OSI Model: Case Study & Report

Table of Contents

1. OSI model Research

OSI stands for Open Systems Interconnection. It has been developed by ISO – 'International Organization for Standardization ', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

Layers of OSI Model

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

What is the OSI Model?

The OSI Model breaks down network communication into seven layers. These layers are useful for identifying network issues.

The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other.

The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.

What are the 7 layers of the OSI Model?

The seven abstraction layers of the OSI model can be defined as follows, from top to bottom:

7. The application layer

The Application Layer: content requested and returned in required format

This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.

Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

6. The presentation layer

The Presentation Layer: encryption, compression, translation

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand. If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

Finally, the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

5. The session layer

The Session Layer: session of communication

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100-megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

4. The transport layer

The Transport Layer: segment, transport, reassembly

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection does not overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.

Transport layer protocols include the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

3. The network layer

The Network Layer: packets creation, transport, packets assembly

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

Network layer protocols include IP, the Internet Control Message Protocol (ICMP), the Internet Group Message Protocol (IGMP), and the IPsec suite.

2. The data link layer

The Data Link Layer: frame creation, frames sent between networks

The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

1. The physical layer

The Physical Layer: sending cable, bitstream, receiving cable

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

2. Attack vector at each layer of OSI model

1. **Physical Layer:**
    - Physical attacks: Tampering with network cables, cutting or disconnecting wires, or physically damaging networking equipment.
    - Eavesdropping: Unauthorized individuals listening in on network communications by tapping into physical connections.
2. **Data Link Layer:**
    - MAC Address Spoofing: Manipulating the Media Access Control (MAC) address to impersonate another device on the network.
    - ARP (Address Resolution Protocol) Spoofing: Manipulating the ARP cache to associate a false MAC address with an IP address.
    - VLAN Hopping: Exploiting misconfigurations to gain unauthorized access to different Virtual LANs (VLANs).
3. **Network Layer:**
    - IP Spoofing: Forging the source IP address in an IP packet to impersonate another system.
    - Denial of Service (DoS) Attacks: Overloading network resources or services to make them unavailable to legitimate users.
    - Routing Attacks: Manipulating routing tables or protocols to redirect or intercept network traffic.
    - Man-in-the-middle attack: Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message, leaving them vulnerable cause an attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.
4. **Transport Layer:**
    - SYN Flood: Exploiting the TCP three-way handshake by sending a flood of SYN requests, exhausting system resources.
    - Connection Hijacking: Intercepting and taking control of an existing TCP connection.
    - Session Hijacking: Taking over an established session by stealing session tokens or compromising session management mechanisms.
    - Reconnaissance: In the context of cybersecurity, reconnaissance is the practice of discovering and collecting information about a system. One of the most common techniques involved with reconnaissance is port scanning, which sends data to various TCP and UDP (user datagram protocol) ports on a device and evaluates the response. Some common examples of reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering, and internet information queries.
5. **Session Layer:**
    - Session Replay: Capturing and replaying session data to impersonate a legitimate user.
    - Session Fixation: Forcing a user's session ID to a predetermined value, enabling an attacker to hijack the session.
    - Session Hijacking: also known as **cookie hijacking** is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft

of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many websites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

6. **Presentation Layer:**
    - Code Injection: Exploiting vulnerabilities in data formats or parsers to inject malicious code.
    - Malformed Data: Sending malformed or unexpected data to disrupt or crash applications.
7. **Application Layer:**
    - Cross-Site Scripting (XSS): Injecting malicious scripts into web applications to steal sensitive information or perform unauthorized actions.
    - SQL Injection: Exploiting vulnerabilities in database queries to manipulate or extract unauthorized data.

    - Remote Code Execution (RCE): Executing arbitrary code on a target system to gain unauthorized access.

3. Impact on Network Security

OSI layer attacks can have a profound impact on network security, potentially leading to various consequences that affect the confidentiality, integrity, and availability of network resources and services. Understanding the potential impacts of such attacks is essential for organizations to implement robust security measures and mitigate the risks effectively. Here is a comprehensive overview of the impact of OSI layer attacks on network security:

Physical Layer Attack

Attacks targeting the physical layer, such as cable tampering or device manipulation, can have severe consequences. By physically accessing network infrastructure, attackers can intercept, modify, or disrupt data transmissions. This can lead to unauthorized access, data leakage, service interruptions, and compromised network integrity

Data Link Layer Attacks:

Data link layer attacks, like MAC address spoofing or VLAN hopping, can enable attackers to bypass network security controls and gain unauthorized access to network resources. This can result in data breaches, information disclosure, unauthorized system control, or the compromise of network devices.

