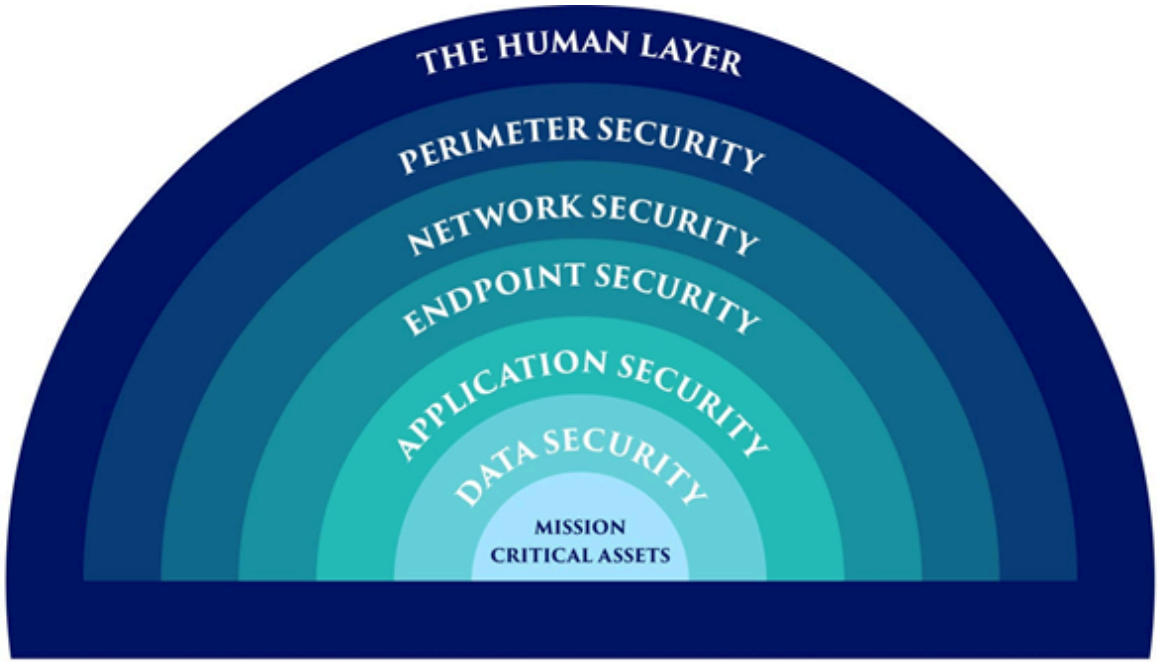
The Seven Layers of Cyber security:

When you look at the OSI model, it's pretty clear you need more than just a few security protocols in place to be fully protected. You need to carefully consider all the potential access points and areas where hackers may gain entry to your network, data, and business. Let's take a closer look at the 7 layers, how they're vulnerable, and what you can do to protect them.



THE 7 LAYERS OF CYBERSECURITY

1. Human Layer:

Humans alone are responsible for 90% of data breaches, making them the weakest link in any cyber security strategy. Human security includes the following measures: Phishing simulations,

Access management guidelines which controls the mission-critical assets from a range of human threats,

Cybercriminals,

Malicious insiders, and

Irresponsible users.

The human layer, often regarded as the most vulnerable layer, focuses on the human element within an organization. It involves implementing practices and policies that ensure that employees, contractors, and other users do not fall victim to phishing attacks and other security threats due to human error or lack of knowledge.

Examples of human layer security measures include security awareness training, strong password policies, and multi-factor authentication, ensuring that users can identify and respond appropriately to security threats. Access restriction is a good idea for safeguarding the human layer since they can lessen the potential damage from a successful assault.

2. Perimeter Security Layer:

Perimeter security layer is akin to the walls of a fortress. It serves to protect the network by controlling incoming and outgoing network traffic based on an organization's previously established security policies.The perimeter security controls have digital and physical security measures that protect the entire business. When identifying the type of data being transferred across this layer, we must first determine our perimeter. After that, we must secure both data and the device. At its core, it involves implementing firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and VPNs to create a barrier between your secure internal network and untrusted external networks such as the internet.

An example of how this works is a firewall that filters incoming traffic to allow or block packets based on the organization’s security policies, thus preventing unauthorized access to networked resources.

Security Plan: Installation of firewalls, data encryption, antivirus software, and device management are the security strategies which are crucial when a company allows their employees to use their own device. This layer also establish a safe demilitarised zone to enhance security.

3. Network Layer:

The network layer is crucial in managing and protecting the communication between applications and devices on your network. There are various methods of network security used to

protect a company's network and helps in preventing unauthorized access. The main concern with the network layer is what people and devices may access once they are on a network. Network Security methods/techniques are mainly used to protect the important data of an organization from network attacks. This layer employs various security measures and controls to prevent attackers from intercepting and tampering with information as it travels over the network. Examples of network layer security include the use of secure protocols like HTTPS, employing network segmentation to separate sensitive parts of the network from less sensitive ones, and implementing security solutions like anti-malware and antivirus software to monitor and analyze network traffic for malicious activity and unauthorized access.

The network layer is pivotal in the cyber security landscape as it serves as the communication bridge connecting various components within a network, facilitating data transfer between them. It holds immense importance because it is inundated with a multitude of information exchanges, making it a lucrative target for cyber adversaries aiming to intercept, modify, or disrupt the data flow. By securing the network layer through strategies like encryption, secure protocols, and robust network architectures, organizations can ensure the integrity, availability, and confidentiality of the transmitted information, thereby protecting against unauthorized access and potential cyberattacks, and maintaining seamless and secure organizational operations.

Security Plan: If no individual has access to everything, then any successful hack only compromises a tiny piece of the network. At this stage, the security measures only allow the devices and workers to access only those network resources that are essential for them to perform their tasks.

