ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Base of the Networking Protocol – TCP/IP Its Design and Security Aspects

Shreya Gangane, Prof. Vinit Kakade

Student of Master of Engg, Dept. of CSE, Raisoni College of Engg. and Tech., Amravati, India

Assistant Professor, Dept. of CSE, Raisoni College of Engg.and Tech., Amravati, India

ABSTRACT: TCP/IP is very much important alayered protocol in the networking. Each layer builds upon thelayer below it, adding new functionality.The Transmission Control Protocol (TCP) and InternetProtocol (IP) are the two most important communicationprotocols used in computer networking from its evaluation and keeping its importance increasing till date. In this paper wedescribe the evolution and the basic functionality of theTCP\IP protocol suit and all the three basic protocols TCP, IP, UDP used for basic networking functions. In this article we try to provide a brief knowledge of the origin and evolution of TCPand IP, as well as their structure, operational properties andheader format. In spite of usefulness of this very much important networking protocol there are many vulnerabilities and corresponding attacks have been identified targeting TCP/IP protocol suite. The attackincludesIP spoofing attacks, denial of service attacks, DNS Spoofing, Connection hijacking, etc. The Design flaws of TCP/IP can be mitigated by applying some layers of security mechanism in a network.The usefulness of this protocol suitegive rise to various tools have been designed to analyze and identify the presence of such vulnerabilities of exploitation in TCP/IP suite. Some of the defense mechanism of attacks against TCP/IP suite are like firewalls, encryption techniques, intrusion detection systems, protocol analyzers,sniffers and vulnerability scanners,etc are also discussed.

KEYWORDS: TCP/IP protocol suite, OSI model, SYN flooding, IP Address Spoofing, Connection Hijacking, DNS spoofing.

I. INTRODUCTION

The TCP & IP are the two most important protocol for networking which belongs to the Transport Layer in the OSI model an abstraction model for computer communication through networks [1]. The TCP protocol ensures a reliable communication between two hosts on an unreliable network also. And IP provides a service to the communicating application at the other end.This protocol suit is developed for both sociological and technological purposes,from around 1960 the military in collaboration with several different universities in the U.S. started working in the implementation of a global network which purpose wasconnecting different locations working under differentprotocols and share information with several kinds ofstorage systems.

Asthe TCP was declared to be a reliable connection-oriented, end-to-end protocolandit operate on top of the IP protocol we give some basic functionalities of theTCP protocol and how it works along with its layer format. It will perform connection establishment, connection release and proper transfer of data over the network it also provide important services to some other layers and protocols in the networking [3].The header format of all the most important protocols like TCP, IP, UDP are giver in further sections of the paper. Some recent discoveries and implementation about TCPand IP are also given in this paper.

TCP/IP protocol suite is a collection of various communication protocols operating at different layers of OSI model or TCP/IP network layer model over the Internet. This protocol suit is also useful for other private communication networks also. By the emergence of the computer networks, provides us much benefit that is difficult or even impossible to achieve by the traditional networking system, but along with this there are lots of security breaches also born with this increasing use of the networking and sending the data over the internet [4]. The attack that can be happened with this are mentioned in the last section of this paper. We also provides some of the possible solutions to all types of attack we are mention here [12]. By increasing the types of security mechanism we should make our networking model more powerful, useful and use without any hacking problem. Finally, we conclude the paper.

