STUDY OF VARIOUS SECURITY ISSUES AT APPLICATION LAYER

Pooja Dahiya(M.tech)*,Sonal Beniwal**
***M.tech Student , ** Assistant Professor**
Department of Computer Science &Engineering, BPS mahila vishwavidyalaya khanpur kalan (sonipat)
poojadahiya902@gmail.com

Abstract: - Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Effective network security manages access to network. It targets a variety of threats and stops them from entering or spreading on your network. The various types of attacks that came under the category of active attack and passive attack have been discussed. In this paper we have discussed various security issues and attack's at application layer.

Keyword: - Security, network security, Active attack, Passive Attack, application layer.

1. Introduction

1.1 Security

Data Security is an essential aspect of IT for organizations of every size and type. Data Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers databases and websites. Data Security also protects data from corruption. So it has been considered the big issues. These security technologies involve data masking, data removal and backups.

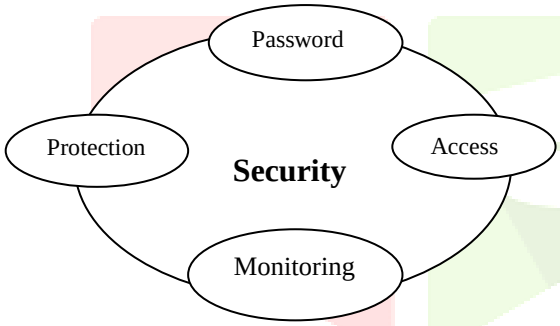

Fig 1 Security

A key data security technology measure is encryption, where digital data, software, hardware and hard drives are encrypted and therefore rendered unreadable to unauthorized users and hackers. At the time of authentication, users must provide a password, code, biometric data, or some other form of data in order to verify his identity [1].

1.2 Network security

Network security is activity that has been considered to secure reliability and usability of network. It involve both hardware and software technologies. Effective network security manages is important in order to access network. Network security combines multiple [2] layers of defenses at edge and in network. The security layers of network enhance documents and controls. The users received entry to network resources, but malicious actors are blocked from carrying out exploits attack.

1.3 Types of attacks

There are some kinds of attack on networks. Some are attractive dangerous and some are safe although annoying. It does not damage to computer, but has capability to empty numbers in bank account [3].

1.3.1 Passive attack

A passive attack checks data which has been not converted traffic. It would check for sensitive information and clear-text passwords that are used in different types of attacks. Passive attacks comprise of traffic analysis decrypting & encrypted traffic monitoring of unprotected communications. It also consist of capturing validated information as passwords that user enter to login [4].

Type of passive attacks:

(i)Eavesdropping: In case of Eavesdropping there is unauthorized real-time interception of communication such as phone call, instant message, fax transmission or videoconference. Customer cannot switch from one service provider to another quickly so he is dependent on service provider for service. Customer management interface is usually accessible on network in case of such attacks [5].

(ii)IP Spoofing: It is a method of attacking a network in order to gain unauthorized access. It is related to networking. Several types of spoofing are having common theme that hacker transmits packets with IP address that shows that the packets are originating from another trusted machine [6].

(iii)War driving: It detects vulnerable Wi-Fi networks by scanning them from nearby locations with a portable antenna. Attack is carried out from a vehicle in motion with GPS based systems that hackers are using in order to plot out areas with vulnerabilities on a map [7].

(iv)Dumpster diving: Intruder gets information stored on discarded computers and other devices or passwords from recycle bins.

1.3.2 Active attack

Active attack is attack where a hacker attempts to modify data on target. Hacker may also change the route to the target in such attack [8].

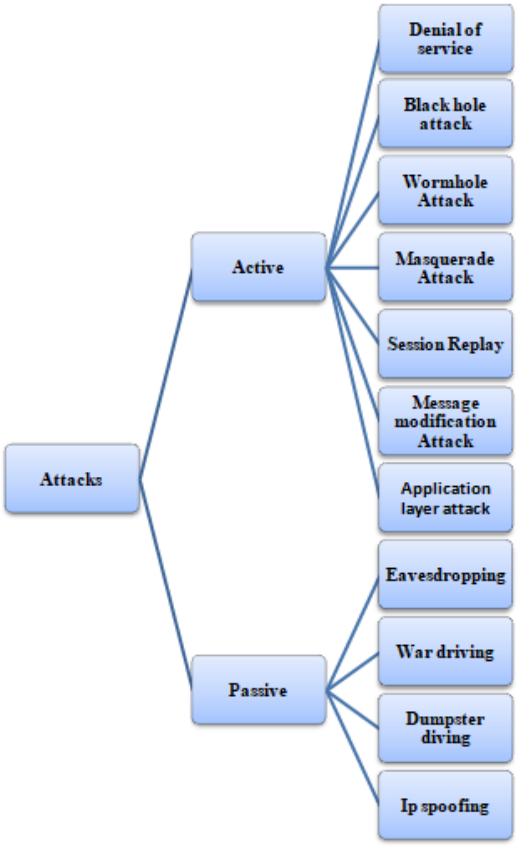

Fig2.Classification of Active and Passive type of Attacks

Types of active attacks:

