Cyber
Security
Club

INTRODUCTION SESSION

CYCBER SECURITY THREATS AND NETWORKING

PREREQUISITES

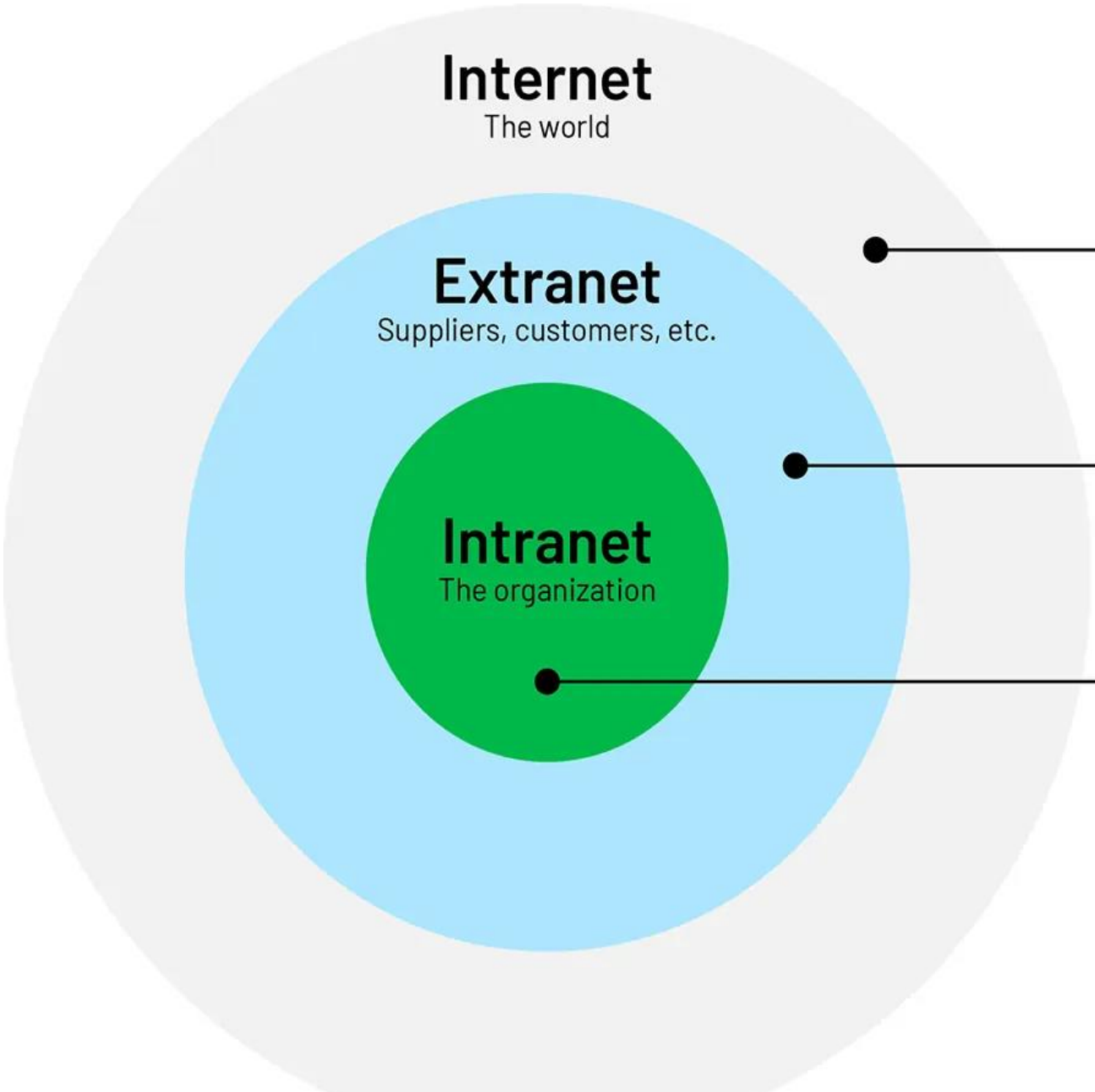
•**Network** - A network comprises two or more devices connected via a communication link.

•**Link** - A link is a medium that can be wired or wireless that connects the devices in a network for communication. Examples of a wired medium can be cables/wires, while microwaves or radio-waves are some examples of wireless medium.

•**Nodes/Devices** - Any device capable of receiving and sending data in a network is referred to as nodes/devices in the network.
Examples - laptops, computers, smartphones, etc.

NETWORK VS INTERNET

A network is a collection of two or multiple connected computer systems that may share resources, such as an internet connection, an app, a printer, etc. In contrast, the internet is a network of interconnected devices that are spread around the globe.



The **internet** creates connections between computers around the world.

An **extranet** creates connections beyond (or outside) an organization.

An **intranet** creates connections inside an organization.

What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com.

Web browsers interact through Internet Protocol(IP) addresses.

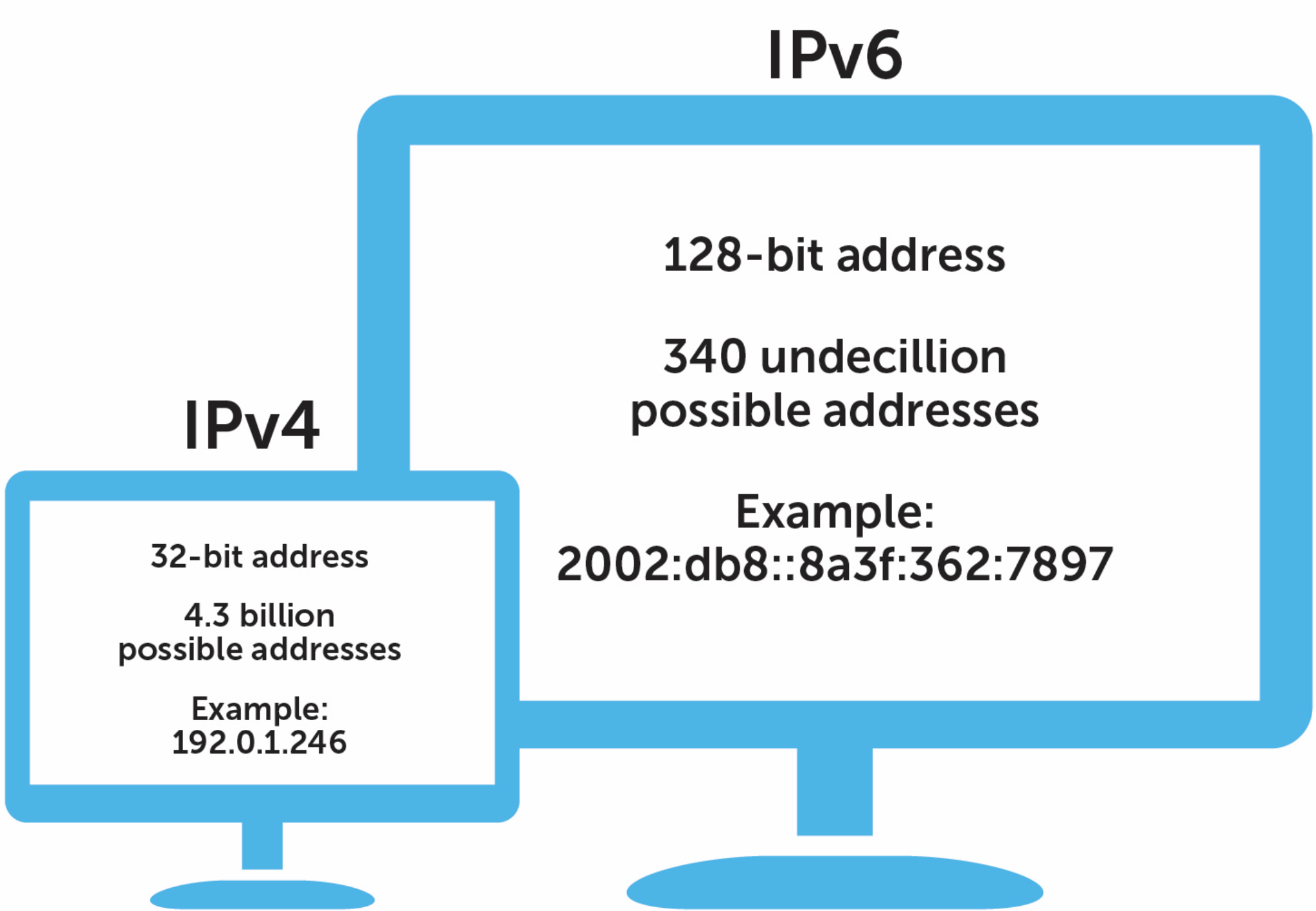
DNS translates domain names to IP Addresses so browsers can load Internet resources.

