PMCA605L : Cyber Security

Module 3 : Tools and Methods in Cyber Crime

Courtesy: Nina Godbole, Sunit Belapure *& Other Sources of Internet*

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Dr. R. K. Nadesh

Virus, Worm and Trojan Horse

- **Virus:**

Virus is a computer program or software that connect itself to another software or computer program to harm computer system. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system. Virus can't be controlled by remote.

- **Worms:**

Worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system. Worms can be controlled by remote.

- **Trojan Horse:**

Trojan Horse does not replicate itself like virus and worms. It is a hidden piece of code which steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.

How Do Computer Viruses Reach You?

1. **Opening email attachments from fake accounts.**

2. **Clicking inappropriate internet advertisements without understanding fully.**

3. **Installing/downloading the free games, toolbars or system utilities.**

4. **Visiting an infected web page**

5. **Setting up of software without licensing agreements.**

6. **Getting malware from websites through online ads because of their weak passwords or software flaws.**

7. **Inserting or connecting infected external device and disk.**

8. **Installing pirated software.**

Not only with web activities, if you are not running the latest updates of your operating system and not using the good antivirus software, but computer viruses would also reach you quickly.

Virus - Types

- Resident virus
- Non-resident virus
- Boot sector virus
- Macro virus
- File-infecting virus
- Polymorphic virus
- Metamorphic virus
- Stealth virus
- Companion virus
- Cavity virus.

Resident virus

- Virus that embeds itself in the memory on a target host.
- In such way, it gets activated every time the OS starts or executes a specific action.
- Also known as the **Terminate and Stay Resident** (TSR), it finds a way to load in the computer's RAM and then infects the executable files that are opened by the user when a certain conditions are met.
- A few **examples** of this kind of virus are Jerusalem Virus, One-half virus, Magistr, Junkie, Satanbug etc.

Non-Resident Virus

- **Non-resident Viruses** is a kind of **virus** that does not stay or complete itself from the computer's memory.

- When executed, this type of virus actively seeks targets for infections either on local, removable or on network locations. Upon further infection, it exits.

- **Examples** are CMJ, Mr Klunky, Randex, and Meve

Boot sector virus

- A boot sector virus is a computer virus that infects a storage device's **Master Boot Record** (MBR).
- It is not mandatory that a boot sector virus successfully boot the victim's PC to infect it.
- These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table.
- Examples of boot- sector viruses are Michelangelo and Stoned.

Macro virus

- Virus written in macro language, embedded in Word, Excel, Outlook etc. documents.
- This type of virus is executed as soon as the document that contains it is opened.
- This corresponds to the macro execution within those documents, which under normal circumstances is automatic.
- **Example** of a macro virus is the **Melissa virus** which appeared in March 1999. When a user opens a Microsoft Word document containing the Melissa **virus**, their computer becomes infected.

File-infecting virus

- When the infected file is being executed, the virus seeks out other files on the host and infects them with malicious code.

- The malicious code is inserted either at the beginning of the host file code (prepending virus), in the middle (mid-infector) or in the end (appending virus).

- A specific type of viruses called "cavity virus" can even inject the code in the gaps in the file structure itself.

  Examples include Jerusalem and Cascade.

Polymorphic virus

- Polymorphic virus is a complicated computer virus that affects data types and functions.
- It is a self-encrypted virus designed to avoid detection by a scanner.
- Upon infection, the polymorphic virus duplicates itself by creating usable, albeit slightly modified, copies of itself.
- RSNIF, VIRLOCK, VOBFUS, and BAGLE or UPolyX are some of the most notorious **polymorphic viruses** in existence.

Metamorphic virus

- This virus is capable of changing its own code with each infection.
- The rewriting process may cause the infection to appear different each time but the functionality of the code remains the same.
- The metamorphic nature of this virus type makes it possible to infect executable from two or more different operating systems or even different computer architectures as well.
- The metamorphic viruses are one of the most complex in build and very difficult to detect. **Eg. Zmist**

Stealth virus

- Memory resident virus utilizes various mechanisms to avoid detection.
- The virus can also maintain a clean copy of the infected files in order to provide it to the antivirus engine for scan while the infected version will remain undetected.
- Furthermore, the stealth viruses are actively working to conceal any traces of their activities and changes made to files.
- Example : BRAIN

Armored virus

- Armored Virus may also protect itself from antivirus programs, making it more difficult to trace.

- Type of virus designed to thwart attempts by Analysts from examining its code by using various methods to make tracing, disassembling and reverse engineering more difficult.

- Trick the antivirus program into believing that its location is somewhere other than where it really is on the system.

Eg. Whale Virus

Multipartite virus

- These virus attempts to attack both the file executable as well as the master boot record of the drive at the same time.

- This type may be tricky to remove as even when the file executable part is clean it can re-infect the system all over again from the boot sector if it that is not cleaned as well.

- Example : Tequila Virus

Camouflage virus

- This virus type is able to report as a harmless program to the antivirus software.

- In such cases where the virus has, similar code to the legitimate non-infected files code the antivirus application is tricked into believing that it has to do with the legitimate program as well.

Companion virus

- A companion virus is a complicated computer virus, which, unlike traditional viruses, does not modify any files.

- Instead, it creates a copy of the file and places a different extension on it, usually .com.

- This unique quality makes a companion virus difficult to detect, as anti-virus software tends to use changes in files as clue.

Example : a bogus CHKDISK.COM file would be executed before the legitimate CHKDISK. EXE

Cavity virus

- Unlike traditional viruses the cavity virus does not attach itself to the end of the infected file but instead uses the empty spaces within the program files itself (that exists there for variety of reasons).
- This way the length of the program code is not changed and the virus can more easily avoid detection.
- The injection of the virus in most cases will not affect the functionality of the host file at all.
- The cavity viruses are quite rare though.
- For **example**, the CIH **virus**, or Chernobyl **Virus**.

Types of Worms

- Worm is a malicious program category, exploiting operating system vulnerabilities to spread itself into the system.
- In its design, worm is quite similar to a virus - considered even its sub-class.
- Unlike the viruses, though worms can reproduce/ duplicate and spread by themselves.
- During this process worm does not require to attach itself to any existing program or executable.

Types of Worms

- **Email worms**: Spread through email messages, especially through those with attachments.
- **Internet worms**: Spread directly over the internet by exploiting access to open ports or system vulnerabilities.
- **Network worms**: Spread over open and unprotected network shares.
- **Multi-Vector worms**: Worms having two or more infestation capabilities

How to Identify a Worm ?

- **Unusual Slowdowns:** If your computer suddenly becomes slow without any resource-heavy tasks running, a worm could be consuming CPU or memory.
- **High Disk or Network Usage:** Unexpected spikes in disk or network activity might indicate a worm spreading or communicating with a remote server.
- Open **Task Manager (Windows)** and look for unknown or suspicious processes consuming high CPU, RAM, or disk usage.
- Use **Resource Monitor (Windows)** or **Wireshark** to check for unusual outbound connections.
- Check for **Unauthorized Admin Access**.
- Look for **Unusual Registry Entries** (Windows)

Types of Trojans

- **Computer Trojans** or **Trojan horses**

- A type of malware software that masquerades itself as not-malicious even useful application but it will actually do damage to the host computer after its installation.

- Trojans *do not self-replicate* since its key difference to a virus

- and require often end user intervention to install itself - which happens in most scenarios where a user is tricked into believing that the program he is installing is a legitimate one (this is often connected with social engineering attacks on end users).

