PMCA605L : Cyber Security

Module 1 : An Overview

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

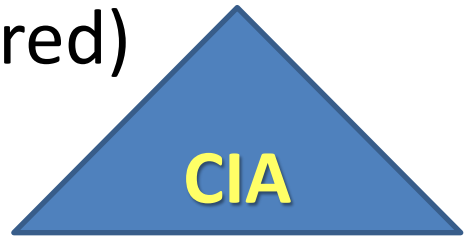
Cyber Security

- Cybersecurity is the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, damage, or theft.

- It encompasses a wide range of technologies, processes, and practices to ensure the **Confidentiality**, **Integrity**, and **Availability** of information and systems.

CIA Traid

- **Confidentiality**
  (Prevention of unauthorized disclosure or use of information assets)
- **Integrity**
  (Prevention of unauthorized modification of information assets Availability)
- **Availability**
  (Ensuring authorized access of information assets when required for the duration required)



Key Components of Cybersecurity

- Network Security: Protecting the infrastructure and data transmitted across networks from intrusions and threats like malware, hacking, or phishing.
- Application Security: Ensuring software and applications are designed and maintained to resist cyber threats.
- Information Security (InfoSec): Safeguarding sensitive data from unauthorized access or breaches.
- Endpoint Security: Protecting individual devices like computers, smartphones, and IoT devices.
- Cloud Security: Ensuring data and applications stored in the cloud are safe.
- Identity and Access Management (IAM): Ensuring only authorized users have access to specific data or systems.

Common Cyber Threats

- Malware (e.g., viruses, ransomware, spyware)
- Phishing: Deceptive attempts to steal sensitive information via fake emails or websites.
- Denial-of-Service (DoS) Attacks: Overloading a system to make it unavailable.
- Man-in-the-middle (MitM) Attacks: Intercepting and altering communication between two parties.
- SQL Injection: Exploiting vulnerabilities in databases

Importance of Cybersecurity

- Protects sensitive information (e.g., personal, financial, or business data).
- Maintains trust and credibility for businesses.
- Prevents financial losses and legal repercussions.
- Ensures continuity of operations in critical infrastructure sectors.

RISK

Risk refers to the potential for loss, damage, or harm that could result from a threat exploiting a vulnerability in a system, network, or organization.

It is the possibility that an event will occur and negatively impact an organization's assets, operations, or reputation.

A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and **that may be avoided through pre-emptive action.**

Risk Identification

- Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives.
- Identify assets (e.g., data, hardware, software) that need protection.
- Recognize potential threats (e.g., malware, insider threats, natural disasters).
- Identify vulnerabilities (e.g., outdated software, weak passwords).

Cybercrime

- **Cybercrime refers to criminal activities (directly or indirectly) carried out using computers, networks, or digital devices.**

- It targets individuals, organizations, or governments to steal data, disrupt operations, or cause harm. **These crimes leverage the internet or other digital systems as their medium.**

- Any **illegal act** where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution.

- Any **traditional crime** that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.

- Any **financial dishonesty** that takes place in a computer environment.

- Any **threats to the computer**, such as hardware or software theft, sabotage, and ransom demands.

Two types of attack are prevalent in cybercrimes:

- **Techno-crime:** A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt, or otherwise deface or damage parts of or the complete computer system.

- **Techno-vandalism:** These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature.

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

Definitions and Scope

- Cyber Law is a framework created to give legal recognition to all risks arising out of the usage of computers, computer networks, or related technology.

- "Cyber Law" is a term used to describe the legal issues related to the use of Computer and Communications Technology.

- The Indian Parliament passed the Information Technology Bill on 17th May 2000, known as the ITA 2000, aimed at providing legal infrastructure for E-Commerce in India.

Cybernetics

- Cybernetics is an interdisciplinary field that studies systems of control, communication, and feedback in both living organisms and machines.

- It focuses on understanding how systems—whether biological, mechanical, or social—process information, respond to inputs, and adapt to changes.

Cyberspace

- "Cyberspace" is where users mentally travel through matrices of data.
- Conceptually, "cyberspace" is the nebulous place where humans interact over computer networks.
- Most definitely a place where you chat, explore, research, and play.

Cyber Squatting

- The term is derived from "squatting," which is the act of occupying an abandoned space/building that the user does not own, rent, or otherwise have permission to use.

- Cyber squatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cyber squatters through the registration process.

Cyberpunk

- According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism.“
- The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement.“
- It explores how technological advancements, especially in computers, artificial intelligence, and cybernetics, impact society, often highlighting themes of social decay, corporate domination, and individual rebellion.

Cyberwarfare

- **Cyberwarfare** refers to the use of digital attacks by organizations, or individuals to disrupt, damage, or destroy the digital infrastructure of another nation or entity.

- It is considered a significant part of modern conflicts and involves a variety of tactics aimed at achieving political, economic, or military objectives through cyber means.

Examples of Cyberwarfare

- Stuxnet (2010): A sophisticated worm reportedly developed by the U.S. and Israel to sabotage Iran's nuclear program by targeting its centrifuges.
- Russia-Georgia Conflict (2008): During the military conflict, cyberattacks were used to disable Georgian government websites and spread disinformation.
- NotPetya (2017): A ransomware attack that primarily targeted Ukraine but spread globally, crippling companies and costing billions in damages.
- SolarWinds Hack (2020): A supply chain attack allegedly linked to Russian intelligence targeting U.S. government agencies and private companies.

Who are Cybercriminals?

- Cybercriminals are those who conduct activities such as

✓ Credit card fraud

✓ Cyberstalking *(a crime in which someone harasses or stalks a victim using electronic or digital means)*

✓ Defaming another online

✓ Gaining unauthorized access to computer systems

✓ Ignoring copyright - Software licensing and trademark protection

✓ Overriding encryption to make illegal copies

✓ Software piracy and stealing another's identity to perform criminal acts.