4. Application Security Layer:

This layer of IT security covers all the programs and applications which are using by the user. Various programs like Microsoft Office, Teams, Zoom, and others, which performs our daily tasks would be secured. This layer focuses on keeping software and devices free of threats. Secure coding practices are vital here, as vulnerabilities in the application can serve as entry points for cyber threats. Examples of application security measures include regular security scanning and testing to identify and remedy vulnerabilities and employing application security solutions like Web Application Firewalls (WAFs) to protect against threats such as SQL injection and Cross-Site Scripting (XSS).

Security Plan: In this situation, the simplest thing you can do is to update your programs or applications regularly. Due to this, it is possible to secure and safe the application and also helps in ensuring that the existing security flaws are fixed.

In this stage, the security measures will use sandboxes for browser-based applications and the software restriction guidelines to prevent the unauthorised software which is being executed on your network. Along with this, we can safe the things by using the next-generation firewalls which are working with the integrated app protection

5. Endpoint Security Layer:

Any device that is linked to your network is referred to as an endpoint. As we mentioned above, there are so many endpoints on networks nowadays that it may be a bit daunting. To manage and monitor these devices, it is crucial to present the robust policy. The endpoint security layer concentrates on safeguarding the individual devices that connect to the network, like computers, smartphones, and tablets. Since these endpoints serve as access points to the network, securing them is crucial. An example of endpoint security is employing antivirus programs and endpoint detection and response (EDR) solutions to monitor, detect, and block malicious activities and threats on endpoints, ensuring that even if a device is compromised, the threat does not propagate through the network.

6. Data Security Layer:

In almost every instance, data is the target when it comes to cybercrime. This is the layer that requires the most attention because it's the heart and soul of your business.

The kind of data that you have is going to depend on your business, but it could include customer data, payment information, social security numbers, business secrets (and other intellectual property), and healthcare information. Losing this data erodes your customers' trust in your business, leaves you open to huge regulatory fines, and about 50% of the time, causes your business to close.

This layer is dedicated to protecting the data residing in the network, focusing on maintaining its confidentiality, integrity, and availability. Encryption is a prime example of a data security measure, where sensitive data is converted into a coded format to prevent unauthorized access. Another example is employing backup solutions and establishing robust access controls to

safeguard data from loss, exposure, and unauthorized access, ensuring only authorized personnel can access sensitive information.

7. Mission-Critical Assets:

This is anything your business can’t survive without. This includes operating systems, electronic health records, software tools, financial records, and cloud infrastructure. The challenge at this layer is that what’s mission-critical for one business isn’t necessarily critical for yours. That means you have to determine what your business can’t live without and work backward to protect it.

This layer focuses on safeguarding assets that are crucial to an organization's operations and business continuity. These could include proprietary software, sensitive customer data, or essential hardware. Protection strategies here involve implementing layered defenses like firewalls, intrusion detection and prevention systems, and robust access controls. For instance, regularly updating and patching mission-critical applications ensures that vulnerabilities are addressed, minimizing the risk of exploitation and ensuring the uninterrupted functionality of essential assets.

In the rapidly evolving domain of cyber security, possessing a nuanced understanding of the multi-layered defense mechanisms is indispensable. The proficiency in securing each layer not only opens up a plethora of cybersecurity jobs but also promises a lucrative salary. Attaining a cybersecurity certification is a significant step towards becoming a formidable cybersecurity engineer or a meticulous cybersecurity analyst. By enrolling in a cyber security course or a comprehensive cyber security bootcamp, individuals and corporates can acquire hands-on training, essential in navigating the multifaceted landscape of cyber threats effectively.

Internet governance:

According to Kerr (2003), there are "two dominant perspectives of the Internet" (cited in Frischmann, 2003, p. 205): on the one hand, the Internet is viewed as "a global meta-network that serves as an open platform for the transmission of information among end users that connect computers to the network;" on the other hand, the Internet is viewed "in terms of the applications it enables and the ways in which those applications affect end users" (Frischmann, 2003; pp. 205-206; see also Kerr, 2003, p. 359-360). It is the latter conception of the Internet "that leads to the conception of cyberspace as a sort of virtual reality" (or environment) whereby online activities take place (Frischmann, 2003, p. 206).

Literature on regulation theories pertaining to the Internet and cyberspace governance focus on which individuals, groups, businesses, organizations, and government agencies, regulate the Internet and cyberspace, and the way cyberspace and the Internet are regulated (Chang and Grabosky, 2017, p. 535; for more information on regulations theories, see Drahos, 2017). This view is supported in the literature, which holds that cyberspace and the Internet is regulated by, for example, laws, computer programming code, system architecture, and Internet architecture (Lessig, 2006); individuals, businesses, and organizations with or without some form of government involvement (i.e., a type of self-regulation, see Braithwaite, 1982); and individuals, businesses, and organisations sharing responsibility for governance (i.e., distributed security, see Brenner, 2005) (for more information, see Chang and Grabosky, 2017, pp. 535-542).

According to the World Summit on the Information Society (WGIG), a global forum organized by the United Nations, *Internet governance* refers to "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (WGIG, 2005, p. 4; see also Kurbalija, 2014, p. 5). Mueller (2010) stated that Internet governance does not primarily lie with "formal policy-making institutions;" instead, "most of the real-world governance of the Internet is decentralized and emergent…[,] it comes from the interactions of tens of thousands of network operators and service providers - and sometimes users themselves - who are connected through the Internet" (p. 9). The Internet impacts global interests and its governance "includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN); it also

includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet" (WGIG, 2005, p. 4). For these reasons, a single entity cannot and has not been designated as an international governance body (Reich et al., 2014). Instead, the Internet is primarily governed internationally by multiple stakeholders - government, the private sector, academia, and civil society - covering a range of technical and non-technical issues. Nevertheless, countries vary in terms of their views on which stakeholders should play a primary role in Internet governance. While some countries believe that multiple stakeholders should be responsible for Internet governance, other countries believe that Internet governance should be the exclusive domain of the state (for further information see, Masters, 2014; Chang and Grabosky, 2017).