Network Layer Attacks:

Attacks at the network layer can have a significant impact on network security. IP spoofing attacks, for example, can allow attackers to impersonate trusted IP addresses, bypass access controls, and launch various attacks like DoS attacks, man-in-the-middle attacks, or unauthorized network traversal. These attacks can disrupt network availability, compromise data integrity, and lead to unauthorized access.

Transport Layer Attacks:

The transport layer is responsible for reliable data transfer, and attacks targeting this layer can disrupt communication and compromise security. SYN flood attacks, TCP session hijacking, or UDP flood attacks can overwhelm network resources, causing denial of service, interrupting critical services, or facilitating unauthorized access to systems and applications.

Session Layer Attacks:

Session layer attacks can lead to unauthorized access, data manipulation, or identity theft. Session hijacking, where an attacker takes control of an established session, can compromise the confidentiality and integrity of data, enabling unauthorized actions or access to sensitive information.

Presentation Layer Attacks:

Attacks at the presentation layer can exploit vulnerabilities in data formats, encryption, or compression mechanisms. By bypassing or compromising encryption protocols,

attackers can gain access to sensitive information, modify data, or launch further attacks, compromising the confidentiality and integrity of communications.

Application Layer Attacks:

Application layer attacks are among the most common and damaging. SQL injection, cross-site scripting (XSS), or remote code execution can result in data breaches, compromise of user credentials, unauthorized access, or even complete system compromise. These attacks can lead to financial losses, reputational damage, and significant disruptions to business operations.

The impacts of OSI layer attacks on network security can be far-reaching, including:

Downtime and service disruptions, impacting productivity and revenue generation. Loss or compromise of sensitive data, leading to financial and legal consequences. Unauthorized access to network resources, potentially allowing attackers to gain control over critical systems or launch further attacks. Breach of confidentiality, with sensitive information exposed or intercepted during transmission. Compromise of system integrity, allowing attackers to manipulate data, modify configurations, or disrupt normal operations. Damage to reputation and loss of customer trust due to security incidents and data breaches.

4. Real Life Case Study

Attacks on the OSI Model in the Russia-Ukraine War: A Real Case Study

- **Introduction**

The Russia-Ukraine war witnessed various cyber-attacks targeting critical infrastructure, government systems, and communication networks. This case study focuses on the impact, consequences, and countermeasures for attacks on the Open Systems Interconnection (OSI) model during this conflict.

- **Attack on Physical Layer**

Scenario: Russian hackers target the physical infrastructure supporting Ukraine's communication networks.

- **Impact**

a. Disruption of communication networks, leading to the loss of connectivity between critical systems.

b. Deterioration of military and civilian operations due to the lack of real-time information exchange.

c. Impacted emergency services, hindering disaster response efforts.

- **Consequences**

a. Delayed decision-making processes for defense forces.

b. Public panic and increased vulnerability due to limited access to emergency services.

c. Economic losses resulting from the disruption of businesses relying on internet connectivity.

- **Counter-measures**

a. Enhanced physical security measures for critical infrastructure.

b. Redundant communication channels to ensure alternative connectivity options.

c. Regular security audits and assessments to identify vulnerabilities in the physical layer.

- **Attack on Data Link Later**

Scenario: Ukrainian government networks experience a targeted attack aimed at compromising data integrity and availability.

- **Impact**

a. Manipulation or loss of critical data, affecting decision-making processes.

b. Disruption of government services and databases.

c. Compromised communication channels between military units.

- **Consequences**

a. Compromised military operations due to the dissemination of inaccurate or manipulated information.

b. Reduced public trust in government institutions.

c. Potential leakage of classified information, impacting national security.

- **Counter-measures**

a. Implementation of strong access controls and encryption mechanisms.

b. Regular backups and data redundancy to ensure data availability.

c. Continuous monitoring and intrusion detection systems to detect and mitigate data link layer attacks.

- **Attack on Network Layer:**

Scenario: Russian cyber actors launch a Distributed Denial of Service (DDoS) attack against Ukrainian networks.

- **Impact**

a. Overwhelmed network infrastructure, leading to service degradation or complete unavailability.

b. Limited or no access to critical services and resources.

c. Impacted military operations due to disrupted command and control systems.

- **Consequences**

a. Reduced situational awareness and response capabilities for defense forces.

b. Economic losses for businesses heavily reliant on online services.

c. Increased public frustration and potential social unrest due to restricted access to essential services.

- **Counter-measures**

a. DDoS mitigation solutions to identify and filter malicious traffic.

b. Network traffic monitoring and anomaly detection systems.

c. Collaboration with internet service providers (ISPs) to implement traffic filtering mechanisms.

- **Attack on Transport Layer**

Scenario: Ukrainian financial institutions experience a sophisticated cyber-attack aimed at compromising transactions and customer data.