II. LITERATURE SURVEY

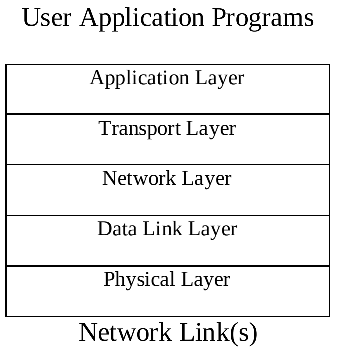
IP was born to cover U.S. Department of Defense'scommunication needs. Last years of the 1960s theAdvanced Research Projects Agency (ARPA), which isknown nowadays as DARPA, was started developing incommon with some partner universities and the corporateresearch community the design of standard protocols andstarted building first multi-vendors networks [2]. ARPANET is the first packetswitching network that was tested in 1969 with four nodesusing Network Control Protocol. After the successful testthe new born network turned into an operational networkcalled ARPA Internet. In 1974 Vinton G.Cerf and RobertE.Kahn designed TCP/IP protocols.In January 1980 the Institute of Information Sciences atUniversity of Southern California elaborated a referencedocument [6] describing the philosophy of the InternetProtocol. It was designed to be used in an environment ofcomputer communication networks oriented to packetswitched systems interconnected between them.

In 1985 ARPANET started suffering from congestion andthe National Science Foundation's developed NSFNET for supporting the previous net which was finally closed in 1989. The NSFNET was based on multiple regional networks andpeer networks such as NASA Science Network. By 1986there was a network architecture connecting campuses andresearch organizations connected also to super computerfacilities. Over the years the speed of transmissions had tobe increased and by 1991 the backbone was moved to aprivate company which started charging for connectionsand companies like IBM developed ANSNET in parallelwhich was nor aimed to enrich these companies.As computer communication became more and moreimportant, especially for the military at past times. It makes torealized that a robust communication standard is needed toreplace the variety of different local network protocols thatwere used. A concept for the TCP was first described in [7]where several issues that would be solved where presented.The TCP was declared to be a reliable connection-oriented,end-to-end protocol. It was meant to operate on top of theIP protocol [5].

III. THE TCP/IP LAYERS

The term "protocol stack" is often used as synonym with "protocol suite" as animplementation of a reference model. However, the protocol suite properlyrefers to a collection of all the protocols that can make up a layer in the referencemodel [4]. TCP/IP reference model is the Internet protocol suite acting as an example of the Internet or, and a TCP/IP protocol stack implements one or more ofthese protocols at each layer.

The TCP/IP protocol stack models a series of protocol layers for networks and systemsthat is useful to allow communications between any types of devices used for communication. This layer model consists of fiveseparate but related layers, as shown in Figure 1 below. These five layers are important as the Internet protocol suite is basedon it. The network and transport layers, and the application layer are most important layers of TCP/IP layered model [15]. These layers defines how to interface the network layerwith the data link and physical layers, but it is also true that this is not directly concerned with these twolayers.The stack consist of communication and networking protocols and not actually the implementations,so by describing a layer or protocols says almost nothing about how these things
That how this actually be built.


User Application Programs

Application Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Network Link(s)

Figure 1.The five layer model of TCP/IP.

Brief description of TCP/IP Layers [14]:

A. Physical Layer:

This layercontains all the functions that are needed to carry the bit stream/packets from source to destination over aphysical medium.Eg. Ethernet, PPP, etc.

B. Data Link Layer:

In this layer the bit stream areorganize into a data units. This data units are also called as “frame” and this frames are delivers to an adjacent system.Eg. WiFi, SLIP, etc.

C. Network Layer:

At this layer, data is converted in the form of packets from source to destination, across as many links as necessary. It can also able to transmit to non-adjacent system.It is responsible for sending and receiving TCP/IPpackets on the network medium. Eg. IP (IPv4, IPv6), ICMP, IGMP, etc.

D. Transport Layer:

This layer is concerned with process-to-process delivery of information.A system can be running file transfer, email, and other network processes all at the same time. This all can be possible over a single physical interface.Eg. TCP, UDP, etc.

E. Application Layer:

Provides applications with the ability to access the services of the other layers. New protocols and services are always being developed in this category and this is concerned with differences in internal representation, userinterfaces, and anything else that the user requires.Eg. HTTP, FTP, SMTP, SSH, POP3, TLS/SSL, DNS, etc.