Internet Governance – Challenges and Constraints:

Internet Governance is defined as the development and application by Government. The private sector and civil sector in their respective roles of shared principles, norms, rules, decision making procedures and programs that shape the evolution and use of the Internet.

The definition developed by the Working Group of Internet Governance (WGIG) dates back to 2005, and has remained unchanged ever since then and is now a complex system involving a multitude of issues, actors, mechanisms, procedures and instruments.

Internet Governance Actors:

According to the definition, there is no single organization incharge of the Internet but various stakeholders – Governments, Inter Governmental Organizations, the private sector, the technical community and Civil Society share roles and responsibilities in shaping the evolution and use of this network.

There are multiple actors which are involved in one wayor another in the governance of Internet.

1. Internet Corporation for Assigned Names and Numbers (ICANN)
2. Internet Engineering Task Force (IETF)
3. International Telecommunication Union (ITU)
4. World Intellectual Property Organization (WIPO)
5. Internet Governance Forum (IGF)

Challenges and Constraints:

- Lack of a Unified Governance Structure
- there's no global legal framework to address cybercrime.

- Privacy and Data Protection: Balancing privacy rights with security and surveillance concerns is a major issue
- Balancing the roles and responsibilities of various stakeholders (especially in countries where governments seek more control) can be difficult
- Digital divide: many people cannot afford the digital devices needed to access e-governance services.
- Internet shutdowns

TAXONOMY OF VARIOUS ATTACKS

1. Based on Attack Methodology

Passive Attacks: These attacks involve unauthorized monitoring of communications or data, without altering it. The objective is to gain information without being detected.

Examples: Eavesdropping, Traffic Analysis, Packet Sniffing.

Active Attacks: In active attacks, the attacker modifies or disrupts the data or systems, often with malicious intent.

Examples: Denial of Service (DoS), Man-in-the-Middle (MitM), Data Tampering.

2. Based on Attack Vector

Network-Based Attacks: Target the network infrastructure or services, exploiting vulnerabilities in protocols or systems to gain unauthorized access or disrupt communications.

Examples: DDoS, IP Spoofing, DNS Spoofing, Packet Injection.

Host-Based Attacks: These target vulnerabilities in individual systems or devices.

Examples: Buffer Overflow, Privilege Escalation, Rootkits, Keyloggers.

Application-Based Attacks: Focus on exploiting weaknesses in software applications or web services.

Examples: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Remote Code Execution (RCE).

3. Based on Attack Goal

Confidentiality Attacks: The goal is to steal or access sensitive information without authorization.

Examples: Data Breaches, Phishing, Keylogging, Password Attacks.

Integrity Attacks: Aim to alter or manipulate data, systems, or communications, potentially causing damage or loss of trust.

Examples: Man-in-the-Middle (MitM), Data Manipulation, File Tampering.

Availability Attacks: The objective is to deny legitimate access to resources or services.

Examples: Denial of Service (DoS), DDoS, Ransomware.

Authentication Attacks: Target the mechanisms used to verify user or system identity.

Examples: Brute Force Attacks, Credential Stuffing, Session Hijacking.

4. Based on Threat Actor or Source

External Attacks: Conducted by individuals or groups outside the organization, often using sophisticated tools and techniques.

Examples: Cybercriminals, Hacktivists, Nation-State Actors, Script Kiddies.

Internal Attacks (Insider Threats): Perpetrated by someone within the organization, such as employees or contractors, either intentionally or unintentionally.

Examples: Sabotage, Data Theft, Unintentional Leaks.

5. Based on Attack Complexity

Simple Attacks: Require little to no technical skill, often using publicly available tools or basic techniques.

Examples: Phishing, Social Engineering, Basic Malware.

Advanced Attacks: Highly sophisticated and often involve multiple stages, advanced techniques, and custom tools.

Examples: Advanced Persistent Threats (APTs), Zero-Day Exploits, Supply Chain Attacks.

6. Based on Automation Level

Manual Attacks: Carried out by attackers in real-time, often involving social engineering or hands-on interaction.

Examples: Phishing, Spear Phishing, Social Engineering.

Automated Attacks: These involve the use of scripts, bots, or malware to automatically scan for and exploit vulnerabilities.

Examples: Botnets, Credential Stuffing, DDoS.

7. Based on Vulnerability Exploited

Software Vulnerabilities: Exploit bugs or weaknesses in software to gain unauthorized access or control.

Examples: Buffer Overflow, Remote Code Execution, Zero-Day Exploits

Human Vulnerabilities: These are vulnerabilities that arise from human errors, lack of awareness, or social engineering techniques.

Examples: Phishing, Social Engineering, Insider Threats

Hardware Vulnerabilities: These arise from flaws or weaknesses in the physical components of devices, such as CPUs or hardware interfaces.

Examples: Side-Channel Attacks, Firmware Exploits(Compromising firmware to control hardware components.)

IP Spoofing

Spoofing is a type of cyber-attack used by hackers to gain unauthorized access to a computer or a network, IP spoofing is the most common type of spoofing out of the other spoofing method. With IP Spoofing the attacker can hide the true source of the IP packets to make it difficult to know the origin of the attack. Once access to a network or a device/host is achieved, cybercriminals usually mine them for sensitive data, with computers they can turn into zombies and can be used to launch Denial-of-Service (DoS) attacks.