(i)Black hole attack: A single black hole attack occurs easily in the mobile ad hoc networks. A black hole problem is situation when one malicious node uses routing protocol in order to claim itself of being the smallest path to destination node. But it drops routing packets without forwarding packets to its neighbors [9].

(ii)Wormhole Attack: Wireless sensor networks could be destabilized by Wormhole attacks. Attacker receives packets at a location in network in a typical wormhole attack [10].

(iii)Masquerade attack: Here intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. Masquerade might be attempted through utilization of stolen login IDs and passwords [11].

(iv)Session replay attack: Hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

(v)Message modification attack: Intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

(vi)Denial of service attack: Users are deprived of access to a network or web resource. It is accomplished by overwhelming target with more traffic than it could handle [12].

(vii)Application layer attack: The application layer is hardest to defend [13]. Vulnerabilities encountered here often rely on complex user input scenarios that are hard to define within an intrusion detection signature. Application layer is must be easy to use over Port 80 or Port 443. The application layer in OSI model is closest to end user. It means both OSI application layer and user interact directly within software application. Transmission Control Protocol or internet protocol specifications described a lot of applications that were at top of protocol stack. Some of them were file transfer protocol, Simple Mail Transport Protocol, Domain Name Server Telnet etc.

(A) Telnets is a two-way communication protocol which allows connecting to a remote machine and run applications on it.

(B) File Transfer Protocol is a protocol. That allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient [14].

(C) Simple Mail Transport Protocol is a protocol, which is used to transport electronic mail between sources to destination, directed via a route.

2. Research problem

Security of information from being hacked typically firewall and virtual private network are used. There are excess of problem to traditional network security. First risk is from hacker person who hacks information in unauthentic way. If hackers are winning in his purpose then information should be converted to non understandable form from plane text.

Number of unlike problems versions and minor differences within these, they set out particular problem that researcher are addressing within this thesis issue had been key contract between both communicating parties within case of symmetric key cryptography.

They would breed user defined server and Client request using socket programming. While attach client to server information had been send from client side within encoded form & decoded at server end.

3. Related work

In this section, a review of various existing research, their methodologies, scope and limitations has been presented for various attack(s).

Various Methodologies on attack(s)

Shari Mohammadi et al.[15],(2011) The existing researches focus on security of WSNs, divide it into four categories and would consider them, include: an overview of WSNs, security in WSNs, threat model on wireless sensor network to attack of layer and a comparison of them. This work enables us to identify purpose and capabilities of attackers; furthermore, goal and effects of link layer attacks on WSNs are introduced .

Wajeb Gharibi et al.[16], (2012) Several authors think that advancement of latest technology in general and social websites in particular would bring new security risks that

might present opportunities for malicious actors, key loggers, Trojan horses, phishing, spies, viruses & attackers.

Tongguang Ni et al.[17],(2013) Some of existing researches are based on characteristics of DDOS attack.They propose a novel approach to detect DDOS attacks. They would make a detailed study of how to set all kinds of parameters in different application scenarios adaptively.

Hong-Ning Dai et al.[18],(2013) In tradition researches some authors have explored using directional antennas in wireless sensor networks to improve network security in terms of reducing eavesdropping probability [18]. They has been explains to directional receiver in one hop network or some hop network could important reduce eavesdropping probability.

Rupam et al.[20],(2013) This paper describe Security of network is an important field that is increasingly gaining attention as internet expands. Security threats & internet protocol were analyzed to determine necessary security technology. Security technology is mostly software based, but many common hardware devices are used.

Amandeep Kaur et al.[10],(2014) The existing researches discuss about security challenges & how different layers protocols become vulnerable to various attacks.

P. Kiruthika Devi et al.[6],(2014) In this paper, various algorithms are proposed. Spoofing attack detection & localization in wireless sensor network have been extensively studied. There is no unique method for identifying & removing spoofing attack in wireless sensor network. Each method has its own advantages & disadvantages.