IV. OVERVIEW OF BASIC NETWORKING PROTOCOL

A. TCP (Transmission Control Protocol):

Transmission Control Protocol is the transport layer protocol used by most Internet applications, like telnet, FTP and HTTP. It is a connection-oriented protocol and provides reliability. As it is reliable protocol, the application that uses it required it to be received correctly. TCP uses checksums on both headers and data. When data is received, TCP sends an acknowledgement back to the sender within a certain timeframe. If it does not receive an acknowledgement then data is resent. TCP sends data using IP, in blocks which are called segments. Each segment contains 20 bytes of header information with IP header [15]. The TCP header starts with 16-bit source and destination portnumber fields, these fields specify the application layers that have sent and are to receive the data.

<table>
<tr><td colspan="3"><b>source port number</b></td><td><b>destination port number</b></td></tr>
<tr><td colspan="4"><b>sequence number</b></td></tr>
<tr><td colspan="4"><b>acknowledge number</b></td></tr>
<tr><td><b>head er</b></td><td><b>reser ved</b></td><td><b>urg,ack ,psh,rst ,syn,fin</b></td><td><b>window size</b></td></tr>
<tr><td colspan="3"><b>TCP checksum</b></td><td><b>urgent pointer</b></td></tr>
<tr><td colspan="4"><b>options (if any)</b></td></tr>
<tr><td colspan="4"><b>data (if any)</b></td></tr>
</table>

Figure 2. TCP Header Format

B. IP (Internet Protocol):

IP is the vital important protocol ofTCP/IP reference model for transmitting data over the network. Every messages and pieces of data packets are sent over any TCP/IPnetwork is sent through as an IP packet.The name: internet protocol is given to this protocol is as to enable data to be transmittedacross and between networks.

Features of IP protocol includes, as it is a connectionless protocol, it has no concept of a job ora session. Each packet is treated as single or unique in itself. Its working is like postal working of sorting letters. This protocol simply routes packets, oneat a time, to the next location towards the target on its delivery route.IP is not take into account whether a packet reaches its proper destination, or don't check the original order of the packet sent. When the datagram is sending, there is no informationin a packet to identify it as partof a sequence or for a particular task. As IP does not check the any security concern it is an unreliable protocol.

<table>
<tr><td><b>version</b></td><td><b>length</b></td><td><b>type of service</b></td><td colspan="2"><b>total length</b></td></tr>
<tr><td colspan="3"><b>identification</b></td><td><b>flags</b></td><td><b>fragment offset</b></td></tr>
<tr><td colspan="2"><b>time to live</b></td><td><b>protocol</b></td><td colspan="2"><b>header checksum</b></td></tr>
<tr><td colspan="5"><b>source IP address</b></td></tr>
<tr><td colspan="5"><b>destination IP address</b></td></tr>
<tr><td colspan="5"><b>options (if any)</b></td></tr>
<tr><td colspan="5"><b>Data</b></td></tr>
</table>

Figure 3. IP header format

An IP packet consists of the IP header and IP data mainly of 20 bytes as shown in below figure 3 [15]. The header includes a 4-bit protocol version number, length of header, a 16-bit total length, along with some control fields, a header checksum for error checking and the 32-bit source and destination IP addresses. Within IP header, there is some important information available like source IP address, destination IP address, which is important for routing the packet around the network through the internet [8].

C. UDP (User Datagram Protocol):

The User Datagram Protocol is avery simple protocol. Itis an unreliable, connectionless protocol and you do not need to establish a basic functionality of IP. Like an Internet Protocolconnection with host before exchangingdata with UDP. Thereis no mechanism for ensuring that datasent is received properly so it is unreliable. The data sent using UDP iscalled a datagram. UDP adds four 16-bit header fields containing fields like a UDP lengthfield, a checksum field again for error checking, and source and destination port numbers. Portnumber in this context represents only software port. The concept of port numbers iscommon for both UDP and TCP protocol.

