacks:** Loading any websites takes certain time. Loading means complete webage appearing on the screen and system is awaiting user's input. Loading consumes some amount of memory.
- Every site given with a particular amount of bandwidth for its hosting, say 50GB. Now if visitor consumes all 50GB bandwidth then hosting of the site can ban this site.
- The does the same- he/she opens 100 pages of a site and keeps on refreshing and consumes all the bandwidth, the site becomes out of service.
- **2. Logic attack:** These kinds of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.

- **3. Protocol attacks:** Protocols are rules that are to be followed to send data over network. These kinds of attacks exploit specific feature or implementation bug of some protocol installed at victim's system to consume excess amount of its resources
- **4. Unintentional DoS attacks:** 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.

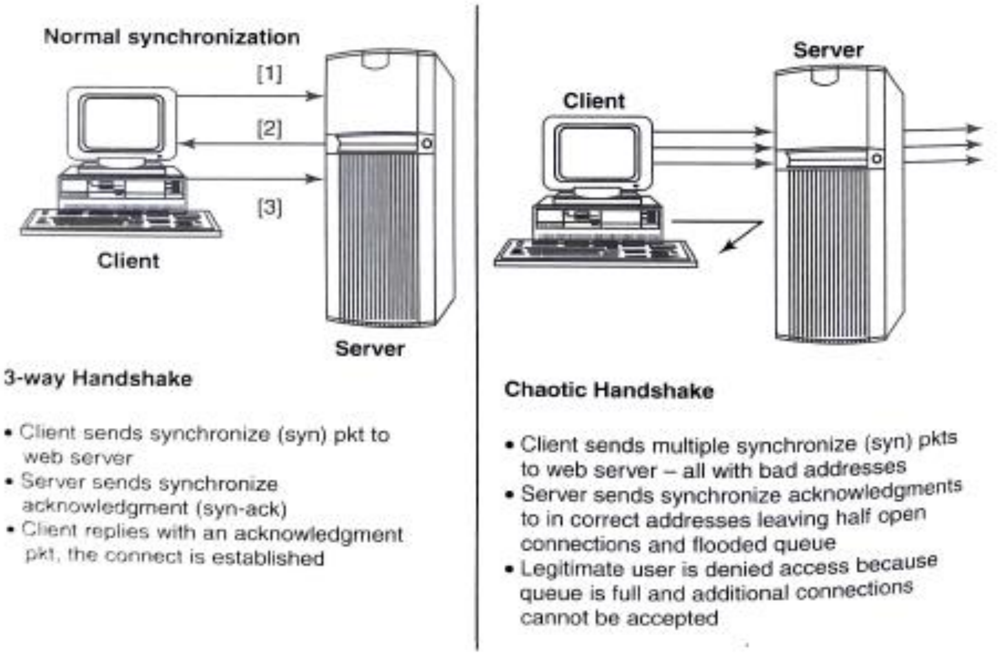
3.9.3. Types or levels of DoS attacks

1. Flood attack (Ping flood)

- This is the warliest form of DoS attack and is also known as ping flood. Attacker sending number of ping packets, using ping command, which result into more traffic than victim can handle.
- This requires the attacker to have faster network connection than the victim
- It is very simple to launch, but Prevention is difficult

2. Ping of death attack

- The ping death attack sends oversized ICMP (Internet Control Message Control) packets, and it is core protocol of IP Suite.
- It is mainly used by networked computers OS's to send error messages indicating datagrams to the victim.
- The maximum packet size allowed is of 65,536 octets. Some system upon receiving the oversized packet, will crash, freeze or reboot system resulting DoS.



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

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

Fig. 3.5 Denial-of-service (DoS) attack.

3. SYN attack (TCP SYN flooding)

- **In this Transmission control protocol** handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address).
- The server replies with an 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 3.5 explains how the DoS attack takes place

4. Teardrop attack

- Teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tires to reassemble them.
- IP's packet fragmentation also is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various Oss due to a bug in their TCP/IP fragmentation reassembly code.
- Windows 3.1x, 95 and NT, Linux versions 2.0.32 and 2.1.63 are vulnerable to this attack

5. Smurf attack

- Generating significant computer network traffic on victim network using foods via spoofed broadcast ping message
- Attack consists of a host sending ICMP echo request to network broadcast ping address
- Every host receive this packet and send back ICMP echo response
- Internet relay chat (IRC) servers are primarily victim of smurf attack

6. Nuke:

- An old DoS attack against computer network is consisting of fragmented or otherwise invalid ICMP packets sent to target.
- Achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until comes to complete stop
- Eg. WinNuke which is exploited the vulnerability in the NetBIOS handler in windows 95. A string of out of band data was sent to TCP port 139 of victim's machine, causing it to lock up and display Blue Screen of Death (BSOD)