- **Impact**

a. Disrupted financial services, leading to financial instability and loss of consumer trust.

b. Compromised personal and financial information of individuals and businesses.

c. Potential monetary losses due to fraudulent transactions.

- **Consequences**

a. Economic destabilization and loss of investor confidence.

b. Increased incidents of identity theft and financial fraud.

c. Legal and regulatory implications for financial institutions.

- **Counter-measures**

a. Implementation of secure protocols such as Transport Layer Security (TLS) for encrypted communication.

b. Regular security assessments and vulnerability scanning.

c. Enhanced authentication mechanisms, such as multi-factor authentication, to protect customer accounts.

- **Conclusion**

The Russia-Ukraine war highlighted the significant impact of cyber-attacks targeting the OSI model. The consequences ranged from disrupted critical infrastructure and military operations to economic losses and compromised national security. Implementing robust countermeasures, including physical security measures, encryption protocols, intrusion detection systems, and collaboration with

Here's a real-world example of an attack on each layer of the OSI model, along with its impact, consequences, and countermeasures:

- **Physical Layer Attack:**

Example: The 2008 undersea cable cut incident in the Mediterranean Sea.

Impact: Disruption of international communications, affecting internet connectivity between countries.

Consequences: Economic losses due to disrupted business operations, impacted emergency services, and limited communication.

Countermeasures: Implementing redundant communication channels, regular maintenance and monitoring of physical infrastructure, and diversifying cable routes.

Data Link Layer Attack:

Example: The Stuxnet worm targeting Iran's nuclear facilities.

Impact: Manipulation of critical industrial control systems, specifically programmable logic controllers (PLCs).

Consequences: Damage to equipment, disrupted operations, and potential release of hazardous substances.

Countermeasures: Strong access controls, network segmentation, regular security updates, and intrusion detection systems.

- **Network Layer Attack:**

Example: The Mirai botnet DDoS attack on DynDNS in 2016.

Impact: Overwhelmed network infrastructure, causing major service outages for popular websites.

Consequences: Inaccessible online services, financial losses for businesses, and reduced user trust.

Countermeasures: DDoS mitigation solutions, network traffic monitoring, and collaboration with ISPs for traffic filtering.

Transport Layer Attack:

Example: The Heartbleed vulnerability in OpenSSL.

Impact: Compromised data privacy and security, allowing attackers to steal sensitive information.

Consequences: Data breaches, identity theft, and financial fraud.

Countermeasures: Prompt patching of vulnerable systems, implementation of secure protocols (e.g., TLS), and regular security assessments.

- **Session Layer Attack:**

Example: Session hijacking through unsecured Wi-Fi networks.

Impact: Unauthorized access to user sessions, allowing attackers to impersonate legitimate users.

Consequences: Unauthorized actions, compromised privacy and data integrity.

Countermeasures: Secure session management techniques, such as session tokens and timeouts, strong encryption, and user awareness of secure Wi-Fi usage.

- **Presentation Layer Attack:**

Example: Phishing attacks targeting bank customers through fraudulent emails.

Impact: Compromised user credentials, financial fraud, and unauthorized access to accounts.

Consequences: Monetary losses for individuals and financial institutions, damaged reputation, and loss of customer trust.

Countermeasures: User education on recognizing phishing emails, email filtering, and multi-factor authentication.

- **Application Layer Attack:**

Example: The Equifax data breach in 2017.

Impact: Unauthorized access to personal and financial information of millions of individuals.

Consequences: Identity theft, financial fraud, and legal and regulatory repercussions for the company.

Countermeasures: Regular application security testing, patch management, secure coding practices, and encryption of sensitive data.

These real-world examples demonstrate the impact, consequences, and countermeasures associated with attacks on different layers of the OSI model. Implementing comprehensive security measures at each layer is crucial for protecting critical infrastructure, data, and systems from cyber threats.

5. Mitigation & Strategies

1. Physical Layer

The possible attacks on this layer are

- Interruption of electric signals
- Physical damage of wires
- Natural disasters
- Vandalism • Short circuits

The mitigations for these kinds of interruptions are

- Multiple circuits
- Backup servers
- Wireless connectivity
- Redundant cloud data centers

Example of DOS technique that can be applied at this layer:

Physical destruction, obstruction, manipulation, or malfunction of physical assets.

Impact of DOS attack:

Physical assets will become unresponsive and may need to be repaired to increase availability.

2. Data Link Layer

The possible attacks on this layer are

- Spoofing • DHCP attacks
- DOS New Frontiers in Communication and Intelligent Systems 807
- Broadcasting
- Port stealing
- VLANS or lack of VLANS
- Misconfigured NICs
- Sniffing
- MAC Flooding or cloning
- ARP Spoofing

The mitigations for these attacks are:

- Intrusion Detection system
- Intrusion prevention system
- Port limits
- Static ARP

Example of DOS technique that can be applied at this layer:

MAC flooding - inundates the network switch with data packets.

