AKTU

Cyber Security

Unit :- 3

BCC-301 (3rd Sem)
BCC-401 (4th Sem)

TOOLS AND METHODS USED IN CYBERCRIME

TOOLS AND METHODS USED IN CYBERCRIME : Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan-horses and Backdoors, Steganography, DoS and DDoS At-tacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction to Phishing, Identity Theft (ID Theft).

Introduction

- Different forms of attacks through which attackers target the computer systems are as follows

1. Initial uncovering:

2. Network probe (investigation) :

3. Crossing the line toward electronic crime (E-crime):

4. Capturing the network:

5. Grab the data:

6. Covering tracks:

Stages of an attack on network

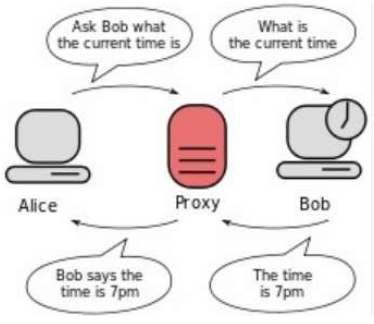
1. **Initial covering:** two stages
   1. Reconnaissance- social networking websites
   2. Uncovers information on company's IP
2. **Network probe:**
   1. Ping sweep- seek out potential targets
   2. Port scanning
3. **Crossing the line toward electronic crime:**
   1. Commits computer crime by exploiting possible holes on the target system

4. **Capturing the network:**
   - attackers attempts to own the network
   - uses tools to remove any evidence of the attack
   - trojan horses, backdoors
5. **Grab the data:**
   - attacker has captured the network
   - steal confidential data, customer CC information, deface webpages…
6. **Covering the attack:**
   - extend misuse of the attack without being detected.
   - start a fresh reconnaissance to a related target system
   - continue use of resources
   - remove evidence of hacking

Proxy server

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

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



Purpose of a proxy server

- **Improve Performance:**
- **Filter Requests**
- **Keep system behind the curtain**
- **Used as IP address multiplexer**

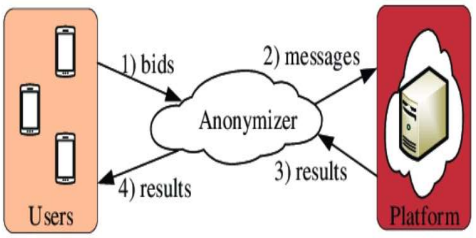
- **Its Cache memory can serve all users**

Attack on this: the attacker first connects to a proxy server- establishes connection with the target through existing connection with the proxy.

An Anonymizer

- *An anonymizer* or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
- Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client.

- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.
- For example, large news outlets such as CNN target the viewers according to region and give different information to different populations



Phishing

- Stealing personal and financial data
- Also can infect systems with viruses
- A method of online ID theft

- **"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?

1. Planning : use mass mailing and address collection techniques- spammers
2. Setup : E-Mail / webpage to collect data about the target
3. Attack : send a phony message to the target
4. Collection: record the information obtained
5. Identity theft and fraud: use information to commit fraud or illegal purchases

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.

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.
- Usually, an attacker follows a common approach – repeatedly making guesses for the password.

The purpose of password cracking is as follows:

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

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

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

Passwords can be **guessed** sometimes **with knowledge** of the user's personal information. 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,
4. user's name or login name;
5. name of user's friend/relative/pet;
6. user's birthplace or date of birth, or a relative's or a friend's;
7. user's vehicle number, office number, residence number or mobile number;
8. name of a celebrity who is considered to be an idol (e.g., actors, actress, spiritual gurus) by the user;

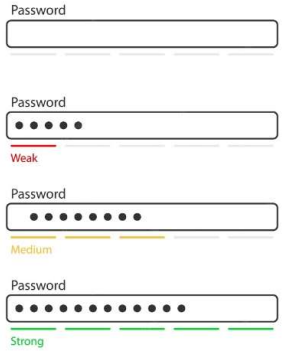
- An attacker can also create a script file (i.e., automated program) which will be executed to try each password in a list.
- This is still considered manual cracking, is time-consuming and not usually effective.
- **Passwords are stored in a database** and password verification process is established into the system when a user attempts to login or access a restricted resource.
- To ensure confidentiality of passwords, the **password verification data is usually not stored in a clear text format**.

