ISSN:0975-9646

M. Sri Lakshmi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2540-2542

A Review on Wireless Network Attacks

M. Sri Lakshmi[#1], Dr. S. Prem Kumar[*2], S. Ashok[#3]

[#1] *Asst. Professor, Department of Computer Science Engineering, G. Pullaiah College of Engineering and Technology Nandikotkur Road, Kurnool, Andhra Pradesh, India.*

[#3] *Department of Computer Science Engineering, G. Pullaiah College of Engineering and Technology Nandikotkur Road, Kurnool, Andhra Pradesh, India.*

[*2] *Professor & HOD,Department of Computer Science and Information Technology, G. Pullaiah College of Engineering and Technology,Nandikotkur Road, Kurnool, Andhra Pradesh, India.*

***Abstract*—Wireless network communications has been facilitating a way to exchange data between the participating nodes. Due to the open nature of wireless networks, it makes adversaries to launch different types of attacks. Hence wireless network communication remains a challenging and critical issue. Wireless networks are being used in many commercial and military applications to collect real time data and event driven data. In this paper we are going to address different types of attacks in wireless networks.**

1. INTRODUCTION

Wireless Networks consists of large number of nodes interconnected to each other, are becoming a viable solution to many applications like domestic, commercial, and military applications. Wireless networks collects and sends the data from the areas even where ordinary networks are unreachable for various environmental and strategic reasons.

The most promising concepts of wireless networking are auto-configurable and self-organizing. And it provides an adaptable and flexible wireless connectivity to the mobile users. The same notion can be used for different classes of wireless technologies such as wireless local area network (WLAN), wireless personal area network(WPAN), and wireless metropolitan network (WMAN). The work in **[1]**, states that wireless mesh networks are expected to resolve the limitations and improve the performance of ad-hoc networks, like WLANs (Wireless Local area Network), WPANs (Wireless Personal Area Network), and WMANs (Wireless Metropolitan Area Network).

Wireless networks are more vulnerable to security threats, due to the computation and power limitations. Now a day's many laptops are coming with pre installed networks cards. The ability to enter into a network while moving has a great benefit. However, there are many security issues with the wireless networking. As the security techniques becoming old, it becomes easy to crack. To overcome this, the network administrators or the users must stay up-to-date on any new risks that arise.

2. WIRELESS ATTACKS

2.1. Cipher attacks:

Cipher attack is an attack model in cryptanalysis. In cipher attack, cryptanalyst gathers information data that is exchanged between two parties and decrypts the gathered data under an unknown key. Some of the cipher attacks are WEP attacks, WPA-PSK Dictionary attacks, WPA/TKIP attacks, LEAP attacks.

a. **WEP attacks:**

Wired Equivalent Privacy (WEP) is relatively trivial to defeat. There exist numerous attacks with WEP. It is first level of security, build into any wireless device. WEP security enabled devices works on the Wired Equivalent Privacy (WEP) algorithm. This WEP algorithm is designed and used to overcome the most security threats. The recipient with correct WEP address is the only one can decrypt information. Basically, this algorithm is designed to prevent unauthorized access on wireless networks **[2]**.

There are some security threats with this WEP, they are easy access, rouge access points, data tampering, masquerading. WEP algorithm has been broken for more than 10 years. So, this should not be used for securing our wireless networks.

b. **WPA-PSK dictionary attack:**

WPA stands for Wi-Fi Protected Access, is the security protocol and security certification program developed by the Wi-Fi Alliance. This WPA also prone to many security problems. The weak point in WPA PSK is its passphrase. Users often choose to configure short passphrase, dictionary based passphrases leaving them vulnerable to attack. Attackers can capture the packets on air during the key exchange of a client for joining the wireless network. Then performing the offline dictionary attack on the passphrase.

c. **WPA/TKIP**:

TKIP protocol was designed by the IEEE 802.11i task group and Wi-Fi Alliance as to replace the WPA without requiring the replacement of legacy hardware. TKIP is not considered as secure and deprecated in the 2012 revision of 802.11 standards. The TKIP attacks works in a similar way to WEP chopchop attack and can provide the clear text but doesn't expose the key. This attack severe can be reduced with a short keying time of 120 seconds or less. However, WPA2/AES would be the recommended solution.

And it is recommended that sites can use a more robust authentication mechanism such as EAP/TTLS, PEAP, etc.

