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. 4, Issue 5, May 2016

Study of Computer Network Security and It's Issues

Nikita, Shikha Gupta

M.Tech Scholar, Dept. of C.S., Maharshi Dayanand University, Rohtak, India

Assistant Professor, Dept. of C.S., Maharshi Dayanand University, Rohtak, India

ABSTRUCT: As use of internet increases in day to day life, the need of security has become more important. In this paper we discuss about importance of network security and threats related to this and various types of security protocols used at different layers of networking models and security issues in that protocols. Security plays important role in today's growing world to provide secure access of internet to users. This paper will help to learn about security issues and attacks and how we can deal with them.

KEYWORDS: Computer Network, Network security, Security Issues, Security protocols

I. INTRODUCTION TO COMPUTER NETWORK

In today's world scenario, Data communication and network grown significantly and changed the way of business and other daily networking tasks like social networking, e-mailing, mobile-networking and many more.
[1]A computer network can be defined as a series of computers connected to share information and resources. So, it's just a way for computers to share data and information to communicate. There are so many benefits of having computer network in our organization, colleges' etc. i.e. it manages data capabilities, employees can share office equipment, high authorities can control employee access, user need not to take tension about data backup as it provides automated data back system etc.
In 1940, George stibitz used a teletype machine to send instructions for a problem from his model to New York and received results back in same manner. [3]This was the starting of computer network and now computer network communication grown to provide us 100 gigabit Ethernet services. So, now computer networks are the core part of modern communication. All existing and upcoming modern aspects of public switched telephone network (PSTN) are computer controlled and our telephonic communication increasingly runs over the internet protocol.
The scope of communication and networking has increased significantly in past decade and this boom in data communication and network would not have been possible without the progressive advancement in computer network. [1]Data communication using computer networks and technologies needed to connect and communicate through and between them, which helps in driving computer hardware, software and peripheral industries.
The main use of internet is to forward data with equal priority with quality of service, independent on the source and destination.

II. TYPES OF NETWORK

A. Wired Network Connection:

Two types of network connections are present in today's world i.e. wired and wireless network. [2]A simple wired network connection dispenses with the server and only consists of computers and other networked devices connected via their Ethernet interfaces using the hub or switch. This type of connection is called wired peer to peer network.
In today's world, security is the most critical issue or concern in networking and wired networks provide users plenty of security and ability to move lot of data on high speed. Wired networks are typically faster than wireless networks and they are affordable. To set up a wired network connection, user needs three basic systems i.e. Twisted Copper-Pair Transport system (Commonly used Unshielded twisted pair (UTP)) cable, a phone line and finally a broadband.

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. 4, Issue 5, May 2016

B. Wireless Network Connection:

The easiest and least expensive way to establish connection between computers is to use a wireless network connection. Wireless connection uses radio waves for communication instead of wires. The absence of wires makes the network very easy and flexible for users like they can move their laptops anywhere without any tension about the network cables and without losing network connection.[4] To set up a wireless network, user needs only a wireless router. Signals from a wireless router can be extended about 100 feet (30.5 meters) in all directions. If user need more network coverage, it is possible using repeater to provide enough coverage. The downside of wireless network is that they are generally slower than the wired network connections and they can have security issues if appropriate measures will not be followed. [7]To provide security to our wireless network connection, user generally used various security methods like: **Open system authentication (OSA)** – This method grants access to station authentication requested based on the security policies. **Shared Key Authentication (SKA)** – This method sends an encrypted key to the station for requesting access. This station decrypts the key and then responds. If the key matches with AP value, then access is grant.

III. ISSUES IN COMPUTER NETWORK

In our Today's world, dynamic computing environment is increasing significantly.[5] With this advancement, the threat of major attacks or issues of security in computer networks also increasing. So, users should be aware about different types of issues in computer network that can occur.

1) **Performance degradation:** This is a common issue which refers to the issues related to loss of speed and data integrity due to poor transmissions. Although each network have performance issues, but large networks are especially susceptible due to additional distances, end points and additional midpoint equipment.

2) **Host Identification:** Proper and effective configuration is very essential in maintaining proper host identification. Computer networks cannot deliver messages without some form of addressing. Host identification is easy in small networks with the help of manual addressing which is impractical in large networks.[7]
3) **Security Issues:** Another major issue concerned with computer networks is network security issue which involves maintaining network integrity and preventing authorized access from the system and protecting the network denial of service attacks.

Large networks are more affected with security issues and attacks because of more vulnerable points at which intruders can gain access.

IV. HOWSECURITYPLAYSROLEINCOMPUTERNETWORK

Recently in our growing world, computer networks become bigger and bigger due to which network security has become an important issue or factor for companies to consider. [6]By increasing network security, chance of privacy spoofing, identity or information theft decreases. Now a day, Super-intelligence is not required to hack someone's computer or server as this can be easily done using hacker tools which are more sophisticated. Today, to hack a computer, users don't need to possess high level programming skills but should have knowledge of tools available on internet. The role of network security is simply to protect the network from unauthorized access and misuse by hackers. Networks are vulnerable because of remote access facility. For example, hackers can have access of a computer as physical access would be vital.