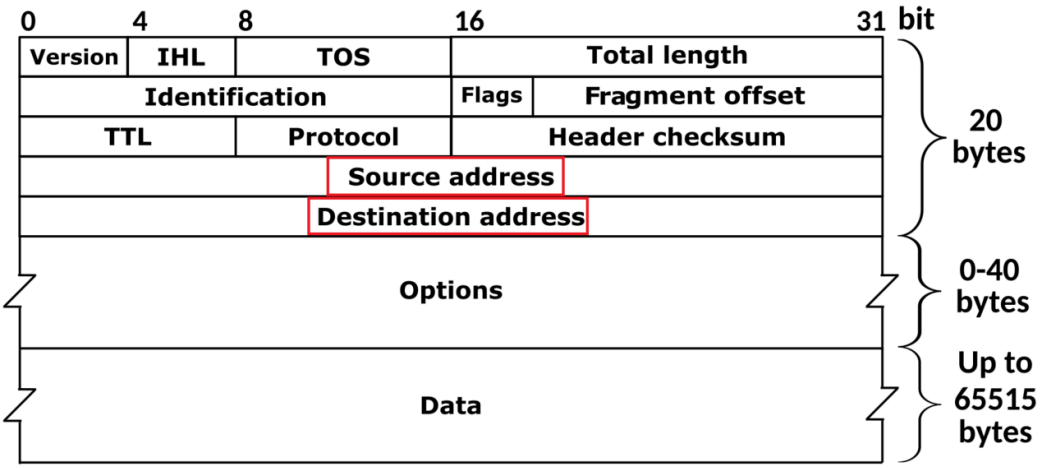
What Is IP Spoofing?

IP addresses are used for communication between devices on the internet. Cybercriminals use a false source IP address to hide and impersonate another system. Essentially making it harder for the destination system to detect. Such attacks come with the intent to steal sensitive data, infect your computer with malware or viruses, or even crash your server.

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. This occurs at the network level, so there are no external signs of tampering.

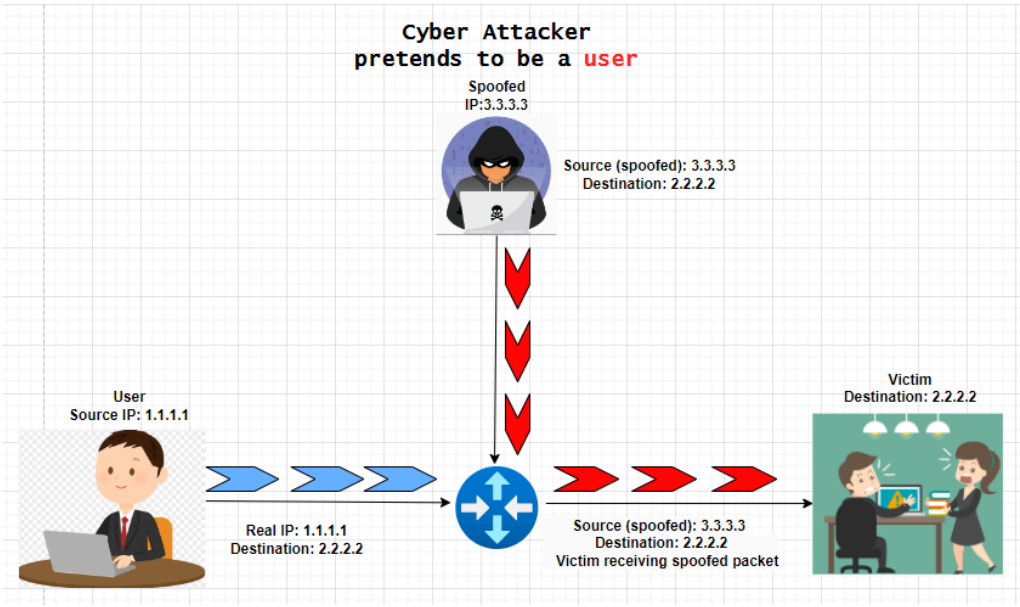
How IP Spoofing Works

So, let's get deeper into how IP spoofing works. An IP address is a series of numbers that identifies your device on the internet and every device that connects to the internet has an IP address with its use they are able to exchange data., below is what an IP header packet looks like

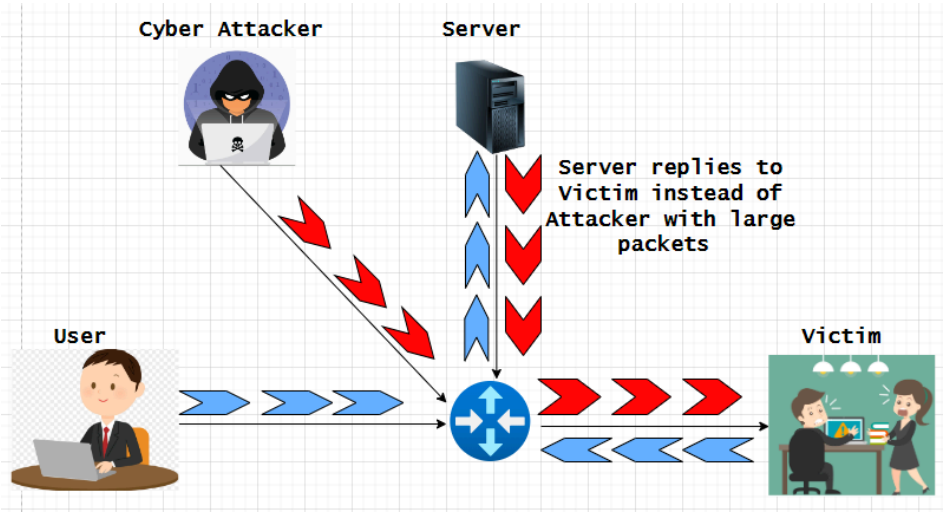


Spoofing takes advantage of the source by faking the source inside the packet similarly it's like putting a fake return address on an envelope in a mailbox. Most of the time when an IP packet travels to reach its destination it goes over multiple intermediate devices or routers which do not inspect the source address at all.

In the below example, you can see that the cyber attacker has successfully changed the source IP of the packet from 1.1.1.1 to 3.3.3.3 (changed IP).



Now, let's say that someone wants to disrupt and completely disconnect their internet service, they can send packets with a fake source address to that victim with so many packets that the victim has no resources to process legitimate packets. An attacker can use many different fake source addresses across many packets and often it's not feasible to trace back the attacker to its origin to block the attack at the victim it gets even worse when an attacker can commandeer intermediate nodes to amplify an attack by triggering that node to send the victim very large packets which takes more resources to process as seen in the image below.