Password Cracking Tools: Default Password, Cain & Abel , John the Ripper, THC-Hydra , Aircrack-ng LophtCrack, AirSnort , Solar Winds , Pwdump , RainbowCrack , Brutus

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).

Strong , Weak and Random Passwords



Netizens should practice password guidelines to avoid being victim of getting their personal E-Mailaccounts hacked/attacked by the attackers.

keyloggers

- 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.

Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usuallyare located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruseswithout the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public placesand can obtain the required information about the victim very easily.

Hardware Keyloggers

Hardware keyloggers are small hardware devices.

Some Important Keyloggers are as follows

All In One Keylogger	Stealth Keylogger	Perfect Keylogger
KGB Spy	Spy Buddy	Elite Keylogger
CyberSpy	Powered Keylogger	

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.

Spywares

- Spyware is a type of malware (i.e., malicious software) 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.**

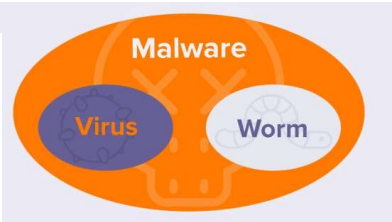
Some Important Spywares are as follows

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

TYPES OF SPYWARE

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

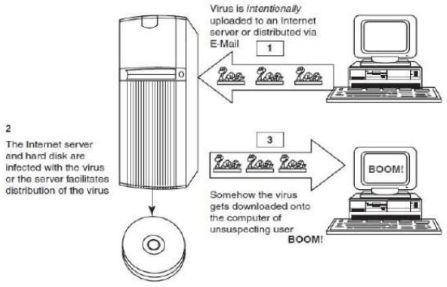
Virus and Worms



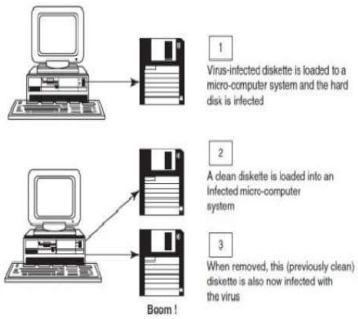
- Computer virus is a program that can "infect" legitimate programs by modifying them to include a possibly "evolved" copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from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

Viruses can take some typical actions:

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

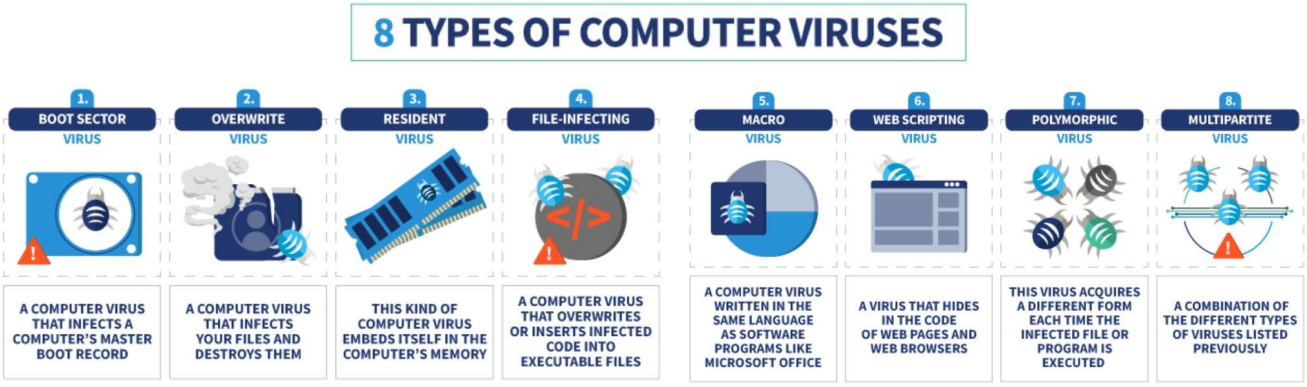


- **Computer virus** has the ability to copy itself and infect the system.
- The term *virus* is also commonly but erroneously used to refer to other types of malware, Adware and Spyware programs that do not have reproductive ability.
- A true virus can only spread from one system to another (in some 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.



