A Review Paper on Security of Wireless Network

Kirti Kaushik
Department of Computer Science and Engineering of DPGITM
Maharishi Dayanand University, Gurgaon
Haryana, India
Kaushikkirti77@gmail.com

Nidhi Sewal
Department of Computer Science and Engineering of DPGITM
Maharishi Dayanand University, Gurgaon
Haryana, India
Sewal.nidhi1@gmail.com

Abstract— In the past few years, wireless networks, specifically those based on the IEEE 802.11 Standard, have experienced tremendous growth. A team at Rice University recovered the 802.11 Wired Equivalent Privacy 128-bit security key which is used by an active network. This Standard has increased the interest and attention of many researchers in recent years. The IEEE 802.11 is a family of standards, which defines and specifies the parts of the standard. This paper explains the survey on the latest development in how to secure an 802.11 wireless network by understanding its security protocols and mechanism. In order to fix security loopholes a public key authentication and key-establishment procedure has been proposed which fixes security loopholes in current standard. The public key cryptosystem is used to establish a session key securely between the client and Access point. Knowing how these mechanism and protocols works, including its weakness and vulnerabilities can be very helpful for planning, designing, implementing and/or hardening a much secure wireless network, effectively minimizing the impact of an attack. The methods used in current research are especially emphasized to analysis the technique of securing 802.11 standards. Finally, in this paper we pointed out some possible future directions of research.

Keywords- *IEEE 802.11, wireless LANs, threats, Wi-Fi, WEP, Access Points, DoS, Wireless Security (key words)*

*****

I. INTRODUCTION

Wireless networks are emerging as a significant aspect of networking; wireless local area networks (WLANs, see Acronyms and Abbreviations), Bluetooth, and cellular systems have become increasingly popular in the business and computer industry, with consequent security issues. WLANs, especially the Institute of Electrical and Electronics Engineers (IEEE) 802.11 networks, are becoming common access networks in private and public environments. The freedom of movement and simplicity in its implementation has made WLANs popular in the home and businesses sectors, as well as hotspots 1 such as airports and cafes. The increasing availability of, and therefore increasing reliance on, wireless networks makes it extremely important to maintain reliable and secure communications in the wake of network component failures or security breaches.

The IEEE 802.11 standard for WLANs is one of the most widely adopted standards for broadband wireless Internet access. The first 802.11 standard came out in 1997. It featured data transfer speed of a maximum of 2 Mbps. The second version came out in 1999 and was called 802.11b. Data transfer speed of 11mbps. At the same time IEEE 802.11t was also released which allowed 802.11 to run outside the crowded 2.4-Ghz industrial, scientific and medical band and in the 5-GHz Unlicensed National Information Infrastructure band. It could support maximum data transfer rate of 54 Mbps then in 2003, they released another speed boost, 802.11g, which brought 54 Mbps, while also utilizing the 2.4-GHz band. The next speed increase is 802.11n, which allows speeds of 100Mbps. The standard provides three physical (PHY) layers and one medium access control (MAC) layer for deploying wireless communication in local networks. As for the logical link control (LLC) layer, there is no difference between wireless (802.11) and wired (802) LANs, such as the IEEE 802.3 Ethernet network. The MAC protocol provides two service types Asynchronous using the distributed coordination function (DCF) and synchronous using the point coordination function (PCF) that is contention-free.

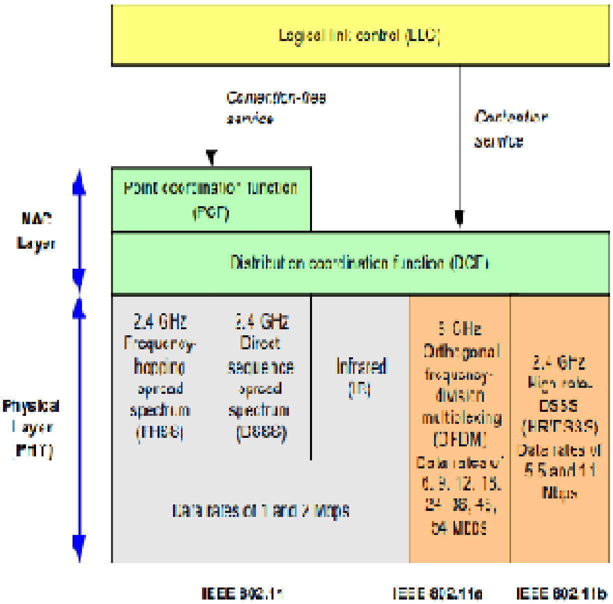
Logical link control (LLC)
Contention-free service
Contention service
MAC Layer
Point coordination function (PCF)
Distribution coordination function (DCF)
Physical Layer (PHY)
2.4 GHz Frequency-hopping spread spectrum (FHSS)
2.4 GHz Direct sequence spread spectrum (DSSS)
Infrared (IR)
Data rates of 1 and 2 Mbps
5 GHz Orthogonal frequency-division multiplexing (OFDM) Data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps
2.4 GHz High rate DSSS (HR/DSSS) Data rates of 5.5 and 11 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b