Types of IP spoofing

The three most common forms of IP spoof attacks are:

1. **Distributed Denial of Service (DDoS) attacks**

In a DDoS attack, hackers use spoofed IP addresses to overwhelm computer servers with packets of data. This allows them to slow down or crash a website or network with large volumes of internet traffic while concealing their identity.

2. **Masking botnet devices**

IP spoofing can be used to obtain access to computers by masking botnets. A botnet is a network of computers that hacker's control from a single source. Each computer runs a dedicated bot, which carries out malicious activity on the attacker's behalf. IP spoofing allows the attacker to mask the botnet because each bot in the network has a spoof IP address, making the malicious actor challenging to trace. This can prolong the duration of an attack to maximize the payoff.

3. **Man-in-the-middle attacks**

Another malicious IP spoofing method uses a 'man-in-the-middle' attack to interrupt communication between two computers, alter the packets, and transmit them without the original sender or receiver knowing. If attackers spoof an IP address and obtain access to personal communication accounts, they can then track any aspect of that communication. From there, it's possible to steal information, direct users to fake websites, and more. Over time, hackers collect a wealth of confidential information they can use or sell – which means man-in-the-middle attacks can be more lucrative than the others.

How to detect IP spoofing

It is difficult for end-users to detect IP spoofing, which is what makes it so dangerous. This is because IP spoof attacks are carried out at the network layers – i.e., Layer 3 of the Open System Interconnection communications model. This doesn't leave external signs of tampering – often, spoofed connection requests can appear legitimate from the outside.

However, organizations can use network monitoring tools to analyze traffic at endpoints. Packet filtering is the most common way to do this. Packet filtering systems – which are often contained in routers and firewalls – detect inconsistencies between the packet's IP address and desired IP addresses detailed on access control lists (ACLs). They also detect fraudulent packets.

The two main types of packet filtering are ingress filtering and egress filtering:

Ingress filtering looks at incoming packets to assess whether the source IP header matches a permitted source address. Any packets which look suspicious will be rejected.

Egress filtering looks at outgoing packets to check for source IP addresses that don't match those on the organization's network. This is designed to prevent insiders from launching IP spoofing attacks.

How to protect against IP spoofing

IP spoofing attacks are designed to conceal the attackers' true identity, making them difficult to spot. However, some anti-spoofing steps can be taken to minimize risk. End-users can't prevent IP spoofing since it's the job of server-side teams to prevent IP spoofing as best they can.

IP spoofing protection for IT specialists:

Most of the strategies used to avoid IP spoofing must be developed and deployed by IT specialists. The options to protect against IP spoofing include:

- Monitoring networks for atypical activity.
- Deploying packet filtering to detect inconsistencies (such as outgoing packets with source IP addresses that don't match those on the organization's network).
- Using robust verification methods (even among networked computers).
- Authenticating all IP addresses and using a network attack blocker.
- Placing at least a portion of computing resources behind a firewall. A firewall will help protect your network by filtering traffic with spoofed IP addresses, verifying traffic, and blocking access by unauthorized outsiders.

Web designers are encouraged to migrate sites to IPv6, the newest Internet Protocol. It makes IP spoofing harder by including encryption and authentication steps. A high proportion of the world's internet traffic still uses the previous protocol, IPv4.

IP spoofing protection for end users:

End-users can't prevent IP spoofing. That said, practicing cyber hygiene will help to maximize your safety online. Sensible precautions include:

1. Make sure your home network is set up securely:

This means changing the default usernames and passwords on your home router and all connected devices and ensuring you use strong passwords. A strong password avoids the obvious and contains at least 12 characters and a mix of upper- and lower-case letters, numbers, and symbols. You can read Kaspersky’s full guide to setting up a secure home network here.

2. Take care when using public Wi-Fi:

Avoid carrying out transactions such as shopping or banking on unsecured public Wi-Fi. If you do need to use public hotspots, maximize your safety by using a virtual private network or VPN. A VPN encrypts your internet connection to protect the private data you send and receive.

3. Make sure the websites you visit are HTTPS:

Some websites don’t encrypt data. If they don’t have an up-to-date SSL certificate, they are more vulnerable to attacks. Websites whose URL starts with HTTP rather than HTTPS are not secure – which is a risk for users sharing sensitive information with that site. Ensure that you’re using HTTPS websites and look for the padlock icon in the URL address bar.

4. Be vigilant when it comes to phishing attempts:

Be wary of phishing emails from attackers asking you to update your password or other login credentials or payment card data. Phishing emails are designed to look as though they come from reputable organizations but, in reality, have been sent by scammers. Avoid clicking on links or opening attachments in phishing emails.

5. Use a comprehensive antivirus:

The best way to stay safe online is by using a high-quality antivirus to protect you from hackers, viruses, malware, and the latest online threats. It's also essential to keep your software up-to-date to ensure it has the latest security features.

SECURITY MODELS

Additional links to study:
https://sprinto.com/blog/types-of-security-models/

https://media.techtarget.com/searchSecurity/downloads/29667C05.pdf

https://www.geeksforgeeks.org/introduction-to-classic-security-models/

What are security models?

Information security models are systems that specify which people should have access to data, and the operation of the operating system, which enables management to organize access control. The models offer a mathematical mapping of theoretical goals, strengthening the chosen implementation.

A security model may have no theoretical underpinnings, or it can be based on a formal computing model, a distributed computation model, an access rights model, or even a model of distributed computation.

What is the objective of a security model?

The core aim of any security model is to maintain the goals of Confidentiality, Integrity, and Availability of data. It can achieve these goals by:

- Allowing admins to choose the resources that users are allowed access to.
- Verifying user identities with authentication mechanisms that incorporate password strength and other variables.
- Allowing users who have been permitted to access resources provisioned and defined by authorization systems.
- Regulating which functions and rights are given to accounts and users.
- Giving admins access to a user's list of activities on a request or assignment basis.
- Safeguarding private data, such as account characteristics or user lists.

