International Journal of Computer Networks and Communications Security

VOL. 5, NO. 5, MAY 2017, 96–104
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Security issues in Protocols of TCP/IP Model at Layers Level

Albandari Mishal Alotaibi[1], Bedour Fahaad Alrashidi[2], Samina Naz[3] and Zahida Parveen[4]

[1, 2, 3, 4] University of Hail, Department of Computer Science, Hail, Saudi Arabia

[1]a.alotebe@uoh.edu.sa, [2]b.alrashidi @uoh.edu.sa, [3]s.naz@uoh.edu.sa, [4]z.mali@uoh.edu.sa

ABSTRACT

It is widely recognized that data security has become of critical importance for most organizations. This paper gives an overview of the security issues in the Transmission Control Protocol (TCP)/Internet Protocol (IP) model, specifically the protocol of each layer. The paper defines the functionality of each layer in TCP/IP model within the popular protocol for each. Then it investigates each protocol attack by covering their purposes and how they work. Overall, the objective of this research is to conclude which layer and protocol have become the biggest issues in TCP/IP layers.

Keywords: *Network Security, TCP/IP Models, Security Threats, Data Protection, Internet Protocol, Flood*.

1 INTRODUCTION

Computer network technology is developing rapidly. A computer network, or simply a network, is a collection of connected computing devices to share information and/or recourses. Network security is a main issue in computing because different kinds of attacks are increasing daily. With the development and popularization of Internet application technology, network security needs to be paid more and more attention.

Network security covers all phases associated with the security of the sensitive information resources present on the network. It deals with all the measures to protect data throughout their transmission. The specific goals of network security are confidentiality, integrity and availability. To formalize and maintain the secure and well-organized network, abundant research has been devoted to offer a sophisticated methodology for data communication. The TCP/IP model is not same as the OSI model, which is a seven-layered standard, whereas TCP/IP is a four-layered standard. The model has been influential in the growth and development of TCP/IP standard, and that is why much of OSI terminology is applied to TCP/IP. The TCP/IP reference model that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

One formal system that has been present as a conceptual model is the TCP/IP Protocol Suite that was formed in 1980 as an internetworking solution with only slight concern for protection aspects. That is the reason that serious security faults are in the TCP/IP protocol, despite its implementation. TCP/IP model is divided into four layers and each layer works using a variety of protocols with specific functions. The lower protocols have flaws with open possibilities for attacks on the security of data exchange.

This paper provides a review of all the layers, particular protocols and the security issues at each protocol. The review paper is organized as follows. Section 2 describes the structure of TCP/IP model, explaining different layers, functions of each layer with related protocols. Security issues in each layer at the protocol level are discussed in Section 3. The findings of this study are concluded in Section 4.

2 TCP/IP MODEL

The TCP/IP Protocol Suite is a group of different communication protocols working through the Internet and other private communication networks, and it carries most of the essential services running over the network. It provides end-to-end connectivity by establishing, maintaining, and releasing connections between the sender and receiver. It provides for flow control, error control, IP addressing and the routing of network traffic and an interface between the node and the physical network [1].

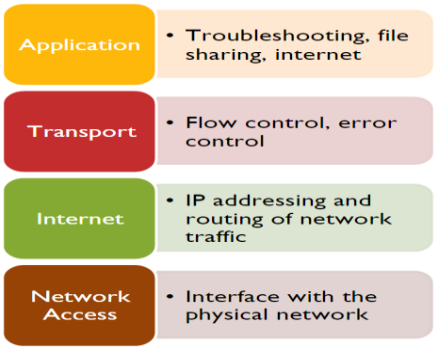


Fig. 1. The OSI Model and the TCP/IP Protocol Suite by Roland Shepherd [1]

The layers with their protocols and functions are described below.

2.1 Application Layer

The application layer is the uppermost layer of the four-layer TCP/IP model and it merges the three most significant layers of the OSI model: application, presentation and session. This layer is primarily concerned with human interaction and how software applications are implemented. The application layer consists of interface methods and underlying communication protocols that can be applied in process-to-process communications. It standardizes communication and does not define specific rules or data formats that applications need to consider when connecting; the original description does depend on and recommend the general design guideline for software [2].