Addressing Schemes

IPv4

IPv6

MAC address


IPv6
128-bit address
340 undecillion
possible addresses
Example:
2002:db8::8a3f:362:7897
IPv4
32-bit address
4.3 billion
possible addresses
Example:
192.0.1.246

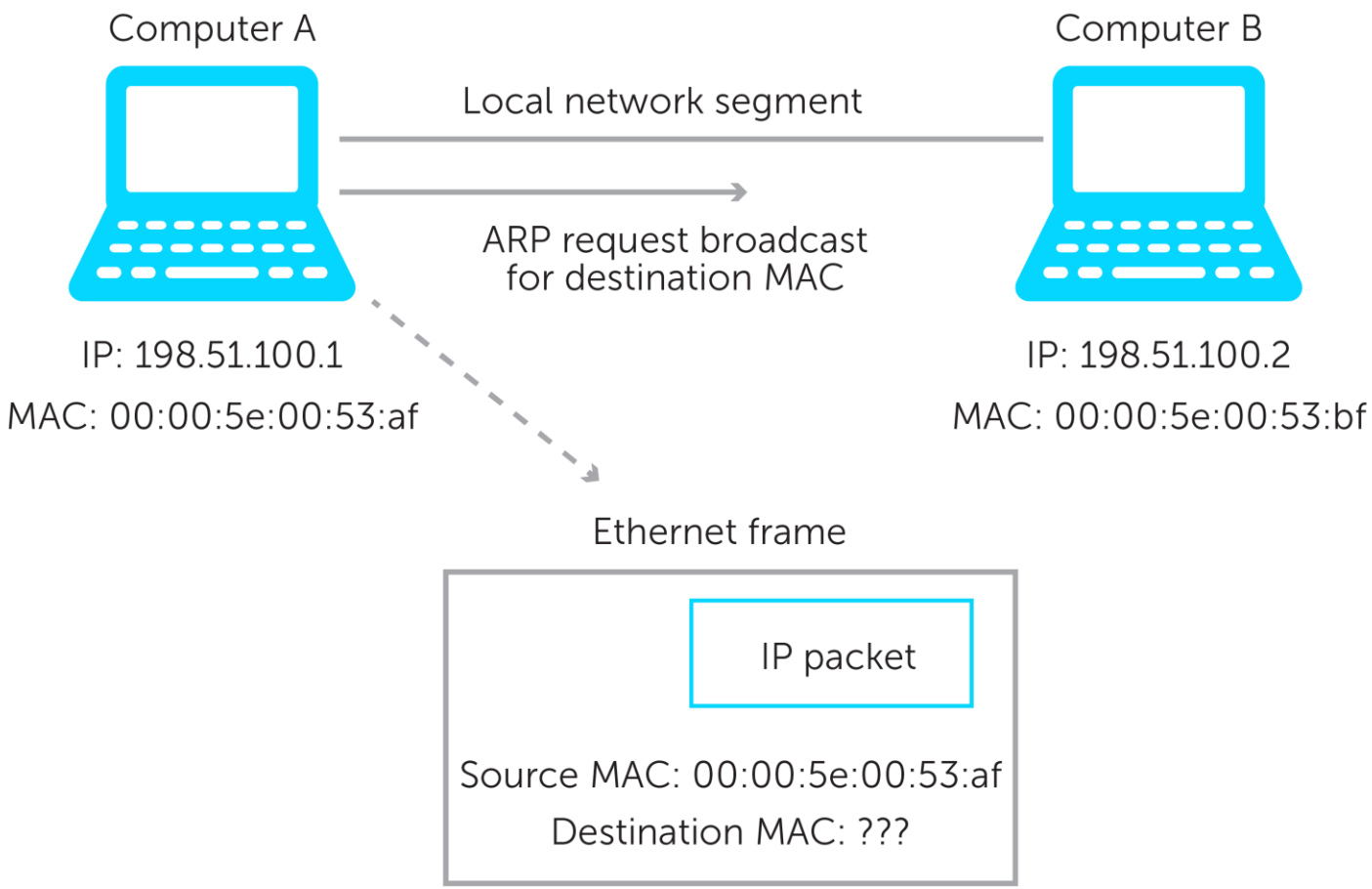
IPv4 vs. IPv6

IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	7.9×10^{28} addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

MAC ADDRESS

A media access control address is a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth.

MAC address vs IP address: How ARP works between them



Network Protection Best Practices

Segregate Your Network
A basic part of avoiding network security threats is dividing a network into zones based on security requirements. This can be done using subnets within the same network, or by creating Virtual Local Area Networks (VLANs), each of which behaves like a complete separate network. Segmentation limits the potential impact of an attack to one zone, and requires attackers to take special measures to penetrate and gain access to other network zones.

Regulate Access to the Internet via Proxy Server
Do not allow network users to access the Internet unchecked. Pass all requests through a transparent proxy, and use it to control and monitor user behavior. Ensure that outbound connections are actually performed by a human and not a bot or other automated mechanism. Whitelist domains to ensure corporate users can only access websites you have explicitly approved.

Network Protection Best Practices

Monitor Network Traffic

Ensure you have complete visibility of incoming, outgoing and internal network traffic, with the ability to automatically detect threats, and understand their context and impact. Combine data from different security tools to get a clear picture of what is happening on the network, recognizing that many attacks span multiple IT systems, user accounts and threat vectors.

Use Deception Technology

No network protection measures are 100% successful, and attackers will eventually succeed in penetrating your network. Recognize this and place deception technology in place, which creates decoys across your network, tempting attackers to “attack” them, and letting you observe their plans and techniques. You can use decoys to detect threats in all stages of the attack lifecycle: data files, credentials and network connections.