Cybercriminals

- **Type I: Cybercriminals – hungry for recognition**
- **Type II: Cybercriminals – not interested in recognition**
- **Type III: Cybercriminals – the insiders**

Classifications of Cybercrimes

1. Cybercrime against individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against Society
5. Crimes emanating from Usenet newsgroup

Computer as a Target

Computer as a Weapon

Target of the crime

- Single event of cybercrime
- Series of events

E-Mail Spoofing

- **E-Mail Spoofing** – The sender forges the "From" address in an email to make it appear as though the message is coming from a trusted or legitimate source.
- The goal is to deceive the recipient and exploit their trust for malicious purposes.

(Friend- Enemy, Mail)

Example of E-Mail Spoofing:

An employee receives an email that appears to be from their company's IT department:

Subject: Urgent: Password Reset Required
From: it-support@company.com
Message:
Dear Employee,
Our security systems have detected unusual activity on your account. Please reset your password immediately by clicking the link below.
[Reset Password Here]

Note: The link redirects to a phishing website designed to steal login credentials.

Spamming

- People who create electronic Spam are called *spammers*.
- Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately.
- Spamming is widely detested and has been the subject of legislation in many jurisdictions – for example, the CAN-SPAM Act of 2003.
- Email Spam - SMS Spam- Social Media Spam- Voice Spam (Robocalls)- Instant Messaging Spam

Search engine spamming

- Search engine spamming is an alteration or creation of a document with the intent to deceive an electronic catalog or a filing system.

- Some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number of returned search results.

Internet Time Theft

- Internet time theft occurs when an unauthorized person uses the Internet hours paid for by another person.

- It comes under hacking because the person gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means.

Salami Attack/Salami Technique

- Type of cybercrime where small amounts of money or data are deducted or stolen over time, often in a way that goes unnoticed by victims.

- **Banking Fraud**: An employee programs a banking system to round down all fractional interest payments and deposit the fractions into a secret account.

Data Diddling

- **Data Diddling** is a type of cybercrime where data is altered either before it is entered into a system, during processing, or before output.

- This manipulation often involves unauthorized changes to data to commit fraud, cause damage, or achieve other malicious objectives.

➢ A data diddling attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

➢ Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.

Forgery

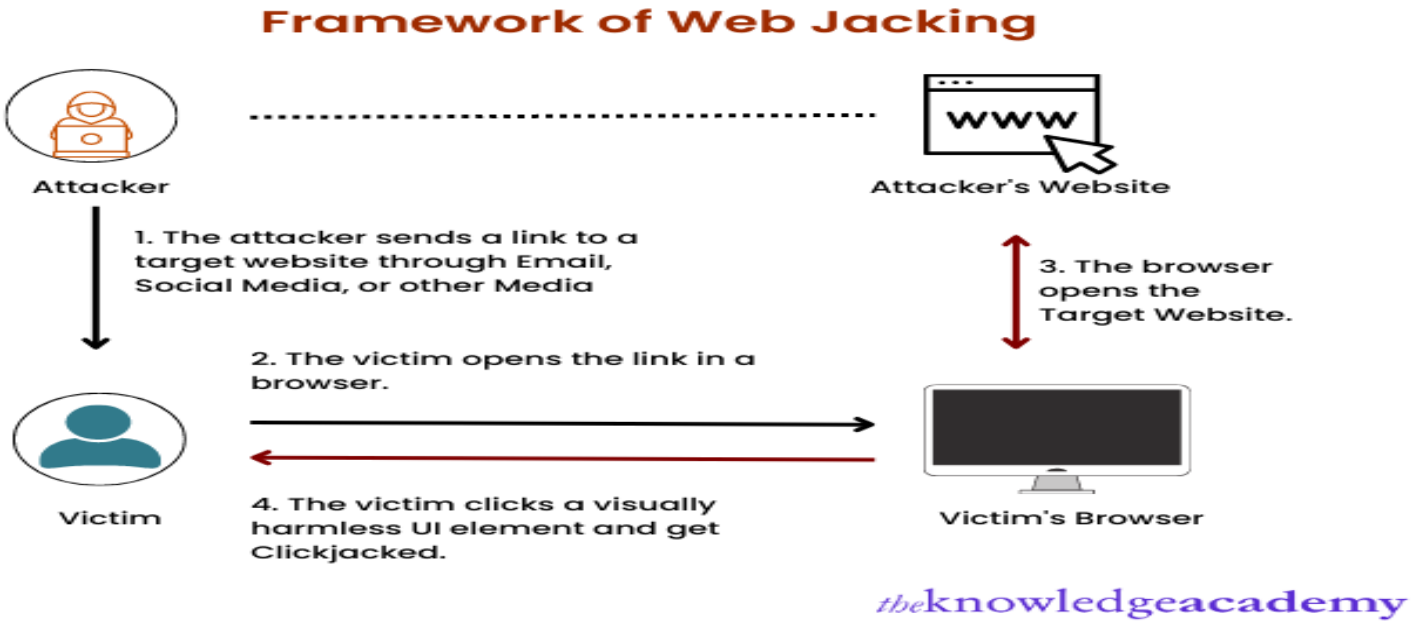
- **Forgery** in the context of cybercrime refers to the creation, alteration, or manipulation of digital documents, data, or communications to deceive, defraud, or harm individuals or organizations.

- It involves falsifying information with the intent to mislead.

- Forging counterfeit currency notes, postage, revenue stamps, mark sheets, etc. using sophisticated computers, printers, and scanners.

Web Jacking

- Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it).
- Web Jacking refers to the unauthorized control or hijacking of a website by an attacker.
- Unauthorized Access- Manipulation of Website Content- Redirection of Traffic- Phishing or Malware Distribution



Financial Institution Website Hijacking (2019)

- Hackers took control of a prominent financial institution's website by exploiting vulnerabilities in its hosting service.
- They used web jacking techniques to change the website's DNS records, redirecting visitors to a fraudulent page that resembled the original bank's login page.
- The fake page was designed to harvest login credentials and financial data from customers.

Web Jacking


1. The attacker initial a client side QR session and clone the Login QR Code into a phishing website
Now a well crafted phishing page with a valid and regularly updated QR Code is ready to be sent to a Victim.
2. The Attacker Sends the phishing page to the victim.
4. The Attacker gains controls over the victim's Account.
3. The Victim Scans the QR Code with a Specific Targeted Mobile App.
5. The service is exchanging all the victim's data with the attacker's session.