2.2. Man-in-the-middle attacks (MITM):

Man in middle attacks is an active attack, in which attackers eavesdrops over the independent connections of the victims and relays messages between them. And the two victims believe that they are conversing directly to each other but, actually the entire conversation is controlled by the attacker.

Man-in-the-middle attacks are easy when the packets are not encrypted or using poor security mechanism. To overcome this type of attacks, some cryptographic protocols are used which includes endpoint authentication, particularly to prevent MITM attacks (for example, SSL authenticates the parties using mutually trusted certificate authority).

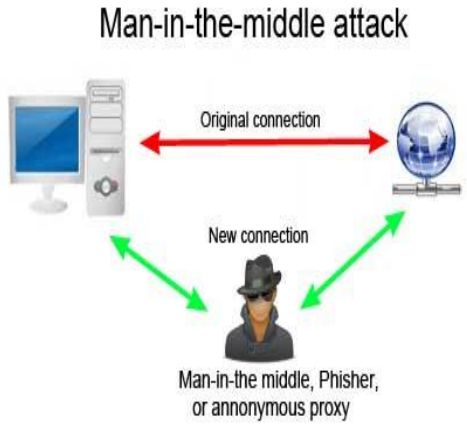

Fig. 1: Man-In-The—Middle attack

Some different types of Man-in-the-Middle attacks are Captive portal, 80.21X/EAP

a. Captive portal:

Sometime due to no proper authentication and no certificate exchanges, the attacker may attack and grab the important information by developing the web page which resembles to that which the party requested. Attackers can even acts as proxy passing the credentials that were grabbed onto the real authentication server.

Hence data can be captured by the attacker. So, to overcome this, an exchange of certificate should be done prior to the communication, the certificate specifies the properties of authentication and the type of encryption that going to be done on the data **[3]**. And even this exchange of certificate should be automatic. So that there would be no more overhead of separately requests of certificates.

b. 802.1X/EAP:

IEEE 802.1X is an IEEE standard for Port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

EAP is Extensible Authentication protocol (EAP). IEEE 802.1X defines the encapsulation mechanism of the extensible authentication protocol over IEEE 802 which is known as EAP over LAN or WLAN.

Many clients are not configured correctly, leaving them vulnerable to attacks. This vulnerability arises due to not verify the RADIUS server. To overcome the wrong certificate exchange a model is introduced. In this model i.e., 802.1 X authentications involves three parties: authentication server, supplicant, an authenticator. Client devices are the supplicants. Supplicants are the devices that wish to connect to the LAN or WLAN **[4]**. And these devices provide their credentials to the authenticator. Authenticator is a network device, such as an Ethernet or wireless access point. Authentication server is host running software that supports the RADIUS and EAP protocols.

The authenticator acts like a security guard to the protected network. The client device i.e., supplicant is not allowed to access through the authenticator to the protected side of network. Supplicant is allowed to accesses the network only after the supplicant identity is validated and authorized.

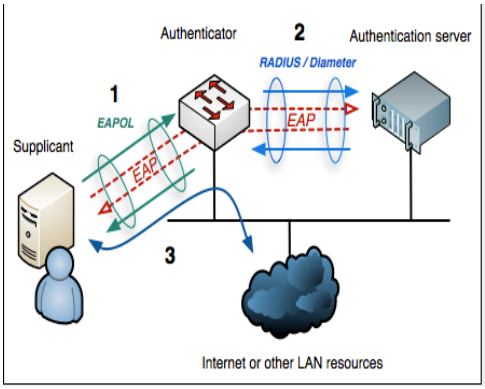

Fig. 2: 802.1X/EAP

The above figure shows how the supplicant is authorized in the wired network.

2.3. Denial of services attacks:

Denial of service (DoS) of attack is an attack that is made to makes a network resource unavailable to the targeted users. Denial of Service attack is characterized by an explicit attempt by the attackers to prevent the legitimate users of services from using the services. There are two different forms of the DoS attacks: they are crash services and flooding services.

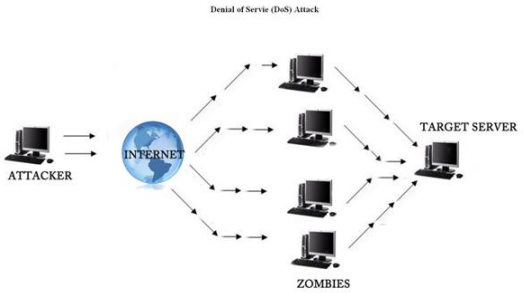

Fig. 3 : Denial of Service Attack

Denial of services attack can be done in many ways. Dos attack types can be categorized into five families:

1) Interruption of physical network components.
2) Interruption of routing information.
3) Disruption of sate information, i.e., restoring settings of TCP session.