Remote Access Trojans (RAT) aka Backdoor. Trojan

- This type of Trojan opens backdoor on the targeted system to allow the attacker remote access to the system or even complete control over it.

- A computer with a sophisticated backdoor program installed also may be referred as a "zombie" or a "bot". A network of such bots may often be referred to as a "botnet"

Trojan-DDoS

- This Trojan is installed simultaneously on a large number of computers in order to create a zombie network (botnet) of machines that can be used (as attackers) in a DDoS attack on a particular target.

Trojan-Proxy

- A proxy Trojan is a virus, which hijacks and turns the host computer into a proxy server, part of a botnet, from which an attacker can stage anonymous activities and attacks.

Trojan-FTP

- This Trojan is designed to open FTP ports on the targeted machine and allows a remote attacker access to the host.

- Furthermore, the attacker can also access as well network shares or connections to further extent more and other threats.

Destructive Trojan

- This is designed to destroy or delete data. It is much like a virus.

Security Software Disabler Trojan

- This is designed to stop security programs like antivirus solutions, firewalls or IPS either by disabling them or by killing the processes.
- This kind of Trojan functionality is combined often with destructive Trojan that can execute data deletion or corruption only after the security software is disabled.
- Security Software Disablers are entry Trojans that allow next level of attack on the targeted system.

Info Stealer (Data Sending/ Stealing Trojan)

- This Trojan is designed to provide an attacker with confidential or sensitive information from compromised host and send it to a predefined location (attacker). The stolen data comprise of login details, passwords, credit card information etc.

- The most common techniques may include log key strokes, screen shots and web cam images, monitoring internet activity often for specific financial websites.

- Store-Local-Remote- Encrypt

Trojan

- Key logger Trojan
- Trojan-PSW (Password Stealer)/SPY
- Trojan-Banker
- Trojan-IM
- Trojan-Game Thief
- Trojan Mail Finder
- Trojan. Downloader

Trojan-Dropper

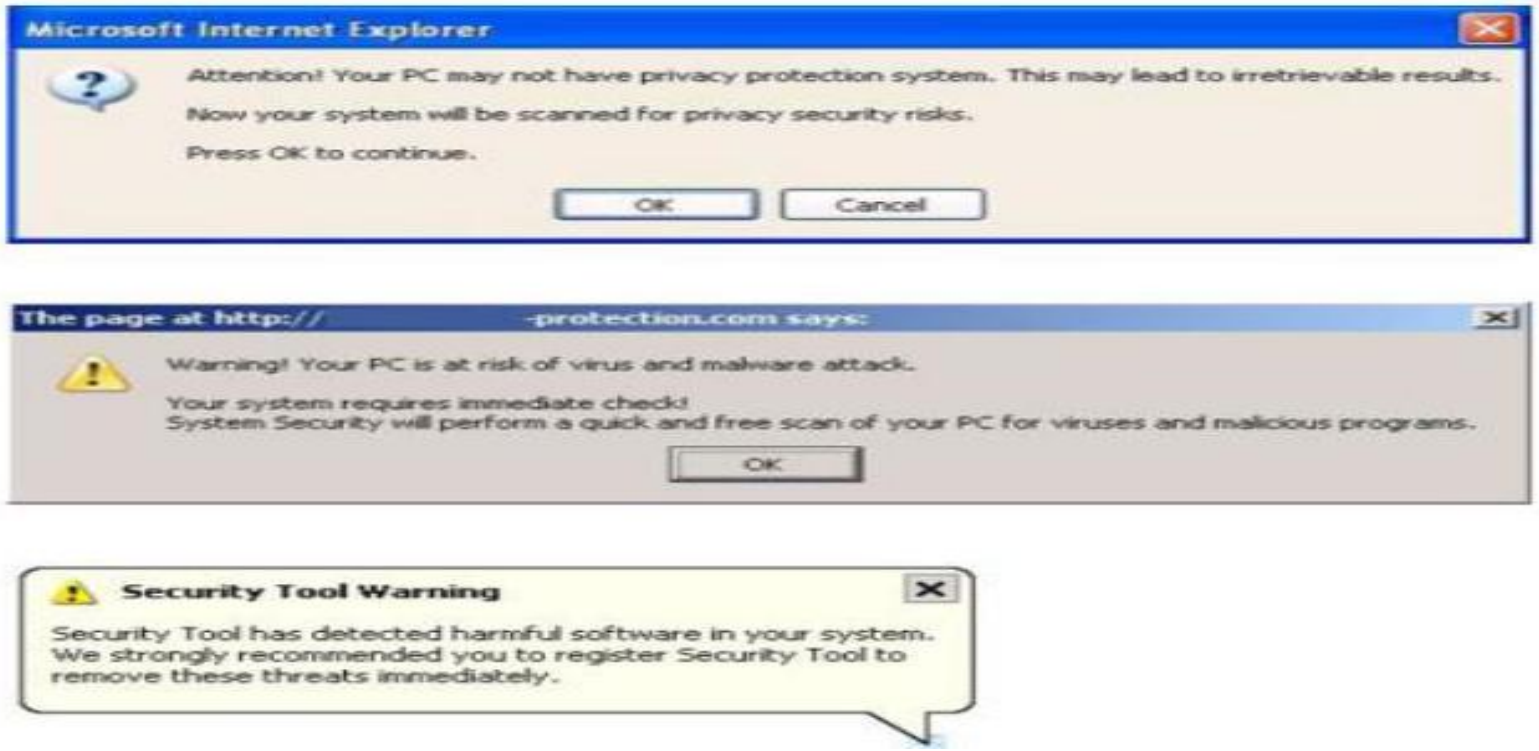
- Trojan-Dropper is a type of Trojan that drops different type of standalone malware (Trojans, worms, backdoors) to a system.
- It is usually an executable file that contains other files compressed inside its body.
- When a Trojan-Dropper is performed, it extracts these compressed files and saves them to a folder (usually a temporary one) on the computer.

Trojan-ArcBomb

- These Trojans are archives designed to freeze or trigger slow performance or to flood the disk
- With a large amount of “empty” data when an attempt is made to unpack the archived data.
- The so-called archive bombs pose a particular threat for file and mail servers
- When an automated processing system is used to process incoming data: an archive bomb can simply crash the server.

Trojan.FakeAV

- Trojan.FakeAV is a detection for Trojan horse programs that intentionally misrepresent the security status of a computer



Trojan

- **Trojan-Clicker** or **Trojan-AD clicker**
- **Trojan-SMS**
- **Trojan-Ransom (Trojan-Ransomlock)**

  Locks computer screen or some part of computer functionality

- **Cryptolock Trojan (Trojan.Cryptolocker)**

  Cryptolock Trojan encrypts and locks individual files.

  (public-key cryptography with strong RSA 2048 encryption.)

  Examples > CryptoLocker, CryptoWall, CoinVault, TorLocker, CoinVault and CTB-Locker, *TeslaCrypt*

Backdoor

- A backdoor is a means of access to a computer program that bypasses security mechanisms.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- Attackers often use backdoors that they detect or install themselves as part of an exploit.

Backdoors can be installed through:

- **Malware & Trojans** – Hidden in fake software or malicious attachments.
- **Exploiting Software Vulnerabilities** – Hackers find security loopholes in software.
- **Pre-Installed Backdoors** – Some manufacturers add secret backdoors for remote troubleshooting.