The application layer is concerned with providing network services to applications. It provides a mechanism to the next level, transport services, for interfacing with host programs for efficient use of network. At this layer each application's path and session can be distinguished by the use of specific sockets and port numbers [3]. Application layer includes all the higher-level protocols like:

- **Hypertext Transfer Protocol (HTTP):** The HTTP protocol enables the connection between a web server and a client and also distributes the information on the World Wide Web (WWW). It uses port number 80.On server side, the main examples are Apache Web Server and Internet Information Server (IIS), while on client sideFirefox, Internet Explorer, Mozilla and Google Chrome are most common.
- **Simple Mail Transfer Protocol (SMTP):** SMTP is the only standard for electronic mail (E-mail) over the TCP/IP network; it handles the message services by the use of well-known port 25.
- **Dynamic Host Configuration Protocol (DHCP):** It is used to dynamically (automatically) allocate TCP/IP configuration constraints (DNS server, Subnet Mask, IP address, Default Gateway etc.) to network devices.
- **Domain Name System (DNS):** The IP addresses which are the actual addresses of network recourses are very difficult for the users to remember, DNS is an excellent solution to this problem it contains the distributed database of the mapping records of user-friendly alphanumeric names with that of embedded IP addresses to make network resources easy to remember.
- **Simple Network Management Protocol (SNMP):** This is a popular protocol that allows for remote and local management of network devices such as servers, workstations, hubs, routers, switches and other managed devices.
- **File Transfer Protocol (FTP):** The passive mode protocol used to send and receive large files from remote servers without requiring a "hot" connection established previously.
- **Trivial File Transfer Protocol (TFTP):** This protocol is a simplified version of FTP, especially designs for UDP and resource hungry computers. It contains only a small subset of the capabilities of FTP lacking packet-monitoring and error-handling capabilities, hence the process overhead is lower than FTP.Then again, and these limitations also reduce the process overhead. Security is of evident concern when using TFTP. Examples:
    - Telnet
    - SSH
    - X Windows
    - RDP (Remote Desktop Protocol)

By using applications and application protocols, data can be moved between hosts, and remote users can communicate easily [4].

2.2 Transport Layer

The transport layer is the second layer in TCP/IP model, it is responsible for a flow of data between two hosts (client and server) [5]. It provides end-to-end connections efficiently, offering delivery of data in sequence, avoiding duplication or dropping [6].Two protocols are in this layer, whereas TCP refers to Transmission Control Protocol, UDP refers to User Datagram Protocol. These two protocols are different depending on reliability.

Using TCP ensures high reliability and a special mechanism to make sure that the data reaches the destination completely [7].It provides reliability in the flow of data which has led to ignoring all reliability issues in an application layer. The data is divided into a suitable size to pass to the next layer and then acknowledging messages are sent by a receiver to make sure that the packets are sent.

By contrast, UDP uses a simple mechanism that depends on the lower layer to transmit the data, and upper-layer protocols to make sure the data is transmitted successfully to the required level. It is simple protocol, and the responsibility of this protocol is to send the packet

(datagram) without concern for reliability, which is handled on the application layer. Furthermore, TCP is used by the applications whereas reliability is more important than performance. This can be seen in case of transferring files or important data between two hosts, the application such HTTP, SMTP and FTP use TCP. All messages sent in this protocol are acknowledged, so the reliability is achieved, and lost data will be resent automatically [8].

On the other hand, UDP is used when losing a byte of data will not be a significant effect, and the application layer will be responsible for detecting lost data and retransmitted when the application layer chooses to use UDP. It has been seen in case of small amount of data, and streaming data and video [8].

