ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS

Original Research Article

A STUDY OF CYBER SECURITY THREATS IN THE OSI-REFERENCE MODEL

Ms. Shubhangi Mohan Ingole

Assistant Professor, Pragati College Of Arts & Commerce College in Dombivli, Maharashtra,
Email: ingoleshubhangi61@gmail.com

Abstract :

In this paper, I review the role of OSI-Model. This paper examines the problem of cybersecurity threats that are implemented on networks . OSI-Model 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 all around the world. networks as being structured in the seven layers of the ISO-OSI model, it makes sense that cybersecurity threats can happen at any layer. We can think of these layers as the "links" in our metaphorical chain. Moving outward from the user, data is entered into the network through software running on the Application layer. Through the Session, Transport, Network, and Data-Link layers and arriving at the other end, the Physical layer, the data travels back up the seven layers to arrive at its intended destination. Each layer has its own protocols and other communication standards that govern its efficient operation. Each instance of osi Model provides services that use an instance directly. To provide the service itself uses an instance of the next lower instance.

Key words: *ISO-International Standard Organization, OSI-Open System Interconnection,Seven Layers Protocol, Cyber Security Attack, Cyber Security Threats*

Introduction :

OSI stands for Open Systems Interconnection. It was developed by ISO – 'International Organization of Standardization', in 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. Cyber Security plays an important role in the field of information technology. Securing the information has become one of the biggest Challenges in the present day. Whenever we think about cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes.

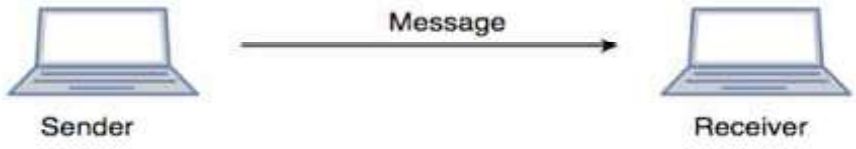
ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS

Original Research Article



Today man is able to send and receive any form of data, be it an e-mail or an audio or video just by the click of a button but did he ever think how securely his data is being transmitted to the other person . In today's technical environment many latest technologies are changing the face of mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 80 percent of total commercial transactions are done online, so this field requires a high quality of security for transparent and best transactions. Hence cyber security has become the latest issue.

Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security. Making the Internet safer has become integral to the development of new services as well as governmental policy. Benefits of the osi model by separating the network communications into logical smaller pieces, the OSI model simplifies how network protocols are designed.

The OSI model was designed to ensure different types of equipment would all be compatible even if built by different manufacturers.

The OSI model has many benefits which include:

a. Compatibility: The OSI model can fit any compatible software/hardware from different users in other parts of the world. As software/hardware differs among various users so OSI is a model that is compatible to all.
b. Easy Troubleshooting: Since each layer in an OSI is independent of each other it makes it easier to detect and solve all errors prevailing in it.
C. Security: OSI models have functionality for Encryption and Decryption which has a major.

Literature Reviews :

OSI is a standard description or a reference model for defining how messages should be transmitted between any two points in a telecommunication network. Cybersecurity professionals define where the network is and they will point at "the wires in the walls." What they are saying is that the copper and fiber-optic cables that connect everything together create the actual network that everything else uses. According to Network World, "Many businesses use Transport Layer Security (TLS) to secure all communications between their Web servers and browsers regardless of whether sensitive data is being transmitted.

Objectives :

To understand the osi model .
How secure is data transmitted ?
Where is the Security layer?

ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS

Original Research Article

Main Body of Research : Osi Layers Model :

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

1. Physical Layer (Layer 1) : The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
2. Emotet: Emotet as "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware."
3. Denial of Service: A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS. A botnet is a type of DDoS in which millions of systems can be infected with malware and controlled by a hacker. Botnets, sometimes called zombie systems, Botnets are in different geographic locations and hard to trace.
4. Man in the Middle:A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.
5. Phishing: Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. "The goal is to steal sensitive data like credit card and login information," Cisco reports.
6. SQL Injection:A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website

ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS Original Research Article

7. Password Attacks:With the right password, a cyber attacker has access to a wealth of information."a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices." Other types of password attacks include accessing a password database or outright guessing.
8. Types of Cyber Security Threats : A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber attackers can use an individual's or a company's sensitive data to steal information or gain access to their financial accounts, among other potentially damaging actions, which is why cyber security professionals are essential for keeping private data protected. Cyber security professionals should have an in-depth understanding of the following types of cyber security threats. Such as below