Network Protection Best Practices

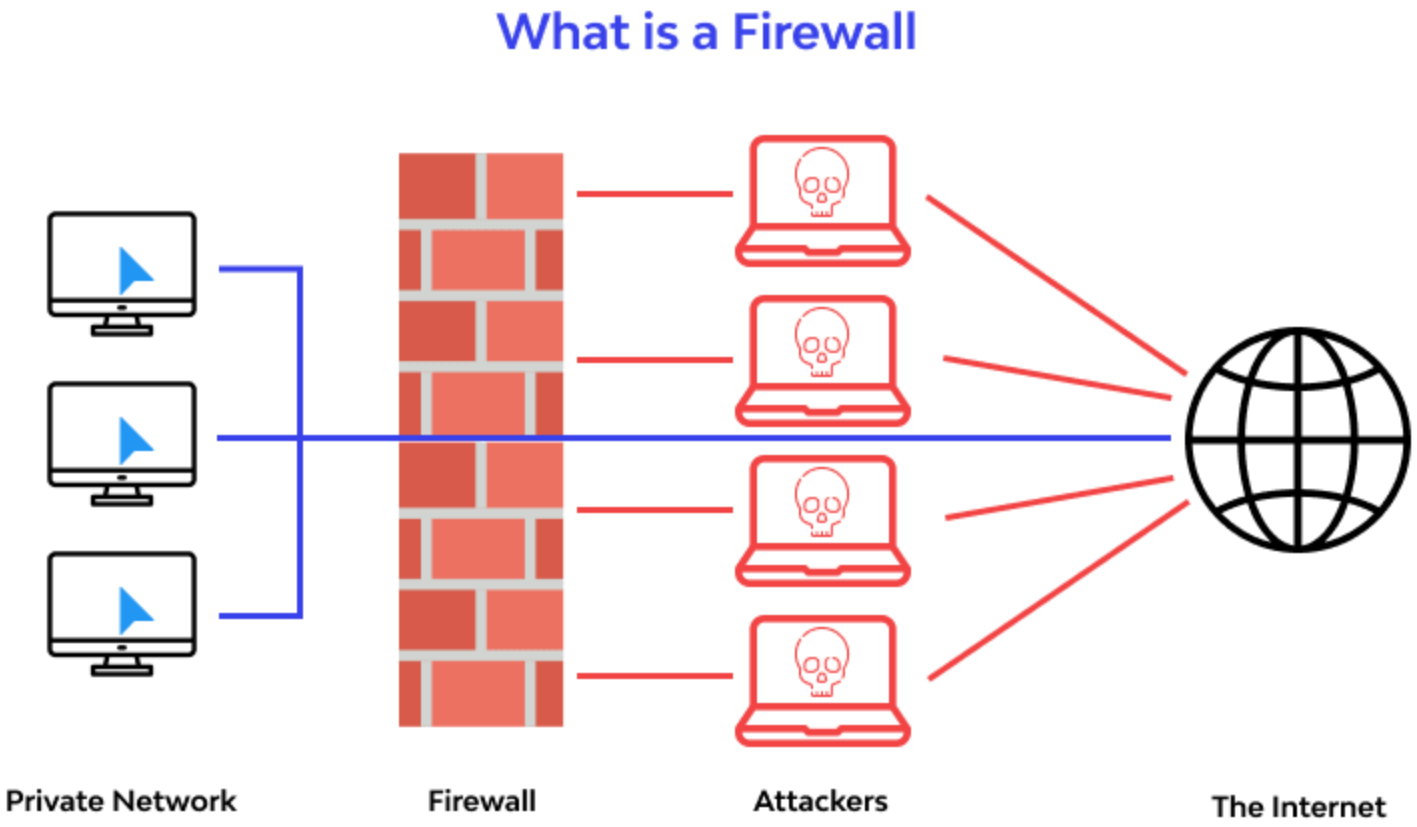
Place Security Devices Correctly

Place a firewall at every junction of network zones, not just at the network edge. If you can't deploy full-fledged firewalls everywhere, use the built-in firewall functionality of your switches and routers. Deploy anti-DDoS devices or cloud services at the network edge. Carefully consider where to place strategic devices like load balancers – if they are outside the Demilitarized Zone (DMZ), they won't be protected by your network security apparatus.

Use Network Address Translation

Network Address Translation (NAT) lets you translate internal IP addresses into addresses accessible on public networks. You can use it to connect multiple computers to the Internet using a single IP address. This provides an extra layer of security, because any inbound or outgoing traffic has to go through a NAT device, and there are fewer IP addresses which makes it difficult for attackers to understand which host they are connecting to.

WHAT IS FIREWALL ?



A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protections and entrusts them to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down.

Types of Firewalls

- **Packet filtering**
A small amount of data is analyzed and distributed according to the filter’s standards.

- **Proxy service**
Network security system that protects while filtering messages at the application layer.

- **Stateful inspection**
Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

- **Next Generation Firewall (NGFW)**
Deep packet inspection Firewall with application-level inspection.

What is the OSI Model

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

No.	Layer Name	Responsibility	Information Form (Data Unit)	Device
7	**Application Layer**	Helps in identifying the client and synchronize communication	Message	-
6	**Presentation Layer (Translation Layer)**	Data from application layer is extracted and manipulated as required format for transmission	Message	-
5	**Session Layer**	Establishes connection, maintenance, authentication and ensure security	Message	Gateway
4	**Transport Layer (HEART of OSI)**	Take service from network layer and provide it to application layer	Segment	Firewall
3	**Network Layer**	Transmission of data from one host to other. Located in different network	Packet	Router
2	**Data Link Layer**	Node to node delivery of messages	Frame	Switch, Bridge
1	**Physical Layer**	Establishing physical connection between devices	Bits	Hub, Repeater, Modem, Cables

TCP/ IP PROTOCOL

TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet).

The entire IP suite -- a set of rules and procedures -- is commonly referred to as TCP/IP. TCP and IP are the two main protocols, though others are included in the suite. The TCP/IP protocol suite functions as an abstraction layer between internet applications and the routing and switching fabric.

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management and is designed to make networks reliable with the ability to recover automatically from the failure of any device on the network.