3.9.4 Tools used to launch DoS attack

Jolt2: attack against window based machine consume 100% of CPU time on processing of illegal packets

Nemesy: generates random packets of spoofed source IP

Targa: used to run 8 different DoS attack

Crazy Pinger: send large packets of ICMP

SomeTrouble: Remote flooder and bomber developed in Delhi

Blended Threat: It is more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan Horses and Malicious code into one single threat

Use server & Internet vulnerabilities to initiate, transmit and thereafter spread attack

Characteristics:

- Cause harm to the infected system or network
- Propagate using multiple methods as attack may come from multiple point
- Exploit vulnerability
- Server multiple attacks in one payload to use multiple mode of transport rather than a specific attack on predetermined ".exe" files, it could do multiple malicious acts, such as modify your ".exe" files, HTML files and registry keys

Permanent DoS attack

- Damages a system so badly that it require replacement or reinstallation of hardware.
- Pure hardware sabotage,
- PhlashDance is a tool created by Rich Smith who detected and demonstrated PDoS.

3.9.5 DDOS Attacks

- In a DDoS attack, an attacker uses your computer to attack another computer
- By taking **advantage of security vulnerabilities or weaknesses**, an attacker could tack control of your computer, 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** to launch the DoS attack
- Large number of **zombie systems are synchronised to attack a particular system**.
- Zombie systems are called secondary victims and main target is called primary victim.

3.9.6 How to Protect from DoS/DDoS Attack

1. Implement router filter, it lessens your exposure to certain attacks.
2. If such filters are available in your system, install patches to guard against TCP 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 performance and establish baselines for ordinary activity.

6. Routinely examine your physical security with regard to your current needs.
7. Use tools (eg. Tripware) to detect changes in configuration information or other files
8. Invest and maintain "hot spares" – Machine that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configuration
10. Establish and maintain regular backup schedules and policies, fr 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.

3.10 Attacks on Wireless networks

> Discuss the different types of mobile workers? (05M)
>
> What are the different components of wireless network? (05M)
>
> what is the difference between WEP and WPA2?
>
> Discuss the traditional techniques of attacks on Wireless network?
>
> What is the difference between WAPkitting and WAPjacking?

- In security breaches, penetration of a wireless network through unauthorized access termed as wireless cracking
- Traditional techniques are
- Sniffing

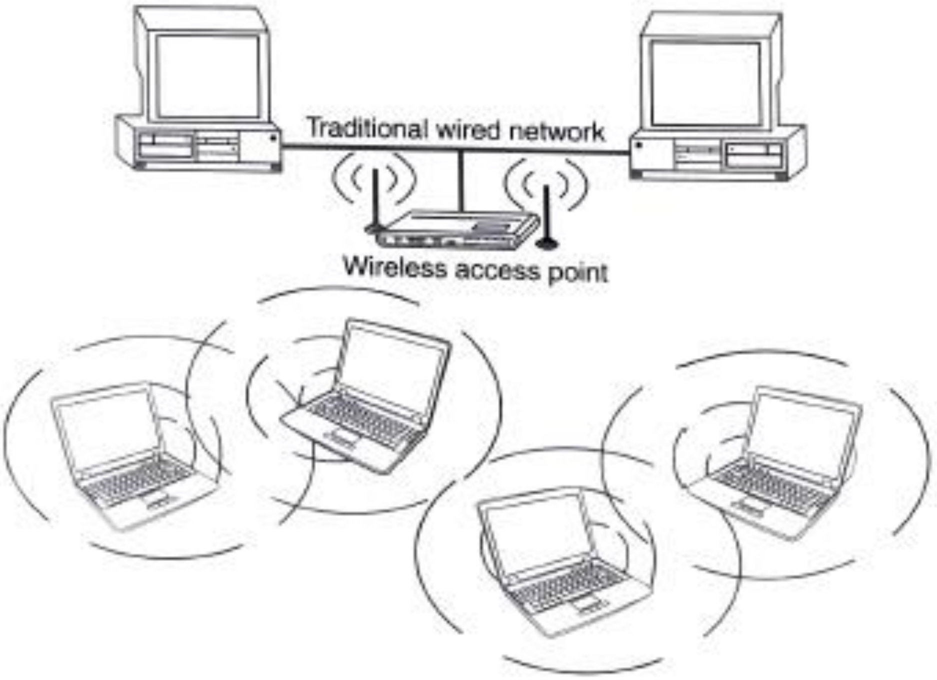
Different Types of Mobile workers

- 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 system. This includes home workers, tele cottagers and in some cases branch worker.
- 2. **Roaming user**→ This is an employee wo works in environment (e.g., warehousing, shop floor etc.) or in multiple areas.
- 3. **Nomad** → This category covers employees requiring solution in hotel room s 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.