Industrial Spying

- **Industrial Spying**, also known as **Industrial Espionage**, is the illegal practice of obtaining confidential information, trade secrets, or proprietary data from businesses or organizations, typically for competitive advantage.

- **Corporate Espionage (Apple vs. Samsung)**: In the early 2010s, there were numerous legal battles between Apple and Samsung. Apple accused Samsung of using stolen design information from their iPhone to create their own smartphones.

- This was a classic example of industrial espionage, where trade secrets (such as product designs) were allegedly stolen and used to gain a competitive edge.

Hacking

- Individuals skilled in computer programming and system manipulation, who access computer systems or networks to understand, test, or exploit them.
- The person who is able to discover weakness in a system and managed to exploit it to accomplish his goal referred as a Hacker, and the process is referred as Hacking.
- Some hackers crossed over to the dark side, and these villains were more properly known as "crackers."
- A hacker is an unauthorized user who attempts to or gains access to an information system.

Purpose of Hacking

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset

Categories

White-Hat Hackers:

- Ethical hackers who test security systems to find and fix vulnerabilities.
- Operate with permission and within legal boundaries.
- Example: Penetration testers.

Black-Hat Hackers:

- Malicious hackers who exploit systems for personal or financial gain, revenge, or disruption.
- Operate illegally and harm systems or steal data.
- Example: Ransomware attackers.

Grey-Hat Hackers:

- Operate between white-hat and black-hat, often without authorization but not with malicious intent.
- May report vulnerabilities but also break the rules.
- Example: Exploring system flaws without explicit permission.

Hackers, Crackers and Phrackers

Aspect	Hackers	Crackers	Phreakers
Focus	Computers, networks, and systems.	Security systems/ software.	Telephone systems.
Intent	Ethical (white-hat), neutral (grey-hat), or malicious (black-hat).	Almost always malicious.	Initially exploratory or disruptive.
Timeframe	Ongoing and modern.	Ongoing and modern.	Mostly historical (pre-digital era).
Tools	Code, exploits, programming.	Password crackers, hacking tools.	Tone generators, telecom tools.

Online Frauds

Types of crimes under the category of hacking

- Spoofing website and E-Mail security alerts
- Hoax mails about virus threats
- lottery frauds
- Spoofing.

Spoofing websites and E-Mail security threats

- Fraudsters create authentic-looking websites that are actually nothing but a spoof.
- The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts.
- This kind of online fraud is common in banking and financial sector.
- It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate.

Types of crimes under the category of hacking

Virus hoax E-Mails

- The warnings may be genuine, so there is always a dilemma whether to take them lightly or seriously.
- A wise action is to first confirm by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, such as forwarding them to friends and colleagues.

Lottery frauds

- Typically letters or E-Mails that inform the recipient that he/she has won a prize in a lottery.
- To get the money, the recipient has to reply, after which another mail is received asking for bank details so that the money can be directly transferred.

Spoofing

- A hacker logs-in to a computer illegally, using a different identity than his own.
- He creates a new identity by fooling the computer into thinking that the hacker is the genuine system operator and then hacker then takes control of the system.

Software Piracy

- Software piracy refers to the illegal copying, distribution, or use of software without proper authorization or a valid license from its creator or owner.
- It is a form of intellectual property theft and violates copyright laws.
- Theft of software through illegally copying genuine programs or the counterfeiting and distributing products intended to pass for the original.

Forms of Software Piracy

- **Softlifting:**

✓ Installing a single licensed copy of the software on multiple computers.
✓ Example: Using one license key to activate the software on several personal or office computers.

- **Counterfeiting:**

✓ Creating and distributing fake copies of software, often disguised as genuine products.
✓ Example: Selling pirated copies of software with fake packaging and manuals.

- **Internet Piracy:**

✓ Downloading or sharing software illegally over the internet (e.g., through torrents or illegal websites).
✓ Example: Downloading a cracked version of a paid application for free.

Forms of Software Piracy

- **Hard Disk Loading:**

✓ Installing unauthorized copies of software onto computers being sold to customers.
✓ Example: A computer retailer pre-installing unlicensed software to attract buyers.

- **Cracks and Keygens:**

✓ Using illegal tools (cracks, key generators) to bypass software license protections.
✓ Example: Using a keygen to generate a fake serial key for paid software.

- **OEM Piracy:**

✓ Distributing OEM (Original Equipment Manufacturer) software separately from the hardware it was meant to accompany.
✓ Example: Selling software bundled with hardware as standalone products.

Disadvantages

(a)getting untested software that may have been copied thousands of times over the software, if pirated, may potentially contain hard-drive-infecting viruses

(b)there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users

(c)there is no warranty protection

(d)there is no legal right to use the product, etc.

Computer Network Intrusions

- **Computer Network Intrusions** are unauthorized activities or breaches into a computer network by individuals or entities aiming to access, manipulate, disrupt, or steal data.

- These intrusions pose a significant threat to organizations, governments, and individuals, often leading to data breaches, financial loss, or damage to infrastructure.

Types of Network Intrusions

1. Passive Intrusions

- Involve unauthorized monitoring of network traffic without causing active disruption.
- Examples: Eavesdropping, sniffing sensitive information, traffic analysis.

2. Active Intrusions

- Involve attackers actively disrupting network operations or gaining access to modify data.
- Examples: Data injection, network spoofing, session hijacking.

3. External Intrusions

- Conducted by attackers outside the organization's network, such as hackers or cybercriminal groups.
- Examples: Exploiting unpatched vulnerabilities, phishing attacks.

4. Internal Intrusions

- Conducted by individuals with legitimate access to the network, such as employees or contractors.
- Examples: Insider threats, privilege abuse.

Methods of Intrusion

Social Engineering

- Deceiving users to gain sensitive information or access (e.g., phishing or pretexting).

Exploitation of Vulnerabilities

- Leveraging outdated software, weak passwords, or unpatched systems to gain unauthorized access.

Malware Deployment

- Installing malicious software like Trojans, ransomware, or spyware to compromise the network.

Brute Force Attacks

- Repeated attempts to crack passwords or encryption through automated tools.