Types of security model

Since network and cyber security are continuously evolving domains, there have been numerous security models proposed in the history of time. However, there are three classic security models which serve as the foundation of many other models. Let's have a look at them in detail:

1. Bell-LaPadula

David Bell and Leonard LaPadula, pioneers in computer security, created the Bell-LaPadula model, a lattice-based security concept, in the 1970s. The Bell-LaPadula model is a multilevel security system. It establishes a set of access rules and security levels (such as Top Secret, Secret, and Confidential) that specify how individuals may access objects at various security levels.

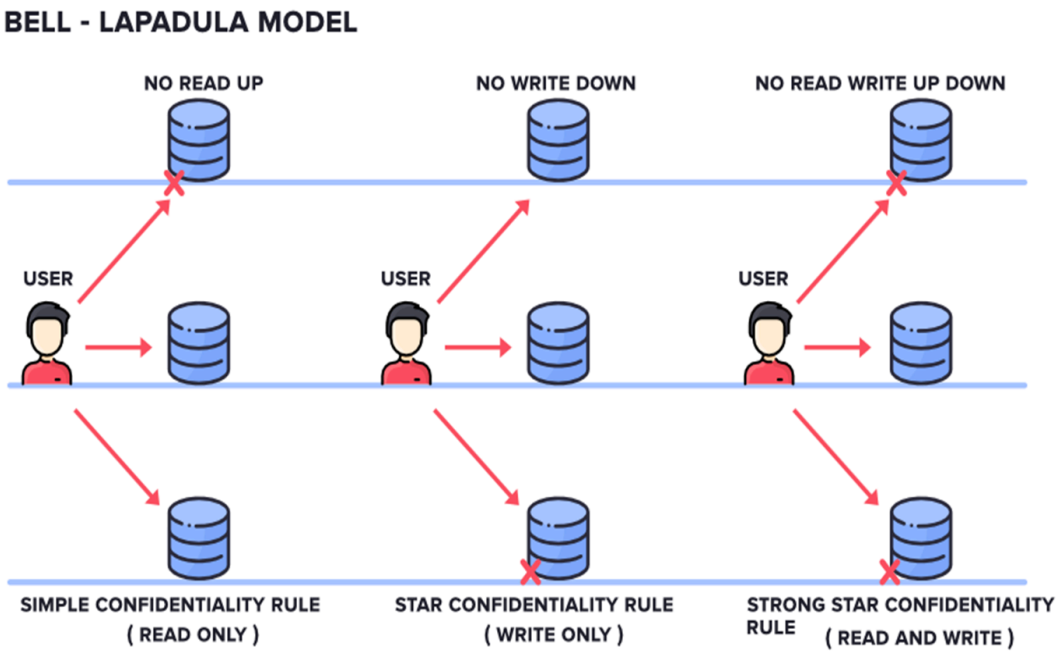


Image source: https://www.geeksforgeeks.org/introduction-to-classic-security-models

Bell-LaPadula only allows users at or above their own security level to create content. However, users are limited to seeing anything that is at or below their own security level.

When sensitive information has to be shielded from unwanted access, military and government institutions commonly employ the Bell-LaPadula model. It is sometimes employed in civil organizations, such as banks and hospitals, where a robust cyber security architecture and data protection are vital.

Rules of the Bell-LaPadula model:

- **SIMPLE Confidentiality Rule:** Simple Confidentiality Rule specifies that the Subject may only read documents protected by the same layer of secrecy and the lower layer of secrecy, but not the upper layer of secrecy. For this reason, we refer to this rule as NO READ-UP.
- **STAR Confidentiality Rule:** According to the Star Confidentiality Rule, the Subject may only write files on the same layer of secrecy and the upper layer of secrecy, but not the lower layer of secrecy. For this reason, the rule is known as NO WRITE-DOWN.

- **STRONG STAR Confidentiality Rule:** The Strong Star Confidentiality Rule is the strongest and most secure, stating that the Subject may only read and write files on the same layer of secrecy and not on an upper or lower layer of secrecy. Because of this, the rule is known as NO READ WRITE-UP OR DOWN.

Significance of the Bell-LaPadula Security Model

Being among the earliest modern security models to be created, the Bell-LaPadula model is important. This model has influenced the creation of many security models. The lattice-based security model structure of the Bell-LaPadula model has additional relevance because it was unique when it was first developed.

The Bell-LaPadula model is a key security tool that fulfills several functions. The concept initially sets several security layers to protect information from unauthorized access. The model gives a technique for controlling access to information at multiple security levels by offering a set of access rules that govern how subjects can access objects at different degrees of security. The methodology may also be used to audit information access and ensure that no unauthorized access occurs.

2. Biba model

The Bell-LaPadula Model's shortcomings inspired the development of the Biba Model. Data integrity is not addressed by the Bell-LaPadula paradigm; only data confidentiality is.

The Biba Model, which articulates a set of access control rules for maintaining data integrity, is a formal state transition system for data security regulations. Data and subjects are organized or categorized according to how reliable they are. Biba aims to prevent data corruption at levels rated higher than the topic and minimize data corruption at levels rated lower than the subject.

