CLASSIFICATION OF ATTACKS IN CRYPTOGRAPHY AND NETWORK SECURITY

[1]Kondabathini..Keerthi, [2]N.Venkateswaran, [3]MD Asma, [4]Daravena.Akhila
[1,3,4]Students, [2]Associate Professor, Department of Computer Science and Engineering,
Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana-505001.

Abstract: Nowadays internet security has become a problematic part of everywhere, so network security plays a significant role. Criminals are easily accessing the individual's data because of everything in the world becomes digitalized way through the internet. The network administrator has to maintain a track of advance updates regarding software and hardware to avoid the attacks. This paper describes Network security aims at internal protection by monitoring the passwords, internet access, firewalls, backups, encryption and more. The information security focuses on safeguard of all the data while cybersecurity focuses only to secure the digital data; it is the subset of information security. Mobile ad-hoc network (MANET) is a kind of ad-hoc network that can administrate/manage by itself, and it can connect to different systems using wireless connections.

Keywords: Network security, information security, mobile ad-hoc network (MANET)

I.INTRODUCTION

The communication between two devices is done by connecting those devices. The connection may be wired(ex: cabling) or wireless(ex: wireless networking cards). The connected devices can access resources like internet, file services, printers, etc. Nowadays computer technology is developing rapidly, as computer technology is developing then the development of internet technology also increasing more.

This age of universal electronic connectivity, where the activities like

-attacks
-hacking
-viruses are prevalent.

So that it is very critical to protect computer& network security, the implementation of the security mechanism is essential to secure or protect the data from unauthorized users. In this paper, we have described some attacks that occurred in MANET, information security and network security.

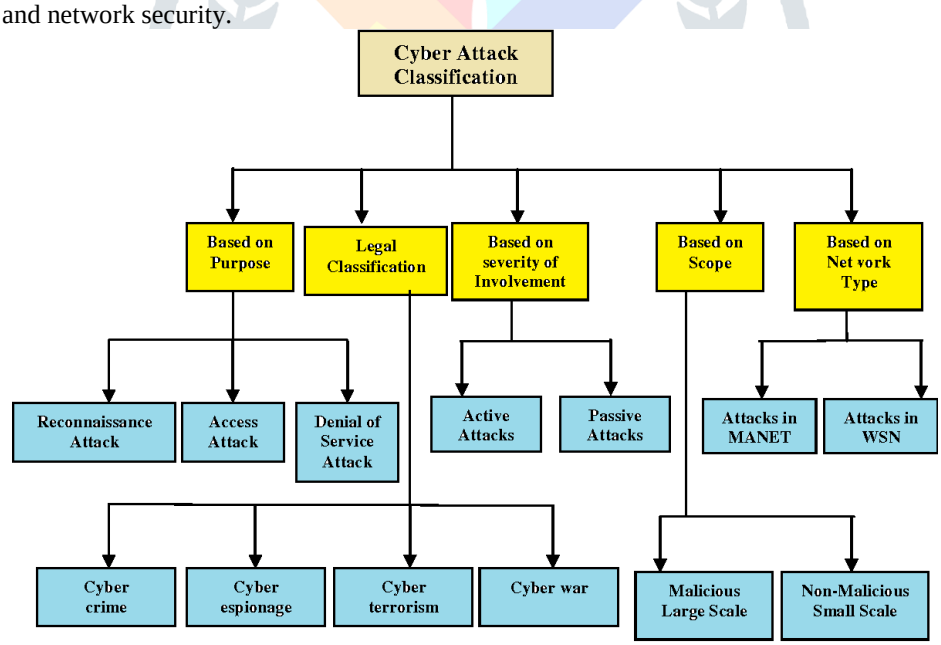

Figure 1: Attack classification diagram

II.MAJOR ATTACKS IN MANET

Black hole Attack: Attacker uses the routing protocol to have the best path for a node to which packets he wants to intercept. A flooding based protocol which is used by the hacker that when a user request a package, the hacker will send a reply before the user receives the original response so that the user thinks it is the shortest path to reach the receiver.
Wormhole Attack: The user thinks that he found the shortest path in the network because of attacker tunnels the packet from one point to another point. It is also called a tunneling attack.

Snooping: In snooping unauthorized users access the personal data of the authorized users. It is similar to eavesdrop, but the accessing of data is not limits during the transmission. It includes the casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing.

Sybil Attack: This attack can occur due to one node shares its secret key with other malicious nodes so that the attack increased according to the number of malicious nodes are increased.

Denial of service(DOS): Attacks attempts to prevent authorized users from accessing some services, which they are eligible. For Instance, an authorized user might send too many login requests to a server using random user Ids frequently to overload the server, to flood the network and deny other authorized users from using the network facilities.