Man-in-the-Middle (MitM) Attacks

- Intercepting and manipulating communication between two parties in the network.

Vulnerabilities in the networks

- An attacker would look to exploit the vulnerabilities in the networks such as:
  - **I**nadequate border protection (border as in the sense of network periphery);
  - **R**emote Access Servers (RASs) with weak access controls;
  - **A**pplication servers with well-known exploits;
  - **M**isconfigured systems and systems with default configurations.

Signs of a Network Intrusion

Unusual Traffic:

- Unexpected spikes in network activity or large outbound data transfers.

Unauthorized Access:

- Unknown devices connecting to the network or failed login attempts.

Performance Issues:

- Slower network performance due to potential resource hijacking.

Altered Data:

- Unexplained changes in files or settings.

Presence of Unknown Tools:

- Discovery of unfamiliar programs or scripts running on systems.

How Criminals Plan the Attacks?

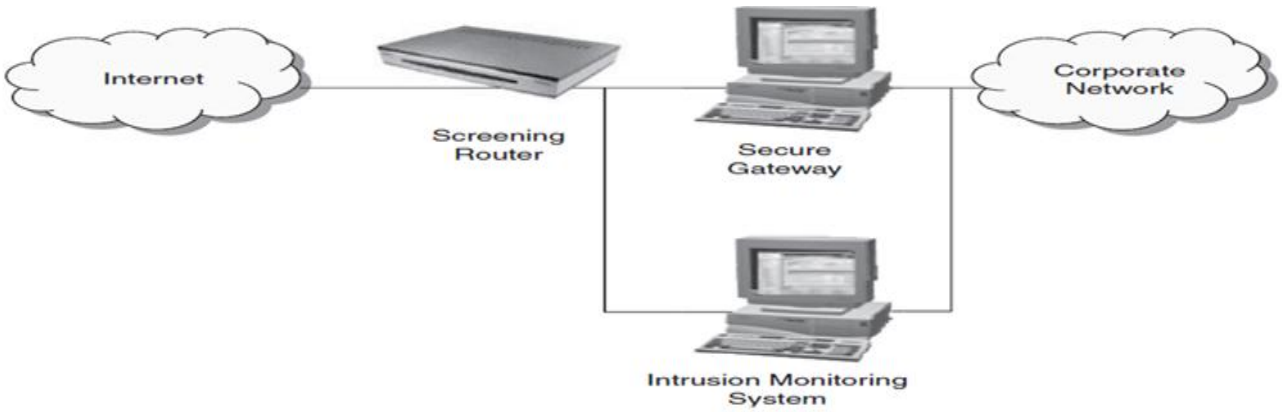
1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.

2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.

3. Launching an attack (gaining and maintaining the system access).

Intrusion Detection System (IDS)

- Monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.



Intrusion Detection System (IDS)

- An IDS essentially reviews the network traffic and data and identify probes, attacks, exploits and other vulnerabilities.

- It is considered to be a passive-monitoring system, since the main function of an IDS product is to warn of suspicious activity taking place – not prevent them and an IDS is not a replacement for either a firewall or a good antivirus program.

- A Host-based IDS (HIDS) is installed on the host it is intended to monitor. The host can be a server, workstation, or any networked device (such as a printer, router, or gateway).

- A Network-based IDS (NIDS) is designed to protect more than one host. It can protect a group of computer hosts, like a server farm, or monitor an entire network.

- Captured traffic is compared against protocol specifications and normal traffic trends or the packet's payload data is examined for malicious content.

- If a security threat is noted, the event is logged and an alert is generated.

- Going far beyond mere monitoring and alerting, second-generation IDSs are being called *intrusion-prevention systems* (IPSs).
- Mandatory inspection point with the ability to filter real-time traffic, it is considered *inline*.
- Inline IPSs can drop packets, reset Connections, and route suspicious traffic to quarantined areas for inspection

Passive IDS

- Functionality: **Monitors network traffic and logs detected suspicious activities or possible intrusions.**
- Response: Does not take any action to prevent the intrusion. Instead, it **alerts the administrator or logs the event for later analysis.**
- Example: A system that detects unusual traffic patterns and sends an alert to a network administrator without interrupting the traffic flow.
- Use Cases: **Situations where real-time intervention is not necessary,** or where the network administrators prefer to analyze threats manually before taking any action.

Active IDS (also known as Intrusion Prevention System - IPS)

- Functionality: Monitors network traffic like a passive IDS but also **takes immediate action** when a potential threat is detected.
- Response: Can **block or reject suspicious network traffic**, reset connections, or reconfigure firewalls to prevent an attack.
- Example: A system that not only detects a potential malware download but also automatically blocks the download and quarantines the affected files.
- Use Cases: Environments where immediate threat mitigation is critical, such as **financial institutions, government networks, or other high-security environments.**

Password Sniffing

- Password Sniffers are programs that monitor and record network users' names and passwords as they log in, threatening site security.

- Whoever installs the Sniffer can then impersonate an authorized user and log in to access restricted documents.

- Malicious actors often use these tools to steal sensitive information.

Password Sniffing

How It Works:

- **Password sniffers monitor network traffic to capture data packets.**
- **They search for patterns that resemble login credentials, such as HTTP POST requests or unencrypted data**.

Vulnerabilities:

- Unencrypted Connections: Sniffers can capture data from protocols like HTTP, FTP, or Telnet.
- Weak Network Security: Open Wi-Fi networks are particularly vulnerable.

Prevention:

- Encryption: Use HTTPS, SSH, or VPNs to ensure data is encrypted.
- Network Security: Use secure networks and avoid public Wi-Fi for sensitive activities.
- Two-Factor Authentication (2FA): Adds a layer of protection even if a password is intercepted.

Existing Implementations

- SniffPass from NirSoft.
- Password Sniffer Spy.
- FTP password sniffer.
- Sniffing Out Passwords and Cookies.
- Ace Password Sniffer.
- Password Sniffing with Metasploit

Cyber Stalking

- Cyber stalking refers to the use of digital platforms, the internet, or electronic devices to harass, intimidate, or monitor someone persistently.