Trojan Backdoor

Common Ports used by Trojan

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	GirlFriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers Trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack'99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Virus, Worm and Trojan Horse

VIRUS	WORM	TROJAN HORSE
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.
Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility software.

Password Cracking

- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

Examples of guessable passwords include:

1. Blank (none);
2. the words like “password,” “passcode” and “admin”;
3. series of letters from the “QWERTY” keyboard, for example, qwerty, asdf or qwertyuiop;
4. user’s name or login name;
5. name of user’s friend/relative/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;
9. simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

Password Cracking Attacks

- 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).

Password Cracking Attacks

Online Attacks

- The most popular online attack is man-in-the middle (MITM) attack, also termed as “bucket-brigade attack” or sometimes “Janus attack.”
- It is a form of active eavesdropping in which the attacker establishes a connection between a victim and the server to which a victim is connected.

Common Forms of Bucket-Brigade Attacks

- SSL Stripping – Downgrading HTTPS to HTTP to capture login credentials.
- DNS Spoofing – Redirecting users to fake websites.
- ARP Spoofing – Trick a device into sending network traffic to the attacker.
- Session Hijacking – Stealing cookies to take over an authenticated session.

Offline Attacks

- Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media.

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.
- A strong password is long enough, random or otherwise difficult to guess – producible only by the user who chooses it.

Common Password Cracking Techniques

- **Brute Force Attack - Tries all possible character combinations** until it finds the correct password.

  Tools: **John the Ripper**; **Hashcat**

- **Dictionary Attack** - Uses a **predefined list of common passwords** instead of random guesses.

  Tools: **Cain & Abel ; Medusa**

- **Rainbow Table Attack** - Uses **precomputed hash values** instead of brute-forcing from scratch.

  Tools: **RainbowCrack; Ophcrack**

Rainbow Table Attack

- A Rainbow Table Attack is a type of cryptographic attack used to crack hashed passwords efficiently.
- It precomputes **hash values for a large set of possible passwords and stores them in a rainbow table for quick lookup.**
- Password: "password123"
  Hash: "ef92b778bafee3b5d1e241b7c2cbeff2“
- **Attackers generate hashes for millions of possible passwords and store them in a rainbow table.**
- **Instead of hashing each password during an attack, they simply look up the hash in the table.**
- **When an attacker gets access to a hashed password (e.g., from a data breach), they search for it in the rainbow table.**
- **If found, they retrieve the corresponding plaintext password.**

Salting

- **Salting** is a security technique used to protect stored passwords by adding a **random, unique string (salt)** to each password before hashing.

- This prevents **dictionary attacks** and **rainbow table attacks**.

- ✓ User Chooses a Password (“mypass”)
- ✓ A Unique Random Salt is Generated(@dfe#)
- ✓ Salt is Added to the Password (mypass@dfe#)
- ✓ The Combined String is Hashed (Hash (mypass@dfe#)
- ✓ The Hash and Salt are Stored in the Database
- ✓ **During Login, the Same Process is Repeated**
- ✓ The system **retrieves the stored salt**, applies it to the entered password, **hashes it again**, and checks if it matches the stored hash.

Online Password Cracking & Recovery Tools

- https://www.onlinehashcrack.com/
- Have I Been Pwned: Check if your email has been compromised in a data breach
- https://hashcat.net/hashcat/
- https://crackstation.net/

Strong Password Policy

- Password Complexity Requirements- Minimum Length: At least 12–16 characters (longer passwords are more secure).
- No Common Words
- No Personal Information
- Password Expiration and Rotation
- Change passwords every 90–180 days (or use a risk-based approach
- Prevent Reuse: Maintain a history of at least 5–10 previous passwords to prevent reuse.
- Lockout and Monitoring Policies- Account Lockout- Session Timeout- Monitor Login Activity
- Secure Storage and Encryption(Use **salting** to add extra security to hashed passwords.)

Strong Random Password

- A **random password** is a secure, unpredictable combination of **letters, numbers, and special characters** used to protect accounts from brute force and dictionary attacks.

- Strong Passwords:

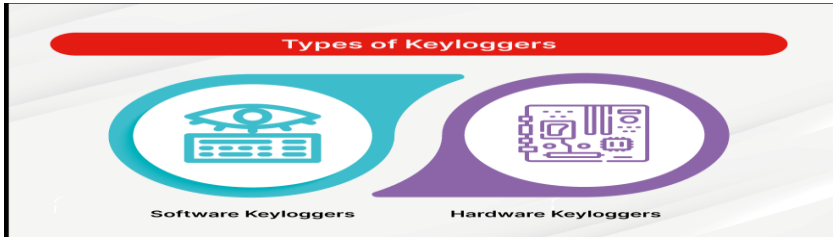
  G!9xL@2#fVk%P

  3^hTz&N0QdY*X

Keyloggers

- A keylogger (keystroke logger) is a type of software or hardware that records every keystroke a user types on a keyboard.

- While they can be used legally for monitoring employees, parental control, or password recovery.



- Cybercriminals often misuse them for stealing login credentials, banking details, and other sensitive information.

Software Keyloggers

- 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.

- 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.

- How They Work:

✅ Installed via phishing emails, malicious downloads, or infected USBs.

✅ Runs as a hidden process, recording keystrokes and screenshots.

✅ Sends logs to the attacker via email, FTP, or a remote server.

Examples: Spyrix Free Keylogger , Refog Keylogger , DarkComet RAT

Hardware Keyloggers

- Hardware keyloggers are small hardware devices connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.

- These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

How They Work:

- ✅ Must be physically installed on the target computer.
- ✅ Logs keystrokes and stores them in internal memory.
- ✅ Some models **send data remotely** over Wi-Fi or Bluetooth.

Some URL

- https://www.hoverwatch.com/
- https://www.relytec.com/

  (All-in-one Keylogger)
- https://www.spyrix.com/spyrix-free-keylogger.php

AntiLogger Tools

https://zemana.com/us/antilogger.html

https://www.malwarebytes.com/

https://www.spyshelter.com/

How to Detect A Keylogger?

- The simplest way to detect a keylogger is to check your **task manager**. You can see which processes are running. It can be tough to know which ones are legitimate and which could be caused by keyloggers.

- Another good place to look for keyloggers is under the **Startup tab**. Keyloggers get set up to run all the time on a computer, and to do that, they need to be started up with the operating system.

- You can also check for keyloggers by examining your **computer's internet usage report**. To access this in Windows, press the Windows button and "I" at the same time.

- You can do the same form of investigation with **browser extensions**. If there are extensions you do not recall installing, disable them because they could be keyloggers.

Spyware

- **Spyware** is a type of **malicious software (malware)** that secretly gathers information from a device **without the user's consent**.

- It can steal **passwords, banking details, browsing history, emails, messages, and even record keystrokes or webcam footage**.

Types of Spyware

- **Trojan Spyware**
  - Disguised as **legitimate software** but secretly runs in the background. Can steal files, screenshots & webcam/microphone recordings.
  - **Examples:** Emotet, DarkComet, FinSpy.

- **Adware (Advertising Spyware)**
  - Tracks **browsing habits & personal interests** for targeted ads. Slows down your system and **floods you with pop-ups**.
  - **Examples:** CoolWebSearch, Gator, Fireball.