1. Malware: Malware is malicious software. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software. Cisco reports that malware, once activated, can:
   Covertly obtain information by transmitting data from the hard drive
   Block access to key network components.
   Install additional harmful software
2. Emotet: Emotet as "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware."
3. Denial of Service: A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS. A botnet is a type of DDoS in which millions of systems can be infected with malware and controlled by a hacker. Botnets, sometimes called zombie systems, Botnets are in different geographic locations and hard to trace.
4. Man in the Middle:A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.
5. Phishing: Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. "The goal is to steal sensitive data like credit card and login information," Cisco reports.
6. SQL Injection:A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website
7. Password Attacks:With the right password, a cyber attacker has access to a wealth of information."a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking

ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS Original Research Article

standard security practices." Other types of password attacks include accessing a password database or outright guessing.

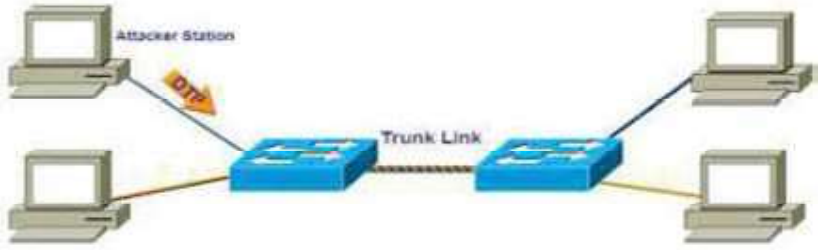
Cybersecurity Threats Exist At All OSI Layers Model :

Physical Layer Threats:

Most threats at this layer involve interruption of the electrical signals that travel between network nodes including the physical cutting of cables, natural disasters that bring flood waters which can cause short-circuits. The aftermath of many disasters illustrates the superior strategy being the placement of all network core elements such as servers and storage at multiple redundant cloud data centers. Should a major carrier cable be cut, only users will be affected, and they can switch to wireless access or other locations until repairs are completed

Data-Link Layer Threats:

"The data link layer provides reliable transit of data across a physical link. The data link layer is concerned with physical, as opposed to logical addressing, network topology, network access, error notification, and flow control. Frame-level exploits and vulnerabilities include sniffing, spoofing, broadcast storms, and insecure.Network interface cards (NICs) that are misconfigured can cause serious problems on the entire network."Most companies that have experienced Address Resolution Protocol (ARP) spoofing, Media Access Control (MAC) flooding or cloning, Dynamic Host Configuration Protocol (DHCP) Attacks, Denial of Service Attacks have immediately focused on improving port security. They also configure their switches to limit the ports that can respond to DHCP requests, implement static ARP and install Intrusion Detection Systems (IDS).



Network Layer Threats :

Network layer threats are generally router-related, including information gathering, sniffing, spoofing, and distributed denial of service (DDoS) attacks in which multiple hosts are enlisted to bombard a target router with requests to the point where it gets overloaded and cannot accept genuine requests.The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations. At the router itself it is important to constantly assure that the router operating system is up to date on all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled

ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS Original Research Article

Transport Layer Threats :

TLS is a cryptography protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP."

Session Layer Threats :

D Dos-attackers exploit a flaw in a Telnet server running on the switch, rendering Telnet services unavailable. In the regular maintenance portion of your plan be sure to remind operators to check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability.

presentation layer threats :

The most prevalent threats at this layer are malformed SSL requests. Knowing that inspecting SSL encryption packets is resource intensive, attackers use SSL to tunnel HTTP attacks to target the server. Include in your mitigation plans options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure.

Application Layer Threats :

The application layer is the hardest to defend. The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world. For the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS)."

Limitation of Study :

Technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively.
Every individual must also be trained on this cybersecurity and save themselves from these increasing cyber crimes.

Conclusion :

In this paper I have tried to explain what exactly an OSI reference model is, why it is used and contribution of various researchers in this reference. OSI is basically an architecture which only gives us an idea how packets transfer over the network during any communication. OSI enhancements are done from time to time for developing new technologies Proposed seven different layers in his paper for improvising security in any network. Future implementation in OSI will lead to enhancement in security and many other fields.

ISSN-2278-5655

AMIERJ Aarhat Multidisciplinary International Education Research Journal

Volume–XI, Issue No.–II
Mar – April 2022

OPEN ACCESS Original Research Article

Reference :

1. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
2. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
3. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole .
4. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

Cite This Article:

Ms. Shubhangi Mohan Ingole, (2022). *A study of cyber security threats in the osi-reference model. Aarhat Multidisciplinary International Education Research Journal, XI (II),273-279*