The two main protocols in the IP suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

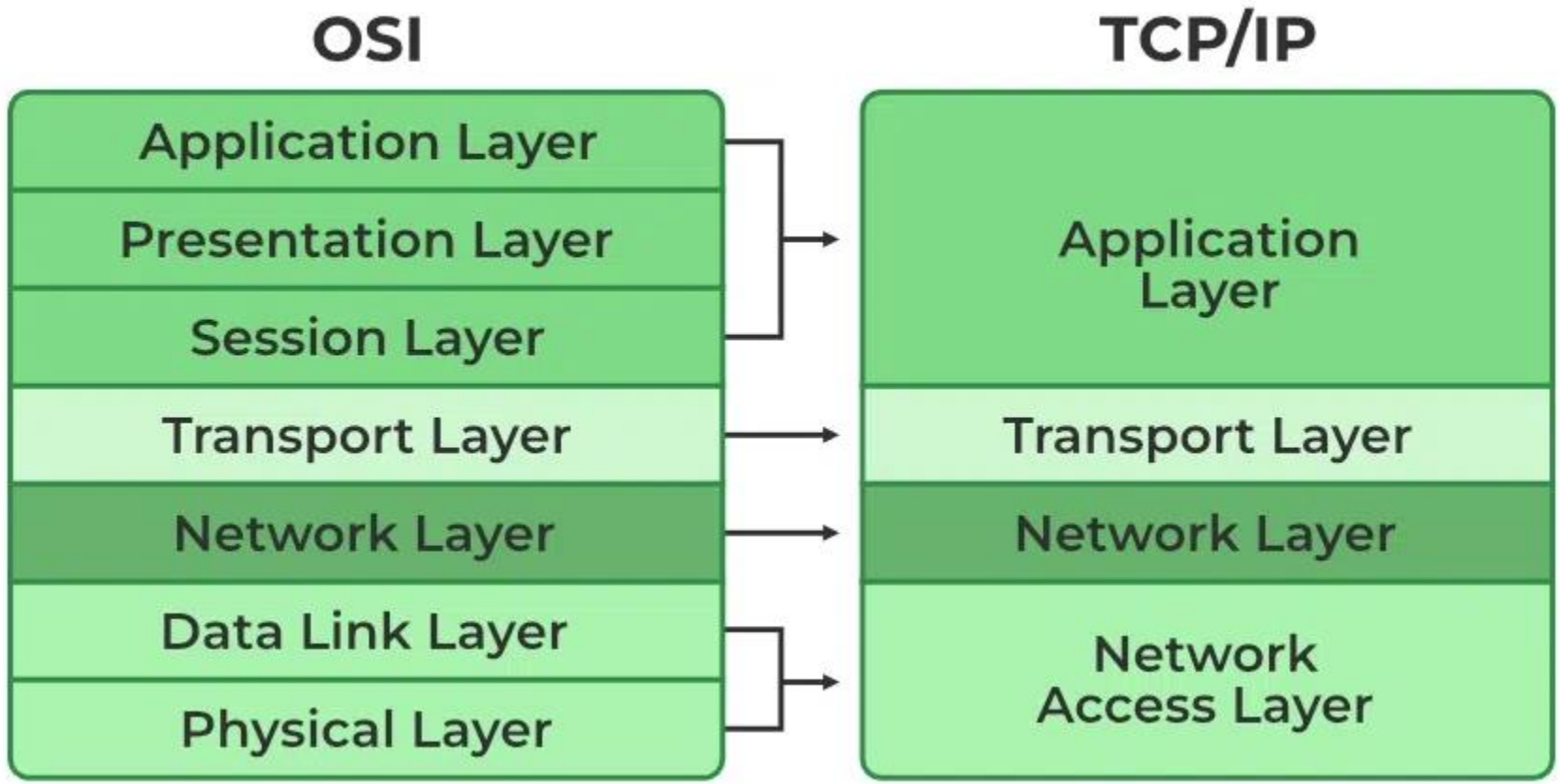
IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

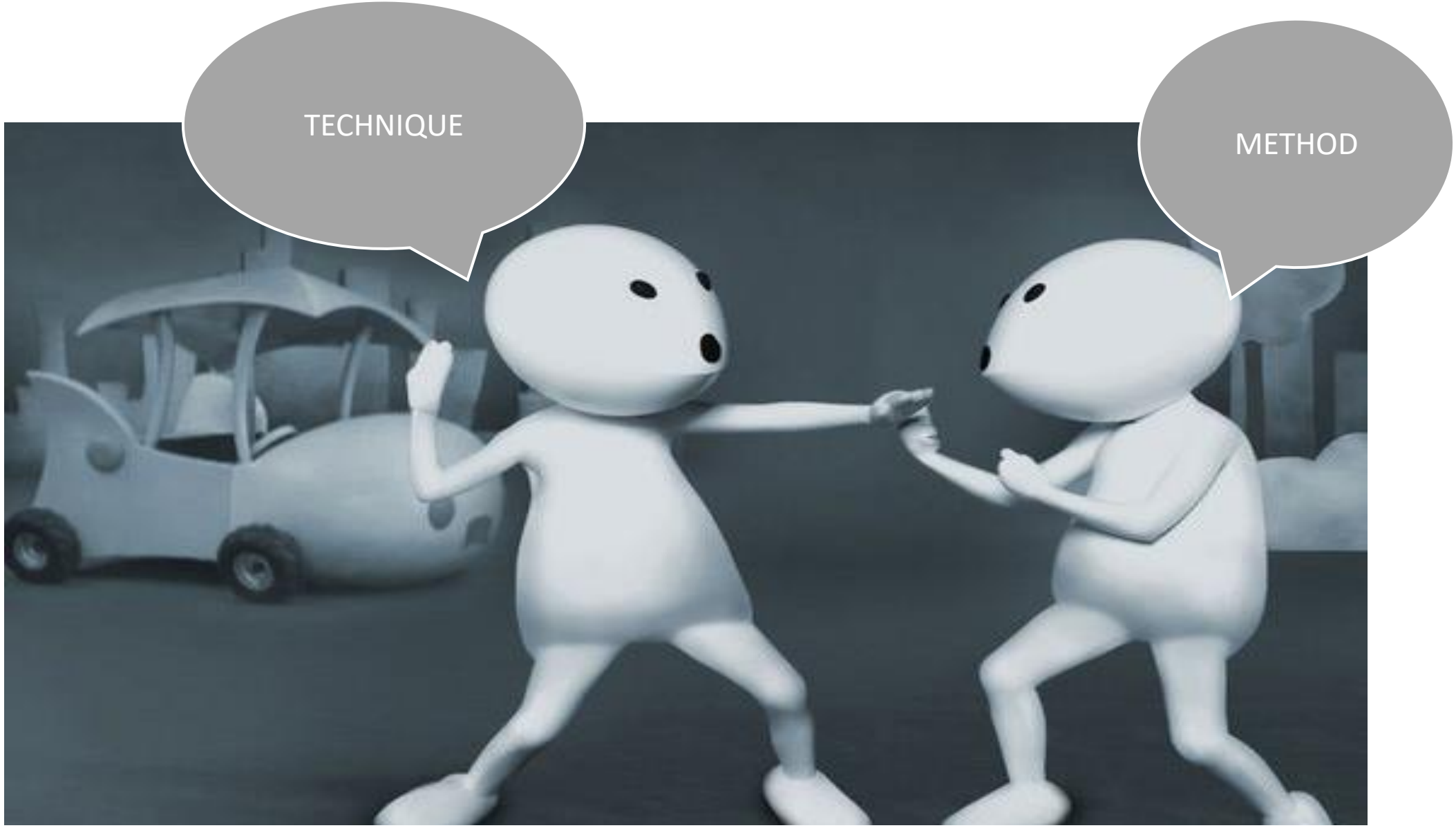
A subnet mask tells a computer, or other network device, what portion of the IP address is used to represent the network and what part is used to represent hosts, or other computers, on the network.