- **Infostealers (Data Theft Spyware)**

- **Mobile Spyware (Phone Tracking & Surveillance Apps)**

Signs of Spyware Infection

- **Device Running Slow** – Background spyware consuming CPU & RAM.
- **Excessive Pop-ups & Ads**
- **Unexpected High Data Usage** – Spyware sending data to remote servers.
- **New Unknown Programs** – Check **Task Manager (Windows)**
- **Battery Draining Fast** – Spyware running in the background.
- **Strange Logins & Unauthorized Access** – Check the login history for your accounts.

How to Prevent Yourself ?

- ✓ **Enable Two-Factor Authentication (2FA)** – Adds an extra layer of security.
- ✓ **Use a Password Manager** – Prevents keystroke logging.
- ✓ **Avoid Clicking Suspicious Links & Emails** – Common spyware infection method.
- ✓ **Keep Your OS & Software Updated** – Security patches fix spyware vulnerabilities.
- ✓ **Use a Secure Browser with Privacy Extensions** – Blocks tracking scripts & ads.
- ✓ **Scan Your System Regularly** – Use **Malwarebytes or Bitdefender** for real-time protection.

Security threats

Designed to cause damage to a targeted computer or cause a certain degree of operational disruption.

- **Malware** (software viruses, spyware, adware, worms, trojans, ransomeware)
- **Rootkit** **are malicious software designed to hide certain processes or programs from detection.**
- **Tracking cookies-** **Small pieces of data stored on your web browser that track your online activity, including websites you visit, login details, and preferences. Advertisers, analytics companies, and websites use them to monitor user behavior across multiple sites**
- **Riskware-** **A remote desktop tool (like TeamViewer) is useful for IT support but can be exploited by hackers to gain control over your system if not secured properly.**
- **Scareware** **is a class of malware that includes both Ransomeware (Trojan.Ransom) and FakeAV software.**

Other security threats

- **Spam** is the term used to describe unsolicited or unwanted electronic messages, especially advertisements. The most widely recognized form of spam is email spam.

- **Creepware** is a term used to describe activities like spying others through webcams (very often combined with capturing pictures), tracking online activities of others and listening to conversation over the computer's microphone and stealing passwords and other data.

- **Blended threat** defines an exploit that combines elements of multiple types of malware components. Usage of multiple attack vectors and payload types targets to increase the severity of the damage caused and as well the speed of spreading.

Proxy Servers and Anonymizers

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

A proxy server has the following purposes:

1. Keep the systems behind the curtain.
2. Speed up access to a resource (through “caching”).
3. Specialized proxy servers are used to filter unwanted content such as advertisements.
4. A proxy server can be used as an IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address.

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.

Basic stages of an attack

1. Initial uncovering:

In the first step called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means.

In the second step, the attacker uncovers as much information as possible on the company's internal network.

2. Network probe: A "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool is used to discover exactly which services are running on the target system.

3. Crossing the line toward electronic crime (E-crime): Now the attacker is toward committing what is technically a "computer crime" by exploiting possible holes on the target system.

4. Capturing the network: At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily.

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.

6. Covering tracks: This is the last step in any cyberattack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

Steganography

- Steganography is the practice of concealing information within other non-secret data to prevent detection.

- The word “steganography” comes from the two Greek words: steganos meaning “covered” and graphein meaning “to write” that means “concealed writing.”

- It is often used for covert communication.

Types of Steganography

- **Text Steganography** – Hiding messages within text files using techniques like spacing, font changes, or invisible characters.
- **Image Steganography** – Embedding hidden data within images by altering pixel values in a way that is imperceptible to the human eye.
- **Audio Steganography** – Concealing information within audio files by modifying sound frequencies or embedding data in silent sections.
- **Video Steganography** – Hiding messages inside video frames or metadata.
- **Network Steganography** – Concealing data within network traffic, such as unused TCP/IP fields or packet headers.

Stego Media

- Stego media refers to digital media (images, audio, video, or text) that contain hidden information using steganography techniques.

- This allows covert communication, copyright protection, and security applications.

- **Stego Images -** Hides information inside image files.

Uses Least Significant Bit (LSB) replacement, DCT (Discrete Cosine Transform), or DWT (Discrete Wavelet Transform) techniques.

- **Stego Audio -** Embeds data in inaudible frequency ranges or silent sections of an audio file.

  Techniques: LSB substitution, Phase Coding, Echo Hiding.

Stego Media

- **Stego Video -** Hides data within video frames or metadata.

  Techniques: Motion Vector Modification, LSB in keyframes, DCT-based embedding.

- **Stego Text** - Conceals data in text using spacing, font changes, or invisible characters.

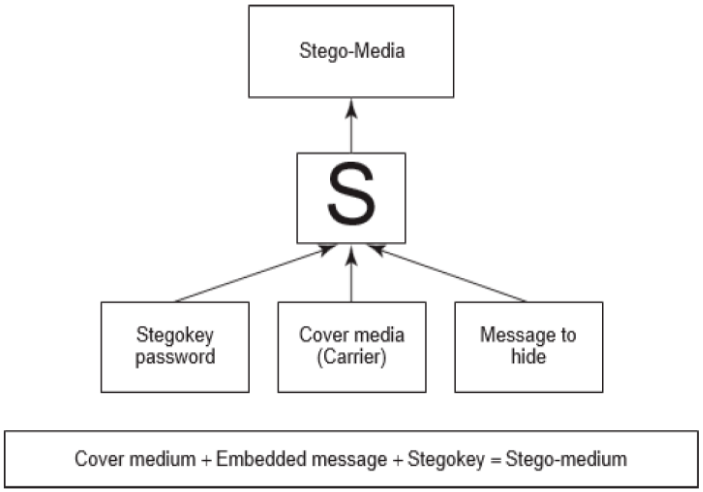
  Techniques: Whitespace manipulation, Synonym substitution, Unicode Zero-width characters.

- **Stego Network Data**

  Hides data within network packets (TCP/IP headers, timing of packets).

Key Components of Stego Media

- **Cover Media** (Carrier File) (The original image, audio, video, text, or network packet that will carry the hidden data.)
- **Secret Message** (Payload) (The data to be hidden, such as text, images, or other files)
- **Steganographic Algorithm**
- **Stego Key**
- **Steganographic Output**
- **Extraction and Detection Method**



Steganalysis

- Steganalysis is the art and science of detecting messages that are hidden in images, audio/video files using steganography.