2.3 Internet Layer

The Internet layer is the third layer in TCP/IP model, and it is equivalent to the network layer in the OSI model. The main function for the Internet layer is to handle communication from one PC to another. This layer is responsible to request and send a packet from the transport layer by knowing to which PC it will be delivered. Moreover, it is more responsible for packing, addressing and routing. The most important protocol in the internet layer is TCP/IP which known as internet protocol .The Internet Protocol is the structure block of the Internet beside the block it's functions are defining the datagram, which is the basic unit of transmission in the Internet, defining the Internet addressing scheme, moving data between the network access layer and the host-to-host transport layer, routing datagram to remote hosts and performing fragmentation and re-assembly of datagram. The Internet software will deeply encapsulate the transport packet in an IP packet. The Internet layer includes four core protocols and it can be listed as:

- **Internet Protocol *(IP):*** The main functions for IP are addressing, routing and transmitting the packets over the network.
- **Address Resolution Protocol *(ARP):*** The main function for APR is the linking and translation from the Internet layer address to the Network Interface layer address such as a MAC address.
- **Internet Control Message Protocol *(ICMP)***: The main function for ICMP is to generate the error message for an unsuccessful delivering message then report it to the source IP address. This is the protocol responsible for detecting network error conditions and reporting on them. Reports include:
  - Dropped packets (when packets are arriving too fast to be processed).
  - Connectivity failure (when a destination host cannot be reached).
  - Redirection (which tells a sending host to use another router).
- **Internet Group Management Protocol (IGMP)** The main function for IGMP is the communication between hosts and multicast routers [9].

2.4 *Network Layer*

The network layer is the fourth layer in the TCP/IP Protocol Suite and is responsible for the host-to-host delivery of datagram [10]. The main liability network layers generate a connection between the source computers to the destination computer. The communication at the network layer is host to host. The network layer is responsible for choosing the best route for each packet, routing packets from source to destination incoming or outgoing a subnet [11]. The network layer focal function is path tenacity and logical addressing. This layer provides logical addresses to the packets received which in turn helps them to find their path.

The key functionality of a network layer is end-to-end routing of packets, from the source computer to the targeted computer, from the use of first to last next-hop-routing approach. For getting point-to-point communication, it supports three features:

• Forwarding:

Forwarding is a packet switching. When a node after communication receives input interfaces through an IP packet, the appropriate output process selecting of an interface to transmit the packet based on the node's packet's destination, routing table and the IP address, it is called forwarding.

• Routing:

The process of the calculating a job from various sources is known as routing, route or the best next hop node. This is for reaching different networks and sub networks' target from a given node and storing it in tables recognized by routing tables [12]. The processes' lists of routing protocols are termed as the control plane or path control, as they control the actual path taken by data packets.

• Logical Addressing (IP Addresses)

The communication over a network with every device must associate with it a logical address. For defining the rules and structure related to IP addresses, the network layer is answerable. Network interfaces of communicating nodes are unique end-point identifiers of IP addresses. On the public Internet, every communicating node needs to have at least one public IP address to communicate successfully with other computers on the Internet.

• Other Features of Networking Layer

For receiving point-to-point communication, it supports three specific features—forwarding, routing and logical addressing —after that network layer also support services like packet fragmentation/ multicasting, reassembly, network layer error reporting (ICMP), broadcasting, IP Security (IPSec), QOS, etc.

Network layer protocols include: Ethernet, FDDI, Token Ring, ATM, OC, HSSI, or even Wi-Fi. The purpose of a network interface is to allow your computer to access the wire, wireless, or fibre optic network infrastructure and send data to other computers.

The network layer offers two types of protocols for delivering the packets over the network.

- Connection-oriented: Connection-oriented services provided by the transport layer for example (TCP) is connection-oriented.
- Connectionless services: In different protocol groups, the network layer protocol is known as a connectionless protocol. For example, in TCP/IP, the IP is connectionless:

Dropped packets (when packets are arriving too fast to be processed)
Connectivity failure (when a destination host cannot be reached)
Redirection (which tells a sending host to use another)[13].

3 SECURITY PROBLEMS IN TCP/IP MODELS PROTOCOL

3.1 Application Protocol

One of the main purposes of an application is the encryption and decryption as a technique for securing the data. The security threat of this layer is at the application level. Applications need to secure sensitive data that is sent to the network, hence applications needs to be well formulated to protect the data. The security vulnerabilities at the two most common protocols of the application layer are being discussed below.