Impact of DOS attack:

Disrupts the usual sender-to-recipient flow of data - blasting across all ports.

3. **Network Layer**

The possible attacks on this layer are

- IP Address spoofing
- Information gathering
- DDOS attacks
- Packet spoofing

The mitigations are

- Route filters
- Firewall
- Router and switch configurations
- Anti-spoofing filters

Example of DOS technique that can be applied at this layer:

ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth.

Impact of DOS attack:

Network bandwidth and impose extra load on the firewall.

When a network reaches its bandwidth limit, it becomes unable to handle any more traffic and may become unresponsive or even crash. This can lead to disruptions in service, loss of data, and financial losses for businesses and organizations that rely on the network for their operations. Additionally, the extra load on the firewall can cause it to slow down or even crash, allowing malicious traffic to bypass its protections and reach the network.

4. **Transport Layer**

The possible attacks on this layer are

- Reconnaissance
- SYN Flood
- Smurf Attack

The possible attacks on this layer are

- Reconnaissance
- SYN Flood
- Smurf Attack

The mitigations for these kinds of attacks are

- Limiting accessibility
- Locking of ports

- Firewall configuration of incoming requests

Example of DOS technique that can be applied at this layer:

SYN flood: The attacker sends a large number of TCP SYN (synchronization) packets to the target system, with the aim of overwhelming the system's ability to process them.

Smurf attack: The attacker sends a large number of ICMP echo request packets to an intermediate network or device, using the spoofed IP address of the victim as the source address.

Impact of DOS attack:

Reach bandwidth or connection limits of hosts or networking equipment.

When a host or networking equipment reaches its bandwidth or connection limits, it becomes unable to handle any more requests or traffic and may become unresponsive or even crash. This can lead to disruptions in service, loss of data, and financial losses for businesses and organizations that rely on these systems.

The mitigations for these kinds of attacks are

- Limiting accessibility
- Locking of ports
- Firewall configuration of incoming requests

Example of DOS technique that can be applied at this layer:

SYN flood: The attacker sends a large number of TCP SYN (synchronization) packets to the target system, with the aim of overwhelming the system's ability to process them.

Smurf attack: The attacker sends a large number of ICMP echo request packets to an intermediate network or device, using the spoofed IP address of the victim as the source address.

Impact of DOS attack:

Reach bandwidth or connection limits of hosts or networking equipment.

When a host or networking equipment reaches its bandwidth or connection limits, it becomes unable to handle any more requests or traffic and may become unresponsive or even crash. This can lead to disruptions in service, loss of data, and financial losses for businesses and organizations that rely on these systems.

5. **Session Layer**

The attacks that can be performed on this layer are

- Cross-site scripting
- Session hijacking
- Brute force attempts
- Fixation
- Cookie theft
- Side jacking

The mitigations for these attacks are

- Implementing SSL
- Prevent client-side cookie access

- Updating Session key from time to time
- Fix bugs on the application

Example of DOS technique that can be applied at this layer:

Telnet DDos-attacker exploits a flaw in telnet server software running on the switch, rendering Telnet Services unavailable.

Impact of DOS attack:

Prevents administrators from performing switch management functions.

The impact of a DoS attack on switch management functions could be significant. Depending on the severity of the attack, administrators may be unable to access the switch, monitor its performance, or perform maintenance tasks. This can result in degraded network performance, increased downtime, and potential security risks. If an attacker exploits vulnerability in the switch's firmware or software, they may be able to gain unauthorized access to the switch, preventing legitimate administrators from managing it.

6. **Presentation Layer**

The possible threats in this presentation layer are

- Encryption attacks
- SSL Hijacking
- Decryption downgrade attacks
- Man, in the middle attack
- Encoding attacks

The mitigation for this layer is

- Update anti-virus database
- Verify links and sites
- Patch system updates

Example of DOS technique that can be applied at this layer:

Malformed SSL Requests - Inspecting SSL encryption packets as resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server.

Impact of DOS attack:

The affected systems could stop accepting SSL connections or automatically restart.

If the SSL service stops accepting SSL connections, it means that clients trying to connect to the affected system using SSL will be unable to establish a secure connection. This can result in various error messages being displayed on the client side. Depending on the severity of the issue, it may also impact other services or applications that rely on SSL for secure communication.

On the other hand, if the affected system automatically restarts, it could potentially interrupt or terminate any ongoing SSL connections. This could result in data loss or other issues, depending on the nature of the connections and the applications involved.