Online Stalkers

- Unlike physical stalking, it involves virtual spaces but can have real-world consequences, causing emotional, psychological, or even physical harm to the victim.

Offline Stalkers

Forms of Cyber Stalking

Social Media Stalking:

- Monitoring and interacting with the victim's posts to intimidate or manipulate.

Email and Messaging:

- Sending excessive, abusive, or threatening emails or messages.

Tracking Devices and Apps:

- Using GPS tracking or spyware to monitor the victim’s movements or communications.

Online Impersonation:

- Misusing the victim’s identity to post harmful content or send malicious messages.

Doxxing:

- Publicly exposing personal information like address, phone number, or workplace to provoke harassment.

How Stalking Works?

- Personal information gathering about the victim
- Establish contact with the victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
- Stalkers will almost always establish contact with the victims through E-Mail. The stalker may use multiple names while contacting the victim.
- Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threatening the victim.
- The stalker may post the victim's personal information on any website related to illicit services
- The stalker will use bad and/or offensive/attractive language to invite the interested persons.
- Whosoever comes across the information, start calling the victim on the given contact details asking for services or relationships.
- Some stalkers subscribe/register the E-Mail account of the victim, because of which the victim will start receiving such kinds of unsolicited E-Mails.

Social Engineering

Social Engineering

- It is the “technique to influence” and “persuasion to deceive” people to obtain information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- The sign of truly successful social engineers is that they receive information without any suspicion.

Classification of Social Engineering

1. Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information.

2. Computer-Based Social Engineering

- Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

Common Types of Social Engineering Attacks

Phishing:

- Fraudulent emails, messages, or websites that appear legitimate.
- Designed to trick individuals into revealing sensitive information like passwords or credit card details.

Pretexting:

- An attacker creates a fabricated scenario to steal personal information.
- Examples include pretending to be a bank representative or a government official.

Baiting:

- Offering something enticing (like free software or a USB drive) to trick individuals into installing malware or providing access.

Quid Pro Quo:

- Offering a service or benefit in exchange for information.
- Example: A fake IT support call offering to fix a system issue.

Common Types of Social Engineering Attacks

Vishing (Voice Phishing):

- Phone calls that impersonate trusted entities to extract information.
- Example: Fake customer service calls asking for bank details.

Dumpster Diving:

- Searching through discarded materials to find sensitive information like documents or hardware.

Tailgating/Piggybacking:

- Gaining physical access to a restricted area by following someone who is authorized.

Cybercafe and Cybercrimes

- Cybercrimes such as the stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.

- Cybercafes have also been used regularly for sending obscene emails to harass people.

- Indian Information Technology Act (ITA) 2000 interprets cybercafes as “network service providers” referred to under the erstwhile Section 79, which imposed on them responsibility for “due diligence” failing which they would be liable for the offenses committed in their network.

Cybercafe and Cybercrimes

- **Cybercriminals can install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.**

- Here are a **few tips for safety and security** while using the computer in a cybercafe:
  1. **Always logout**
  2. Stay with the computer
  3. **Clear history and temporary files**
  4. Be alert
  5. **Avoid online financial transactions**
  6. **Change passwords**
  7. **Virtual keyboard**
  8. Security warnings

- Deep Freeze is installed and activated, any changes made to the computer, such as installing software, deleting files, or altering settings, are automatically discarded upon reboot, restoring the system to its original, "frozen" state. – Challenges for crime investigation.

Tips for Safe Banking

Figure 1 Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).

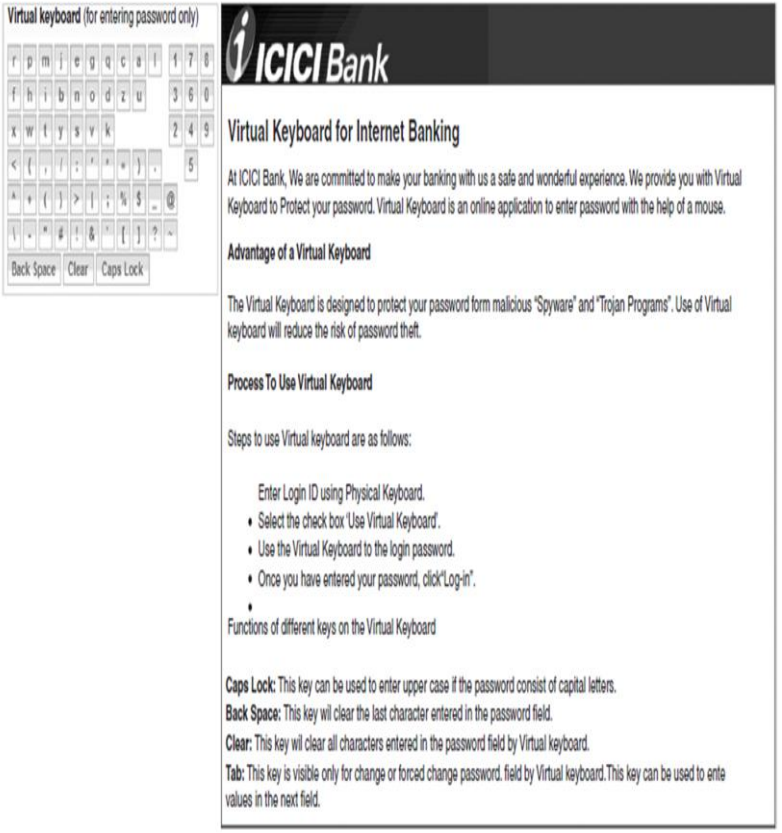


Figure 2 Virtual keyboard.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Botnets: The Fuel for Cybercrime

- A Botnet (also called a zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.

- Your computer system may be a part of a Botnet even though it appears to be operating normally.

- Botnets are often used to conduct various activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

How Botnets Work ?

- Infection: Malware, often spread through phishing emails, malicious websites, or software vulnerabilities, is used to compromise devices and connect them to the botnet.

- Command and Control (C&C): Once infected, the devices communicate with the botmaster through a centralized server or a peer-to-peer (P2P) network.