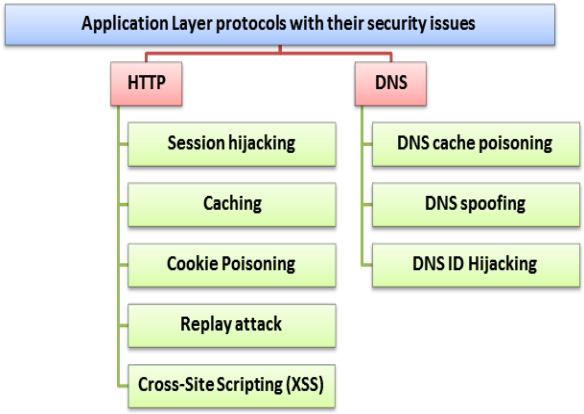


Fig. 2. Application layer protocols with their security issues

3.1.1 Security Threats on HTTP

HTTP is the default communication protocol used by all web browsers. The transfer of files in the form of web pages is done in plain text and therefore is prone to security attacks as listed:

3.1.2 Session hijacking

Hijacking means stealing an HTTP session. A cyber-terrorist usually uses a packet sniffer to capture the packets for stealing the session; hijacking can be possible if in the initialization session strong authentications procedures are not used, opening the way for picking up the session ID or Token ID. Session hijacking provides access to the account as an authentic user and hence attacks the integrity of the target user [14].

3.1.3 Caching

Web browsers temporarily save web pages on a user's machine as he/she visits them to speed up and ease access in case the user wants to visit those pages again. This is known as cashing. The hacker has gained the access of the user's machine and views all the cashed contents of the user that may

contain user IDs, passwords and pictorial data without any authentication.

3.1.4 Cookie Poisoning

Cookies are created by the web servers when a user visits a website. Cookies are used to save credentials and the interaction information of the user with the website, which the web server can use later when processing the sessions of that particular user [15]. Cookie poisoning is the alteration or stealing of cookie in a user's machine by a hacker to reprieve personal information. If the hacker gets a hold of a cookie containing a password and username, he or she can use the cookie on his or her machine and the web server will not demand any verification.

3.1.5 Replay attack

A replay attack is made possible by man in middle. By repeating the sent data to the server, it is a more serious threat than session hijacking. The resent data can be altered and hence producing wrong or totally different results. More critically, the attacker can take off the client's IP address and thus redirect his/her machine [16].

3.1.6 Cross-Site Scripting (XSS)

This attack involves the hacker inserting malicious code in a web application or browser and is executed on the client side. The essence of this attack is to perform a session hijack by stealing session tokens and cookies of a genuine user's session.

3.1.7 Domain Name System

The domain name system (DNS) is used to translate domain names to IP addresses for the sake of user convenience, as they use alphabetical names. The security issue started in DNS when a hacker changed record to resolve to an incorrect IP address; hackers can direct all traffic for a site to the wrong server or client computer. The most common security attacks for this protocol are:

3.1.8 DNS cache poisoning

Caching poisoning through DNS is a reliability attack that involves modifying the information saved in the DNS cache. This fabricated information will map the name to a wrong IP address and mislead the request to a false site[17]. This attack can lead to pharming or phishing. The most critical situation can occur if the user does not notice anything and enters a user name and password. The hacker then can take the user's credentials for misuse.

3.1.9 DNS spoofing

A DNS spoofing attack uses a fake IP address of a computer to match the DNS server's IP address. The user request then will be directed to the hacker's machine. In this attack, the clients and other servers will consider the hacker's machine to be a genuine DNS server and send their requests and receive the reply from the wrong server.

3.1.10 DNS ID Hijacking

The most common method for DNS ID hijacking is through installing malware on a user's computer that changes the DNS. This malware changes the default DNS service provider to something that the cybercriminals want. From there, they control user's URL resolutions (DNS lookups), and then they keep on poisoning the DNS cache [18].

3.2 Transport PROTOCOL (TCP)

The main purpose of this layer is that controlling the flow of data between client and server, avoiding repetitions, or omitting part of data. TCP is one of its protocols that concerned with reliability and delivering data completely to the destination. In this part, the most security threats and attacks at this protocol will be discussed.