7. **Application Layer**

The attacks that are possible in this layer are

- Data theft,
- SNMP problems such as buffer overflow or denial of service,
- HTTP Floods,
- Exploits including phishing,
- Trojans,
- Viruses,
- backdoors,
- keyloggers,
- program logic flaws and bugs,
- cross-site scripting,
- SQL injections
- DDOS.

The mitigations for this layer are

- Bug-Free Application
- Access control lists
- Firewalls • Anti-virus
- Zero trust security
- Multi-factor authentication
- Regular sweep for trojans and backdoors
- Failsafe backup system

Example of DOS technique that can be applied at this layer:

PDF GET requests, HTTP Get, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)

Impact of DOS attack:

Resource starvation

When a service exceeds its resource limits, it can lead to resource starvation, which can cause the service to slow down, crash, or stop working altogether. This can have a cascading effect on other services that depend on the affected service, leading to a larger system failure.

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols	Example of Denial of Service Technique at each level	Potential Impact of DoS Attack	Mitigation options for Attack type
Application Layer (7)	Data	Message and packet creation begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the protocols FTP, HTTP, POP3, & SMTP and its device is a gateway.	PDF GET requests, HTTP Get, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero-day and application layers. Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDOS attacks
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the protocols Compression and Encryption.	Malformed SSL Requests -- Inspecting SSL encryption packets as resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server.	The affected systems could stop accepting SSL connections or automatically restart.	offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attack traffic at an application delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host.
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the protocol logon/logoff	Telnet DDos-attacker exploits a flaw in telnet server software running on the switch, rendering Telnet Services unavailable.	Prevents administrator from performing switch management functions.	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability. You can implement appropriate security measures, such as firewalls, intrusion detection systems, and access controls.
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the protocols TCP and UDP	SYN flood, Smurf attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking commonly referred to as blackholing is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Blocking holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted services.
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the protocols IP, ICMP, ARP, & RIP and uses routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's	Network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the protocols 802.3 & 802.5 and its devices are NICs, switches bridges & WAPs	MAC flooding - inundates the network switch with data packets	Disrupts the usual sender-to-recipient flow of data - blasting across all ports	Many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization, and accounting (AAA) server and subsequently filtered.
Physical (1)	Bits	Includes but not limited to cables, jacks and hubs	Uses the protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets.	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

6. Recommendation for defending against attack

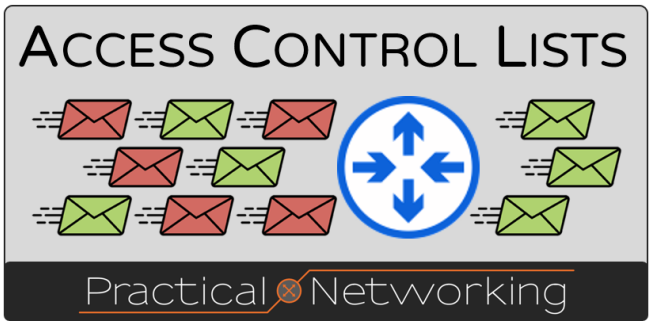
1. Application Layer

- **Bug-Free Application:**

A bug in a mobile application refers to a defect in the software that causes the app to behave unexpectedly. Bugs can range from minor issues, such as visual glitches to major problems that prevent the app from functioning properly.

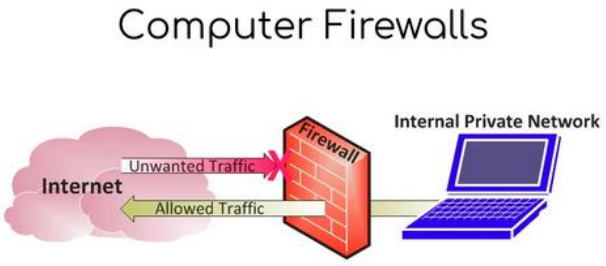
- **Access control lists**

A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors



- **Firewalls**

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules



- **Anti-virus**

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage

- **Zero trust security**

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data

- **Multi-factor authentication**

Multi-factor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint.

- **Regular sweep for trojans and backdoors**

Backdoor malware and viruses circumvent authentication protocols in order to gain access to systems and avoid detection. Once a Trojan has gained a footing in a system, it adds itself to the starting routine of the computer, preventing harmful programs from being permanently terminated by rebooting the machine.

- **Failsafe backup system**

A Fail-Safe is a backup system designed to prevent or allow recovery from a primary system failure. If the primary system fails in some way, well-designed fail-safes can keep the system from collapsing unexpectedly. You can find backup systems anywhere consistent performance is critical

2. Presentation Layer

- **Update anti-virus database**

Antivirus databases contain threat descriptions and methods used to combat them. They eliminate application vulnerabilities, develop the existing functions and add new ones. By default, the update is run every 2 hours.