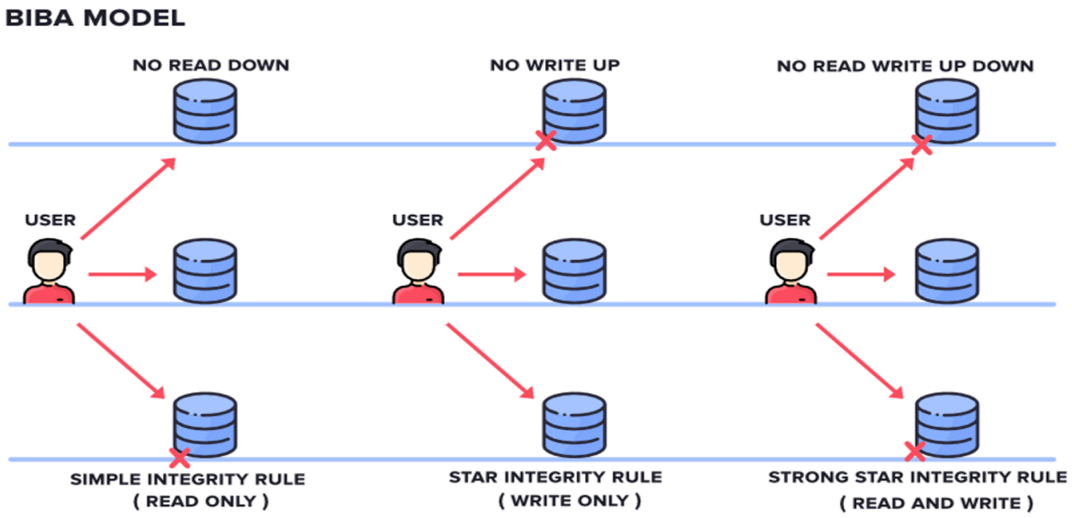


Image source: https://www.geeksforgeeks.org/introduction-to-classic-security-models/

Rules of the Biba Model:

No Write-Up (Integrity Axiom): According to this rule, no one is permitted to add to or change data that has a lower integrity level. This guards against low-quality sources, tainting information of high quality.

No Read Down (Simple Security Property): A user cannot read an item with a higher integrity level, as per this rule. This suggests that the data you are allowed to access is not more important than the data you are not allowed to see or read. For example, in a school, a student would never need access to the principal's file.

Importance of the BIBA model: The Biba Model is a collection of rules for a computer system that aids in maintaining valid and secure data. The name comes from Kenneth J. Biba's proposal in 1977. The Biba Model's main goal is to prevent people without the necessary authorization from tampering with data.

The model implements stringent integrity-based access restrictions. While users are prevented from downgrading data integrity, they are also prevented from accessing data from higher integrity levels. This ensures data isolation and confidentiality.

3. Clark-Wilson model

The Clark-Wilson security model is built upon protecting information integrity from hostile data-altering attempts. The security model states that the system should maintain consistency between internal and external data and that only authorized users should be able to generate and alter data—unauthorized users should not be able to do so at all.

The primary goal of this model is to formalize the idea of information integrity by preventing data corruption in a system due to errors or malicious intent. An integrity policy specifies how the system's data items should behave to maintain their validity when they change from one system state to another. The model outlines certification and enforcement procedures as well as the capabilities of the principals deployed inside the system.

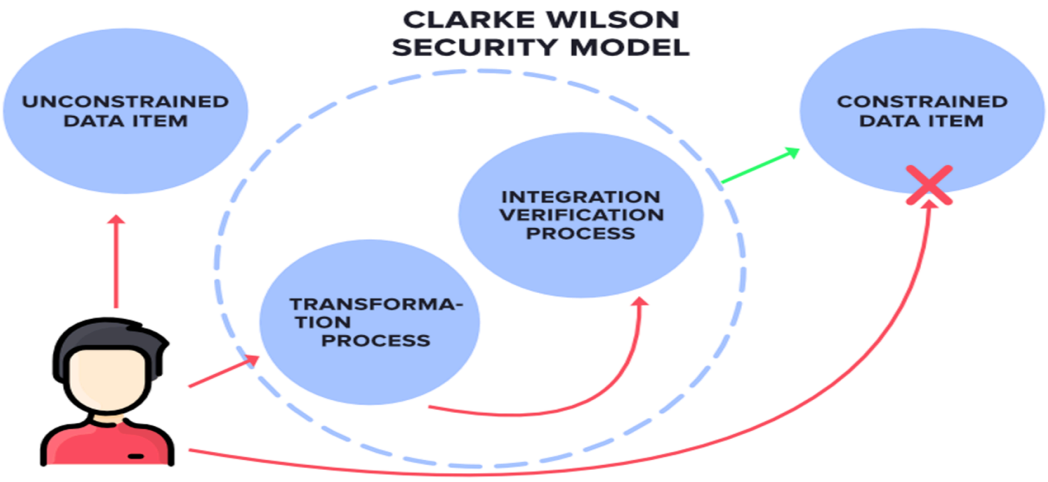


Image source: https://www.geeksforgeeks.org/introduction-to-classic-security-models/

The Clark-Wilson security concept prohibits direct access to constrained data objects. You can use these two processes to access constrained data objects:

1. Transformation process

Constrained data items can be requested by the user and managed by the transformation process. This process is intended to ensure that data changes maintain data integrity and follow the prescribed certification standards. It is transformed into authorization by the procedure before being sent to the integration verification procedure.

2. Integration verification process

It carries out authentication and permission. The user is granted access to the restricted data items if this verification is successful.

Chinese Wall Focus is on conflicts of interest.

• Principle: Users should not access the confidential information of both a client organization and one or more of its competitors.

• How it works – Users have no “wall” initially. – Once any given file is accessed, files with competitor information become inaccessible. – Unlike other models, access control rules change with user behavior

• This model provides access controls that can change dynamically depending upon a user’s previous actions.

• The main goal of this model is to protect against conflicts of interests by user’s access attempts.

• It is based on the information flow model, where no information can flow between subjects and objects in a way that would result in a conflict of interest.

The model states that a subject can write to an object if, and only if, the subject cannot read another object that is in a different data set.

Formally, the policy restricts access according to the following two properties:

(Chinese Wall) Simple Security Rule: A subject *s* can be granted access to an object *o* only if the object:

- is in the same company datasets as the objects already accessed by *s*, that is, "within the Wall," or
- belongs to an entirely different conflict of interest class.

(Chinese Wall) *-property: Write access is only permitted if:

- access is permitted by the simple security rule, and
- no object can be read which is:
  - in a different company dataset than the one for which write access is requested, and
  - contains unsanitized information.

Harrison-Ruzzo-Ullman (HRU) Model:

Introduced in 1976 by Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman.

The Harrison Ruzzo Ullman Model (HRU) is established to address security concerns related to information flow . Unlike the BLP model which is based on mandatory access control, the HRU model adopts discretionary access control. It utilizes an access matrix to understand permissible actions that subjects (such as users) can perform on objects (such as files).