Ms. Vidya Vijayan et al.[21],(2014) There are many methods & techniques can conduct password cracking, in on-line or offline environment. Tools that can guess passwords for differential goals, & certain prevention tactics are presented here. This paper also focused on finding & documenting commonly available attacks on passwords. After analyzing all cracking strategies this paper enforce users to select passwords easy to remember but hard to guess.

Venkadesh et al.[3],(2015) This survey paper gives knowledge regarding password stealing activities & protection mechanism available on online network communication. Protection of passwords is a vital activity in an on-line system.

Amandeep Kaur et al.[19],(2016) In wireless multi-hop sensor networks, an intruder may launch some attacks due to packet dropping in order to disrupt communication. To tolerate or mitigate such attacks, some of schemes have been proposed. But very few could effectively & efficiently identify intruders. Packet Droppers & Modifiers are common attacks in wireless sensor networks. It is very difficult to identify such attacks & this attack interrupts communication in wireless multi hop sensor networks [19].

Amandeep Kaur Grewal et al.[22],(2017) The existing researches discuss about the behaviour and challenges of security threats in mobile ad hoc networks with solution finding technique.

Sr No	Auth-or	Year	Tech ni-que	Benefits	Limitations
1	Shari Mohammadi	2011	WSN	This work enables us to identify purpose & capabilities of attackers; furthermore, goal & effects of link layer attacks on WSNs are introduced.	This research does not enhance the data security.
2	Wajeb Gharibi	2012	New technology	It can also safely manipulate huge amount of information in internet & in social websites as well.	This research is limited to website security.
3	Hong-Ning Dai	2013	Wireless sensor	Security improvements of using directional antennas owe to smaller exposure region & fewer hops due to longer transmission range.	Research is limited to eavesdropping attack.
4	Rupam	2013	Detect Packets Using Packet Sniffing	Packet sniffer is designed for capturing packets & a packet can contain clear text passwords, user names or other sensitive material.	Research is limited to packet sniffing.
5	Amandeep Kaur	2014	MANETs	They have discuss about security challenges & how different layers protocols become vulnerable to various attacks	There is lack of technical work in this research.
6	Md. Wal	20	Wireless	They can be easily	This research lack the security

	iullah	14	LAN	downloaded & run by anyone	of data.
7	P. Kiruthika Devi	2014	Spoofing attack detection	Spoofing attack detection & localization in wireless sensor network have been extensively studied.	Research is just considering spoofing attack.
8	Blessy Rajra	2015	Black Hole Attack	Security technology is mostly software based, but many common hardware devices are used.	This is just survey no technical work has been discussed here.
9	Amandeep Kaur	2016	Packet Droppers	Today wireless communication technique has become an essential tool in any application that requires communication between one or more sender(s) & multiple receivers.	It is very difficult to identify such attacks & this attack interrupts communication in wireless multi hop sensor networks.
10	Amandeep Kaur Grewal	2017	MANET	They have analyzed the behaviour and challenges of security threats in mobile ad hoc networks with solution finding technique.	Research is limited to Black Hole attack.

4. Challenges

There are lots of challenges to existing network security. First threat is from hacker person who hacks data in unauthentic way. In order to secure data from being hacked usually firewall & virtual private network are used. But if hackers are successful in his objective then data should be converted to non understandable form from plane text.

5. Conclusion and future work

In this paper different type of attacks from hacker end has been discussed. The discussed related to Security Issues at Application Layer has been made. This research paper would act as base for proposed design that would more secure. Proposed design would best suited for application layer security and much suitable to prevent attack. This portion of framework requires human intervention arid lacks intelligence to incorporate new signatures automatically. They help organizations to understand present hidden problems in their servers and amp; corporate network. Such system is beneficial to carry on FTP, http, Telnet services with minimum attack.

6. EXPECTED CONTRIBUTION OF RESEARCH

There are lots of shortcomings of tradition works. Some of them just concentrated on energy efficient routing instead of packet lifetime enhancement. Several researches considered Life time of packet but they did not considered the packet size. Because of such shortcoming there are issues related to congestion. Some research has worked on energy efficiency but they just made a survey they did not perform the packet life time enhancement. We have made comparative analysis of along with outcomes and shortcomings of previous paper.

7. References

[1] Mubina Malik, Trisha Patel, "Database Security - attacks and control method", International Journal of Information Sciences and Techniques (IJIST), Vol.6, No.1/2, March 2016, pp. 175-183.