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

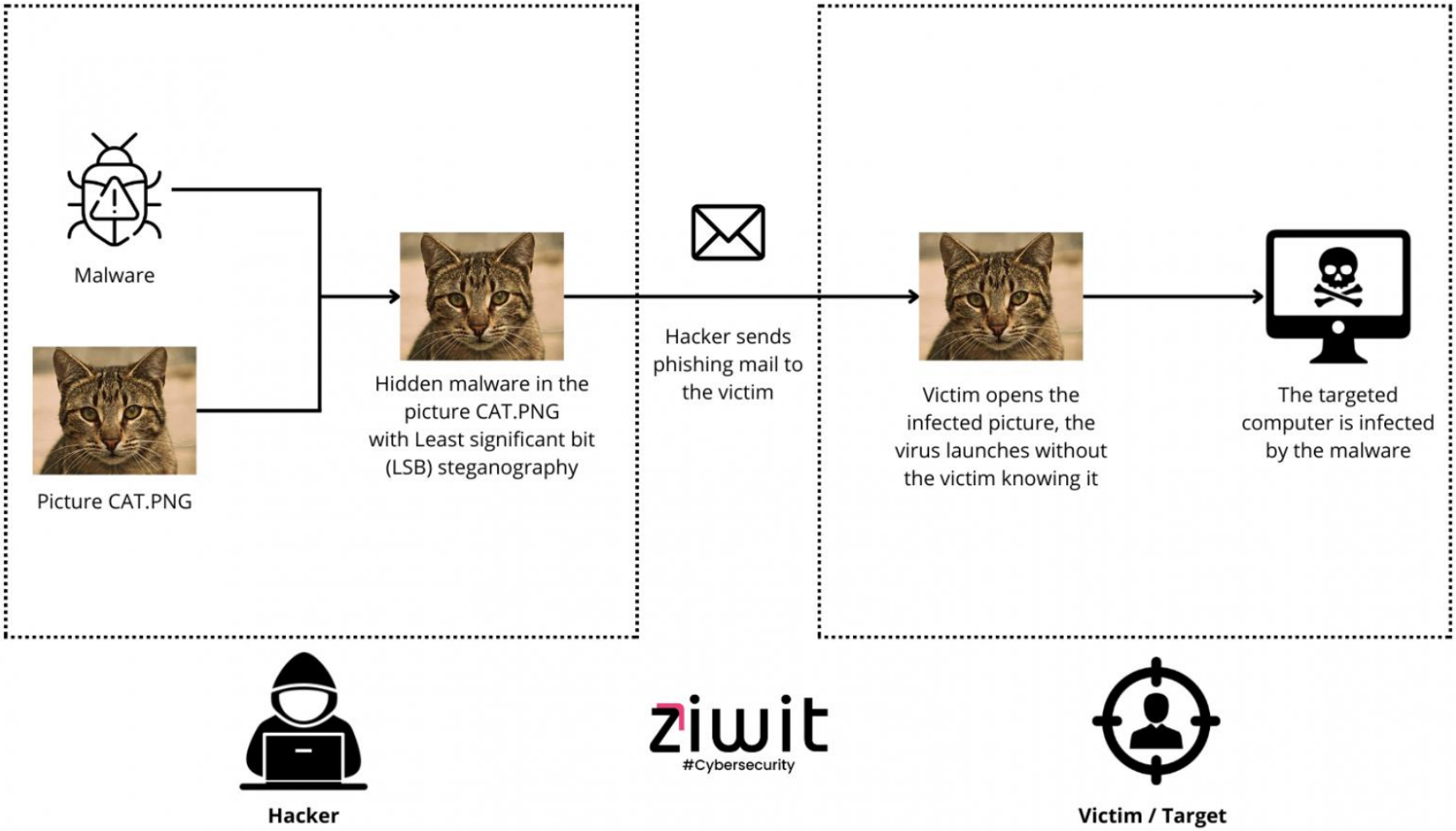
Comparison Between Steganography and Cryptography

Feature	Steganography	Cryptography
Definition	Hides the existence of data within another medium.	Converts data into an unreadable format using encryption.
Purpose	Conceals the fact that communication is taking place.	Ensures confidentiality by making the message unreadable without a key.
Technique	Embeds secret data in images, audio, videos, or text.	Uses encryption algorithms like AES, RSA, and DES.
Security	Relies on secrecy of the method; detection makes it vulnerable.	Stronger security; even if detected, encrypted data remains unreadable.
Detection Risk	High – If discovered, the hidden data can be extracted.	Low – Even if intercepted, the data remains encrypted.
Computational Complexity	Generally low; involves simple embedding techniques.	High; involves complex mathematical algorithms.
Use Cases	Digital watermarking, covert communication, data hiding in media.	Secure data transmission, authentication, financial transactions.
Examples	LSB (Least Significant Bit) method in images, audio steganography.	RSA, AES, Blowfish encryption for securing data.
Resistance to Attacks	Vulnerable to steganalysis (detection techniques).	Resistant to cryptanalysis if strong encryption is used.

Tools Weblink

- https://www.openstego.com/
- https://steghide.sourceforge.net/
- https://georgeom.net/StegOnline/upload

How do cybercriminals use Steganography?



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 unavailable to its intended users.

- Malicious attempts to disrupt the normal functioning of a network, service, or website by overwhelming it with traffic or resource requests.

Denial-of-Service attack (DoS attack)

- The attacker floods the bandwidth of the victim's network or fills his E-Mail box with Spam mail depriving him of the services he is entitled to access or provide.

- The goal of *DoS is not to gain unauthorized access* to systems or data but to prevent intended users (i.e., legitimate users) of a service from using it.

1. Flood a network with traffic, thereby preventing legitimate network traffic.

2.Disrupt connections between two systems, thereby preventing access to a service.

3. Prevent a particular individual from accessing a service.

4. Disrupt service to a specific system or person.

DDoS Attacks

- In a DDoS attack, an attacker may use your computer to attack another computer.
- By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He/she could then force your computer to send huge amounts of data to a website or send Spam to particular E-Mail addresses.
- A DDoS attack is a distributed DoS wherein a large number of zombie systems are synchronized to attack a particular system. The zombie systems are called “secondary victims” and the main target is called “primary victim.”
- DDoS attacks involves hardcoding the target IP address prior to release of the malware, hence no further interaction is necessary to launch the attack.
- A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent

Common Types of DoS Attacks

- Volume-Based Attacks (Flood Attacks)
- Protocol-Based Attacks
- Application Layer Attacks
- Distributed DoS (DDoS) Attacks
- Advanced DoS Attacks

Volume-Based Attacks (Flood Attacks)

These attacks generate massive amounts of traffic to exhaust the target's bandwidth.

Attack Type	Description
ICMP Flood (Ping Flood)	Overloads the target by sending excessive ICMP Echo Request (ping) packets.
UDP Flood	Sends large numbers of UDP packets to random ports, making the system waste resources responding to false requests.
SYN Flood	Exploits the TCP handshake by sending SYN requests but never completing the handshake, exhausting connection slots.
HTTP Flood	Overwhelms a web server by sending a high number of HTTP requests.

Protocol-Based Attacks

These attacks exploit weaknesses in network protocols, consuming server resources.

Attack Type	Description
SYN-ACK Flood	Overwhelms a server by sending SYN-ACK responses without waiting for an acknowledgment.
Smurf Attack	Spoofs the victim's IP and sends ICMP requests to a network, causing the network to flood the victim with replies.
Ping of Death	Sends malformed or oversized packets, crashing the target system.
Fraggle Attack	Similar to Smurf but uses UDP instead of ICMP to flood the target.
DNS Amplification	Sends small DNS requests with a spoofed IP, causing large DNS responses that flood the victim.

Application Layer Attacks (Layer 7 Attacks)

These attacks target specific applications, consuming their processing power.

Attack Type	Description
Slowloris Attack	Sends partial HTTP requests slowly, keeping server connections open indefinitely.
RUDY (R-U-Dead-Yet?)	Uses long-form field submissions to exhaust server resources.
HULK (HTTP Unbearable Load King)	Sends unique HTTP GET requests to evade caching and overload a server.
Xerxes Attack	A powerful attack that floods the target with fake HTTP requests.

Distributed DoS (DDoS) Attacks

DDoS attacks use multiple infected devices (botnets) to attack the target.