Network address translation (NAT) is the virtualization of IP addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

Common TCP/IP protocols include the following:

Hypertext Transfer Protocol (HTTP) handles the communication between a web server and a web browser.
HTTP Secure handles secure communication between a web server and a web browser.
File Transfer Protocol handles transmission of files between computers.


OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer



TECHNIQUE VS METHOD

Technique is a procedure or skill for completing a specific task.

Method is a way something is done.

IN TERMS OF CYBER ATTACKS?

METHODS

Malware
Phishing
SQL Injection
Cross-Site Scripting (XSS)
Denial of Services (DoS)
Session Hijacking
Man in the Middle Attacks
Credential Reuse

Malware Attack

This is one of the most common types of cyberattacks. “Malware” refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.
The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen. Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

Let’s now look at how we can prevent a malware attack:
•Use antivirus software. It can protect your computer against malware. Avast Antivirus, Norton Antivirus, and McAfee Antivirus are a few of the popular antivirus software.
•Use firewalls. Firewalls filter the traffic that may enter your device. Windows and Mac OS X have their default built-in firewalls, named Windows Firewall and Mac Firewall.
•Stay alert and avoid clicking on suspicious links.
•Update your OS and browsers, regularly.

Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.

Phishing attacks can be prevented by following the below-mentioned steps:
•Scrutinize the emails you receive. Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.
•Make use of an anti-phishing toolbar.
•Update your passwords regularly.

Password Breach Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Air crack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.

Listed below are a few ways to prevent password attacks:
•Use strong alphanumeric passwords with special characters.
•Abstain from using the same password for multiple websites or accounts.
•Update your passwords; this will limit your exposure to a password attack.
•Do not have any password hints in the open.

Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.

MITM attacks can be prevented by following the below-mentioned steps:

•Be mindful of the security of the website you are using. Use encryption on your devices.

•Refrain from using public Wi-Fi networks.

SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

To prevent a SQL injection attack:

•Use an Intrusion detection system, as they design it to detect unauthorized access to a network.

•Carry out a validation of the user-supplied data. With a validation process, it keeps the user input in check.

Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.
When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.
It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

Let’s now look at how to prevent a DDoS attack:
•Run a traffic analysis to identify malicious traffic.
•Understand the warning signs like network slowdown, intermittent website shutdowns, etc. At such times, the organization must take the necessary steps without delay.
•Formulate an incident response plan, have a checklist and make sure your team and data center can handle a DDoS attack.
•Outsource DDoS prevention to cloud-based service providers.

Insider Threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.
Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data.

Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

To prevent the insider threat attack:
•Organizations should have a good culture of security awareness.
•Companies must limit the IT resources staff can have access to depending on their job roles.
•Organizations must train employees to spot insider threats. This will help employees understand when a hacker has manipulated or is attempting to misuse the organization's data.

Crypto jacking

The term Crypto jacking is closely related to cryptocurrency. Crypto jacking takes place when attackers access someone else’s computer for mining cryptocurrency.
The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

Crypto jacking can be prevented by following the below-mentioned steps:
•Update your software and all the security apps as crypto jacking can infect the most unprotected systems.
•Have crypto jacking awareness training for the employees; this will help them detect crypotjacking threats.
•Install an ad blocker as ads are a primary source of crypto jacking scripts. Also have extensions like Miner Block, which is used to identify and block crypto mining scripts.

Zero-Day Exploit

A Zero-Day Exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers.

Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

Zero-day exploits can be prevented by:
•Organizations should have well-communicated patch management processes. Use management solutions to automate the procedures. Thus it avoids delays in deployment.
•Have an incident response plan to help you deal with a cyberattack. Keep a strategy focussing on zero-day attacks. By doing so, the damage can be reduced or completely avoided.

Watering Hole Attack

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

Let's now see how we can prevent the watering hole attack:
•Update your software and reduce the risk of an attacker exploiting vulnerabilities. Make sure to check for security patches regularly.
•Use your network security tools to spot watering hole attacks. Intrusion prevention systems(IPS) work well when it comes to detecting such suspicious activities.
•To prevent a watering hole attack, it is advised to conceal your online activities. For this, use a VPN and also make use of your browser’s private browsing feature. A VPN delivers a secure connection to another network over the Internet. It acts as a shield for your browsing activity. NordVPN is a good example of a VPN.

Spoofing
An attacker impersonates someone or something else to access sensitive information and do malicious activities. For example, they can spoof an email address or a network address.

Identity-Based Attacks
Perform to steal or manipulate others' personal information, like login someone's PINs to steal unauthorized access to their systems.

Code Injection Attacks
Performed by inserting malicious code into a software application to manipulate data. For example, the attacker puts malicious code into a SQL database to steal data.

Supply Chain Attacks
Exploit software or hardware supply chain vulnerabilities to collect sensitive information.

DNS Tunneling
Attacker uses the Domain Name System (DNS) to bypass security measures and communicate with a remote server.

DNS Spoofing
Cyberattack in which an attacker manipulates the DNS records from a website to control its traffic.

IoT-Based Attacks
Exploit vulnerabilities in the Internet of Things (IoT), like smart thermostats and security cameras, to steal data.

Ransomware
Encrypt the victim's data and demands payment in exchange.

Distributed Denial of Service (DDos) Attacks
Flood a website with traffic to make it unavailable to legitimate users and to exploit vulnerabilities in the specific network.

Spamming
Send unauthentic emails to spread phishing scams.

Corporate Account Takeover (CATO)
Hackers use stolen login credentials to access others' bank accounts.

Spear-Phishing Attacks:
Target specific individuals or groups under an organization. Attackers use social engineering techniques to get sensitive information.

URL Interpretation
A web browser interprets a URL (Uniform Resource Locator) and requests the corresponding web page to exploit vulnerabilities in the URL interpretation.

Session Hijacking
The hacker gets access to a user's session ID to authenticate the user's session with a web application and take control of the user's session.

Brute Force Attack
An attacker gets unauthorized access to a system by trying various passwords until the correct one is found. It can be highly effective against weak passwords.

Web Attacks
Targets websites and can insert SQL injection, cross-site scripting (XSS) and file inclusion.

Trojan Horses
Malware that appears to be a legitimate program but which contains malicious code. Once installed, it can perform malicious actions like stealing data and controlling the system.

Cross-Site Scripting (XSS) Attacks

An attacker inserts unauthorized code into a legitimate website to access the user's information to steal sensitive information like the user's passwords and credit card details.

Eavesdropping Attacks

An attacker intercepts communication between two parties to access sensitive information.

Birthday Attack

A cryptographic attack exploits the birthday paradox to access a collision in a hash function. The attacker successfully generates two inputs to get the same output hash value. This can be used to compromise to bypass access controls.

Volume-Based Attacks

The attacker floods a system with heavy data to make it inaccessible to legitimate users. For instance, DDoS attacks in which various compromised computers flood a specific website with traffic to crash it.

Protocol Attacks:

Exploits vulnerabilities in network protocols to gain unauthorized access to a system or disrupt its regular operation. Examples include the Transmission Control Protocol (TCP) SYN Flood attack and the Internet Control Message Protocol (ICMP) Flood attack.

Application Layer Attacks

Targets the application layer of a system, aiming to exploit vulnerabilities in applications or web servers.