<u>Wireless networks</u>

- 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 wo 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. It has modems, routers, hubs and firewall are the integral part of wired and wireless networks. The wirless network is shown in figure 3.6.



- **Fig. 3.6** Wireless networks

Discuss the different wireless technologies.

Wireless Technology

- 1. **802.11 networking standards**
- Computer communication in the frequency band 2.4, 3.6, and 5 GHz.

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).

802.11a: 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 code
Cy1ng (CCK) modulation to improve speeds. In 1999, ratification was made to the original standard, and was termed as 802.11b, which allowed wireless functionality comparable to Ethernet.

802.11g: It provides 54 Mbps transmission in the 2.4 GHz band and the same OFDM 802. Coding as 802.11a, hence it is a lot faster than 802.11a and 802.11lb.

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
Theoretical.

802.15 WLAN → This standard is used for personal WLANs and covers a very short range. Hence it is used for Bluetooth technology

802.16: It is WiMax [broadband and wireless]: 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.
2. Access Points (AP): It is also termed as AP. It is a hardware device and/or a software that acts 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: 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 hotpots
Commercial hotspots
4. Service set identifier (SSID): 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.
5.Wired Equivalence Privacy (WEP): Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.1li Protocol in 1997.
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 W'LANs. WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. WIPA2 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 stating which addresses are allowed.

3.10.1 Traditional Techniques of Attacks on Wireless Network

1. **Sniffing** → Sniffers (passive scanning, detection of SSID, MAC address, collecting the frames 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 areas as a legitimate network.

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. **DoS:** 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 if entitled to access or provide.
   The attacker typically sites or services hosted on high profile web servers such as bank credit card payment gateways mobile phone networks and even root name servers.

4. **Man-in-the middle attack (MITM):** It is the most popular online attack. It is also called as bucket-brigade attack or sometimes Janus attack. It is active eavesdropping 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 servers the MITM Server intercepts the call, hashes the password and passes the connection to the victim server.
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 held. 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.

25. Discuss the theft Internet hours and Wi-Fi based Frauds and Misuses.

3.10.2 Theft of Internet Hours and Wi-Fi based frauds and misuses

1. Computer with ICT → Wireless Internet access→ most homes equipped with Internet.
2. Router configured easily with plug and play feature.
3. Internet is in fingertip of all users, when he/she visit malicious page, the router is exposed to attack.
4. Jupiter research tells that 14% of wireless network owners have access→ neighbour network.

Cybercriminals know that they should not steal Internet hour purchased by others but somehow, they want to get their work done without paying for the internet connection.

- Find IP address of router that you are using
- Open command prompt
- Type “ipconfig/all” and press enter
- look at the default gateway you will get the IP address,
- Type IP address in browser to get information about who you are stealing.

The New “Wars” in the Internet Era

- First word wardriving derived from wardailing came in the film WarGames
-
- **Warwalking/war jagging:** [Pocket PC]and similar in nature to war driving. Except that it is done on foot rather than conducted from a moving vehicle.
- **Warbiking** same as wardriving → WiFi capable device on vehicle itself. (Bicycle or motorcycle)
- **Warkitting** wardriving and rootkitting
- **WAPKitting:** In this attack. external software clutches the control of router's firmware that can be easily accomplished by Exploiting open administrative access.
- WAPkitting can theoretically proceed by more traditional means Such as buffer overflow
- **WAPjacking:** similar DNS poisoning attack. it changes the settings of firmware, that’s helps an attacker to engage in malicious configuration of firmware settings.
- A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer

26. How to secure the Wireless network?

3.10.3 How to secure the wireless Networks

Security features of Wi-Fi networking products are not that time consuming and non-intuitive; sometimes they are still ignored, by home users. The following steps heps to improve the security of wireless Networks

1. Change the default settings of all the equipment’s /components of wireless network
2. Enable WPA (Wi-Fi Protected Access) /WEP (wired Equivalent Privacy) encryption
3. Change the default SSID **(Service Set Identifier)**
4. Enable MAC address filtering.
5. Disable remote login

6. Disable SSID broadcast
7. Disable the features that are not used in AP (access point) [E.g., printing/music support]
8. Avoid providing the network a name which can be easily identified [My_Home_Wifi]
9. Connect only to secured wireless network
10. Upgrade router's firmware periodically
11. Assign static IP address 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.

The following are the Tools to protect wireless network

- http//www.zamzom.com/ Zamzom Wireless Network Tool
- http://www.airdcfense.net/ AirDefense Guard
- http://www.loud-fat-bloke.co.uk/tools.html Wireless Intrusion Detection System (WIDZ)
- http://www.dachb0den.com/projects/bsd-airtools.html BSD-Airtools
- http://wifi. google.com/ Google Secure Access

****