© INNOVATIVE RESEARCH THOUGHTS | Refereed | Peer Reviewed | Indexed
ISSN : 2454 – 308X | Volume : 04 , Issue : 06 | July - September 2018

INVESTIGATION OF SECURITY OF NETWORK: A REVIEW

RAMESH KUMAR, RESEARCH SCHOLAR

ABSTRACT: In this paper the concept of security of network has been discussed. The main focus of this paper is to review the existing researches in field of network security. . Security of network is combining more than on layers of defense in network. Every Security of network layer is performing policies controls. The authorized users would be able to gain access to network resources but malicious actors may be blocked from performing threats related to exploits. Different mechanism proposed by different researchers is discussed in this paper. The scope of network security is also discussed at the end of research.

Keywords: Security, Protocol, Encryption, Peer to peer, Network

[1] INTRODUCTION

It is the term which is used for the protection of digital information in information technology .It protects them from all the different kind of threats. These threats can be internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of software tools and IT services. Data security also protects data from corruption. So it has been considered big issues. These security technologies involve data masking, data removal backups.

[2] Security of Network

Security of network is known as any activity that was made in order to secure usability integrity of computer network Information. It is consisting hardware as well as software technologies. It is focusing on variety of threats in order to prevent them from accessing computer network. The Effective Security of network is going to manage the access of network. Security of network is combining more than on layers of defense in network. Every Security of network layer is performing policies controls. The authorized users would be able to gain access to network resources but malicious actors may be blocked from performing threats related to exploits. Each company which needs to provide services that user's employees requirement should protect the network. Security of network also helps user to save proprietary data from hackers attack. It saves customers reputation [6]. Security of network is security given to a network from unauthorized access.

[4] LITERATURE REVIEW

Shahriar Mohammadi (2011) [2]: It has been researched here that wireless sensor networks (WSNs) have many applications which has a great potential. [1, 5] There are unique challenges. These are made of small sensors nodes which are hundreds or thousands in number. The examples are MICA2. These are operated autonomously. Here are conditions like cost and invisible deployment.

Rupam, Atul Verma, Ankita Singh (2013) [4]: In the past decades computer network have kept up growing in size, complexity and along with it the number of its user is also being increased day by day.

Mohan V. Pawar, Anuradha J (2015) [6]: The computer network technology is developing rapidly, and the development of internet technology is more quickly, people more aware of the importance of the network security.

Shari Mohammadi etal (2011) [14]: This paper focus on security of WSNs, divide it into four categories & will consider them, include: an overview of WSNs, security in WSNs, threat model on WSNs, a wide variety of WSNs' link layer attacks & a comparison of them. This research is enabling us for identifying purpose.

Ankit Mehto, Prof. Hitesh Gupta (2013) [8]: it is a new form of Ad-hoc Network. It has gained the attention

of today's research efforts. It is automotive for industries .It improves road safety. It enables a wide variety of value added services. It needs security to implement the wireless environment and serves users with safety and non safety applications. Many forms of attacks against MANET have emerged recently that attempt to compromise the security of such networks. Such security attacks on MANET may lead to catastrophic results such as the loss of lives or loss of revenue for those value—added services. In this paper, we discuss some of the main security threats that can be exploited in MANET and present the corresponding security solutions that can be implemented to thwart those attacks.

Ms.Neha Kamdar Assistant Professor (2016) [9]: RFID (Radio Frequency Identification) system is one of the most pervasive computing technologies with technical potential and cost-effective opportunity in a different area of applications. Among their advantages is included their low price and their wide area applicability. However, they also present a number of inherent vulnerabilities. This paper explains a categorization of RFID attacks. They present their important features. Here feasible countermeasures are discussed. The aim of the researchers is to standardize the present weaknesses of RFID communication. The aim is to provide better thought of RFID attacks. It may be get. In the result it is more efficient. The valuable algorithms, techniques and procedures to combat by these attacks may be developed.

Shari Mohammadi etal (2011) [14]: This paper focus on security of WSNs, divide it into four categories & will consider them, include: an overview of WSNs, security in WSNs, threat model on WSNs, a wide variety of WSNs' link layer attacks & a comparison of them. This research is enabling us for identifying purpose. Here the abilities of attackers are introduced with their goal & effects on link layer attacks. With, this here researchers explains acquainted approaches of security detection. By this IT security managers would enable to manage link layer attacks. These attacks of WSNs are more effective.