Dictionary Attacks

An attacker attempts to guess a user's password by trying a list of common words. This attack becomes successful because many users use weak or easy passwords.

Virus

Malicious software can replicate itself and spread to other computers. Viruses can cause significant damage to systems, corrupt files, steal information, and more.

Worm

Replicates itself and spreads to other computers, but unlike viruses, worms don't require human interaction.

Backdoors

This vulnerability allows attackers to bypass standard authentication procedures and gain unauthorized access to a system or network.

Bots

These software programs automate network or internet tasks. They can be used for malicious purposes, such as Distributed Denial of Service (DDoS) attacks.

Business Email Compromise (BEC)

Targets businesses and organizations by using email. The attackers impersonate a trusted source to trick the victim into transferring funds or sensitive information to the attacker.

Cross-Site Scripting (XSS) Attacks

Targets web applications by injecting malicious code into a vulnerable website to steal sensitive information or to perform unauthorized attacks.

AI-Powered Attacks

Use artificial intelligence and machine learning to bypass traditional security measures.

Rootkits

Provide attackers privileged access to a victim's computer system. Rootkits can be used to hide other types of malware, such as spyware or keyloggers, and can be challenging to detect and remove.

Spyware

Is malware designed to collect sensitive information from a victim's computer system. This can include passwords, credit card numbers, and other sensitive data.

Social Engineering

is a technique cybercriminals use to manipulate users to make them divulge sensitive information or perform actions that are not in their best interest.

Keylogger

Is a malware designed to capture keystrokes a victim enters on their computer system. This can include passwords, credit card numbers, and other sensitive data.

Botnets

Are networks of compromised computers controlled by a single attacker. Botnets can launch distributed denial of service (DDoS) attacks, steal sensitive information, or perform other malicious activities.

Adware

Is malware that displays unwanted advertisements on a victim's computer system. Adware can be annoying and disruptive, but it's generally less harmful than other types of malware.

Fileless Malware

Doesn’t rely on files to infect a victim's computer system. Instead, fileless malware executes malicious code using existing system resources, such as memory or registry keys.

Angler Phishing Attacks

Target individuals or organizations using highly targeted and personalized emails. Angler phishing attacks can be difficult to detect and are often successful in stealing sensitive information.

Advanced Persistent Threat (APT)

Is a cyberattack characterized by long-term, persistent access to a victim's computer system. APT attacks are highly sophisticated and difficult to detect and remove.

Whale-Phishing Attacks

Target high-profile individuals like executives or celebrities using sophisticated social enginnering techniques to get sensitive information.

Drive-by Attacks

The user's system is flooded with malware by visiting its compromised website to exploit vulnerabilities in other software to insert the malware without the user's knowledge.

Emotet

Is malware designed to steal sensitive information and spread it to other computers on a network. Emotet is often spread through phishing emails and can be very difficult to detect and remove.

Automated Teller Machine (ATM) Cash Out

Hackers get close to a bank's computer systems to withdraw large amounts of cash from ATMs.

TECHNIQUES

Eavesdropping

Tampering

Impersonation

Virus

Eavesdropping

An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices.

To further explain the definition of "attacked with eavesdropping", it typically occurs when a user connects to a network in which traffic is not secured or encrypted and sends sensitive business data to a colleague. The data is transmitted across an open network, which gives an attacker the opportunity to exploit a vulnerability and intercept it via various methods. Eavesdropping attacks can often be difficult to spot. Unlike other cyber security attacks, the presence of a bug or listening device may not adversely affect the performance of devices and networks.

How to Prevent Eavesdropping Attacks

The increasingly digital world makes it easier for hackers to intercept corporate information and user conversations. However, it also presents opportunities for organizations to prevent attackers' malicious intent. Common methods that help prevent eavesdropping attacks include:

1. **Military-grade encryption**: One of the best ways to prevent eavesdropping attacks is to encrypt data in transmission and private conversations. Encryption blocks attackers' ability to read data exchanged between two parties. For example, military-grade encryption provides 256-bit encryption, which is near impossible for an attacker to decode.

2. **Spread awareness**: Ensuring that employees are aware of the risks and dangers of cybersecurity is a crucial first line in protecting organizations from any cyberattack. This is very much the case with eavesdropping attacks, so organizations must provide training that advises users about how attackers go about launching the attacks. Employees need to understand the methods attackers use to listen in to conversations, follow best practices to limit the risk, and be constantly aware of the signs of an attack. They should also avoid downloading insecure applications or software and never connect to weak or open networks.

3. **Network segmentation**: Organizations can limit the possibilities of attackers eavesdropping on networks by restricting their availability. Network Segmentation enables organizations to limit resources to only the people that require access to them. For example, people on a marketing team do not require access to HR systems and people on the IT team do not need view to financial information. Network segmentation divides the network up, which decongests traffic, prevents unwanted activity, and improves security by preventing unauthorized access.

4. **Avoid shady links**: Related to spreading awareness is the need to avoid shady or untrusted links. Eavesdropping attackers can spread malicious software that includes eavesdropping malware through shady links. Users should only download official software from trusted resources and providers, and only download applications from official app stores.

5. **Update and patch software**: Attackers can also exploit vulnerabilities in software to target organizations and users. This makes it crucial to turn on automatic updates and ensure all software is patched immediately as a new release or update is available.

6. **Physical security**: Organizations can also protect their data and users through physical security measures in their office spaces. This is crucial to protecting the office from unauthorized people who may drop physical bugs on desks, phones, and more.

7. **Shielding**: The risk of eavesdropping through computer radiation can be prevented by installing security measures and shielding. For example, TEMPEST-protected computers enable organizations to block unintended radiation and keep their data and users secure.

Tampering

Tampering means changing or deleting a resource without authorization. A web application is an application that is accessed through a web browser over the internet. Data tampering in web applications simply means a way in which a hacker or a malicious user gets into a web site and changes, deletes or to access unauthorized files. A hacker or malicious user can also tamper indirectly by using a script exploit that is the hacker would get the script to execute by masking it as a user input from a page or as a web link.

Tampering is one of the biggest security threats faced by web applications. It is used to change or edit files found in web applications which are usually used by multi-million business corporations across the world. Tampering started in the late 1980's as a way to sabotage data or plant a malicious or destructive program to delete data. Since then it has progressed and enhanced through the years. In the year 2000, hackers were able to perform data fabrication and falsification to deceive the uses of the web application. From then on, tampering with web applications are becoming easier for attackers because of the advanced technology being produced and released every year, that is to say that these technologies provide easy to use tools and application programs to simplify data tampering or data manipulation in computer systems.

Types of Data Tampering

Data tampering or data manipulation can usually be done through the following ways: Cookies, HTML Form Fields, URL Query Strings, HTTP Headers and Password Cracking.

1. **COOKIE TAMPERING:** Cookies are used as a mechanism to store user details and preferences and other data including session tokens. Cookies that are persistent and non-persistent, insecure or secure can be altered by the user and sent to the server with Uniform Resource Locator requests, therefore any malicious user or hacker can modify cookie content to his advantage allowing the attacker to access the files needed.