- **Verify links and sites**

URL Void is a popular link checker tool. It uses blocklist databases and online website reputation services to check unsafe links. Other notable URL checker tools include: Norton Safe Web

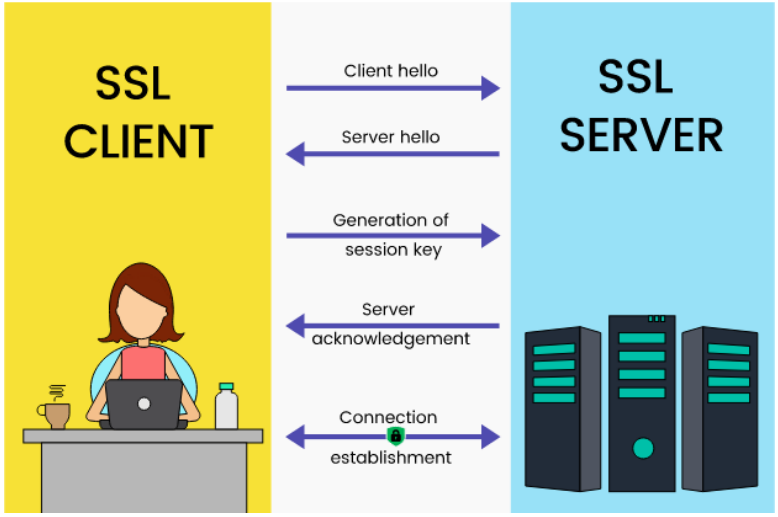
- **Patch system updates**

A patch is a software update for an existing application or operating system to resolve bugs (errors) or vulnerabilities. Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features

3. Session Layer

- **Implementing SSL**

SSL is standard technology for securing an internet connection by encrypting data sent between a website and a browser (or between two servers). It prevents hackers from seeing or stealing any information transferred, including personal or financial data.



- **Prevent client-side cookie access**

Cookies are client-side files that are stored on a local computer and contain user information. Sessions are server-side files that store user information. Expiry. Cookies expire after the user specified lifetime. The session ends when the user closes the browser or logs out of the program.

- **Updating Session key from time to time**

A session key is an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers. Session keys are sometimes called Symmetric key because the same key is used for both encryption and decryption. By refreshing the page, we can update the session key.

- **Fix bugs on the application**

The elimination of software errors is called bug fixing. A bug fix is the result of a bug removal, bug fixing is the activity of fixing bugs. What sounds relatively easy in theory is often a challenge in the practice of software development. Before a bug fix can be implemented, a bug must be identified and located. The process of finding and correcting bugs is termed "debugging" and often uses formal techniques or tools to pinpoint bugs.

4. Transport Layer

- **Limiting accessibility**

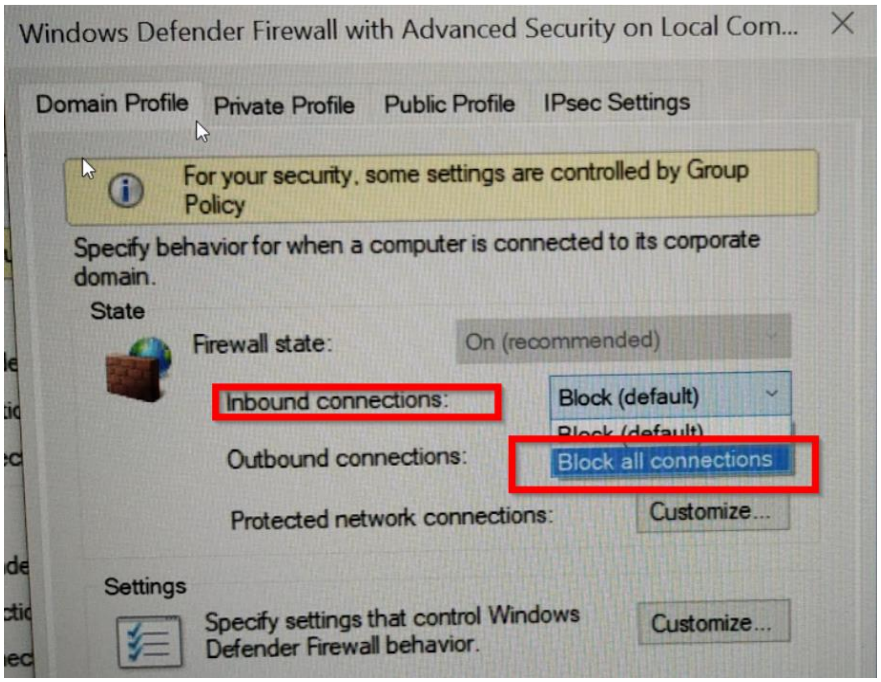
Accessibility is the measure of the capacity of a location to be reached from, or to be reached by, different locations. Therefore, the capacity and the arrangement of transport infrastructure are key elements in the determination of accessibility. It is safe to say that accessibility benefits all members of society including people with disabilities. Improving accessibility brings about increased quality of life; creates more independence and better social integration. It also leads to better health and can result in cost saving in a number of areas.