III.MAJOR ATTACKS IN NETWORK SECURITY:

Byzantine Attack: While sending the data from sender to the receiver the middle notes perform some modifications such as sending a packet through the non-optimal path, creating routing loops which result in degradation or disruption of routing services.
Rushing Attack: When the sender sends a message to the receiver, the unauthorized user receives the signal and duplicate the word and will continuously transmit the replicated packets to the receiver. Receiver thinks that packet sent from a sender and it becomes busy.

Location disclosure attack: Unauthorized user collect the information about the node and the route by computing the traffic so malicious node may perform more attacks on network security.

Phishing Attack: In this attack, the attacker creates a fake website which exactly looks like a popular web site. When the user login to the particular fake website by using username and password then attacker access that details and he/she can perform any operation.

Hijack Attack: In this attack, an attacker takes over a session hijacking between innocent user and server and the attacker sends a fake request to the server.

IV.MAJOR ATTACKS IN INFORMATION SECURITY:

Man-in-the-Middle Attack: it occurs when a hacker itself inserts between the communication of a client and a server there are some types of man-in-the-middle attacks as follows.

Session Hijacking: A session hijacked between the trusted client and a network server. In this the client is connected to the server; the attackers control the client system and disconnect the client from the server. And it replaces its own IP-address in place of clients IP-Address, it continues communication with the server, but the server believes that it is communicating with the client.

Spoofing: It is used by the attacker to communicate with the server. The attacker convinces a system that it is corresponding with the known and it can access to the system.

Eavesdropping Attack: It occurs through interception of network traffic. An attacker can obtain confidential information that the user might be sending over the network. Detecting a passive attack is more important than active ones. Data encryption is the best countermeasure for eavesdropping.

Birthday Attack: It is used to verify the integrity of a message, Software or digital signature. It finds two random words which operate when processing the same message digest by the hash function.

V.SECURITY GOALS:

Confidentiality: It specifies leads to only the sender and the intended receiver. Should able to access the contents of a message. Privacy gets compared if an unauthorized person can obtain a signal.

Authentication: Authentication mechanisms help establish proof of identities. The authentication process ensures the identification of the origin of an electronic message or document identified. For instance, suppose that user C sends an electronic report over the internet to user B. However, the problem is that user C had replay the modified content of the message and posed as user A when he/she posted this document to user B.

Integrity: when the content of the message will change after the sender sends it, but before it reaches the intended recipient, we declare that the integrity of the word will be ost. This type of attack is called "modification."

Non-repudiation: User sends a message and later on refuses that she/he had sent that message. Non-repudiation does not allow the sender of a message to deny the claim of not sending that message.

Access Control: The principle of access control determines who should be able to access what.

Availability: The principle of availability states that resources should be available to authorized parties at all times.

VI.LITERATURE SURVEY:

In network security, routing protocols cannot provide complete protection for the path. In this paper, they described providing a secure data path from the malicious node. For that, some of the existing routing protocols illustrated. Network security is the major issue in this competitive world, as many members connected to the internet. So they need to know about the basics of safety in a networked world. The workstations are neither centrally managed and nor they have boundary protection; they may have some hardware, software, operating system, different protocols with several levels of cyber awareness among the users. In the companies internet is connected by the employees who are unsecured, this unsecured requirement may leads to hackers to attack quickly and modified total data and shows vulnerabilities. There are several attacks are there in the network security, to prevent them some of Trust Oriented Secured Routing protocols were implemented such as WAP- Wormhole Attack Prevention, Jain and Jain and also some of the attacks that can be eliminated by using different protocols[1].

In this paper, they were explained about the network security integrity vector, network security confidentiality vector, network security availability vector and also they have explained some essential types of attacks in MANET such as spoofing, modification, wormhole, black hole attack, etc. Network security is commonly initiated with user name and password which means authorization as the internet technology is increasing day by day, security issues becoming very difficult to identify[2]. To reduce the security issues they were researched about types of attacks, security for the internet access, history of the network security, etc. designing network depends upon the OSI(open system interface) model. OSI model has several advantages when designing network security. It also offers flexibility, modularity, ease-of-use and standardization of protocols. MANET is a wireless network. It is an infrastructure less network. In this network, it is challenging to identify the attacks. To avoid the security problems, the antivirus program must be updated and operating system also to be regularly updated.