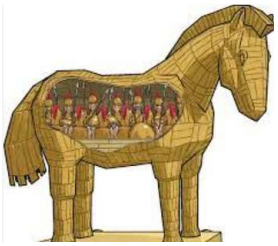
- A worm spreads itself automatically to other computers through networks by exploiting security vulnerabilities, whereas a Trojan is a code/program that appears to be harmless but hides malicious functions.
- Worms and Trojans, such as viruses, may harm the system's data or performance.
- Some viruses and other malware have noticeable symptoms that enable computer user to take necessary corrective actions, but many viruses are surreptitious or simply do nothing for user's to take note of them.
- Some viruses do nothing beyond reproducing themselves.

Virus	Worm
• The virus is the malicious code which will destroy the functioning of the computer system and transfer from one to another system.	• The malicious program that will copy itself and spread from one system of the computer to another through a network is called a worm.
• The virus is created by human action.	• The creation of a worm doesn't need human action.
• The speed of spreading the virus is slow.	• The speed of spreading of worms is fast.
• The host is needed for spreading the virus.	• No host is needed for spreading the virus.



Trojan horses and Backdoors

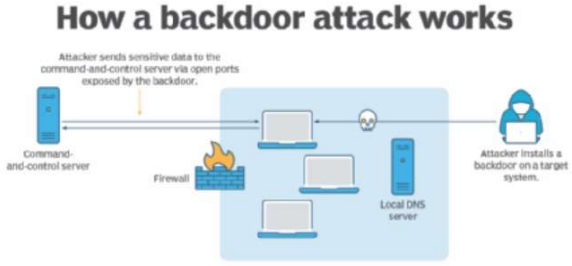
Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example, ruining the fileallocation table on the hard disk.



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

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

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



Following are a few examples of backdoor Trojans:

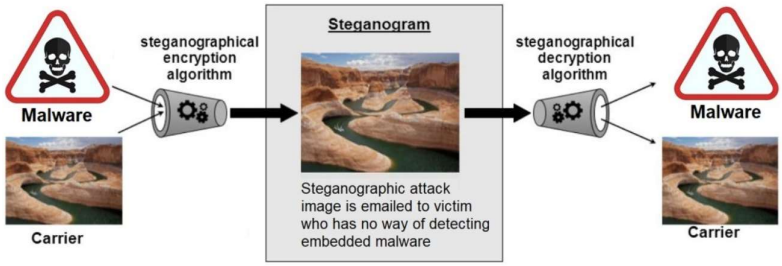
1. Back Orifice 2. Bifrost: 3. SAP backdoors 4. Onapsis Bizploit:

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

1. Stay away from suspect websites/weblinks:
2. Surf on the Web cautiously:
3. Install antivirus/Trojan remover software:

Steganography

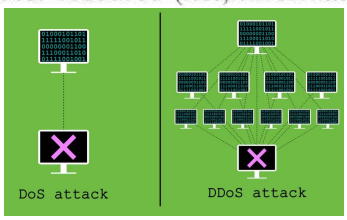
A steganographic attack is the art and science of embedding hidden messages or malware in a carrier medium such as an image or video file in a way the recipient does not realize the file is malicious.



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

DoS and DDoS attacks

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



A DoS attack, or **denial of service attack,** is when a hacker uses a **single system to target another single system** in an attempt to decommission it. This attack works by **flooding the victim system** with transmission control protocol (TCP) or user datagram protocol (UDP) packets (basic units of data sent over a computer network) to the point where **the system becomes inaccessible**, meaning it can **no longer respond to new requests** from other devices. DoS attacks usually won't destroy a system and their effects can be corrected through a series of device and network resets. But as they say: time is money.