Fig. 3. Transport layer protocol security issues

3.2.1 TCP "SYN" attack

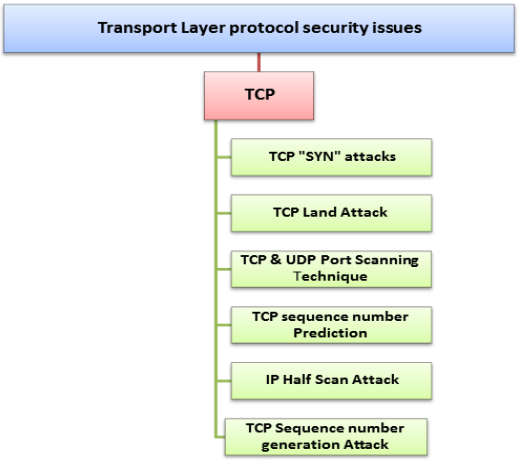
This happens during a three-way handshake between a client and server when the client sends a synchronization request and then the server send back synchronization and acknowledgment and reserve all resources for this request. However, an acknowledgment message will not be sent, which makes half of the connection open, and the attacker sends many synchronous requests to make the server busy without responding to the server [19].

3.2.2 TCP land attack

This attack happens when the attacker pretends to be an authorized person by spoofing the source IP address, then he or she tries to send a SYN packet to open the TCP post in the server [20].

3.2.3 TCP & UDP port scanning technique

This is an attacker port scanning to find an available port in the machine [20].



3.2.4 TCP sequence number prediction

Each packet sent between a client and server has a sequence number. The client and server exchange the sequence number, which has limited boundaries. In this case, an attacker predicts a sequence number counterfeit packet to pretend to be an authorized person, and tries to send these packets after spoofing the IP victim [21].

3.2.5 IP half scan attack

SYN-scanner, or IP half scanning, occurs in a three-way handshake when the TCP connection is never established, when the client sendsthe SYN packet, and waits for a SYN/ACK or rest from the server to determine the open post. When the SYK/ACK received from the server, the client will send a rest which destroys the connection [22].

3.2.6 TCP sequence number generation attack

The most crucial part in TCP segment is sequence number which is helpful in tracking the data, every data sent has sequence number which is exchange between server and client at the beginning of the connection, the sequence number must be within bound which is called receiver window size, any segment out of this bound will be discarded.

One of the security issues is predicating sequence number without receiving any response from the server, which gives the attacker an opportunity to spoof the trusted host in the lock network [22].

3.3 Internet Protocol

The Internet layer mostly depends on the communications between the nodes and deals with secure nodes from sources to destinations. Common attacks for the Internet layer can be in the categories of: denial of service (DoS), disclosure, modification, destructive and escalation of privilege [23].

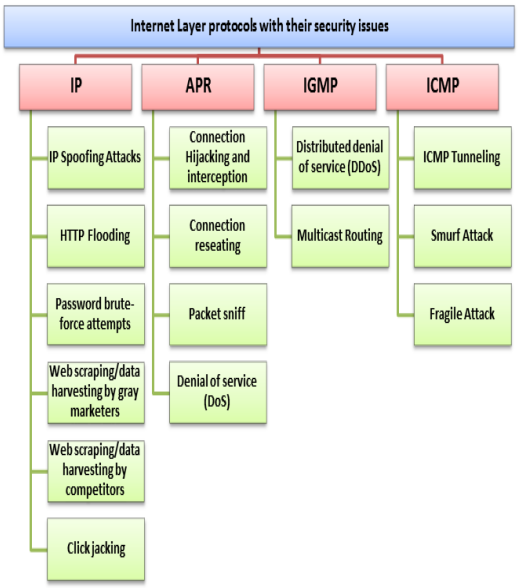


Fig. 4. Internet layer protocols with their security issues

3.3.1 IP

3.3.1.1 IP Spoofing Attacks

The purpose for this attack is to hide the identity for the IP sender. As a result, it will generate the wrong source IP address. There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target's IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target's IP address, all responses to the spoofed packets will be sent to (and flood) the target's IP address.