Wajeb Gharibi etal (2012) [15]: They think that advancement of new technology in general & social websites in particular will bring new security risks that may present opportunities for malicious actors, spies, key loggers, , phishing, , viruses Trojan horses & attackers. Here we should interchange big amount of information on internet. It is in the social websites as well.

Tongguang Ni etal (2013) [16]: Based on characteristics of DDOS attack, this paper proposes a novel approach to detect DDOS attacks. Here two type of contributions are provided by work. Here HRPI is defined for detecting DDOS attacks. Here some important features of attacks are reflected. There is a detection scheme which is against DDOS attacks. It can achieve high detection efficiency & flexibility. In our future work, we will make a detailed study of how to set all kinds of parameters in different application scenarios adaptively.

Hong-Ning Dai etal (2013) [17]: They have explored using directional antennas in wireless sensor networks to improve Security of network in terms of reducing eavesdropping probability. In particular, we analyzed eavesdropping probability of single-hop networks & that of multi hop networks. It has been found that by using directional antennas. There is either a single hop network. With this there is a multi hop network. It could importantly reduce probability of eavesdropping

Rupam etal (2013) [18]: This paper proposes an approach to detect packets through packet sniffing. There are many negative aspects. But besides these negative aspects it is useful in sniffing of packets. Packet sniffer is not only used for hacking purpose but also it is used for network traffic analysis, packet/traffic monitoring, troubleshooting & other useful purposes. Packet sniffer is designed for capturing packets & a packet can contain clear text passwords, user names or other sensitive material. Sniffing is possible on both non switched & switched networks.

Sharmin Rashid etal (2013) [19]**:** This paper describes use of IP spoofing as a method of attacking a network in order to gain unauthorized access & some detection & prevention methods of IP spoofing. The main aim of attack is to enhance a connection. It will permit the attacker for gaining root access to host. It permits creation of a backdoor entry path. It is targeted into a system. We may think that our traditional methods will be very helpful for knowing & stopping IP spoofing. It will give a secured communication system.

Mukesh Barapatre etal (2013) [20]: This paper explains data security into client-server communication will be decreased. Thus, true WLAN security is always going to be a game of balancing acceptable risk & countermeasure to mitigate those risks. Here we have to understand business risk. We have to take action. This has been done to deter the most important & most frequent attacks. We have to follow industry good practices. it gives us better security solutions.

Amandeep Kaur etal (2014) [21]: Due to dynamic infrastructure of MANETs & having no centralized administration makes such network more vulnerable to many attacks. In this paper, we discuss about security challenges & how different layers protocols become vulnerable to various attacks. These attacks can classified as an active or passive attacks. Different security technologies are introduced to prevent such network. In future study we will try to invent such security algorithm, which will be work along with routing protocols that helps to reduce impact of different attacks.

Md. Waliullah etal (2014) [22]**:** Securing wireless network is an ongoing process. Realistically, still there is no single true security measure in place. In the case of introduction of a new technology, firstly, the hackers study protocol. After that they find its vulnerabilities. Then they cobble some program together. In the end they try to exploit those vulnerabilities. With the passage of time these tools become further focused. These are more automated. Many times they are readily available. They may be published on open source network. Hence, there downloading is very easy. Anyone can run it. So threats & vulnerabilities are never excluded. If we do so, we will end up wastage of money. It will defeat some low probability & attacks of low impact. On other hand, if we start eliminating biggest security loopholes, attackers may turn to easier targets.

P. Kiruthika Devi etal (2014) [23]: In this paper, various algorithms are proposed. Spoofing attack detection & localization in wireless sensor network have been extensively studied. The spoofing attack in wireless sensor network cannot be identified and removed because there is no unique method. There are advantages & disadvantages of each method. Number of issues such as detecting presence of spoofing attacks, determining number of attackers, localizing multiple adversaries & eliminating them are not solved

effectively. This paper can help researcher further. It is to invent a novel method. By this we can recognize spoofing attack. This will remove or disable the same in wireless sensor network. It is so effective that it has low cost.

Barleen Shinh etal (2014) [24]: Ad-hoc networks have become a new standard of wireless communication in infrastructure less environment. MANET is a Mobile Ad-hoc Network in which nodes get connected with each other without an access point. Messages are exchanged & relayed between nodes. Routing algorithms are utilized for forwarding packets between indirect nodes i.e. not in direct range with aid of intermediate nodes.