4) Consumption of computational resources, i.e., bandwidth, flooding etc.,
5) Blocking the communication between the target users and the victim so that there could be no longer communication between them.

a. Jamming attack:

Jamming is the transmission of radio signals that interrupts communication by decreasing the SNR (Signal to Noise Ratio). Unintentional jamming happens when an operator transmits a busy frequency without prior inspect of whether it is in use or not **[5]**. This works simply by generating the Radio Frequency (RF) noise within the frequency range used by the wireless networking equipment. The devices which operate under the same frequency may prone to the jamming of the communication, for example microwaves, radars, monitor etc. which are nearby. Jamming attacks are much difficult to find. They have been shown to severe DoS attacks towards wireless networks **[7]**, **[8]**, **[9]**, **[10]**.

These attacks can be categorized into two types, external jamming attacks and internal jamming attacks. External jamming attacks are the attacks made by the attackers which are not the part or not the member of that wireless network. Internal jamming attacks are made by the nodes (intermediate node) that are the part of the wireless network. Internal jamming attacks are the attacks made by the adversaries who are aware of network secrets and implementation details of network protocols. The solution for these internal jamming attacks has been addressed in **[6]**.

b. Flooding:

Flooding is the type of Denial of Service attacks, in which flooding may be Authentication flooding, De-Authentication flooding, etc. In this attack a continuous transmission of a particular type of packets are sent into the network. For example, in authentication flooding the wireless network can be attacked by flooding with authentication and association frames at Access Point (AP). Thus the attacking device will spoof its MAC address continuously, trying to associate with the access point. At each and every attempt the attacker will change the MAC address, mimicking the existence of different clients. Thus this consumes the access point (AC) processing ability, memory, denying the service of other clients **[11]**.

3. CONCLUSION

There are different types of attacks that exist for wireless networks. Many of these attacks can be mitigated through using the latest techniques and best practice. And the minimum security measure should be taken to overcome the wireless attacks, such as proper authentication, finding rough access points, best encryption techniques etc. By using the protected management frames like 802.11W, the management traffic attack such as authentication and de-authentication packets can be mitigated. Probably the most important is to use the best encryption techniques such as WPA/AES with proper implementation on 802.1X authentication system.

REFERENCES

[1] Ian F. Akyildiz, Xudong Wang and Weilin Wang, “wireless mesh networks: a survey,” Computer Networks, vol. 47, pp. 445-487, Jan.2005.

[2] Kcng H., “Security Guidelines for Wireless LAN Implementation.” SAN Institure ,August 271h 2003., http://www.Sansorin/lwhitepapcrs/wirelcss/1233.html,LastAccessed: December 6 , 2010

[3] Detecting and Blocking Unauthorized Access in Wi-Fi networks N. Mitrou et al. (Eds.) : NETWORKING 2004, LNCS 3042, pp. 795-806, 2004. IFIP International Federation for Information Processing 2004

[4] X.GU and R.Hunt, “wireless LAN attacks and Vulnerabilities” In the Proceeding of IASTED Networks and Communication Systems. April

[5] Denial of Service Attacks in wireless networks: The case of Jammers, Pelechrinis ; Univ. of California, Riverside, CA, USA ; lliofotou, M.; Krishnamurthy, S.V. IEEE 2011 Volume: 13, Issue: 2.

[6] Packet-Hiding Methods for Preventing Selective Jamming Attacks. Proano,A; Dept. of Electr. & Comput. Eng., Univ. of Arizona, Tucson, AZ, USA ; Lazos, L. IEEE 2012, Volume: 9, Issue:1

[7] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

[8] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review, 7(3):29–30, 2003.

[9] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of MobiHoc, pages 46–57, 2005

[10] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatialretreats: defenses against wireless denial of service. In Proceedings of the 3rd ACM workshop on Wireless security, pages 80–89, 2004.

[11] Defending against flooding-based distributed denial-of-service attacks: a tutorial, Chang,R.K.C; Hong Kong Polytech. Univ., Kowloon, China. IEEE 2002 Volume:40 Issue:10