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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Review on Security Model for TCP/IP Protocol Suite

Priyanka Pawar [1], Ajay Phulre [2]

P.G. Student, Department of Computer Engineering, SBITM, Betul, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Engineering, SBITM, Betul, Madhya Pradesh, India[2]

ABSTRACT: Mobile Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired", an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. Some history of networking is included, as well as an introduction to TCP/IP and internetworking.

KEYWORDS: Internet, TCP/IP, Security, Protocol

I. INTRODUCTION

The perception of security is traditionally connected to exigencies of defending sensitive data from illegal access. But at the moment network security is often approached from a different perception. With the growing use of the Internet infrastructure for commercial applications, the demand for Quality of service is one of the emerging paradigms in Internet and seems to be the corner stone for more and more network services [1]. An increasing number of applications need multifaceted, consistent control protocols for guaranteeing Quality of service. As an outcome the need for security in network infrastructure is stronger than ever. Internet is based on TCP/IP protocol suite. IP was not planned with security in mind. The severe security flaws of the TCP/IP protocol suite exist since the host relies on IP source address for authentication.

This section reviews temporal relation of network and internet technologies followed by in depth review of the work related to network threats and security. “A network is a conduit for information; it can be as simple as two tin cans tied together with a string or as complicated as the internet” *i\iso1]. Networks can develop at various levels: individual (social network), organizational, inter-organizational, and international etc. Castells explains that a network “is constituted by the intersection of segments of autonomous systems of goals. The evolution of the internet has been widely chronicled. Resulting from a research project that established communications among a handful of geographically distributed systems, the Internet now covers the globe as a vast collection of networks made up of millions of systems. Government corporations, banks, and schools conduct their day-to-day business over the Internet. With such widespread use, the data that resides on and flows across the network varies from banking and securities transactions to medical records, proprietary data, and personal correspondence *95+. The Internet is the “world’s largest collection of networks that reaches universities, government labs, commercial enterprises, and military installations in many countries.

II. TCP/IP ARCHITECTURE OVERVIEW

The TCP/IP protocol suite, as well referred to as the Internet protocol suite, is the set of communications protocols that implements the protocol stack on which the Internet and most commercial networks run. It is named after the two most important protocols in the suite: the Transmission Control Protocol (TCP) and the Internet Protocol (IP). Internet Protocol is the foundation of the TCP/IP protocol suite, since it is the mechanism responsible for delivering datagram’s The TCP/IP protocol suite—like the OSI reference model—is defined as a set of layers.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that are transmitted physically over the network [4]

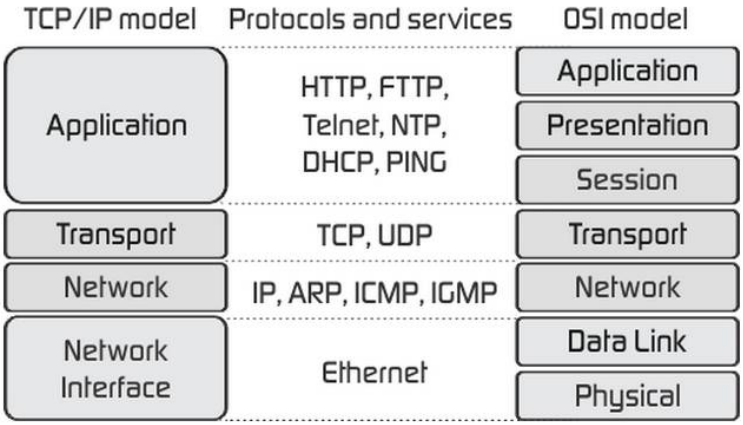

Fig. 1 TCP/IP OSI Model

.

III. TCP/IP : THE LANGUAGE OF INTERNET

TCP/IP (Transport Control Protocol/Internet Protocol) is the ``language'' of the Internet. Anything that can learn to ``speak TCP/IP'' can play on the Internet. This is functionality that occurs at the Network (IP) and Transport (TCP) layers in the ISO/OSI Reference Model. Consequently, a host that has TCP/IP functionality (such as Unix, OS/2, MacOS, or Windows NT) can easily support applications (such as Netscape's Navigator) that uses the network.