- Execution: The botmaster issues commands to the botnet for specific tasks, often for financial or political gain

Botnets

- **Distributed Denial of Service (DDoS) Attacks**: Overwhelm a target server or network with traffic, causing it to crash.
- **Spam Distribution**: Send massive amounts of spam emails, often for phishing or advertising scams.
- **Data Theft**: Steal sensitive information like login credentials, credit card numbers, or personal data.
- **Cryptojacking**: Use infected devices to mine cryptocurrencies without the owner's consent.
- **Click Fraud**: Generate fake clicks on online ads to earn revenue.
- **Malware Delivery**: Distribute additional malicious software, such as ransomware.

Mirai **Zeus**

How to Protect Against Botnets?

- Use antivirus and anti-spyware software and keep it up-to-date.
- Set the OS to download and install security patches automatically.
- Use a firewall to protect the system from hacking attacks while it is connected to the Internet.
- Disconnect from the Internet when you are away from your computer.
- Downloading the freeware only from websites that are known and trustworthy
- Check regularly the folders in the mailbox – “sent items” or “outgoing” – for those messages you did not send.
- Take immediate action if your system is infected.

Attack Vector

- An “attack vector” is a **path** or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.

- An attack vector, or threat vector, is a way for attackers to enter a network or system.

- **An attack vector is a method or path that a cybercriminal uses to gain unauthorized access to a network, system, or application.**

- Attack vectors can be **technical or human-based**, and can exploit vulnerabilities in a system's security

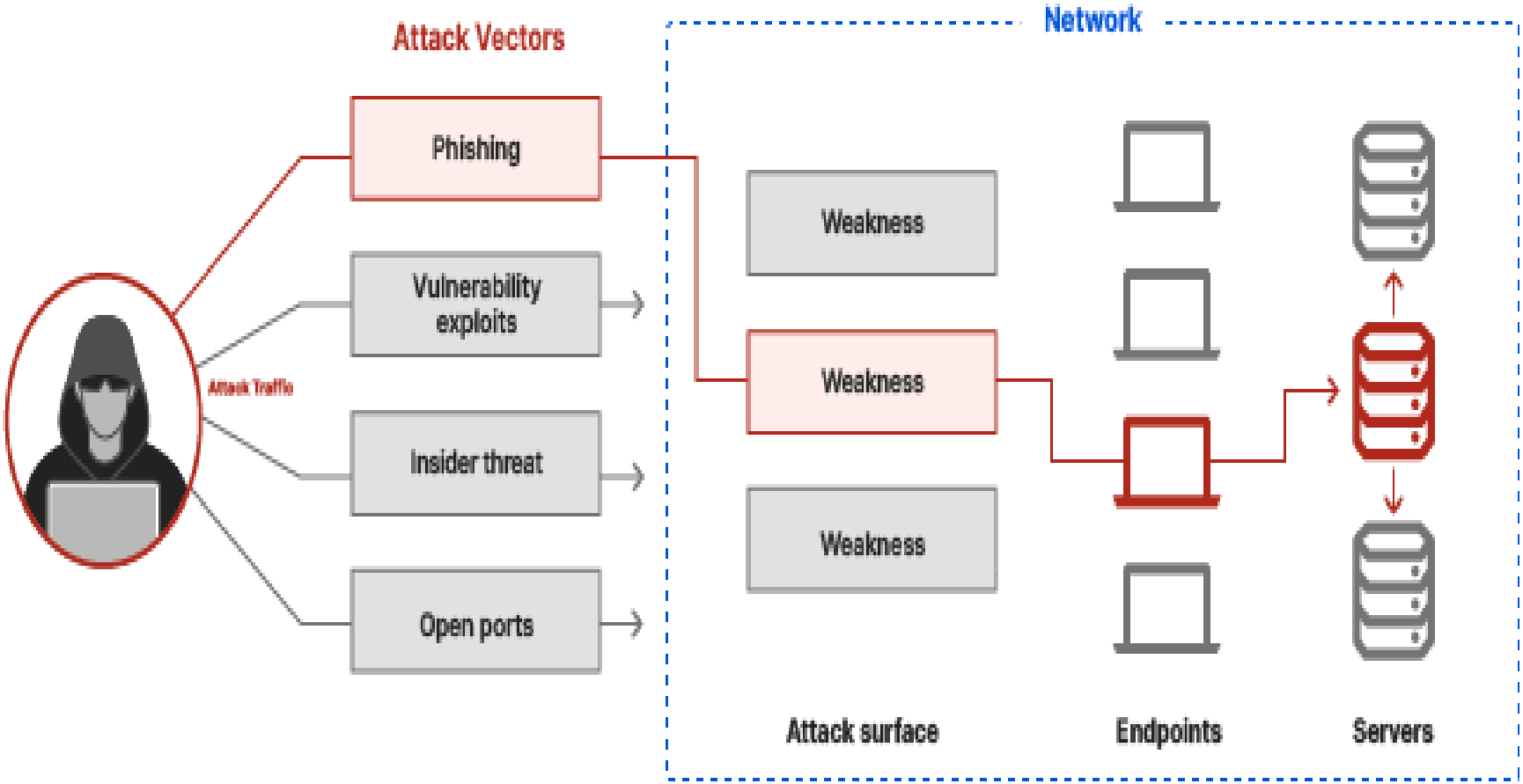
Attack vectors

- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- The most common malicious payloads are viruses, Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
  - ✓ Payload means the malicious activity that the attack performs.
  - ✓ It is the bits that get delivered to the end-user at the destination.