It is primarily concerned with defining how rights (permissions) change dynamically in a computer system. It ensures that the system remains in a secure state as permissions are altered over time. The HRU model focuses on access control and authorization while addressing the problem of whether security breaches can occur in a system when permissions are modified.

Key Features of the HRU Model

Access Matrix:

The HRU model uses an access matrix to represent permissions.

Rows represent subjects (users or processes).

Columns represent objects (files, databases, etc.).

Entries in the matrix denote the permissions a subject holds over an object (e.g., read, write, execute).

Example: If User A has write access to File 1, the matrix entry would reflect that permission.

Operations on Rights:

Rights (permissions) in the access matrix can change over time. These changes occur through specific commands.

Add: Grant a right to a subject (e.g., give write access to a user).

Remove: Revoke a right from a subject.

Transfer: Transfer rights from one subject to another.

Example: A system may allow a user to grant others read access to a document they own.

Commands:

A command is a sequence of primitive operations (like adding or deleting rights).

The execution of a command depends on the current state of the system.

Example: A command might allow User A to add write access to User B for a specific file only if User A has the necessary ownership.

Cyber Threats- Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc

Cyberspace

India's Cyber Security Policy 2013 defines cyberspace as a complex environment comprising interaction between people, software and services, supported by worldwide distribution of information and communication technology devices and networks. It is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers.

Cyberthreats

Cyberthreats can be disaggregated into four baskets based on the perpetrators and their motives - Cyber Espionage, Cyber Crime, Cyber Terrorism, Cyber Warfare

Cyber Crime/ Cyber Attacks

Cyber-attack is "any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks with an intention

to damage or destroy targeted computer network or system." These attacks can be labeled either as Cyber-campaign, Cyber-warfare or Cyber-terrorism depending upon the context, scale and severity of attacks. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the critical infrastructure of entire nations.

Cyber terrorism

The acts of terrorism related to cyber space or executed using cyber technologies is popularly known as 'cyber terrorism'.

"Cyber terrorism is the convergence of terrorism and cyber space. It means unlawful attacks and threats of attacks against computers, networks, and information stored to intimidate or coerce a government or its people to further political or social objectives. . Further, to qualify as cyber terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear. Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact."

It should be noted here that if they create panic by attacking critical systems/infrastructure, there is no need for it to lead to violence. In fact, such attacks can be more dangerous.

Besides, terrorists also use cyberspace for purposes like planning terrorist attacks, recruiting sympathizers, communication purposes, command and control, spreading propaganda in form of malicious content online for brainwashing, funding purposes etc. It is also used as a new arena for attacks in pursuit of the terrorists' political and social objectives.

Cyber warfare

Cyber warfare is defined as, "The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes." These hostile actions against a computer system or network can take any form. On one hand, it may be conducted with the smallest possible intervention that allows extraction of the information sought without disturbing the normal functioning of a computer system or network. This type of intervention is never noticed by the user and happens on a

continuous basis. Other type may be destructive in nature which alters, disrupts, degrades, or destroy an adversary's computer systems.

Cyber Espionage

Cyber espionage is defined as, "The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization." It is generally associated with intelligence gathering, data theft and, more recently, with analysis of public activity on social networking sites like Facebook and Twitter. These activities could be by criminals, terrorists or nations as part of normal information gathering or security monitoring.

Examples of Cyber Espionage include- 2014 hacking of major US companies to steal trade secrets by Chinese officials; Titan Rain; Moonlight Maze; NSA surveillance Program as revealed by Edward Snowden in USA.

Main Cyber players and their motives

- Cyber Criminals: Seeking commercial gain from hacking banks and financial institutions as well as phishing scams and computer ransomware.
- Phishing is a broad term for cyberattacks that use social engineering to trick victims into paying money, handing over sensitive information, or downloading malware.
- Cyber Terrorists with the mission to penetrate and attack critical assets, and national infrastructure for aims relating to political power and "branding".
- Cyber Espionage: Using stealthy IT malware to penetrate both corporate and military data-servers in order to obtain plans and intelligence.
- Cyber Hacktivists: Groups such as "Anonymous" with political agendas that hack sites and servers to virally communicate the "message" for specific campaigns

Additional Links:

https://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf

Comprehensive Cyber Security Policy

NEED FOR CYBER SECURITY POLICIES

- Cyberattacks can result in significant financial loss, reputational damage, and legal liability.
- Building a comprehensive cybersecurity strategy that covers prevention, detection, response, and recovery is crucial for organizations to protect themselves from cyber threats.
- It blocks unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.

A cybersecurity policy establishes the guidelines for data security activities such as encrypting emails, limiting access to critical systems, and maintaining data integrity. These policies are crucial since cyberattacks and data leaks can be extremely expensive.

Comprehensive password security is crucial to an organization's overall cybersecurity strategy. It plays a vital role in protecting sensitive data, preventing unauthorized access, and mitigating various cyber threats from external actors.

Cybersecurity is the body of technologies, practices, and processes designed to secure devices, networks, information, and programs from attacks, unauthorized access, or damage.
The three goals of a comprehensive security policy are the CIA triad: confidentiality, integrity, and availability, describing a model designed to guide policies for information security within an organization.

A comprehensive security strategy provides a framework for establishing and maintaining policies and procedures that meet legal and regulatory requirements.

A security policy describes information security objectives and strategies of an organization. The basic purpose of a security policy is to protect people and information, set the rules for expected behaviors by users, define, and authorize the consequences of violation.

The most popular cyber security domains include threat intelligence, risk assessment, threat management, and application security.

Comprehensive security, based on critical security studies and an ultimate nature of security, reflects and responds to non-military security threats and challenges, which are defined as risks to people and human existence.

Common layers of protection include endpoint detection and response (EDR), next-generation antivirus, advanced firewalls, network analysis, security incident management, and operation controls.

No single person is responsible for the security of the information. It is the responsibility of the whole to ensure the privacy of the information.