1. **Open Design:** One of the most important features of TCP/IP isn't a technological one: The protocol is an ``open'' protocol, and anyone who wishes to implement it may do so freely. Engineers and scientists from all over the world participate in the IETF (Internet Engineering Task Force) working groups that design the protocols that make the Internet work. Their time is typically donated by their companies, and the result is work that benefits everyone.
2. **IP:** As noted, IP is a ``network layer'' protocol. This is the layer that allows the hosts to actually ``talk'' to each other. Such things as carrying datagrams, mapping the Internet address (such as 10.2.3.4) to a physical network address (such as 08:00:69:0a:ca:8f), and routing, which takes care of making sure that all of the devices that have Internet connectivity can find the way to each other.
3. **Understanding IP:** IP has a number of very important features which make it an extremely robust and flexible protocol. For our purposes, though, we're going to focus on the security of IP, or more specifically, the lack thereof.
4. **Attacks Against IP:** A number of attacks against IP are possible. Typically, these exploit the fact that IP does not perform a robust mechanism for authentication , which is proving that a packet came from where it claims it did. A packet simply claims to originate from a given address, and there isn't a way to be sure that the host that sent the packet is telling the truth. This isn't necessarily a weakness, per se , but it is an important point, because it means that the facility of host authentication has to be provided at a higher layer on the ISO/OSI Reference Model. Today, applications that require strong host authentication (such as cryptographic applications) do this at the application layer.
5. **IP Spoofing.:** This is where one host claims to have the IP address of another. Since many systems (such as router access control lists) define which packets may and which packets may not pass based on the sender's IP address, this is a useful technique to an attacker: he can send packets to a host, perhaps causing it to take some sort of action.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

6. **IP Session Hijacking:** This is a relatively sophisticated attack, first described by Steve Bellovin [3]. This is very dangerous, however, because there are now toolkits available in the underground community that allow otherwise unskilled bad-guy-wannabes to perpetrate this attack. IP Session Hijacking is an attack whereby a user's session is taken over, being in the control of the attacker. If the user was in the middle of email, the attacker is looking at the email, and then can execute any commands he wishes as the attacked user. The attacked user simply sees his session dropped, and may simply login again, perhaps not even noticing that the attacker is still logged in and doing things.
7. **TCP:** TCP is a transport-layer protocol. It needs to sit on top of a network-layer protocol, and was designed to ride atop IP. (Just as IP was designed to carry, among other things, TCP packets.) Because TCP and IP were designed together and wherever you have one, you typically have the other, the entire suite of Internet protocols are known collectively as ``TCP/IP.'' TCP itself has a number of important features that we'll cover briefly.
8. **Guaranteed Packet Delivery:** Probably the most important is guaranteed packet delivery. Host A sending packets to host B expects to get acknowledgments back for each packet. If B does not send an acknowledgment within a specified amount of time, A will resend the packet. Applications on host B will expect a data stream from a TCP session to be complete, and in order. As noted, if a packet is missing, it will be resent by A, and if packets arrive out of order, B will arrange them in proper order before passing the data to the requesting application. This is suited well toward a number of applications, such as a telnet session. A user wants to be sure every keystroke is received by the remote host, and that it gets every packet sent back, even if this means occasional slight delays in responsiveness while a lost packet is resent, or while out-of-order packets are rearranged. It is not suited well toward other applications, such as streaming audio or video, however. In these, it doesn't really matter if a packet is lost (a lost packet in a stream of 100 won't be distinguishable) but it does matter if they arrive late (i.e., because of a host resending a packet presumed lost), since the data stream will be paused while the lost packet is being resent. Once the lost packet is received, it will be put in the proper slot in the data stream, and then passed up to the application.
9. **UDP:** UDP (User Datagram Protocol) is a simple transport-layer protocol. It does not provide the same features as TCP, and is thus considered ``unreliable.'' Again, although this is unsuitable for some applications, it does have much more applicability in other applications than the more reliable and robust TCP.
10. **Lower Overhead than TCP:** One of the things that makes UDP nice is its simplicity. Because it doesn't need to keep track of the sequence of packets, whether they ever made it to their destination, etc., it has lower overhead than TCP. This is another reason why it's more suited to streaming-data applications: there's less screwing around that needs to be done with making sure all the packets are there, in the right order, and that sort of thing.