Attack Type	Description
Botnet-Based DDoS	A network of compromised devices (botnets) sends massive requests to flood the target.
IoT-Based DDoS	Uses vulnerable IoT devices (e.g., Mirai botnet) to launch large-scale attacks.
Cloud-Based DDoS	Uses cloud resources to amplify attack power.

Advanced DoS Attacks

- These attacks combine multiple methods or exploit system-specific vulnerabilities.

Attack Type	Description
Teardrop Attack	Sends fragmented packets that crash systems unable to reassemble them.
Land Attack	Sends packets with the same source and destination IP, causing the system to crash.
Zero-Day Exploit DoS	Uses unknown vulnerabilities to attack the system before a fix is available.

DoS and DDoS

Feature	DoS (Denial of Service) Attack	DDoS (Distributed Denial of Service) Attack
Definition	Overloads a system or network with excessive traffic from a single source.	Overloads a system or network using multiple compromised systems (botnets).
Source of Attack	Single attacker/machine.	Multiple attackers (botnets) controlled by a single entity.
Impact	Slows down or crashes a service temporarily.	Causes a massive outage, making recovery more difficult.
Complexity	Easier to detect and block.	Harder to detect due to multiple attack sources.
Attack Methods	Flooding (ICMP, SYN, UDP), resource exhaustion.	Botnet-driven attacks, volumetric, protocol, and application layer attacks.
Mitigation	IP blocking, rate limiting, firewall rules.	Advanced DDoS mitigation services, AI-based detection, and traffic filtering.
Example	A single hacker sending excessive requests to a website.	A botnet of thousands of devices attacking a website simultaneously.

Permanent DoS (PDoS) Attack (Phlashing Attack)

- A **Permanent Denial of Service (PDoS)** attack, also known as a **Phlashing attack**, is a type of cyberattack that **permanently damages hardware or firmware** of a target system, making it **irrecoverable** without hardware replacement or reinstallation.

Attack Type	Description
Malicious Firmware Update	Attacker injects harmful firmware, making devices inoperable.
Electrical Overload	Forces excessive workload, overheating and damaging hardware.
Bricking Devices	The attack corrupts the device's bootloader, making recovery impossible.
IoT-Based PDoS	Targets IoT devices with malicious code, rendering them permanently unusable.

Real-World Examples of DDoS Attacks

- **Mirai Botnet (2016)**: Infected IoT devices to launch massive DDoS attacks, disrupting major websites like Twitter, Netflix, and Reddit.

- **GitHub (2018)**: Hit by a 1.35 Tbps DDoS attack, one of the largest ever recorded.

- **AWS (2020)**: Mitigated a 2.3 Tbps DDoS attack, the largest in history.

How to Protect from DoS/DDoS Attacks

1. Implement router filters.
2. If such filters are available for your system, install patches to guard against TCP SYN flooding.
3. Disable any unused or inessential network service.
4. Enable quota systems on your OS if they are available.
5. Observe your system's performance and establish baselines for ordinary activity
6. Routinely examine your physical security with regard to your current needs.
7. Use Tripwire or a similar tool to detect changes in configuration information or other files.
8. Invest in and maintain "hot spares" – machines that can be placed into service quickly if a similar machine is disabled.
9. Invest in redundant and fault-tolerant network configurations.
10. Establish and maintain regular backup schedules and policies, particularly for important configuration information.
11. Establish and maintain appropriate password policies, especially access to highly privileged accounts such as Unix root or Microsoft Windows NT Administrator.

How to Protect from DoS/DDoS Attacks

1. Use a Web Application Firewall (WAF)	Blocks malicious traffic and filters suspicious requests before they reach your server. (e.g., Cloudflare, AWS WAF)
2. Deploy DDoS Protection Services	Cloud-based DDoS mitigation services absorb and filter attack traffic. (e.g., Cloudflare, Akamai, AWS Shield, Google Cloud Armor)
3. Rate Limiting & Traffic Filtering	Limits the number of requests from a single IP address to prevent excessive load.
4. Intrusion Detection & Prevention Systems (IDS/IPS)	Monitors network traffic and detects/prevents unusual activity. (e.g., Snort, Suricata)
5. Enable Load Balancing	Distributes traffic across multiple servers to prevent overload. (e.g., Nginx, HAProxy, AWS ELB)
6. Anycast Network for Traffic Distribution	Uses multiple servers across different locations to handle traffic more efficiently.
7. Keep Software & Security Patches Updated	Fixes vulnerabilities that attackers exploit for DoS/DDoS attacks.
8. Use AI-based Threat Detection	AI-driven security tools detect abnormal traffic patterns and mitigate attacks in real-time.
9. Geo-blocking & Blacklisting	Blocks traffic from suspicious regions or known malicious IPs.
10. DNS Security Measures	Use protected DNS services like Google DNS (8.8.8.8) and OpenDNS to prevent DNS-based attacks.

SQL Injection

- SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.
- The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.
- Attackers target the SQL servers – common database servers used by many organizations to store confidential data.
- During an SQL injection attack, Malicious Code is inserted into a web form field or the website's code to make a system execute a command shell or other arbitrary commands.
- Just as a legitimate user enters queries and additions to the SQL database via a web form, the attacker can insert commands to the SQL server through the same web form field.

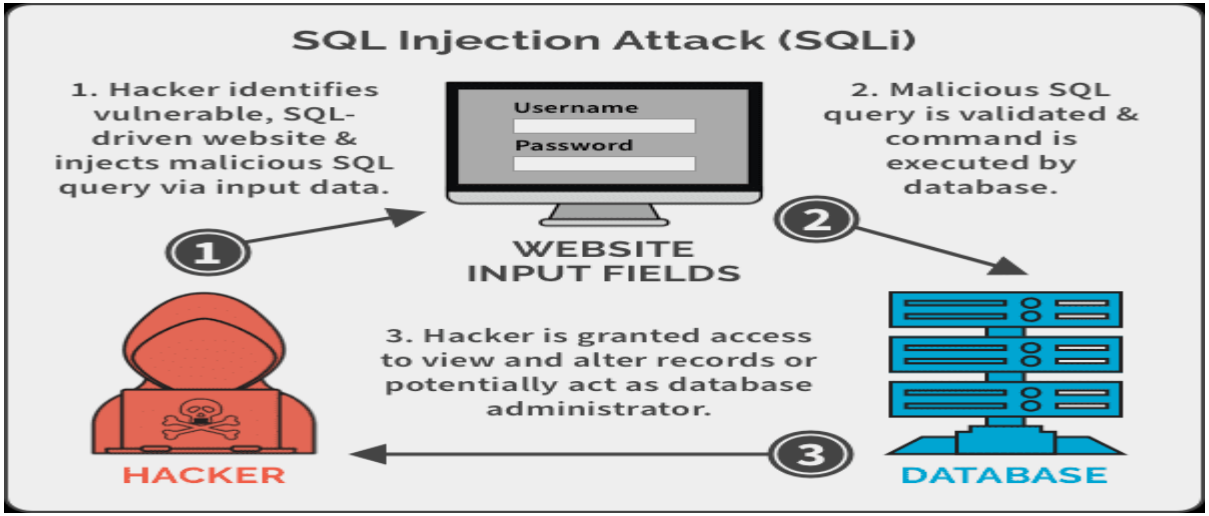
Using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance

2. May gain access to the database by obtaining username and their password

3. Add new data to the database

4. Modify data currently in the database



How SQL Injection Works ?