Network security has become an essential role in protecting the website's servers or domains in the different form of attacks. Nowadays, network security is implemented in every field such as military, banking sector, business, etc. many of them are protecting by modifying the architecture of the network to avert these various forms of attacks. From routers, hackers can easily steal the data by using malware like "Trojan horse." It will affect on website applications social networks. But by using a good antivirus, firewall systems we can protect data. In this paper, the primary intention of the digitalized India to make the digitally authorized country, which will save the human resources and time, in a great extent and Provides the high speed of internet network to access any information as per their requirements. This paper explains about different types of security attacks such as passive attacks, active attacks, Denial of service (DOS) attack and types of network security[13]. And these network attacks can be protected by configuration management, firewalls, encryption, vulnerability testing. They are encrypting the World Wide Web (www) by secure sockets layer, secure HTTP (SHTTP), VPN, E-mail security[12]. There are billions of transactions are going through the internet so that attackers can steal the bank details, credit and debit card information are a threat. Therefore there are various software's to safeguard from these attacks. Researchers are finding new methods to avert the attackers [3].

Network security plays a role in securing confidentiality and sensitive information which can be globally shared. Unauthorized users can easily access the transmission of data through various networks. Therefore different studious are implemented for network security. The common threats, attacks, and attacks cause damage to information — the keywords which are known as network security, network attacks, and risks and network security measures. Also provides the protection that includes cryptography, encryption, information security. When unauthorized persons access sensitive information, the organization faces interruption, modification, interception, fabrication. So this is the reason why network security is becoming important through transferring the data. Globally network attacks that have been damaging the companies are listed in this paper. The various attacks are network virus, an e-mail containing the virus, attack on the server, network user attacks, service rejection attacks. Some other attacks which pose a severe threat to the organization are phishing attacks, close in attacks, viruses worms and Trojans, hijack attack, etc. the security measures can be taken are firewalls, antivirus systems, intrusion detection systems. Hence network security prevents the accessing of information from unauthorized users [4].

Nowadays computers used everywhere are, and every sector, computers which are connected to the network will face more security issues. From small shops to the large organization's computers are available. In this paper, they were described various attacks, threats and how it will be secured. Many attacks are involved in network-based concepts. These attacks are categorized as wired and wireless networks. Networks are used to access information from various places that the distance can be small or large. The types of system are Personal Area Network (PAN), Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Global Area Network (GAN), Virtual Private Network (VPN). The attackers can be classified as Hackers and Crackers. Interruption, interception, modification, fabrication are the four types of attacks. Various algorithms were implemented to gain security based on their level of protection. The security protocols also implemented; some of them are Secure Socket Layer (SSL), services are authentication and confidentiality. This paper deals with the various types of attacks and how to prevent attacks by different mechanisms; algorithms are developed to avoid the attacks. Security protocols are available for each of the attack [5].

This paper tells that, there is considerable overlap between the Information security and Cybersecurity. The term cybersecurity may frequently be related to exchangeable with information security. These two terms are not entirely comparable. The paper puts forward that the cybersecurity goes to the further side of the boundaries of traditional information security to add not only the information resources of protection but also for other reasons that include the person herself/him. Information security can be in some ways. The primary goal of information security is to reduce the damage to organizations. It guarantees the continuity of the business and the effects of security situations are limited. If the Cybersecurity is similar to term information security, then the cybersecurity incidents can be assumed to be the features that can define information security. For example, cybersecurity incidents would also cause in the violation of integrity, confidentiality, availability of information. This paper illustrated both the Information security and ICT security. Information security is the protection of data with assets which are resulting from harmfulness and vulnerabilities. Cybersecurity means protected for not only cyberspace but also the functioning and assets via cyberspace [6].

In this paper, the researchers explained about black hole attack in MANET. Mobile ad-hoc network is a wireless network. In this network devices will communicate with each other without any access point. In mobile ad-hoc network one mobile node communicates with another node in the absence of Infrastructure. That means it doesn't follow any infrastructure to deliver. In this paper, they described a single black hole attack and cooperative black hole attack in MANET. In the Blackhole attack, the attacker uses the routing protocol to have the best path for the node to which packet attacker wants to intercept. One of the routing protocol is flooding based protocol. Some detection and prevention methods are used to protect routing protocol in MANET. They also focused on reactive and proactive routing protocols, hybrid routing protocols. Some solutions are presented to detect and prevent the black hole attack. The researchers included a table that contains the comparison of black hole attack detection scheme [7].

MANET is an infrastructure less network. It does not have any central controller to transfer the data between nodes. As it is an infrastructure less, it is highly vulnerable to various kinds of attacks. Nowadays MANNET not only used in commercial and domestic application areas but also used in intensive research. In this paper they described how to protect MANET using some applications like reactive and proactive protocols, they also defined some security goals such as integrity, confidentiality, authentication, access control, etc. the author also included problem definition. Instead of forwarding the messages, the malicious nodes drop the words. As more packets will be lost, it leads to the delay in network performance. So to avoid this, they used on technique. That is, they compared the message forwarded versus message received so that the user can know how many packets are dropped [8].