IV. NETWORK SECURITY EXPATIATION

Information is important. It is often depicted as the lifeblood of the growing electronic economy [5]. Commercial organizations and governments rely heavily on information to conduct their daily activities. Therefore, the security of information needs to be managed and controlled properly [8,9]. No matter what the information involves: whenever it is customer records or confidential documentation ninny threats that make information vulnerable [8]. The field of security is concerned with protecting general assets. There are many branches of security. Information security is concerned with protecting information and information resources. Network security is concerned with protecting data, hardware, and software on a computer network [4]. Focus of this research work is on Network Security therefore it is important to consider network security in relation to other branches of security as shown in Figure 2. Network security, must follow three fundamental precepts. First, a secure network must have integrity such that all of the information stored therein is always correct and protected against accidental data corruption as well as willful alterations. Finally, network security requires availability of information to its necessary recipients at the predetermined times without exception [2]. These three principles that network security must adhere to evolved from years of practice and experimentation that make up network history.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

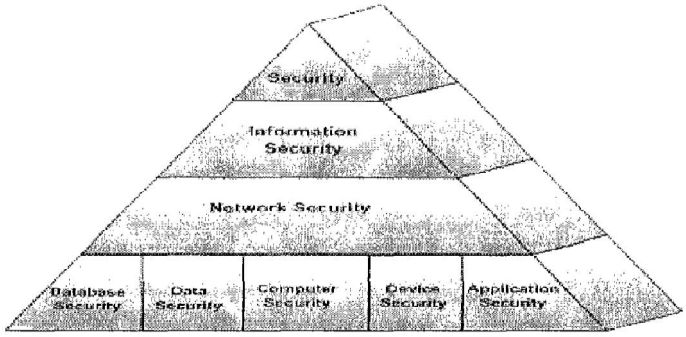

Fig. 2 Network Security TCP/IP model

V. CONCLUSION

Security is a very difficult topic. Everyone has a different idea of what ``security'' is, and what levels of risk are acceptable. The key for building a secure network is to *define what security means to your organization* . Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed will conflict with your security policies and practices.

REFERENCES

1. Francesco Palmieri and Ugo Fiore. “Enhanced security strategies for MPLS signaling”, Journal of Networks, 2(5), 2007
2. Caicedo, C.E, Joshi, J.B.D, Tuladhar. S.R. 2009. IPv6 Security Challenges. IEEE Journal of Computers, 42(2), 36-42.
3. Yongguang Zhang, Malibu.C.A. 2004. A multilayer IP security protocol for TCP Performance enhancement in wireless networks. IEEE Journal on Selected areas in communication, 22(4), 767-776.
4. http://www.ietf.nl/internet-drafts/draft-ietf-ipsec-rfc2401bis-01.txt
5. Douligeris, C, Douligeris, C, Serpanos, D. Serpanos, D. 2007.IP Security (IPSec) . IEEE Book: Network Security: Current Status and Future Directions, 65 – 82
6. Mohammad Al-Jarrah, Abdel-Karim R. Tamimi. 2007. A Thin Security Layer Protocol over IP Protocol on TCP/IP Suite for Security Enhancement. IEEE Conference in Innovations in Information Technology,1-5
7. Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E,” Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect”, International Journal of Computer Science and Network Security, 8(3), 2008
8. Behrouz A. Forouzan. TCP/IP Protocol Suite. 3rd Edition. New Delhi: Tata McGraw Hill Publication. 2003
9. http://www.javvin.com/protocolIPsec.html
10. Bradner, S., “The End-to-End Security,” IEEE Security & Privacy, vol., no.pp., 76-79, Mar.-Apr. 2006
11. Skarmeta, A.F.G. Perez, G.M. Reverte, S.C. Millan.2003. PKI services for IPv6”, IEEE Internet Computing, 7(3), 36-42.
12. Hiromi, R.; Yoshifuji, H., “Problems on IPv4-IPv6 network transition,” Proceedings of the International