3.3.1.2 .HTTP flooding

This technique involves full-page reloads of dynamic content, fetching large elements and by passing the cache. It is also known as a DoS, which happens when a large number of routing messages are flooding into the server via network, then as a result the server will be weighted and led toa DoS.

3.3.1.3 Password brute-force attempts

This attack mostly happens in HTTP and FTP.For each simultaneous client it is issues one request for each IP then it will return back with generating 100 password attempts.

3.3.1.4 Web scraping/data harvesting by grey marketers

The aim of this attack is to extract the data from websites by scraping interfaces or software. It targets an online site that supports buying or selling.

3.3.1.5 Web scraping/data harvesting by competitors

This is similar to the above-mentioned attack with the difference being that this attack is executed to collect competitive pricing and plagiarize content.

3.3.1.6 Click jacking(split the sentence)

Also known as user interface (UI) redressing, this is an attack that traps a web client into clicking a catch, a connection or a photo, that the web client did not plan to click, normally by overlaying the site page with an iframe.[24]

3.3.2 APR

3.3.2.1 Connection hijacking and interception

The premise for session hijacking includes a hacker to assume control over a current session between a client and host machine. By assuming control over the legitimate session, the aggressor then abuses or endeavours the session.

3.3.2.2 Connection reseating

This type of attack is made to cut the connection between the user and the server. This can be done by using crafted code and special software.

3.3.2.3 Packet sniff

A packet sniffs the demonstration of catching packets of data flowing over a computer network. The software or device used to do this is known as packet sniffer.

3.3.2.4 Denial of service (DoS)

A DoS attack is among the most widely recognized dangers to Internet operations. These attacks immerse the system transfer speed to make the system occupied to its proposed clients. They include impacting a site with enough movement to surge the associations between the Internet and the business. This attack happens when numerous frameworks flood the bandwidth or resources of a targeted system [25].

3.3.3 IGMP

3.3.3.1 Distributed denial of service (DDoS)

This attack is similar to a DoS attack with the difference being that a DoS attack can be done by using one computer and one internet connection, while in this attack; they use more than one computer and more internet connections.

3.3.3.2 Multicast routing

The effect of an attack in a multicast environment is significantly higher compared to its unicast partner, as a single attacker can influence transmissions to numerous goals at the same time [26].

3.3.4 ICMP

3.3.4.1 ICMP tunnelling

ICMP tunnels are one type of clandestine channel that is made where in the data stream is not controlled by any security component. An ICMP tunnel burrow sets up a channel between the client and server, constraining a firewall not to trigger caution if information are sent via ICMP. ICMP tunnelling is a covert connection between two endpoints using ICMP echo requests and reply packets. So by utilizing ICMP tunnelling, one can infuse discretionary information into an echo packet and send to a remote computer.

3.3.4.2 Smurf Attack

In a Smurf attack, an attacker will spoof the source address of the ICMP packet and send a broadcast to all computers on that network. If networking devices do not filter this traffic, then they will be broadcasted to all computers in the network. This congests the victim's network heavy traffic, which cuts down the profitability of the whole network.

3.3.4.3 Fraggle attack

A fraggle attack is same as a smurf attack, but instead than ICMP, UDP is utilized. The aversion of these attacks is practically indistinguishable to a fraggle attack [27].

4 CONCLUSION

The main goal of the current study has been to provide a review of the TCP/IP model layers' functionalities. The second aim of this study has been to investigate the main attacks and threats in each layer and each protocol within each layer separately.

In the application layers, the main protocols discussed were: HTTP, SMTP, DHCP, DNS ,SNMP, and FTP; in the following layer they were TCP and UDP; and in the Internet layer they were: IP, ARP, ICMP and IGMP.

This study has reviewed 27 papers; the results of this study have indicated the main threats and attacks that have been discussed since 2010. In the application layers, session hijacking, caching, cookie poisoning, replay attack, and XSS in HTTP, and DNS spoofing, DNS ID Hijacking, and DNS cache poisoning in DNS protocol, that are the main attacks and threats discussed. Furthermore, the SYN attack, TCP land attack, TCP/UDP port scanning techniques, IP half scan attack and TCP generation sequence number generation attack were discussed for the transport layer. In the network layer, the attacks (which are according to IP,ARP,ICMP and IGMP) are the spoofing attack, HTTP flooding, password brute-force attempts, click jacking, DoS, web/scraping/data harvesting, connection hijacking and interception, connection reseating, packet sniff, DDoS, multicast routing, smurf attack, and fraggle attack.