A DDoS attack, or **distributed denial of service attack**, is when a hacker uses a **group of systems to target a single system** in order to put it out of service. When comparing DoS vs DDoS, DDoS attacks are by far the more dangerous of the two, and now pose a daily threat to internet enterprises. Using multiple compromised systems to overload a victim network can be **very effective** and make it **difficult to trace** the source of the attack. It's often used as a distraction to **give hackers more time to infiltrate in other ways,** such as data theft.

A quick summary of DoS vs DDoS

	DoS	DDoS
Acronym	Denial of service	Distributed denial of service
Description	A single system targeting a single system	A network of systems targeting a single system
Method	Floods just enough traffic from a single location to disable the victim network	Floods massive amounts of traffic from multiple locations to disable the victim network
Impact	Moderately effective	Very effective
Traceability	Easily traceable	Difficult to trace
Speed	Slow attack speed	Quick attack speed
Prep & recovery	Minor recovery process; easy to predict	Major recovery process; difficult to predict

Classification of DoS

- Bandwidth attacks
- Logic attacks
- Protocol attacks
- Unintentional DoS attack

Types or levels of DoS attacks

- Flood attack
- Ping of death attack
- SYN attack
- Teardrop attack
- Smurf attack
- nuke

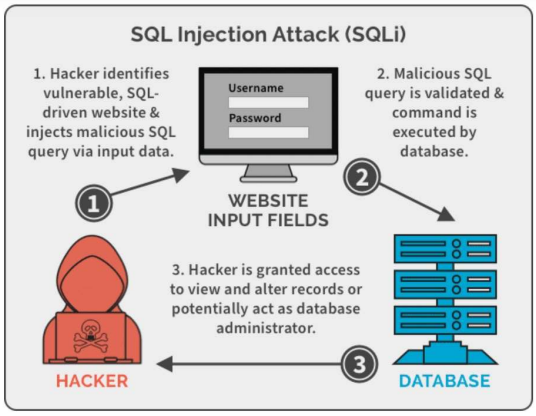
SQL Injection

Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS).

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.



Blind SQL Injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker.

Steps for SQL Injection Attack

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc. The attacker also looks for the webpages that display the HTML commands such as POST or GET by checking the site's source code.
2. To check the source code of any website, right click on the webpage and click on "view source" ,source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the $< FORM >$ and $< /FORM >$have potential parameters that might be useful to find the vulnerabilities.
3. The attacker inputs a single quote under the text box provided on the webpage to accept the username and password. This checks whether the user-input variable is sanitized or interpreted literally by the server. If the response is an error message such as use "a"="a" (or something similar) then the website is found to be susceptible to an SQL injection attack.
4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

How to Prevent SQL Injection Attacks

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

1. Input validation

• Replace all single quotes to two single quotes.

• Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as ; , **--**, select, insert and xp_ can be used to perform an SQL injection attack.

• Numeric values should be checked while accepting a query string value. Function – IsNumeric() for Active Server Pages (ASP) should be used to check these numeric values.

• Keep all text boxes and form fields as short as possible to limit the length of user input.

2. Modify error reports: SQL errors should not be displayed to outside users

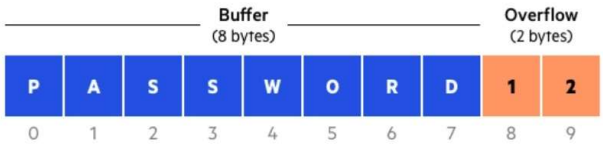
3. Other preventions

• The default system accounts for SQL server 2000 should never be used.

• Isolate database server and web server.