[10]The main importance of network security is to prevent data loss from misuse of data. Many situations and pitfalls can occur if network security will not be implemented properly. Some of these are:

1) **Breaches of confidentiality:** Each organization have confidential data which they need to keep it private from competitor eyes.
2) **Data Destruction:** Confidential data is very valuable for any individual or organization. Hackers can destruct the data which will be harmful for organization. So, it is important to have backup of data using backup technologies.

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. 4, Issue 5, May 2016

3) **Data manipulation:** System break in problem is very common and easily detectable, as some hackers tend to leave tokens of their accomplishment. However, data manipulation is more dangerous and harmful because data values will be changed and its impact can't be apparent or visible immediately.[8]

To stop network attacks, best approach is to implement a good network security strategy which involves four-steps:

1) **Secure:** Ensure that all data and components are well-guarded with good authentication and authorization policies.
2) **Examine:** Regular monitoring over network activities is important.
3) **Test:** To test your security system, try to assess vulnerabilities of network security policies by having them attack by trusted users. If safeguards can be breached, it's time to implement new and more powerful techniques.
4) **Enhance:** After finding reason of safeguard breaches, use it to build better safeguards. Good network security strategy involves constant review and maintenance.[9]

V. NETWORK SECURITY PROTOCOLS

The rapid growth of the internet leads to grow in demand of security and privacy for communication channels. Security and privacy are essential for secure communication. The call for security and privacy led to several security protocols and standards. Network security protocols ensure the security and integrity of data transmission over network connections. Security protocols define the processes and methodologies to secure network data communication from any unauthorized attempt to access or extract the content of data.

Network security protocols uses cryptography and encryption techniques to secure the data which can only be decrypted with only a special algorithm, keys, mathematical formulas. Some of the popular network security protocols are: Secure socket layer (SSL) and Transport layer security (TLS) protocols; Secure IP (IPSec); Secure HTTP (s-HTTP) and many more. Network security protocols in the framework of the network protocol stack as follows:

Application Layer: PGP (Pretty good privacy), S/MIME (Secure / Multipurpose Internet Mail Extension), S-HTTP (Secure-HTTP), HTTPs (Hypertext transfer protocol over secure socket layer), SET (Secure Electronic Transaction), KERBEROS.[11]

Transport Layer: SSL (Secure Socket Layer), TLS (Transport Layer Security)

Network Layer: IPSec (Internet Protocol Security), VPN (Virtual Private Networks). This protocol also addresses internet communication security.

Data-link Layer: PPP (Point-to-Point Networks), RADIUS (Remote Authentication Dial-in User Service), TACACS+ (Terminal Access Controller Access Control System)

VI. SECURITY ISSUESIN PROTOCOL

Without security measures and controls, both public and private networks are susceptible from unauthorized access and monitoring over data. Various security protocols (like PGP, HTTPs, S-HTTP etc.) provides security by creating standard set of rules for communication over network. But this is possibility that unauthorized user change the rules set by protocols which leads to security issues in protocols as well.

These are few types of issues which will affect security of protocols:

1) **Attacks on ARP:** There are many ways an attacker will attack on the physical address of destination to gain access of the system and deliver data to the wrong destination.
2) **Attack on HTTP:** HTTP users rely on Domain Name Secure and are generally faces security issues due to mis-association of IP addresses and DNS names. This leads to problem of DNS spoofing.
3) **Attacks on IPSec:** The security issue in IPSec is IP address spoofing i.e. identity spoofing. Networks generally use IP address to identify valid computers on network. It is possible that hackers use an IP address to be falsely used. An attacker can use a special program to generate IP address that appear to be originated from valid address. After gaining access to the network with valid IP address, the attackers can change or delete data.
4) **Attacks on TCP:** Security problems generated in TCP due to its transport mechanism. TCP sends lengthy data which can lead to guess ability of the sequence in TCP supplies of packets. Attacker can guess the next sequence number and can hijack the TCP session.

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. 4, Issue 5, May 2016

5) **Attack on SSL:** Man-in-the middle attacks are possible using SSL. If you are accessing your bank's site using a public Wi-Fi connection then attacker can connect with bank on your behalf and can harm your bank account by sending data.

VII. ATTACKSON NETWORK SECURITY

Attacks on any network are only possible without appropriate security measures and controls. There are many types of attacks which can harm security of the network users.