- Find vulnerable input fields (e.g., login forms, search bars).
- Craft SQL payloads to manipulate database queries.
- Extract sensitive data or gain control of the system.

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.

- No direct error messages, but attacker infers results from response time or Boolean responses.

- SELECT * FROM users WHERE id = 1 AND (SELECT SLEEP(5)); SLEEP(5) function forces the database to pause execution for 5 seconds.

SQL Injection Based on 1=1 is Always True

- **SQL Injection Based on 1=1 is Always True**
- If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this
- SELECT * FROM Users WHERE UserId = 105 OR 1=1;
- The SQL above is valid and will return ALL rows from the "Users" table, since **OR 1=1** is always TRUE.
- Does the example above look dangerous? What if the "Users" table contains names and passwords?
- SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1;

Bypassing Authentication

- SELECT * FROM users WHERE username = 'admin' --' AND password = 'password';

- Everything after -- is ignored, bypassing authentication.

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

(Validate & Sanitize Inputs (Reject invalid data)**)**

2. Modify error reports

3. Other preventions

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

Buffer Overflow

- **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.**

- As buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

- Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

```
void main()
{
    char bufferA[50];
    char bufferB[16];

    printf("What is your name?\n");

    gets(bufferA);

    strcpy(bufferB, bufferA);

    return;
}
```

For example:

```
int main()
{
    int buffer[10];
    buffer[20] = 12;
}
```

Types of Buffer Overflow

- Stack-Based Buffer Overflow
- NOPs
- Heap Buffer Overflow

Stack-Based Buffer Overflow

- Stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside the intended data structure – usually a fixed length buffer.

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

NOP (No Operation)

- **NOP (No Operation)** instruction is an **assembly language instruction** that **does nothing** for one CPU cycle.

- It is primarily used for **timing adjustments, instruction alignment, and exploit development (NOP sleds in buffer overflow attacks).**

Heap Buffer Overflow

- Heap buffer overflow occurs in the heap data area when an application copies more data into a buffer than the buffer was designed to contain.
- Heap buffer overflow occurs in the heap data area and may be introduced accidentally by an application programmer, or it may result from a deliberate exploit.
- The heap is the memory space that is dynamically allocated new(), malloc() and calloc() functions.

How to Minimize Buffer Overflow ?

The following methods will definitely help to minimize such attacks:

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

Attacks on Wireless Networks

- Even when people travel, they still need to work.
- The employee is no longer tied to an office location and is, in effect, “boundaryless.”

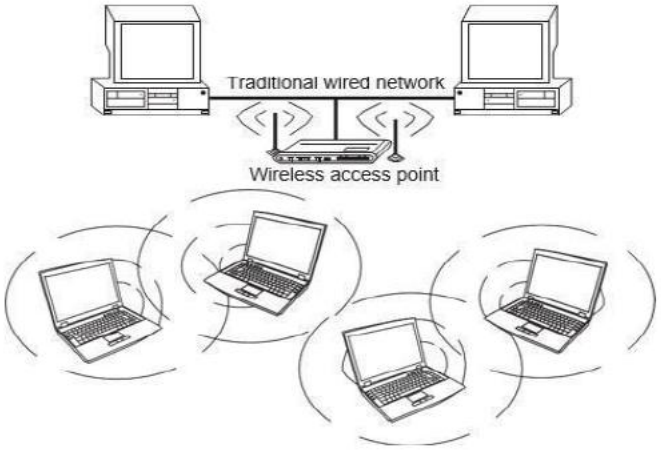
- The following are different types of “mobile workers”:

✓ Tethered/remote worker

✓ Roaming user

✓ Nomad

✓ Road warrior



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).

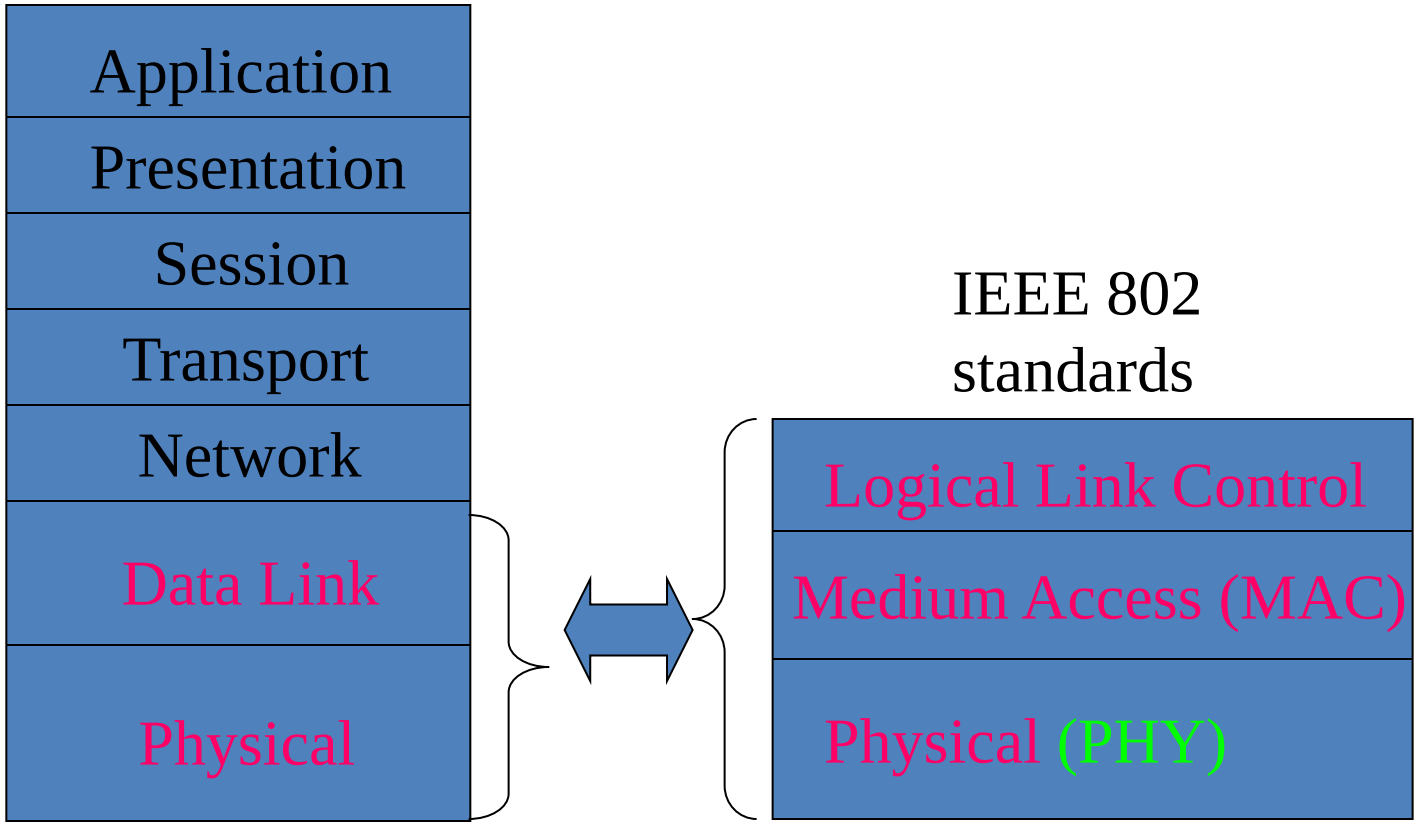
3. **Nomad**: This category covers employees requiring solutions in hotel rooms and other semi tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.