Ms. Vidya Vijayan etal (2014) [25]: 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.

Blessy Rajra et al (2015) [26] : This paper describe Security of network is an important field that is increasingly gaining attention as internet expands..Current development in Security of network is not very impressive. Here it has been summarized that how attacks are working in wireless sensor networks. It has also told how they are classified.

Venkadesh etal (2015) [27]: Here knowledge about password stealing activities is provided . The protection mechanism which is available on the online network communication is also explained here. Protection of passwords is a vital activity in an on-line system. It avoids vulnerable activities & anonymity loss of individual user.

Thin Das etal (2016) [28]: In this paper, we proposed methodology for detecting identity-based attacks like spoofing attacks & hence localizing multiple adversaries in wireless sensor networks with high accuracy & precision.

Amandeep Kaur etal (2016) [29]: 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.

[6] SCOPE OF RESEARCH

In today's time the most vital field is security of network. As the scope of internet is expanding security of network is also gaining attention. The security technology was examined by threats of internet protocol. Security of network is not expanding at a vast rate. The Security technology is based on software. Here many common hardware devices are used. There is a diversified number of Hackers. Hacking may have benefits as well as risks. If we consider risks they can make a company bankrupt. If we consider benefits they can protect data and hence revenues of a company are increased. Ethical & creative hacking had been significant in Security of network, in order to ensure that company's data had been well protected secure. The nasty hackers may breach the security system and cause a great loss to the company.

This research would help organizations to understand present hidden problems in their server's corporate network. Concentrate likewise uncovers that substantial

clients are moral programmers, till their intensions are clear else they are awesome risk, as they approach each bit of information of association, as contrast with add up to semi untouchables. This also concludes that hacking had been important aspect of computer world. This deals within both sides of being good bad. Moral hacking assumes fundamental part in keeping up sparing parcel of mystery information, while vindictive hacking could annihilate everything.

REFERENCES

[1]. Bhawan Bhardwaj,2 Ankur Mittal, "ADVANCED MECHANISMS TO SECURE WIRELESS AD HOC NETWORK WITHPERFORMANCE ANALYSIS" ISSN: 2278-6848, Volume: 08 Issue: 08 ,October - December 2017

[2]. 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**.**

[3]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.

[4]. 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.

[5]. Sharmin Rashid, Subhra Prosun Paul, "Proposed Methods of IP Spoofing Detection & Prevention, International", Journal of Science & Research (IJSR), Volume 2, Issue 8, August 2013, pp.438-444.

[6]. 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.

[7]. MANJIRI N. MULEY, "ANALYSIS FOR EXPLORING THE SCOPE OF NETWORK SECURITY TECHNIQUES IN DIFFERENT ERA: A STUDY", International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-12, Dec.-2015, pp. 33-36.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. Mahendra Kumar, Ajay Bhushan, Amit Kumar, "A Study of wireless Ad-Hoc Network attack and Routing Protocol attack", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012, pp.31-33.

[12]. 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

[13]. G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms inMANETS- A Survey**",** International Journal of Computer Applications, Volume 9, No.9, November 2010, pp.12-17.

[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]. 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.

[19]. Sharmin Rashid, Subhra Prosun Paul, "Proposed Methods of IP Spoofing Detection & Prevention, International", Journal of Science & Research (IJSR), Volume 2, Issue 8, August 2013, pp.438-444.

[20]. 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.

[21]. 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.

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

[23]. 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.

[24]. 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.

[25]. 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.

[26]. 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.

[27]. Venkadesh .S, K.Palanivel , "A Survey on Password Stealing Attacks & Its Protecting Mechanism", International Journal of Engineering Trends & Technology (IJETT) , Volume 19, Number 4 , Jan 2015, pp.223-226.

[28]. Tuhin Das, "A Study on Identity Based Attack Detection and Localization by the Clustering in Wireless Sensor Network, International Journal of Computer Sciences and EngineeringOpen Access, Volume-04, Issue-02, Feb 2016, pp. 96-99 .

[29]. 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.

[30]. Albandari Mishal Alotaibi, Bedour Fahaad Alrashidi, Samina Naz Zahida Parveen, "Security issues in Protocols of TCP/IP Model at Layers Level", International Journal of Computer Networks Communications Security, VOL. 5, NO. 5, MAY 2017, pp. 96-104.