INTERNATIONAL JOUNAL OF: FINANCIAL RES. AND MANAGEMENT SCIENCE

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, NOVEMBER, 2021 EDITIONS
VOL. 7 NO. 7 ISSN: 2773-1040

ANALYZING THE SECURITY THREATS IN IMPLEMENTING WIRELESS AD HOC NETWORKS FOR BUSINESS ENTERPRISES

ABDULLAHI MUHAMMED

Department of Business Administration, Bauchi State University, Gadau. P.M.B 065 Bauchi State. Nigeria.

ABSTRACT

In recent years due to the dynamism of distributed means of communicatio n through wireless channels it has been a challenging task for a secure and uninterrupted communicatio n due to the attack been lunched by intruders to the infrastructure

Introduction

Because wireless ad hoc networks are distributed and they are dynamic which means they have no standard IP addresses it changes as such they have no needed infrastructure for their communication, devices exchange information directly to each other without passing or going through any physical or central infrastructure [1]. In this case securing such a topology is a very tasking process and a bottleneck for security experts. As we all know that there is no maximum security there must be some loopholes still to be exploited in any infrastructure for security. This paper wants to come up with ideas which when added to the existing infrastructures will help improve the current state of the protocol. Both the physical as

of the wireless network. Specialists in network security field have been on alert all this while in coming up with security counter measure in preventing attackers getting access into a network by developing tools such as the Intrusion Detection System, Firewalls and coming up with Access Control Policies to be able to make it hard for any intruder to have access into a network. This paper aims at the deployment of experimental security countermeasures in an ad-hoc environment for wireless networks.

Keywords: *Analyzing, Security, Implementing, Wireless, Business Enterprises*

well as the ad hoc depending on the communication needed at a particular time can relate in some cases. Almost all organizations such as the Military, the Banks or as well as Schools have their own way of securing their communication preventing the leakage of sensitive data such as payroll, customer information e.t.c so they have to implement a security protocol either at gateway of their network or distributed security policies for each section they want to protect depending on the sensitivity of the information they deploy a certain security protocol or can combine two at the same time to add more security. This report analysis possible loopholes and the possible solutions.

Literature Review

Ad hoc networks are meant to be connected instantly between devices an can be releases after it has served its purpose which means is a connection set up there and then to exchange information. The topology organizes itself for communication whereby you don't need any central base for that and it is also self-healing in a case a link breaks in the topology it reorganizes and knows there is a break in that

direction and it finds another route to travel [2]. This kind of topology set up is used mainly where there is no infrastructure for communication or in a situation of disaster and the infrastructures are being burnt and has a significant signal strength for transmission. But attackers normally exploit the vulnerabilities and attack the systems [3].To add to that ad hoc networks transmission range varies with the possible available nodes so packets are sent to a destination node over the network via those mobile nodes and all packets passing through those nodes are exposes which means they are not encrypted as such attackers exploit those vulnerabilities and capture the packets which they may change its integrity as a result. So providing security at those mobile nodes is the daunting task for specialists as it is much more demanding than that of the routing protocols. To use the concept of filtration to filter all packets going through the network which is decentralized you might end up dropping relevant packets which are genuine.As no security is implemented in the OSI network layer on it for the dissemination of packets securing information crossing over this layer is a really important issue [5].

With this in mind if specialists wants to develop new protocols to secure the network level they need to consider the security trio logy which are CIA. The confidentiality assures no third party has seen any information, the integrity means a third party did not change the actual form of the data and the Availability means the data when received is available and accessible [6].

Wireless Ad Hoc Networks

As explained earlier a wireless ad hoc network really helps and is needed for emergency purposes in a situation where we need to retrieve or communicate an information and the wireless infrastructure is down a temporary network can be set up to serve that

purpose. We go through and explore the differences between these two connections the ad hoc and the wireless internet.