<table>
<tr><td><b>source port number</b></td><td><b>destination port number</b></td></tr>
<tr><td><b>UDP length</b></td><td><b>UDP checksum</b></td></tr>
<tr><td colspan="2"><b>Data</b></td></tr>
</table>

Figure 4. UDP Header Format

Although UDP is not reliable, it isstill an appropriate choice for an applications. It is used in real-time applicationslike Net audio and videowhere, if data is lost, it’s better to dowithout it than send it again out ofsequence. It is also used by protocolslike the Simple Network ManagementProtocol (SNMP).

V. SOME ATTACKS ON TCP/IP AND THEIR POSSIBLE DEFENSE METHODS

The distributed nature of computer networks makes it easyfrom potential attack or hackingand on the other hand it is hard to make defense against these methods. Here we are giving some of the possible attack and their defense methods [15].

A. SYN flooding attack

All new TCP connections areestablished by first sending a SYN segment to the remote host,that is, the packet whose SYN flag bit is set [15].SYN flooding is a method that the user of a host client program uses to conduct a denial-of-service (DoS) attack ona computer server.In a SYN flood attack attacker repeatedly sends SYN TCP segments to every porton the server using a fake IP address.The server responds to each such attempt with a SYN+ACK segment from each openport and with an RST segment from each closed port.

In a SYN flood attack, the host client never sends back the expected ACK segment as in a normal three-way handshake, the client would return an ACKsegment for each SYN+ACK segment received from the server [16]. As a connection for a given port gets timedout, another SYN request arrives for the same port from the hostileclient. The intruder has a sort ofperpetual half-open connection with the victim host when a connection for a given port at the server gets into this state of receiving a never-ending stream of SYN segment.

The current firewall product provides some extra functionality, like NAT (Network Address translation) and SYN flooding protector.

B. IP Address Spoofing

The technique of IP address spoofing involves maliciously creating TCP/IP packets using other IP address as source address for either conceal own identity or impersonate the identity of the owner of the IP address used by him [10]. Normally, routers use the IP address of the destination and forward the packet to it on the recipient side he uses the IP address of the source to reply that packet. If in case, the source address is spoofed, the recipient will reply to the spoofed address. In this case, the packet will be hard to be traced back to the attacker. But if attacker will have to sniff the traffic of the spoofed address,if he wants to access the reply also. This behavior of the recipient can be used to launch various types of attacks like:

- Denial of Service Attack (DoS) [13]
- Defeating network security
- Man in The Middle Attack

Following measures can be taken to defense against IP Spoofingattacks [9]:

- Use of encrypted session in router benefits that onlytrusted hosts can communicate securely with the local hosts, as the attackers will not be able to read the encrypted data packets.
- Using Access Control Listone can apply security policy,by configuring to block any traffic coming from outer network with an internal IP address and likewise blocking traffic from internal IPs to go to outside network.By using this technique our IP address is present only inside the network.
- Another technique is filtering packets which blocks the incoming packets not meeting the security policy criteria, like ping requests from outside the network are filtered out. For outgoing packets this method filtered based on the source or destination port/IP address criteria.
- By *i*ncorporating defense mechanisms in upper layers prevents IP spoofing.If in TCP at transport layer if we use sequence numbers then attacker has to guess the sequence number also before spoofing the packet.

C. Connection Hijacking

During the initial stages of the connection setup an authentication between two hosts takes place and afterword's no authentication is required. An attacker can take advantage of this authentication mechanism by sending a reset to the client and killing the connection for the client. Then the attacker spoofs the client and continues session with serverwith spoofed source address [12]. Another way of performing this type of attack is by stealing the cookies stored on that machine or stealing cookies by sniffing the unencrypted network traffic and using these cookies with the web server to establish an authenticated session.

The methods for defensing against Connection Hijacking Attacks are [9]:

- Using the Encryption method one can make the secured the traffic flow as an attacker neither able to read the contents of the packets nor use them for session hijacking.
- Using re-authentication technique*i.e.* after a specified period of time will cause the attacker to lose session after some time even if he initially succeeds,that prevent him from further access.
- For hijacked session not to exploited perpetually,Session timeouts are again a mechanism for enforcing re-authentication after a specified amount of time.