Buffer overflow

- Buffer overflow, or buffer overrun, is an anomaly where a process stores data in a buffer outside the memory the programmer has set aside for it.
- 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

- stack-based buffer overflow
- Heap buffer overflow
- NOPs

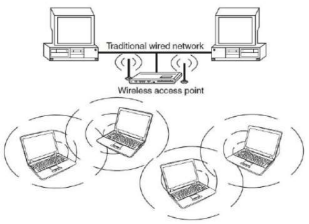
How to minimize buffer overflow

- Assessment of secure code manually
- Disable stack execution
- Compiler tools
- Dynamic run-time checks
- Various tools are used to detect/ defend buffer overflow
  - stackGaurd
  - Propolice
  - LibSafe

Attacks on Wireless Networks

Wireless technologies have become increasingly popular in day-to-day business and personal lives. Hand-held devices such as the PDAs allow individuals to access calendars, E-Mail addresses, phone number lists and the Internet.
Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and PDAs.
Wireless networks are generally composed of two basic elements:

(a) access points (APs) and
(b) other wireless-enabled devices, such as laptops radio transmitters and receivers to communicate or "connect" with each other (see Fig. 4.6).



APs are connected through physical wiring to a conventional network, and they broadcast signals with which a wireless device can connect.
Wireless access to networks has become very common by now in India – for organizations and for individuals.

The following are different types of "mobile workers":

1. Tethered/remote worker: This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems.

2. Roaming user: This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).

3. Nomad: This category covers employees requiring solutions in semi-tethered (connected) environments where modem use frequently.

4. Road warrior: This is the ultimate mobile user and spends little time in the office;

Important components of wireless network

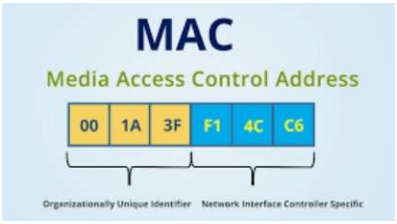
1. 802.11 networking standards: Institute of Electrical and Electronics Engineers (IEEE)-802.11 is a family of standards for wireless local area network (WLAN), stating the specifications and/or requirements for computer communication.

2. Access points: It is also termed as AP. It is a hardware device and/or software that act as a central transmitter and receiver of WLAN radio signals. Users of wireless device, such as laptop/PDAs, get connected with these APs, which in turn get connected with the wired LAN. An AP acts as a communication hub for users to connect with the wired LAN.

3. Wi-Fi hotspots: A hotspot is a site that offers the Internet access by using Wi-Fi technology over a WLAN. Hotspots are found in public areas (such as coffee shops, public libraries, hotels and restaurants) and are commonly offered facility throughout much of North America and Europe.

• *Free Wi-Fi hotspots:* Wireless Internet service is offered in public areas, free of cost and that to without any authentication.

• *Commercial hotspots:* The users are redirected to authentication and online payment to avail the wireless Internet service in public areas.



4. Service Set IDentifier (SSID): It is the name of 802.11i WLAN and all wireless devices on a WLAN must use the same SSID to communicate with each other. While setting up WLAN, the user (or WLAN administrator) sets the SSID, which can be up to 32 characters long so that only the users who knew the SSID will be able to connect the WLAN. It is always advised to turn OFF the broadcast of the SSID.

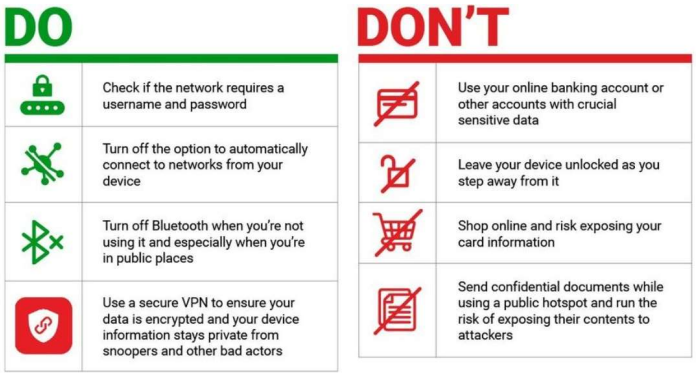
5. Wired equivalence privacy (WEP): Wireless transmission is susceptible to eavesdropping and to provide confidentiality, WEP was introduced as part of the original 802.11i Protocol in 1997. It is always termed as deprecated security algorithm for IEEE 802.11i WLANs. SSID along with WEP delivers fair amount of secured wireless network.