In latin the word ad hoc means for 'that purpose' so these kind of connection we normally use them for a purpose and for a particular period of time to avoid overhead for two devices to communicate they don't go through any access point infrastructure they communicate directly to each and depending on the range or pool of networks. These kind of connection is normally set up when there are some technical error on the internet connection or in the case of disaster. Some examples of this connection is are: peer to peer, Bluetooth connection, infrared e.t.c figure 1.0 shows a typical topology of the ad ho network.While in a wireless network topology they use the idea of wave signals for sending data over the network. And it has the information of all available routes for transmission and learns very fast about newer paths and updates its routing table. So when sending packets it routes through this available paths and each node appends the packet with its own identification and passes it over to the next hop until it reaches its destination, and this is how all the nodes learn about any corresponding node because they add there id and each node gets a copy of the message and updates its table with all the id of neighboring nodes.

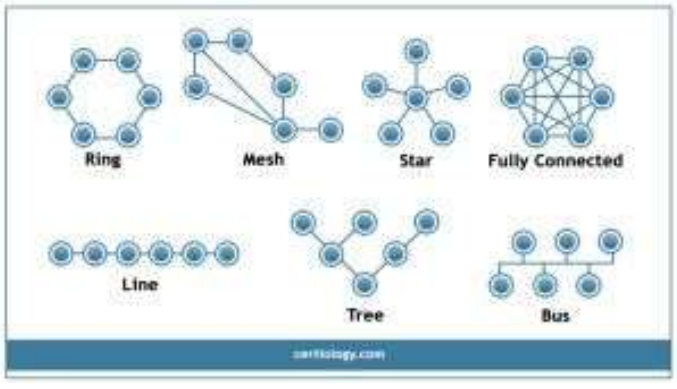

Fig 1.0: Ad hoc topology

Security Implementations

Due to the vulnerability of networks to attacks, policies are being needed to be deployed to minimize some possible attacks which we go in detail to explain in this section. As we are more concentrated on the network layer security can be implemented in many other areas to decrease the probability of possible attacks.In this research we look at some security protocols implemented at the network layer of the internet which are: Secure Shell Layer SSL, Transport Layer Security TSL and the internet protocol security which is commonly known as IPSEC. All this protocols are used or being developed to provide the needed authentication and verification sessions in ip protocol where by a two way authentication is needed. IPSEC protocol provides an end to end secure tunnel for the communicating devices which is user to user or from gateway to gateway and it has two modes of operation which are the Authentication header (AH) and the Encapsulation security Payload (ESP) [6].Where the AH provides authentication and the integrity of the data at both ends whereas the ESP provides an extension to that and gives the authentication, integrity and confidentiality altogether.And the ESP uses both direction key exchange for both encrypting and decrypting at both ends. The TLS protocol provides its security at the node level because each data packet travelling over the network moves from node to node though IPSEC provides us with a secure channel TLS gives us more guarantee in terms of node to node security and it works at layer 4 which is the transport layer[7]. The TLS uses the concept of using public, private key for authentication which gives an improved privacy to reduce eavesdropping in any network communication. The eavesdropper at the beginning might be just monitoring the flow of information without changing the integrity which is called a passive monitoring but when he gets his intended information needed he can turn to an active

one whereby he can make changes to the information in the network. The TLS solves the issue in question and it almost guarantee integrity of data passing over the network where the eavesdropper cannot change the integrity of the data.The secure shell provides security by providing an added shell on the webpages an encrypt every information within a session. Added to that it also authenticates the user as well as the server before the communication is established.The keys are being authenticated by a certificate authority which has both the client and the servers public keys by any request the certificate authority creates a session key between the two parties. Fig 2.0 below shows the mutual authentication between both parties in an SSL session.