These findings enhance our understanding of the TCP/IP security threats and attacks. Moreover, being limited to security threats and attacks, this study lacks solutions and best practices to face the above-mentioned attacks .Further research could be used to explore how the best solutions and practices are used to secure TCP/IP.

5 REFERENCES

[1] The OSI Model and the TCP/IP Protocol Suite by Roland Shepherd
[2] https://tools.ietf.org/html/rfc1123
[3] http://www.omnisecu.com/tcpip/application-layer.php
[4] by Paul Gil Updated November 16, 201 What Is 'Telnet'? What Does Telnet Do?
[5] Fall, Kevin R., and W. Richard Stevens," TCP/IP illustrated", volume 1: The protocols. addison-Wesley, 2011.
[6] Davidson, John. "An introduction to TCP/IP", Springer Science & Business Media, 2012.
[7] Reed, Damon. "Applying the OSI seven layer network model to information security." SANS GIAC GSEC Practical Assignment Version 1.4 b Option One (2003): 8.
[8] Kozierok, Charles M. "The TCP/IP Guide Version 3.0." (2005).
[9] http://www.omnisecu.com/tcpip/internet-layer.php
[10] http://www.omnisecu.com/tcpip/network-access-layer.php
[11] http://www.fidis.net/resources/fidis-deliverables/hightechid/int-d37003/doc/12/
[12] http://www.tcpipguide.com/free/t_IPDatagramSizeMaximumTransmissionUnitMTUFragmentat.htm
[13] https://web.cs.wpi.edu/~cs4514/b98/week4-nl/week4-nl.html
[14] Journal of Computer and Communications, 2016, 4, 39-50 Published Online January 2016 in SciRes. http://www.scirp.org/journal/jcc http://dx.doi.org/10.4236/jcc.2016.41005
[15] Greater Noida ,"Session Hijacking: Threat Analysis and Countermeasure"VineetaJain,DivyaRishi,Dipak Sing Conference: International Conference on Futuristic Trends in Computational analysis and Knowledge management, At amity University, Volume: 1
[16] Vinod Mohan," Product Marketing Specialist Team Lead at SolarWinds with technical expertise in IT management and operations spanning IT security", SIEM, network management, application, systems, storage & Virtualization management.
[17] Emanuel Petr CZ.NIC, "An analysis of the DNS cache poisoning attack", by z.s.p.o., 20 November 2009.
[18] SimarPreet Singh1, A Raman Maini2 ,"Spoofing Attacks of Domain Name System Internet" National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) 2011 Proceedings published in International Journal of Computer Applications® (IJCA).
[19] Alqahtani, Abdullah H., and MohsinIftikhar. "TCP/IP attacks, defenses and security tools." International Journal of Science and Modern Engineering (IJISME) 1.10 (2013).
[20] Rajwal, Deepti, Deepali Band, and AtulYadav. "Study Of Different Attacks On Network & Transport Layer."
[21] Bellovin, Steven M. "Security problems in the TCP/IP protocol suite." ACM SIGCOMM Computer Communication Review 19.2 (1989): 32-48.
[22] Tiwari, Aruna, et al. "TCP/IP Protocol Suite, Attacks, and Security Tools." URl= https://www. academia.

edu/7134687/TCP_IP_Protocol_Suite_Attacks_and_Security_Tools (2014).
[23] https://nsrc.org/workshops/2008/ait-wireless/kemp/network-attacks.pdf
[24] https://security.radware.com/ddos-threats-attacks/ddos-attack-types/dynamic-ip-address-cyber-attacks/
[25] http://www.insecure.in/arp_attack.asp
[26] https://security.radware.com/ddos-threats-attacks/ddos-attack-types/ddos-attacks-on-network-resources/
[27] http://resources.infosecinstitute.com/icmp-attacks/#gref