2. **HTML FORM FIELDS TAMPERING:** When a user makes selections or changes on a web or an HTML page, the selection is stored as form field values which are then delivered to the application as an HTTP request. HTML usually stores field values as Hidden Fields, which are not shown to the screen of the user but are collected and submitted as strings or parameters during form submissions. Whether these form fields can be hidden, pre-selected or free form, they can all be tampered or manipulated by the hacker to submit whatever values he/she chooses.

3. **URL QUERY STRINGS TAMPERING:** URL tampering comes with all of the problems associated with Hidden Form Fields. One of two methods is used by the HTML forms to submit their results, either POST or GET. Usually the method GET is used, showing all form element names and their values in the query string of the next URL that the hacker sees. Hackers find tampering with query strings easier than tampering with hidden form fields. All that the hacker has to do is look at the URL in the user's address bar. For example; a web page allows the authenticated user to select one of his pre-populated accounts from a drop-down box and debit the account with a fixed unit amount. His/her choices are recorded by pressing the submit button. The page is actually storing the entries in form field values and submitting them using a form submit command. The command sends the following HTTP request: http://www.victim.com/example?accountnumber=12345&debitamount=1, now all what the hacker has to do is could construct his/her own account number and change the parameters like the following: http://www.victim.com/example?accountnumber=67891&creditamount=999999999.

4. **HTTP HEADER TAMPERING:** HTTP headers are used by the web server software and the user only. Most web applications do not use them. Some web developers choose to monitor incoming headers and it is important to notice that request headers are originally from the client or user side, and they might be altered by an attacker. Normal web applications do not allow header alteration or modification. A hacker will have to write his own program to perform the HTTP request or may use a freely available proxy that will allow easy modification of any data sent from the web application.

5. **PASSWORD CRACKING TAMPERING:** A password cracker is an application program that is used to help a hacker or malicious user to identify an unknown password to a computer or network resources to obtain or allow unauthorized access to its resources. The hacker would attempt to gain valid credentials from an authentication system by large numbers of repeated authentication attempts by using different passwords. Password cracking application program uses two primary methods to search or identify correct passwords which are the brute force and dictionary searches. When the application program uses brute force, it simply runs through combinations of all kinds of characters with a predetermined length until it identifies the correct combination which is for the computer system. When it uses the dictionary search, the application program searches each word in the dictionary for the correct password for the computer system.

Prevention and Countermeasures

A primary defense against data tampering is to use a firewall and windows security to lock down important files, directories and other resources. The web application should also run with minimum privileges. Guarding against script exploits by not trusting any information that comes from a user or even from a database. Appropriate and safe steps should be taken when getting information from untrusted sources, to make sure it does not contain any malicious executable code.

Counter-Measures to prevent data tampering are done through the following ways: by using data signing and harsing, using digital signatures, using strong authorization, using tamper resistant protocols across communication links, using secure communication links with protocols that provide message integrity, also by using strong and powerful firewalls, and long passwords that consist of alphanumeric characters, by also blocking IP addresses for a certain period of time which will cause repeated failed login attempts by the attacker.
Also by using access controls to protect data in persistent stores to ensure that only authorized users can access and modify the data, and by using role based security to define which users can view data and which users can modify data.

What is Impersonation in Cybersecurity?

Impersonation is one of the most commonly used social engineering techniques used by hackers and cybercriminals to commit fraud, steal private data or gain access to restricted networks and systems.
The classic impersonation attack involves a hacker who pretends to be a trusted friend, colleague or business associate of the target in hopes of tricking them into divulging sensitive data or sending fraudulent payments.

But in 2021, impersonation attacks have evolved to take advantage of the ever-expanding public attack surface. They now include fraudulent communications (email, telephone, voicemail, and SMS), as well as spoofed domains, fake social media accounts and fraudulent apps.

How Does an Impersonation Attack Work?

Impersonation attacks are difficult for SecOps teams to defend against, in part because cybercriminals use diverse strategies to target different points in the public attack surface. Despite the variation in impersonation attacks today, these attacks all tend to follow the same basic pattern of exploiting the victim.

- **Research and Victim Targeting** – Hackers may use business directories, news sites, social media, and other information sources to discover potential targets for an impersonation attack. Organizations of all types and sizes have been targeted by these attacks, but the most sophisticated hackers will target organizations with valuable assets or data and comparatively lax IT security infrastructure.

- **Preparing Fake and Fraudulent Assets** – Once a hacker has identified a target organization, the next step is to prepare assets that will be used in the attack. The hacker might register a spoofed domain, create fake social media profiles, or launch a fake website that resembles a trusted domain. They might also create fraudulent messages that will be used to manipulate the target.

- **Deploying the Attack** – Once the fraudulent assets are prepared, the hacker will leverage those assets to initiate communication and attempt to defraud the target. The attacker might use social media or email to impersonate someone trusted by the target before asking them to send money or directing them to a fake website that will capture their credentials.

What are Some Impersonation Attack Examples?

Malicious actors are constantly finding new ways to implement impersonation attacks against businesses, government agencies, and individual targets. Here a just a few examples to watch out for:

Domain Spoofing

Domain spoofing is a type of impersonation attack where a cybercriminal creates a replica of a trusted website with a similar domain name and user interface. The most common targets for domain spoofing attacks are financial institutions where users must login to access their account information.

Once the spoofed domain has been created, the cybercriminal can begin targeting their victims with links to the spoofed domain, along with some pretext for the target to visit the link and login to their account. When a target takes the bait, their login credentials are compromised and the cybercriminal can attempt to steal money.

Impersonating a Friend or Business Associate

Cybercriminals can impersonate a friend or business associate of the target using spoofed emails or fake social media accounts. They often choose to impersonate high-profile individuals within large companies, in hopes of targeting their employees or customers with fraudulent messages and requests.