6. Wi-Fi protected access (WPA and WPA2): WPA was introduced as an interim standard to replace WEP to improve upon the security features of WEP. 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.

Tools used for hacking wireless networks
NetStumbler: This tool is based on Windows OS and easily identifies wireless signals being broadcast within range.
Kismet: This tool detects and displays SSIDs that are not being broadcast which 0is very critical in finding wireless networks.
Airsnort: This tool is very easy and is usually used to sniff and crack WEP keys
CowPatty: This tool is used as a brute force tool for cracking WPA-PSK and is considered to be the "New WEP" for home wireless security.

Wireshark (formerly ethereal): Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff out 802.11 management Beacons and probes, and subsequently could be used as a tool to sniff out non-broadcast SSIDs.



Traditional Techniques of Attacks on Wireless Networks

1. Sniffing: The attacker usually installs the sniffers remotely on the victim's system and conducts activities such as

- Passive scanning of wireless network;
- detection of SSID;
- colleting the MAC address;
- collecting the frames to crack WEP.

2. Spoofing: The attacker often launches an attack on a wireless network by simply creating a new network with a stronger wireless signal and a copied SSID in the same area as a original network. Different types of Spoofing are as follows.

- *MAC address Spoofing*
- *IP Spoofing:*
- *Frame Spoofing:*

3. Denial of service (DoS): We have explained this attack in detail

4. Man-in-the-middle attack (MITM): It refers to the scenario wherein an attacker on host *A* inserts *A* between all communications – between hosts *X* and *Y* without knowledge of *X* and *Y*. All messages sent by *X* do reach *Y* but through *A* and vice versa. The objective behind this attack is to merely observe the communication or modify it before sending it out.

5. Encryption cracking: It is always advised that the first step to protect wireless networks is to use WPA encryption. The attackers always devise new tools and techniques to deconstruct the older encryption technology, which is quite easy for attackers due to continuous research in this field. Hence, the second step is to use a long and highly randomized encryption key; this is very important. It is a little pain to remember long random encryption; however, at the same time these keys are much harder to crack.

Phishing and Identity Theft: Introduction , Phishing

Identity theft can be done thorough the following ways.

A. Spam E-Mails

- Also known as "junk E-Mails" they involve nearly identical messages sent to numerous recipients. Spam E-Mails have steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80% of Spam.
- Types of Spam E-Mails are as follows:

1. Unsolicited bulk E-Mail (UBE): It is *synonym for SPAM* unsolicited E-Mail sent in large quantities (see Box 5.2).

2. Unsolicited commercial E-Mail (UCE): Unsolicited E-Mails are sent in large quantities from commercial perspective, for example, advertising. See Box 5.3 to know more about US Act on Spam mails.

Examples:

1. HSBC, Santander, CommonWealth Bank: International Banks having large customer base, phishers always dive deep in such ocean to attempt to hook the fi sh.

2. eBay: It is a popular auction site, often mimicked to gain personal information.

3. Amazon: It was the top brand to be exploited by phishers till July 2009.

4. Facebook: Netizens, who liked to be on the most popular social networking sites such as Facebook, are always subject to threats within Facebook as well as through E-Mail. One can reduce chances of being victim of Phising attack by using the services – security settings to enable contact and E-Mail details as private.

1. "Verify your account":

2. "You have won the lottery":

3. "If you don't respond within 48 hours, your account will be closed":

Let us understand the ways to reduce the amount of Spam E-Mails we receive.[11]

1. Share personal E-Mail address with limited people and/or on public websites – the more it is exposed to the public, the more Spam E-Mails will be received.