- **Locking of ports**

Data moves around the internet through ports. When a port is blocked, data can't move through it. There are certain ports that aren't necessary for everyday internet use, but they are commonly used for network attacks. Blocking these ports helps to protect our users from security threats.

- **Firewall configuration of incoming requests**

To block outbound network traffic on a specified TCP or UDP port number, use the Windows Defender Firewall with Advanced Security node in the Group Policy Management console to create firewall rules. This type of rule blocks any outbound network traffic that matches the specified TCP or UDP port numbers



5. Network Layer

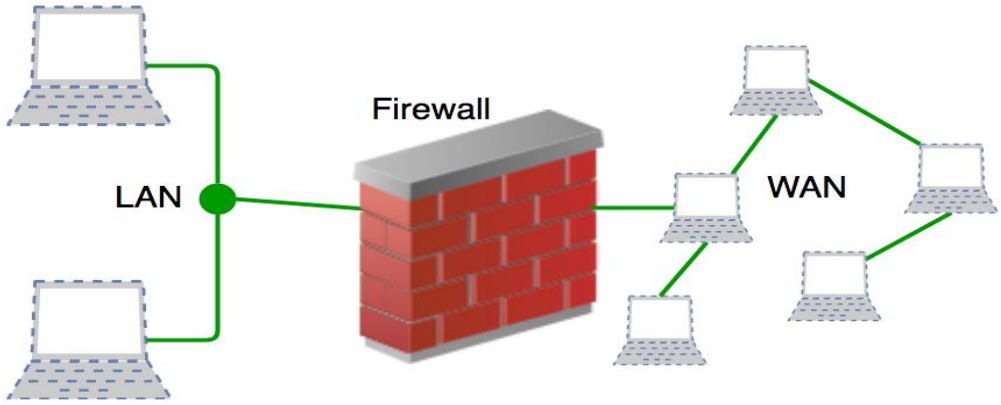
- **Route filters**

Route filtering is a method for selectively identifying routes that are advertised or received from neighbor routers. Route filtering may be used to manipulate traffic flows, reduce memory utilization, or to improve security. For example, it is common for ISPs to deploy route filters on BGP peering's to customers.

- **Firewall**

Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies — any other traffic attempting to access the network is blocked.

The network layer firewall works as a packet filter. Packet filtering: Packet filtering is a security tool that may be used to monitor network access by monitoring both incoming and outgoing packets, as well as preventing packets depending on the source and destination IP address protocols



- **Router and switch configurations**

Router configuration: Specifies the correct IP addresses and route settings, etc. Host configuration: Sets up a network connection on a host computer/laptop by logging the default network settings, such as IP addressing, proxy, network name and ID/password, to enable network connection and communication

switch configurations: Basic switch configuration can be thought of as the minimum network, port, and security provisioning required for the production deployment of a switch.

- **Anti-spoofing filters**

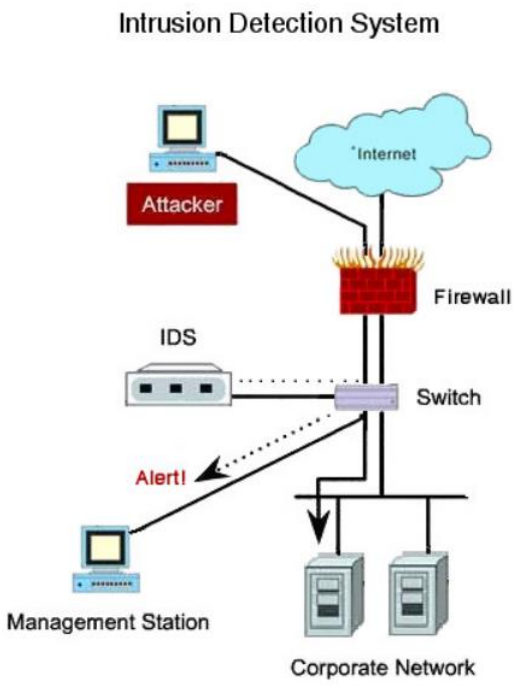
Anti-Spoofing is a technique for identifying and dropping packets that have a false source address. In a spoofing attack, the source address of an incoming packet is changed to make it appear as if it is coming from a known trusted source.