1) **Passive Attack:** In this type of attack, attacker uses a sniffer tool and waits to capture some sensitive information. Attacker will use this information for other types of attacks like packet sniffer tool, filtering clear text passwords etc.
2) **Active Attacks:** In this kind of attacks, attacker don't wait for some sensitive or authenticated information but actively tries to break the secured system using viruses, worms, Trojan horses etc. Active attacks are more dangerous than passive attacks.
3) **Distributed Attacks:** In this type of attack, the attacker hides malicious and harmful code in trusted soft wares. When multiple users uses that software through internet and install it in system, it starts sending useful data from system to attacker.
4) **Insider Attack:** Most of the attacks are insider attacks which is divided into two categories; intentionally and accidently. Intentionally attacks damage the network infrastructure or data intentionally. But accidently attacks are done due to carelessness or lack of knowledge.
5) **Reconnaissance Attacks:** In this, another collects as much information from the network as much he needed to attack. Information like IP address range, running OS, Server location, types of devices etc. Attacker will use this information to attack on your network system.
6) **Hijack Attack:**Hijack attacks are done between running session by joining in a running session and silently break connection with other party. Then attacker will start communication with active party by using identity of disconnected party.[10]
7) **Spoof Attack:** In spoof attacks, attacker changes the source address of packets and receiver thinks the packet is coming from some outside source.
8) **Password Attack:** In this attack, attacker tries to login using guessed passwords using dictionary attack and brute force attack methods.

VIII. CONCLUSIONS

In this paper we discussed about computer network, security issues related to data communication over network and protocols to deal with security issues. In this we also discussed about type of attack user can use to hack your data over network and have unauthorized access of it to manipulate data or delete data which will affect user in many ways. We have mentioned about providing security using various protocols at different layers in networking model and also issues which can occur in that protocols as well. To increase performance of network, one should be aware about its reasons and security measures.

REFRENCES

1. Ritika Sharma, Kamlesh Gupta, Comparison based Performance Analysis of UDP/CBR and TCP/FTP Traffic under AODV Routing Protocol in MANET, International Journal of Computer Applications (0975 – 8887) Volume 56– No.15, October 2012
2. S.Floyd, "Promoting the Use of End-toEnd Congestion Control in the Internet", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 7, NO.4,pp.458-472, AUGUST 1999.
3. Sirwan A.Mohammed, Prof. Dr. Sattar B.Sadkhan, "Design of wireless network based on NS-2", Journal ofGlobal Research in Computer Science, Volume 3, No. 12, December 2012
4. Dr. Neeraj Bhargava, Dr. Ritu Bhargava, Anchal Kumawat, Bharat Kumar, " Performance of TCPThroughput on NS2 by Using Different Simulation Parameters", International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-2 Number-4 Issue-6 December-2012.
5. S.M. bellovin "Security problem in TCP/IP protocol suite", Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989
6. Mr. Ajay Singh and Dr. Pankaj Dashore, " Comparative Analysis of TCP and UDP by using NS-2", International Journal of Computer Science and Information Security (IJCSIS) Volume (1) : Issue (1) IROCS Published Online June 2013

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. 4, Issue 5, May 2016

7. Sirwan A. Mohammed, Prof. Dr. Sattar B. Sadkhan, "DESIGN OF WIRELESS NETWORK BASED ON NS2", Journal of Global Research in Computer Science, Volume 3, No. 12, December 2012.
8. Dr. Neeraj Bhargava, Dr. Ritu Bhargava, Anchal Kumawat, Bharat Kumar, "Performance of TCP-Throughput on NS2 by Using Different Simulation Parameters", International Journal of Advanced Computer Research Volume-2 Number-4 Issue-6 December-2012
9. Y. Xiang, Y. Lin, W.L. Lei ,S.J. Huang, "Detecting DDOS Attack on network Similarity", IEEE Proc.- Commun., Vol. 151, No. 3, June 2004
10. W.Diffie and M.E. Hellman, "New directions in Cryptography", IEEE Transaction on Information Theory, Vol. IT-22, no.6,pp-644-654 , Nov 1976
11. R.L. Rivest, A. Shamir, and L.Adleman, " A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp-120-126 , Feb. 1978.
12. Y. Xiang, Y. Lin, W.L. Lei ,S.J. Huang, "Detecting DDOS Attack on network Similarity", IEEE Proc.-Commun., Vol. 151, No. 3, June 2004

BIOGRAPHY

Ms. Nikita is a M.Tech Scholar in the department of CSE at Advanced Institute of Technology & Management, Palwal, Haryana, India. She did her B.Tech in CSE in 2014 from B. S. Anangpuria Institute of Technology & Management affiliated to MDU Rohtak.

Ms. Shikha Gupta is Assistant Professor in Computer Science Engineering Department in Advanced Institute of Technology & Management, Palwal is pursuing Ph.D. Computer Science from YMCA University of Engineering & Technology, Faridabad. She has completed M.Tech Computer Science Engineering from M.D.University, Rohtak. She has completed B.Tech Computer Science Engineering from M.D. University, Rohtak. She is having more than 2 years of Experience. She has attended 2 Faculty Development Programs, 2 International Conferences and having 5 research papers in National and International Journals. She guided 6 M.tech. Students.