- The attack vectors described here are how most of them are launched:

1. **Attack by E-Mail**
2. **Attachments (and other files)**
3. **Attack by deception**
4. **Hackers**
5. **Heedless guests (attack by webpage)**
6. **Attack of the worms**
7. **Malicious macros**
8. **Foistware (sneakware)**
9. **Viruses**

Attack Vector



Attack Surface

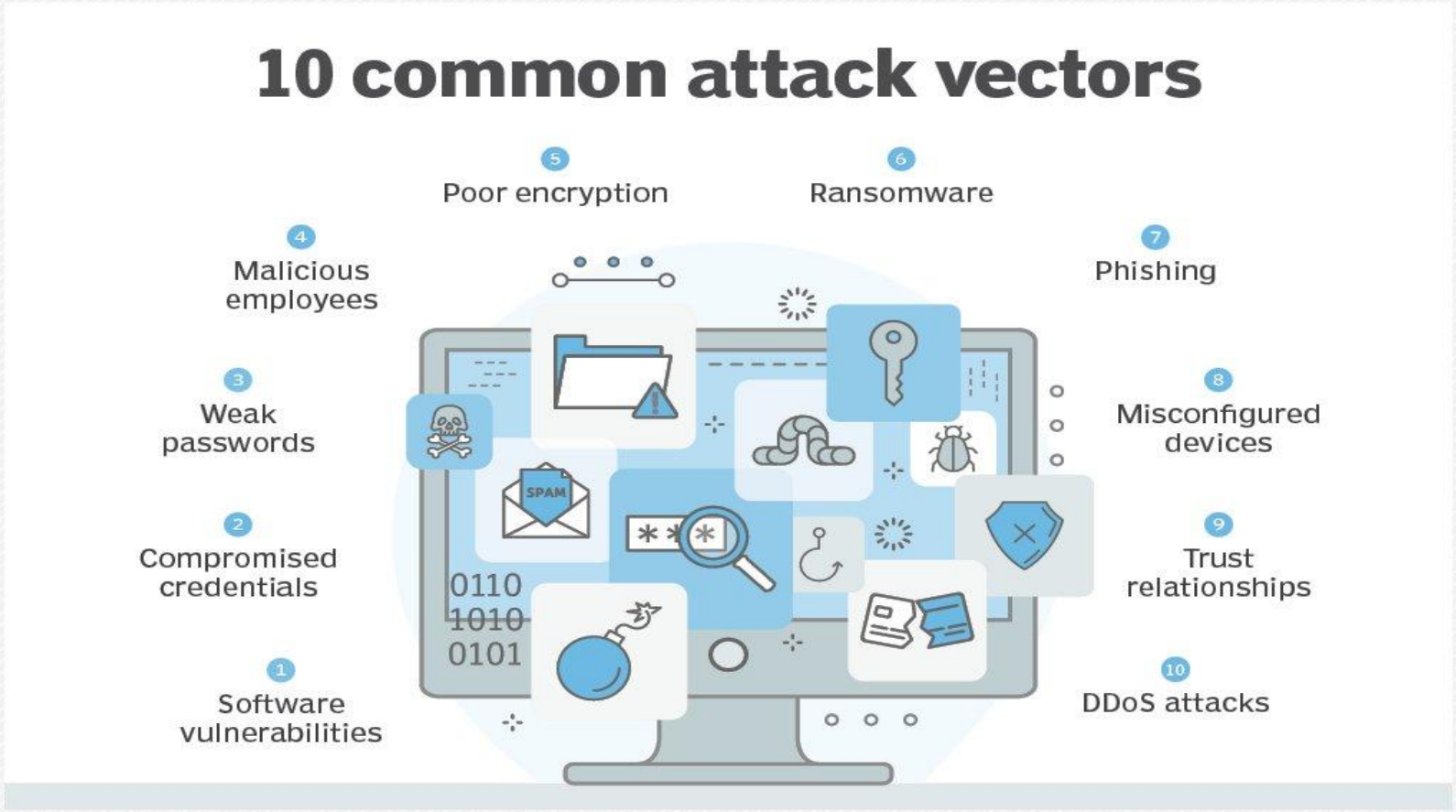
- An attack surface refers to the total set of points, paths, or "entry doors" where an attacker can try to gain unauthorized access to a system, network, or application

- It represents the vulnerabilities and entry points in a software application, system, or network that could potentially be exploited by attackers