D. DNS spoofing attacks

Domain Name System (DNS) is a service used in application layer of TCP/IP protocol suit for mapping an IP address to a domain name and vice versa [11].By poisoning the DNS cache records to spoof a domain nameand binding it with attacker's IP address, the DNS spoofing attacks are launched. If the client uses domain name to authenticate requests, then it will be compromised.

The methods for defensing against DNS Spoofing attacks are [11]:

- Instead of using domain name based authentication, Use authentication based on IP addresses.
- If Domain Name System(DNS) uses encryption it prevents them from forging easily.

VI. **CONCLUSION**

As seen from the history, one of the giant step with growing use of the internet has been demonstrated that TCP protocol mayevolve into a more flexible to manage all the networking process perfectly. As the digitalization grows the. The complexity of networks evolution also growing in parallel so for proper suiting this situation TCP/IP perform its task of data transfer and all networking activities properly along with the other layers and protocol. We can also say that The TCP/IP suite is the only way tosupport the strong increase of users demand and the fast technological development.Along with this useful features, there are some design flaws of TCP/IP suite of protocols that leads to most of the attacks on the Internet. So, it always requires security to be applied as an external layer to the TCP/IP suite. This paper presents various attacks directed on TCP/IP protocol model like IP and DNS Spoofing and SYN attack.We also provides some of the defense mechanisms to identify the vulnerabilities causing these attacks and ways toreduce them. The attack in networking is always a big issue along with the usefulness of the TCP/IP protocol suite for the same work in the field of the networking and internet architecture and protocol organization.

REFERENCES

[1] TCP/IP Fundamentals [Online] available: http://www.sfisaca.org/download/lam.pdf
[2] TCP/IP Tutorial [Online] available: documentation.netgear.com/reference/sve/tcpip/pdfs/FullManual.pdf
[3] The TCP/IP Reference Model [Online] available:
http://www.mif.vu.lt/~adam/courses/npij/scsu-mcs426-fall-1999-3.pdf.
[4] David Espina, DariuszBaha, "The present and the future of TCP/IP". pdf.
[5] Postel, J. (1981), *Transmission Control Protocol*, RFC793.
[6] University of South California (1980), *DOD StandardInternet Protocol*, RFC 760.
[7] Cerf, V. , and R. Khan, "*A Protocolfor PacketNetwork Intercommunication*" (1974)
[8] W. R. Stevens, *TCP/IP Illustrated Vol. 1 – The Protocols*, Addison-Wesley, 1994.
[9] Bellovin, Steven M. "A look back at." Computer Security Applications Conference, 2004. 20th Annual. IEEE, 2004.
[10] Tanase, Matthew. "IP spoofing: an introduction." Security Focus 11 (2003).
[11] Yan, Boru, et al. "Detection and defence of DNS spoofing attack." JisuanjiGongcheng/ Computer Engineering 32.21 (2006): 130-132.

[12] Abdullah H. Alqahtani, MohsinIftikhar, “TCP/IP Attacks, Defenses and Security Tools”, International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-10, September 2013.
[13] C. Cobb and S. Cobb, “Denial of Service”, *Secure Computing*, pp.58-60, July 1997.
[14] KarnatiHemanth*, TalluriRavikiran**, MaddipatiVenkat Naveen, Thumati Ravi, “Security Problems and Their Defenses in TCP/IP Protocol Suite”, International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012 1 ISSN 2250-3153.
[15] Guang Yang, “Introduction to TCP/IP Network Attacks”, *Department of Computer Science, Iowa State University*, Ames, IA 50011.
[16] AviKak, “TCP/IP Vulnerabilities: IP Spoofing andDenial-of-Service Attacks, *Lecture Notes on “Computer and Network Security”*, March 25, 2015.