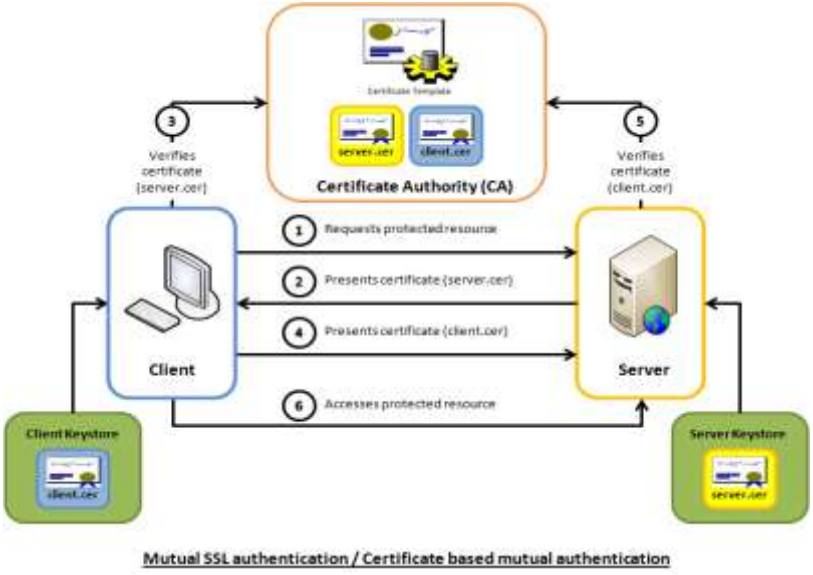

Fig 2.0 SSL Mutual Authentication

Types of Possible Attacks

In this section we will examine various kinds of attacks possible in a wireless network connection, attacks like network session hijacking, the network jamming, the buffer overflow and the man in the middle.

Network Session Hijacking: This occurs where the attacker pretends to be a legitimate user by bypassing his way into the network and will not allow the legitimate user to have access to resources whereby he hijack the session and all client request will go straight to the attacker not the actual server and no resource would be allocated to the user [8].

The Network Jamming Attack: This attack normally tend to target the access point which is the gateway to each network and send some randomly creates radio frequency to disrupt signals going in and out of the point, it is done by bypassing the MAC layer protocol and as a result no communication channel will be available for legitimate users to send or receive packets [9]. The figure below shows how the attack in being done.

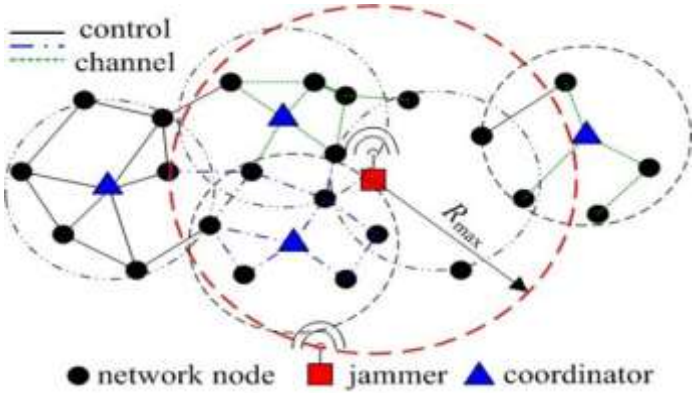

Fig 3.0: Jamming Attack

The Buffer Overflow Attack: In this kind of attack the malicious attacker explores the vulnerability of the buffer where processes are kept for a while before execution, the attacker sends lots of malicious scripts or codes into the buffer queue and once the frame pointer in the buffer points at any of the codes it is being sent into the system for execution and the attacker gets holds of the system and takes any information he needs as the system will start reacting negatively to the legitimate user [10].

Man in the Middle: This is a situation where the attacker intercepts the communication between the user and the server when and sends back the reply claiming its coming from the legitimate server as such the attacker will just be communicating with the attacker ant the attacker can send back the reply message with any malicious code embedded in it and being executed at the user side.

6 Possible Solutions for the Attacks on wireless Ad hoc Networks.

Research is ongoing is the area of wireless networks to be able to bring a lasting solution for the various attacks which are carried out on the network. We tend to propose a few mechanisms for proactive measures to be taken on the network like with the use of Firewalls on the network, packet sniffers, do port scanning, use intrusion detection system IDS e.t.c.

Firewalls: Firewalls are actually being placed to control the flow of traffic and filter all packets coming into a network. They are usually proactive which restricts certain types or kinds of traffic coming in. They are normally placed at the gateway of the network which protects the whole network and there are also host based which protects all traffic coming into a particular machine. So it is also possible to place one on a server gateway to monitor all traffics requests going into the server and restricts certain suspicious packets from gaining access. The picture below depicts the gateway firewall which protects the whole network and as well as the host based firewall which is placed for a particular machine.