Mobile ad-hoc network (MANET) is a particular type of wireless networks and make a group of mobile devices to build a temporary network without any infrastructure. These networks have widely researched for many years. This system may be a collection from declaring the hubs that are connected across a faraway medium to arrange rapidly progressing topologies. Ad-hoc system of communication can do in the mobility of wireless, and it is very familiar due to its self- structuring and self- managing. MANAT performance is slowly decreasing by disturbing many attacks. In MANET there is no physically fixed infrastructure, and each node acts as a router that can be stored and packets are forwarded to the final destination. In this paper they were described at various systems on security issues, routing protocols, separate layer attacks, manage congestion control and challenges that are faced by the MANET. Keywords that mention in this paper are MANET, security, DES algorithm, RSA algorithm, MD5 algorithm. Therefore it examining the study of various security problems, attacks on data, physical and network layers, different algorithms new methods and protocols are adapted to provide the solutions for security [9] & [11].

Mobile ad-hoc networks (MANET) are one of the rapidly developing areas of communicating technology research. It is a useful technology for various applications like strategic and rescue operations due to dynamic infrastructure for the organization was provided by flexibleness. These network doesn't offer any centralized device, and it can communicate among the different portable devices. The specialty of the MANET property makes it unique among the other networks and makes it different. In the future, these mobile communications include different infrastructure-less mobile ad-hoc networks (MANET) and excellent infrastructure wireless networks. This paper presents some of the challenges were MANETs poses technically and illustrated about descriptive research on ad-hoc networking. It is related to background research that includes the features, concepts, and applications of MANET. The keywords in this paper are ad-hoc networking technology, MANETs, infrastructure-less network, and mobile communication infrastructure network. Mobile communication routed in the form of self-making, self-arranging, self-administration wireless network known as a mobile ad-hoc network [10].

VII.CONCLUSION:

In this article, various classification of attacks and its behaviors discussed. There are different types of security issues. To secure the data from the insecured environment, some prevention techniques, acquiring and internet protocol security need to be adopted.

Network security has an essential part of every organization as it prevents the accessing of information by unauthorized persons. There is a dire need for industries or organization in which the sensitive information had to protected from unauthorized users. Therefore cryptography is an art of coding in which it is difficult to capture/ transfer to unauthorized persons. Hence it is known as the science of writing the secret code. To avoid the adversaries, the protocols can be modified and constructed.

REFERENCE:

[1]. Shilpapareek, AshutoshGoutam, and RatulDey, "Different type Network Security Threats and Solutions" IPASJ International Journal of Computer Science (IIJCS).April 2017.
[2]. Mohan v. power, Anuradha J, "Network Security and types of attacks in the network." International conference on intelligent computing, communication, and convergence. (ICCC-2015)
[3]. Shruthiprabhakar, "Network Security in Digitalization: Attacks and Defence," International Journal of Research in Computer Applications and Robotics in the year May 2017.
[4]. Ruzaina Khan, Mohammad Hasan, "Network Threats Attacks and Security Measures: A Review," Available at online: www.ijarcs.info.
[5]. C.Sridevi, "A Survey on Network Security Attacks and Preventive Measures," International Journal of Computer Engineering Applications in the year Jan 2018, website: www.ijcea.com
[6]. Rossouw von Solms, Johan van Niekerk, "From information security to cybersecurity" in the year 2013, Available online at www.sciencedirect.com
[7]. SandeepLalasahebDhende, Dr. S. D. Shirbahadurkar, Dr. S. S. Musale, Shridhar K Galande, "A Survey on Blach Hole Attack in Moblie Ad Hoc Networks" 4th International Conference on Recent Advances in Information Technology|RAIT-2018|
[8]. Manish Wadhwa, Ashwani Sethi, "A Review on Various Kinds of Attacks in MANET"IJCSN International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017 ISSN (online): 2277-5420.
[9]. HiralVgda, NimeshModi, PhD, "Review Paper on Mobile Ad-hoc Networks," International Journal of computer applications(0975-8887) in the year April 2018. Website:www.ijcaonline.org.
[10]. IshuVarshney, Shahjahan Ali, "Study on MANET: Concepts, Features, and Applications," Elk Asia Pacific Journal of Computer and Information System," Website:www.elkjournals.com.
[11].Umapathi,N. & Ramaraj, N and Adlin Mano, R (2012), "A Proactive Ant Colony Algorithm for Efficient Power Routing using MANET", International Journal of Computer Applications, 58(20): 33-36.
Umapathi,N., and Ramaraj, N. (2016), "Wireless Adhoc Telemedicine System: Improving Network Performance for Multimedia
[12].Data', Journal of Medical Imagining and Heath Informatics, vol. 6, pp.1-5, https://doi.org/10.1166/jmihi.2016.1954
[13].Umapathi.N, (2010), "A Novel Approach to Packet Loss Analysis in a Wireless Network", International Journal of Wireless Networks and Communications. ISSN 0975-6507 Volume 2, Number 3 pp.119-124.