[2]Mohan V. Pawar, Anuradha J, "Security of network and Types of Attacks in Network", International Conference on Intelligent Computing, Communication & Convergence, 2015, pp. 503 – 506.

[3]Ankit Mehto, Prof. Hitesh Gupta, "A Review: Attacks and Its Solution over Mobile Ad-Hoc Network", International Journal of Engineering Trends and Technology (IJETT), Volume 4, Issue 5, May 2013, pp. 2009-2011.

[4]P.aruna devi, S.rani laskhmi, K. sathiyavaishnavi**, "**A Study on Security of network Aspects and Attacking Methods", International Journal of P2P Network Trends and Technology, Volume3, Issue2, 2013, pp. 97-103.

[5]P. Kiruthika Devi, Dr. R. Manavalan, "Spoofing attack detection & localization in wireless sensor network", International Journal of Computer Science & Engineering Technology, Vol. 5,No. 09, Sep 2014, pp. 877-886

[6]Md. Waliullah ,Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014, pp. 176-183.

[7]Ms.Neha KamdarAssistant Professor, Vinita Sharma Assistant Professor, Sudhanshu Nayak Assistant Professor, "A Survey paper on RFID Technology, its Applications and Classification of Security/Privacy Attacks and Solutions", International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol.6, No4, July-August 2016, pp.64-68.

[8]Barleen Shinh, Manwinder Singh, "A Review Paper on Collaborative Black Hole Attack in MANET", International Journal of Engineering & Computer Science, Volume 3,Issue 12, December 2014, pp. 9547-9551**.**

[9] Amandeep Kaur, Dr. Amardeep Singh, "A Review on Security Attacks in Mobile Ad-hoc Networks", International Journal of Science & Research, Volume 3, Issue 5, may 2014, pp. 1295-1299.

[10]Salah Alabady,"Design and Implementation of a Network Security Model for Cooperative Network", International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009, pp.26-36.

[11] Mukesh Barapatre, Prof. Vikrant Chole, Prof. L. Patil, "A Review on Spoofing Attack Detection in Wireless Adhoc Network", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013, pp.192-195.

[12] Nitish Aggarwal, Rachit Gupta, Pallavi Saxena, "Comparative Study of OSI & TCP/IP ReferencModel", International Journal for Research in Applied Science & Engineering Technology (IJRASET),November 2014.

[13] Albandari Mishal Alotaibi, Bedour Fahaad Alrashidi, Samina Naz and Zahida Parveen, "Security issues in Protocols of TCP/IP Model at Layers Level", International Journal of Computer Networks and Communications Security, may 2017, pp. 96-104.

[14] Shahriar Mohammadi, Reza Ebrahimi Atani**,** Hossein Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security, April 2011, pp. 69-84**.**

[15] Wajeb Gharibi, Maha Shaabi, "Cyber threats in social networking websites", International Journal of Distributed & Parallel Systems (IJDPS), Vol.3, No.1, January 2012, pp. 119-126.

[16] Tongguang Ni, Xiaoqing Gu, Hongyuan Wang, & Yu Li, " Real-Time Detection of Application-Layer DDOS Attack Using Time Series Analysis", Journal of Control Science & Engineering, Volume 2013, pp. 1-6.

[17] Hong-Ning Dai, QiuWang, Dong Li, & Raymond Chi-Wing Wong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas", International Journal of Distributed Sensor Networks, Volume 2013, pp. 1-13.

[18] Amandeep Kaur, Sandeep Singh Kang, "Attacks in Wireless Sensor Network- A Review", International Journal of Computer Sciences & Engineering, Vol.04, Issue 05, May 2016, pp.157-162.

[19] Rupam, Atul Verma, Ankita Singh, "An Approach to Detect Packets Using Packet Sniffing", International Journal of Computer Science & Engineering Survey (IJCSES),Vol.4, No.3, June 2013, pp. 21-33.

[20] Ms. Vidya Vijayan, Ms. Josna P Joy, Mrs. Suchithra M S, "A Review on Password Cracking Strategies", international Journal of Research in Computer & Communication Technology, 2014, pp.8-15.

[21] Blessy Rajra M B, A J Deepa ME, "A Survey on Security of network Attacks & Prevention Mechanism", Journal of Current Computer Science & Technology, Volume 5, No. 2, February 2015, pp.1-5.

[22] Amandeep Kaur Grewal, Asst. Prof. Gurpreet Singh, "A Review on Attacks in Mobile Ad hoc Network (MANET)", International Journal on Recent and Innovation Trends in Computing and Communication, Volume 5, Issue 1, January 2017,pp.119-124.