4. **Road warrior:** This is the ultimate mobile user and spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels.

Standardization of Wireless Networks

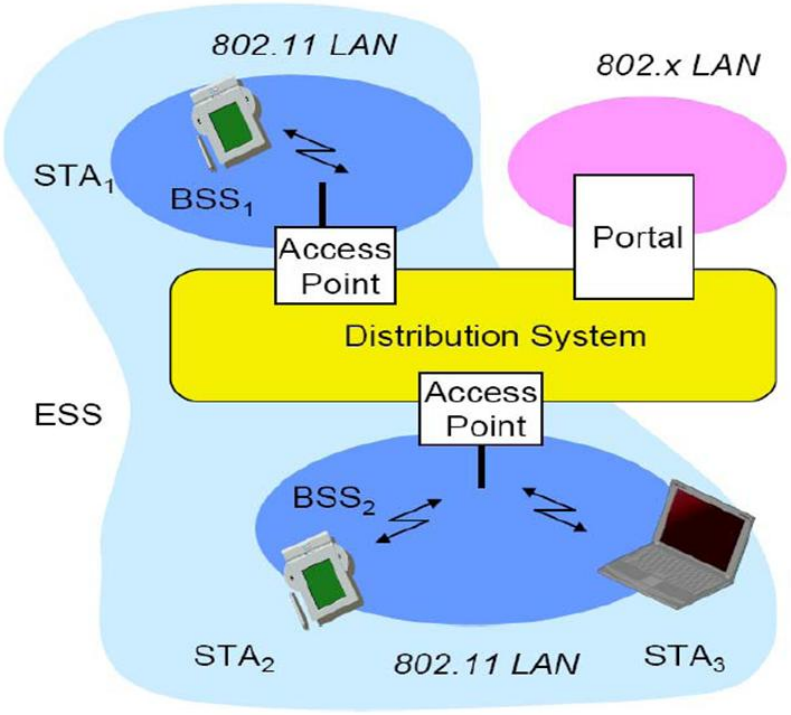
- **Wireless networks are standardized by IEEE.**
- **Under 802 LAN MAN standards committee.**

ISO OSI 7-layer model



Wireless Network

Architecture of an Infrastructure based on IEEE 802.11



Station (STA)
- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)
- group of stations using the same radio frequency

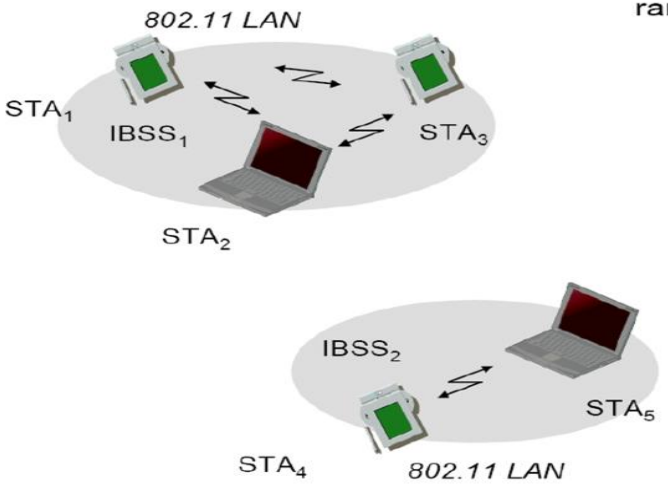
Access Point
- station integrated into the wireless LAN and the distribution system

Portal
- bridge to other (wired) networks

Distribution System
- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

Wireless Network

Architecture of IEEE 802.11 Adhoc Wireless Lan



Direct communication within a limited range

- Station (STA):
  terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS):
  group of stations using the same radio frequency

Wireless Networks

- Access Point
- Service Set Identifier (SSID)
- Wireless Clients (End Devices)
- Wireless Network Interface Card (WNIC)- MAC
- Wireless Standards & Protocols (Common Wi-Fi standards: **802.11a/b/g/n/ac/ax (Wi-Fi 6)**.)
- Security Components (**Encryption: WPA3, WPA2, WEP** (to protect data).) (**WEP (Wired Equivalent Privacy)** and **WPA (Wi-Fi Protected Access)**.)

Traditional Techniques of Attacks on Wireless Networks

- Penetration of a **wireless network through unauthorized access** is termed as **wireless cracking.**

- There are various methods that demand a high level of technological skill and knowledge, and the availability of numerous software tools made it less sophisticated with minimal technological skill to crack WLANs.

1. Sniffing
2. Spoofing
3. Denial of service (DoS)
4. Man-in-the-middle attack (MITM)
5. Encryption cracking

Sniffing

- Passive Scanning of Wireless Network
- Detection of SSID
- Collecting MAC Address
- Collecting the Frames to crack WEP

Spoofing

- Evil Twin Attack - The attacker sets up a **fake Wi-Fi network** with the same **SSID (Wi-Fi name)** as a real one.
- MAC Address Spoofing - A hacker spoofs the MAC address of an authorized device to gain access to a secured Wi-Fi network.
- IP Spoofing - Forges the source IP address in network packets to hide their identity, impersonate another device, or launch malicious activities.
- Frame Spoofing - Forges or manipulates network frames to impersonate legitimate devices, bypass security controls, or intercept data

Denial of Service

- A Denial of Service (DoS) attack in a wireless network aims to disrupt network availability by overwhelming the network, causing legitimate users to lose connectivity.

- These attacks exploit weaknesses in Wi-Fi protocols (e.g., IEEE 802.11) to interfere with communication.

Man-in-the-Middle (MITM)

- The attacker intercepts and potentially alters the communication between two parties without their knowledge.
- **Interception:** The attacker positions themselves between the victim and the wireless access point (AP). This can be done by creating a rogue access point or by exploiting vulnerabilities in the wireless protocol.
- **Decryption:** If the communication is encrypted, the attacker may attempt to decrypt the data. This can be done through various means, such as exploiting weak encryption protocols (e.g., WEP) or using more sophisticated methods like SSL stripping.
- **Manipulation:** The attacker can alter the communication between the two parties, injecting malicious data or stealing sensitive information like login credentials, financial data, or personal information

Encryption Cracking

- Breaking security measures that protect wireless networks, such as WEP, and WPA encryption.

- Attackers use various techniques to intercept data, steal passwords, and gain unauthorized access to Wi-Fi networks.

How to Secure the Wireless Networks

1. **Change the default settings** of all the equipments/components of wireless network (e.g., IP address/ user IDs/administrator passwords, etc.).
2. **Enable WPA/WEP encryption.**
3. **Change the default SSID.**
4. **Enable MAC address filtering.**
5. **Disable remote login.**
6. **Disable SSID broadcast.**
7. **Disable the features that are not used in the AP** (e.g., printing/music support).
8. **Avoid providing the network a name that can be easily identified** (e.g., My_Home_Wifi).
9. Connect only to secured wireless network (i.e., **do not auto-connect to open Wi-Fi hotspots**).
10. **Upgrade the router's firmware** periodically.

Summary

- Password Cracking
- Keyloggers
- Virus-Worms-Trojans
- Steganography
- DoS & DDoS
- Buffer Overflow
- Attacks on Wireless Networks