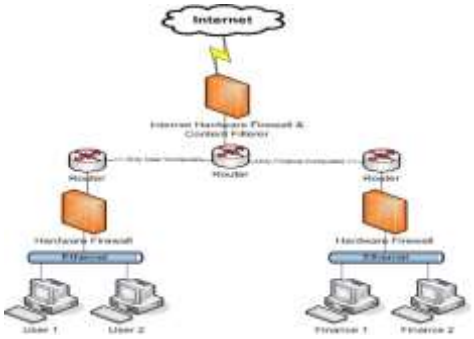

Fig 4.0: Firewalls

Packet Sniffing: This is a technique which is done by installing a software on the client's machine to monitor if there is any anomaly in the traffic which means an intruder is trying to get into the system and it alerts the user of changes in the behavior of the network. And a sniffer software works efficiently when all nodes are connected to the same network.

Port Scanning: The port scanning works to filter packets that are not needed trying to have access into the network by using the scanning technique to scan all the ports available interface weather public or private port network. By doing the port scanning a user will be able to track all activities going on in the network at that particular time and be able to detect any suspicious activity. The range of ports are usually from 0 to 1023 which are used for root privilege and from 1024 to 49151 which are registers [11]

Intrusion Detection System: The IDSs are normally the second line security measures which are normally places after the routers which is the gateway to improve the security of networks or devices. They can be places unlike firewalls they can actually deal with encrypted packets that comes into a network and it protects the system from inside and to monitor the normal behavior of a network and it has a clock which is real time and it keeps up to date the situation of a network or the system. We have two kinds of IDS which are the host based and the network based IDSs, the host based is used mostly to detect attacks on the system such as Trojan as well as it monitors the behavior of the system while the network based reads all incoming packets into the network and protects against attacks like: denial of service DOS and the port scanning attacks [12]. There are still debate on where is the best location to place an IDS but for a best result in a network we can

place two, one at the gateway and the other one at the host so you have two filtrations taking place which is good for privacy, although it's going to make the network a bit slow but it helps in preventing the system from possible attacks such as the masquerading attack.

Conclusion

As it is well known attacks are always possible in ad hoc networks but the challenge at stake is deploying any device or mechanism to stop the attack before it happened or from happening again. In this research the some sensitive mechanisms are being proposed to be able to countermeasure this attacks in wireless network. All organizations that really cares much about security should be able to strengthen the weak points of their network to prevent attackers from exploiting those points to make harm to their sensitive and valuable information.

References

Tung, C.H., Chen, Y.Q., Chen, Z.M. & Tsai, S.R. 2006, "Implementation of security mechanism for ad hoc wireless networks based on X.509 and IEEE 802.1X", IEEE, , pp. 2 pp.

Toumpis, S. & Goldsmith, A.J. 2003, "Capacity regions for wireless ad hoc networks", IEEE Transactions on Wireless Communications, vol. 2, no. 4, pp. 736-748

Murthy, C.S.R. &Manoj, B.S. 2004, Ad hoc wireless networks: architectures and protocols, Prentice Hall PTR, Upper Saddle River, N.J

Day, J.D. & Zimmermann, H. 1983, "The OSI reference model", Proceedings of the IEEE, vol. 71, no. 12, pp. 1334-1340.

Bernard, Ray, and Jim Litchko. "Router Security." Security Technology & Design 18.12 (2008)

Allard, Johan, and Svante Nygren. "IPsec." Data Communications 28.9 (1999)

Elgohary, Ashraf, Tarek S. Sobh, and M. Zaki. "Design of an Enhancement for SSL/TLS Protocols." Computers & Security 25.4 (2006)

Broustis, Ioannis, Ganapathy S. Sundaram, and Harish Viswanathan. "Detecting and Preventing Machine-to-Machine Hijacking Attacks in Cellular Networks." Bell Labs Technical Journal 17.1 (2012)

Xu, Wenyuan, et al. "Jamming Sensor Networks: Attack and Defense Strategies." IEEE Network 20.3 (2006)

Park, Y. -J, et al. "Microarchitectural Protection Against Stack-Based Buffer Overflow Attacks." IEEE Micro 26.4 (2006)

"Researchers Submit Patent Application, "Infrared Scanning Port", for Approval." Politics & Government Week (2013)

Liao, Hung-Jen, et al. "Intrusion Detection System: A Comprehensive Review." Journal of Network and Computer Applications 36.1 (2013)