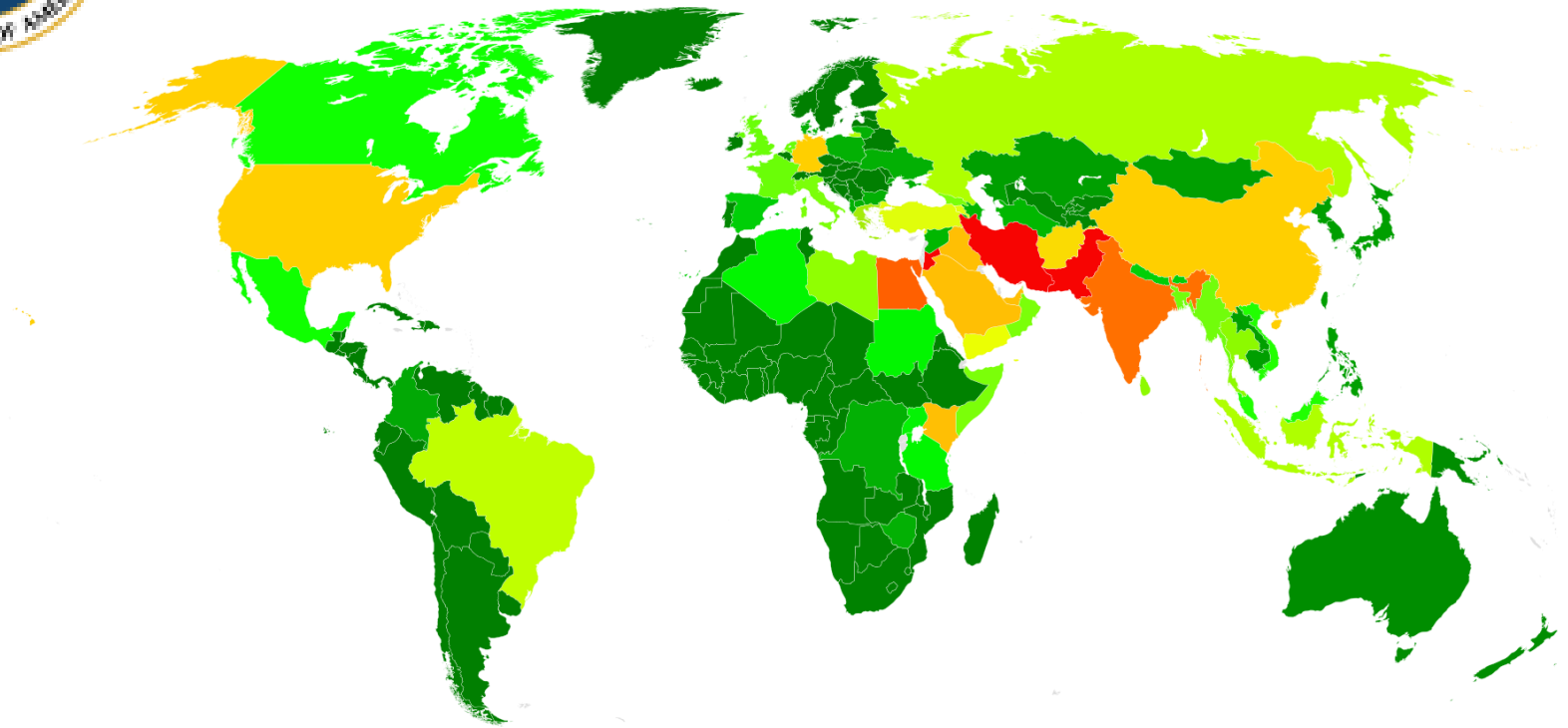
Fake social media profiles and email accounts are easy to create, and can be used to phish, steal information, or fraudulently authorize transactions to the cybercriminal's bank account.

Impersonating a Trusted App

Fake apps are an increasingly common form of impersonation attack in 2021. Threat actors can build a replica of a mobile banking app by copying the layout, graphics, and descriptions from the genuine app. Cybercriminals can distribute fraudulent mobile apps by spamming download links on the web, or through unregulated third-party app stores.

Just like a spoofed domain, fake mobile banking apps are designed to steal access credentials and banking information from victims.

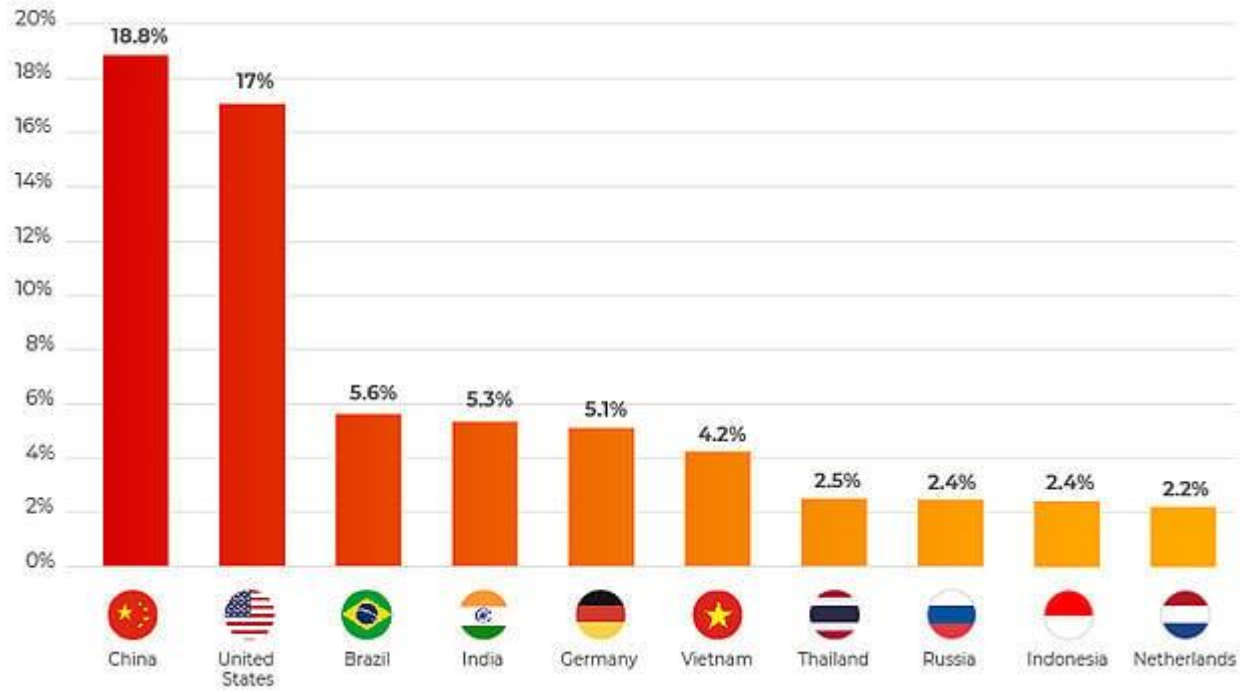
NATIONAL SECURITY AGENCY



National Security Agency surveillance
Map of global NSA data collection as of 2007, with countries subject to the most data collection shown in red

Highest 10 Countries of Origin for Cyber Attacks

1.China – 18.83%
2.United States – 17.05%
3.Brazil – 5.63%
4.India – 5.33%
5.Germany – 5.10%
6.Vietnam – 4.23%
7.Thailand – 2.51%
8.Russia – 2.46%
9.Indonesia – 2.41%
10.Netherlands – 2.20%



EDWARD SNOWDEN

Edward Joseph Snowden (born June 21, 1983) is an American and naturalized Russian former computer intelligence consultant and whistleblower who leaked highly classified information from the National Security Agency (NSA) in 2013, when he was an employee and subcontractor.

BREACHED INTO NSA

What is Cryptography?

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

Caesar-shift cipher

The Caesar shift cipher is one of the earliest methods in cryptography. In this method, the message is hidden from unauthorized readers by shifting the letters of a message by an agreed number. Upon receiving the message, the recipient would then shift the letters back by the same number agreed upon earlier. A cryptanalyst may be able to decrypt the message by observing the cipher method.

Reverse cipher

In reverse cipher method, letters are not shifted. Rather, the message is encrypted in a reverse order. To decrypt a message in reverse, we just reverse the reversed message to the original form. Julius Caesar invented the reverse cipher circa 2000 years ago.

Apart from the reverse and Caesar shift cipher, others such as substitution shift cipher were also used in the early days of cryptography. However, most of these methods can be decrypted easily.

TO BE CONTINUED……

Get in Touch: zende21bcy33@iiitkottayam.ac.in