2. Never reply or open any Spam E-Mails.

3. Disguise the E-Mail address on public website or groups by spelling out the sign "@" and the DOT (.); for example, Rajeev**AT**gmail**DOT**com. This usually prohibits phishers to catch valid E-Mail addresses while gathering E-Mail addresses through programs.

4. Use alternate E-Mail addresses to register for any personal or shopping website. Never ever use business E-Mail addresses.

5. Do not forward any E-Mails from unknown recipients.

6. Make a habit to preview an E-Mail before opening it.

7. Never use E-Mail address as the screen name in chat groups or rooms.

8. Never respond to a Spam E-Mail asking to remove your E-Mail address from the mailing distribution list. More often it confirms to the phishers that your E-Mail address is active.

B. Hoax E-Mails (deceive or trick E-Mail)

- These are deliberate attempt to deceive or trick a user into believing or accepting that something is real, when the hoaxer (the person or group creating the hoax) knows it is false.
- Hoax E-Mails may or may not be Spam E-Mails.
- It is difficult sometimes to recognize whether an E-Mail is a "Spam" or a "hoax."
- **The websites mentioned below** can be used to check the validity of such "hoax" E-Mails.

1. www.breakthechain.org: This website contains a huge database of chain E-Mails, like we discussed, the phisher sends to entice the netizens to respond to such E-Mails

2. www.hoaxbusters.org: This is an excellent website containing a large database of common Internet hoaxes. It is maintained by the Computer Incident Advisory Capability, which is a division of the US Department of Energy.

Identity Theft (ID Theft)

This term is used to refer to fraud that involves someone pretending to be someone else to steal money or get other benefits.

ID theft is a punishable offense under the Indian IT Act (Section 66C and Section 66D).

The statistics on ID theft proves the severity of this fraud and hence a non-profit organization was found in the US, named as **Identity Theft Resource Center (ITRC)**, with the objective to extend the support to the society to spread awareness about this fraud.

Federal Trade Commission (FTC) has provided the statistics about each one of the identity fraud mentioning prime frauds presented below.

1. Credit card fraud (26%):

2. Bank fraud (17%): Besides credit card fraud, cheque theft and Automatic Teller Machines (ATM) pass code theft have been reported that are possible with ID theft

3. Employment fraud (12%): In this fraud, the attacker borrows the victim's valid SSN to obtain a job.

4. Government fraud (9%): This type of fraud includes SSN, driver license and income tax fraud.

5. Loan fraud (5%): It occurs when the attacker applies for a loan on the victim's name and this can occur even if the SSN does not match the name exactly.

It is important to note the various usage of ID theft information.

1. 66% of victims' personal information is used **to open a new credit account** in their name.

2. 28% of victims' personal information is used **to purchase cell phone service**.

3. 12% of victims end up having **warrants issued in their name** for financial crimes committed by the identity thief.

Personally Identifiable Information (PII)

The fraudsters attempts to steal the elements mentioned below, which can express the purpose of distinguishing individual identity:

1. Full name;
2. national identification number (e.g., SSN);
3. telephone number and mobile phone number;
4. driver's license number;
5. credit card numbers;
6. digital identity (e.g., E-Mail address, online account ID and password);
7. birth date/birth day;
8. birthplace;
9. face and fingerprints.

Types of Identity Theft

1. Financial identity theft;
2. criminal identity theft;
3. identity cloning;
4. business identity theft;
5. medical identity theft;
6. synthetic identity theft;
7. child identity theft.

Techniques of ID Theft

1. Human-based methods:

- *Direct access to information:*
- *Dumpster diving:*
- *Theft of a purse or wallet:*
- *Mail theft and rerouting:*
- *Shoulder surfing:*
- *Dishonest or mistreated employees:*
- *Telemarketing and fake telephone calls:*

2. Computer-based technique:

- *Backup theft:*
- *Hacking, unauthorized access to systems and database theft:*
- *Phishing:*
- *Pharming:*
- *Hardware:*