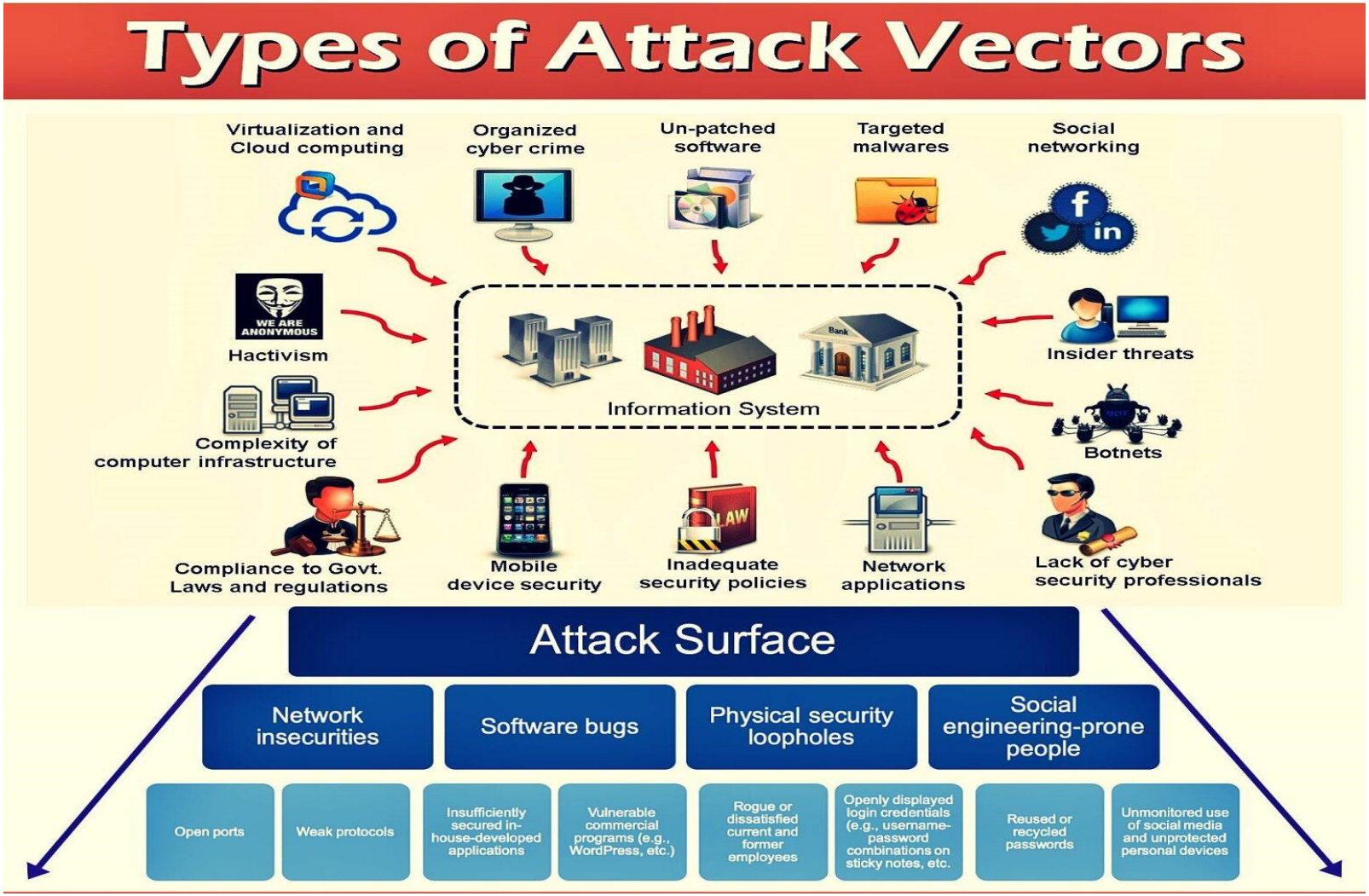
Attack Surface vs. Attack Vector

- Attack Surface: The total number of potential entry points for an attacker.
- Attack Vector: The specific method or path an attacker uses to exploit an entry point.

Common Attack Vectors



Attack Vector



Network-Based Attack Vectors

- Man-in-the-Middle (MitM) Attacks: Intercepting and manipulating data between two parties.
- Denial of Service (DoS)/Distributed Denial of Service (DDoS): Overloading a network or server with excessive traffic to disrupt services.
- IP Spoofing: Pretending to be a trusted IP address to gain unauthorized access.
- DNS Poisoning: Redirecting traffic from legitimate websites to malicious sites.

Social Engineering Attack Vectors

- Phishing: Fraudulent emails or messages to steal sensitive information.
- Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
- Baiting: Using physical media, like infected USB drives, to spread malware.
- Pretexting: Fabricating a story to extract confidential information.
- Vishing and Smishing: Using voice calls or SMS to deceive users.

Software and Application-Based Attack Vectors

- SQL Injection (SQLi): Inserting malicious SQL code into input fields to manipulate databases.
- Cross-Site Scripting (XSS): Injecting malicious scripts into trusted websites.
- Cross-Site Request Forgery (CSRF): Forcing a user to perform unwanted actions on a trusted website.
- Remote Code Execution (RCE): Running malicious code remotely on a vulnerable system.
- Buffer Overflow: Overloading a system's memory to execute arbitrary code.

Endpoint Attack Vectors

- Malware: Includes viruses, worms, ransomware, spyware, and Trojans.
- Cryptojacking: Using a victim's device for unauthorized cryptocurrency mining.
- Keyloggers: Recording keystrokes to steal sensitive information.
- Rootkits: Gaining deep, persistent access to a device’s operating system.

Credential-Based Attack Vectors

- Brute Force Attacks: Systematic guessing of passwords or encryption keys.
- Credential Stuffing: Using leaked credentials to access accounts with reused passwords.
- Password Spraying: Attempting common passwords on many accounts.

Cloud-Based Attack Vectors

- Misconfigured Cloud Settings: Leaving sensitive data exposed due to improper configurations.
- Insider Threats in the Cloud: Employees misusing access to cloud systems.
- Unauthorized API Access: Exploiting weakly secured APIs to gain access.
- Data Exfiltration: Extracting sensitive data stored in cloud services.

Insider Threats

- Malicious Insider: Employees intentionally leaking or sabotaging data.
- Negligent Insider: Mistakes or carelessness leading to security breaches.
- Third-Party Access: Exploiting vendors or contractors with legitimate access.

Physical Attack Vectors

- Hardware Theft: Stealing devices like laptops or hard drives containing sensitive information.
- Unauthorized Access: Gaining entry to secure facilities or data centers.
- Tampered Devices: Embedding malicious components in hardware.
- Eavesdropping Devices: Using hidden devices to record conversations or keystrokes.

Internet of Things (IoT) Attack Vectors

- Device Hijacking: Taking control of IoT devices for malicious purposes.
- Botnets: Using infected IoT devices for large-scale attacks, like DDoS.
- Default Credentials: Exploiting devices with unchanged factory-set passwords.

Zero-Day Attack Vectors

- Exploiting vulnerabilities before they are publicly disclosed or patched.

- Example: Attacking a newly discovered flaw in a web browser before updates are available.

Supply Chain Attack Vectors

- Targeting third-party suppliers or software dependencies.
- Software Supply Chain Attacks: Embedding malware in software updates or packages.
- Hardware Supply Chain Attacks: Compromising hardware during manufacturing.

Wireless Attack Vectors

- Wi-Fi Eavesdropping: Intercepting data on unsecured Wi-Fi networks.
- Rogue Access Points: Setting up fake Wi-Fi networks to steal data.
- Bluetooth Attacks: Exploiting insecure Bluetooth connections.

Mobile Attack Vectors

- Malicious Apps: Apps that steal data or perform unauthorized actions.
- SIM Swapping: Hijacking phone numbers to intercept messages or calls.
- Mobile Phishing: Deceptive links or messages targeting mobile users.

Physical Media Attack Vectors

- Infected USB Drives: Plugging malicious USBs into systems.
- BadUSB Attacks: Reprogramming USB devices to act maliciously.

Summary

- CIA Triad
- Cyber Crimes
- Cyber Offenses
- Virus Total, Zenmap, Wireshark,Hashcalc

References

- Nina Godbole, Sunit Belapure, “Cyber Security - Understanding Cybercrimes, Computer Forensics and Legal Perspectives”, 2018, 1st Edition, Wiley.
- https://www.virustotal.com/
- https://nmap.org/zenmap/
- https://www.wireshark.org/
- https://apps.microsoft.com/detail/9nnq6kkmqxxf?hl=en-US&gl=US