Thus, investing in anti-spoofing technology is extremely important if you deploy biometrics for verification purposes. It ensures only an authorized live person is trying to access a system and not a bad actor using 2D or 3D representations

6. Data Link Layer

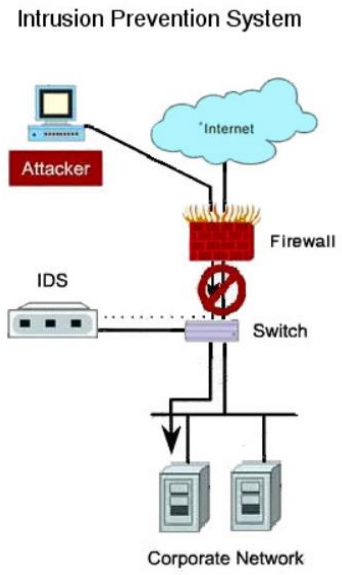
- **Intrusion Detection system**

An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected. Based upon these alerts, a security operations center (SOC) analyst or incident responder can investigate the issue and take the appropriate actions to remediate the threat.



- **Intrusion prevention system**

An intrusion prevention system (IPS) is a network security tool that continuously monitors a network for malicious activity and acts to prevent it, including reporting, blocking, or dropping it, when it does occur. An intrusion prevention system is placed inline, in the flow of network traffic between the source and destination, and usually sits just behind the firewall.

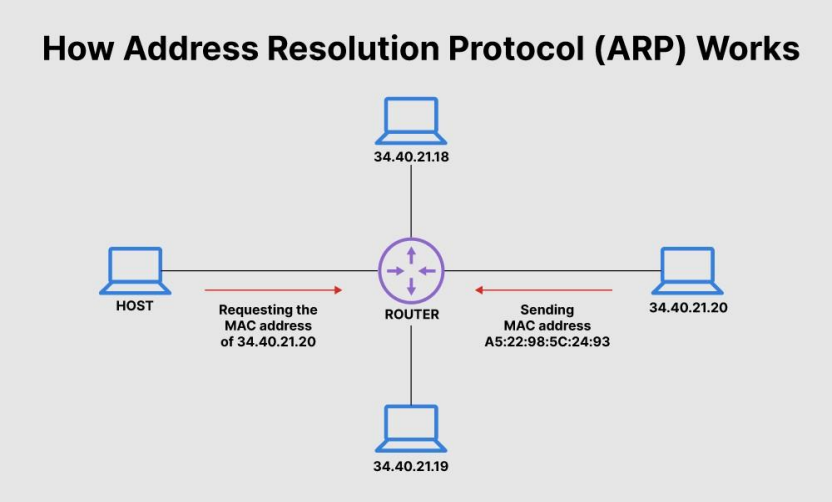


- **Port limits**

The highest TCP port number is 65,535. The TCP protocol provides 16 bits for the port number, and this is interpreted as an unsigned integer; all values are valid, apart from 0, and so the largest port number is (2^16 - 1) or 65,535.

- **Static ARP**

The Static Address Resolution Protocol (ARP) is used for mapping IP network address to the hardware MAC address of a device. entries are address resolutions that are manually added to the cache table for a device and are retained in the cache on a permanent basis. Static ARP entries protect communication between devices, because attack packets cannot modify the IP-to-MAC mapping in a static ARP entry. Static ARP entries can be long or short.



7. Physical Layer

- **Multiple circuits**

The physical layer defines the relationship between a device and a transmission medium, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.

- **Backup servers**

A backup server is a remote or in-house server responsible for storing and retrieving files, folders, applications, databases, and other critical data. It utilizes hardware and software capacities to prevent the loss of data caused by error, hard drive failure or other unwanted scenarios.

- **Wireless connectivity**

Multipath wireless communications produce channels that vary as a function of frequency, time, and space. This physical layer of variability is what makes reliable communication over wireless multipath channels more difficult to achieve.

Increased efficiency. Improved data communications lead to faster transfer of information within businesses and between partners and customers.

- Access and availability.
- Flexibility
- Cost savings
- New opportunities
- Security
- Installation problems
- Coverage

- **Redundant cloud data centers**

Redundancy is important in measuring data center reliability, performance and availability, as are many additional elements. The Uptime Institute offers a tiered classification system that certifies data centers according to four different levels: Level 1, Level 2, Level 3 and Level 4.

- TIER I: Dedicated Infrastructure. 99.671% uptime.
- TIER II: Redundant Infrastructure. 99.741% uptime.
- TIER III: Fully Fault-Tolerant. 99.982% uptime.
- TIER IV: Fully Fault-Tolerant. 99.995% uptime.

8. Git-Hub Repository

GitHub is a web-based platform and a version control system used for hosting and collaborating on software development projects. It provides a cloud-based repository for storing and managing source code, allowing developers to work together on projects and track changes over time.

The references & paper of Team Limonium is present in the following GitHub repository

https://github.com/kisu27/Team-Limonium