Figure 1: The 802.11 Protocol Stack

The IEEE 802.11 standard has defined the following two basic security mechanisms for secure access to IEEE 802.11 networks:

- Entity authentication, including open system and shared key authentication
- Wired Equivalent Privacy

II. LITERATURE REVIEW

The IEEE 802.11 standards and several researchers have made significant contributions on WLAN security aspects. It was examined in how users from the general public understand and deal with privacy threats associated with Wi-Fi use. It was found that users lack knowledge of immediate risks, and this made them unmindful of privacy and security in using Wi-Fi. It was recommended that privacy and Wi-Fi security problem can be effectively handled through end user awareness tools and improving Wi-Fi infrastructure. An approach for providing an end-to-end wireless security for local area network client/server environment was proposed and implemented. Performance of encryption algorithms— Rivest Cipher 4 (RC4) and Advanced Encryption Standard (AES) in terms of time, memory and power were evaluated for different devices, key sizes, and the cryptographic algorithms with and without transmission. The result of the work showed that both RC4 and AES performed similarly in just about all cases. But when transmission of data is considered, RC4 performed slightly better than AES in lightweight devices such as on pocket PC that have very limited processing power and memory. The results question the reality of relying on secret key crypto system in establishing credentials and data protection. A research on IEEE 802.11-2007 Media Access Control (MAC) security in union to IPsec concludes that the security provided by the 802.11 standard is successful in defending against many popular attacks including: session hijacking, denial-of-service attacks against the authenticator, man-in-the-middle attacks, forgery attacks, data manipulation attacks, fragmentation attacks, iterative guessing attacks, redirection attacks, and impersonation attacks but denial-of service attacks against the supplicant are still possible to achieve. The paper concludes that implementing Internet Protocol Security (IPsec) concepts in any part of the Robust Security Network Association (RSNA) would successfully prevent denial-of-service attacks.

III. PROBLEM STATEMENT

In the problem statement part, few ways are defined in order to find various security loopholes in IEEE 802.11 Wireless LAN protocol and provide measures to improve its security at protocol and physical level. This problem can be divided into following sub problems:

a. A more secure authentication and key establishment mechanism is to be design.

b. A centralized Rogue Access Point detection system is to be design.

c. In order to detect Evil-Twin Access Points an algorithm is need to be design.

IV. BACKGROUND STUDIES AND RESEARCH

"A Survey of Wireless Security" presents a summary of security improvements of WEP protocol that can lead to a higher level of wireless network infrastructure protection. In this research comparative analysis shows the advantages of the new 802.11i standard in comparison to the previous security solutions. The access point vulnerabilities to DoS attacks in 802.11 networks with experiments on various network configurations takes place. The experiments showed that the extent of vulnerability to DoS attacks strongly depends on the firmware used by the Access Points. A Pseudo Randomized sequence Number is based on a solution to 802.11 Disassociation DoS attack. It suggests that the solution does not require any additional hardware and can be implemented in both wireless clients and Access Point via firmware upgrade. A Pseudo Random Number is based on an Authentication to counter DoS attacks on 802.11. It presents a mechanism which can be easily deployed as a comprehensive solution to all the discussed DoS attacks without any additional hardware or infrastructure requirements.

The problem of Rogue Access Points still exists in Wireless LANs. Rogue Access Points can cause serious problems like back-door entry to the corporate network to phishing attacks on wireless users. Evil-twin Rogue access Points make the threat even more serious since they are extremely difficult to detect.

From the above research gaps the following are required in a proposed scheme to mitigate security threats in Wireless LANs.

- An authentication and key-establishment scheme, which can prevent denial of service attacks and insider attacks on wireless LANs.
- A mechanism to provide protection to both uni-cast as well as multi-cast management frames.
- A centralized Rogue Access Point Detection and counter-attack system, which can be easily deployed on existing corporate networks.
- A method to detect Evil-Twin access points.

V. NEW PROPOSED TECHNIQUE

A. Proposed Authentication and Encryption Mechanism

A symmetric key cryptosystem is a fast and efficient way to encrypt data. The authentication scheme proposed by us is shown ii figure The Access Point has a public and a private key. The public key can be distributed to the client's offline or can be provided with a certificate. The clients then use this public key to establish a Session Key with the AP as shown in MESSAGE-2. The Session-Key is chosen by the AP. This is done in order to prevent replay attacks in ease a previous session key has been compromised. Since the session key is chosen by the AP, it is guaranteed to be fresh and confidential. The client sends a Pre-Session Key to the AP by encrypting it with the Public Key of the AP.

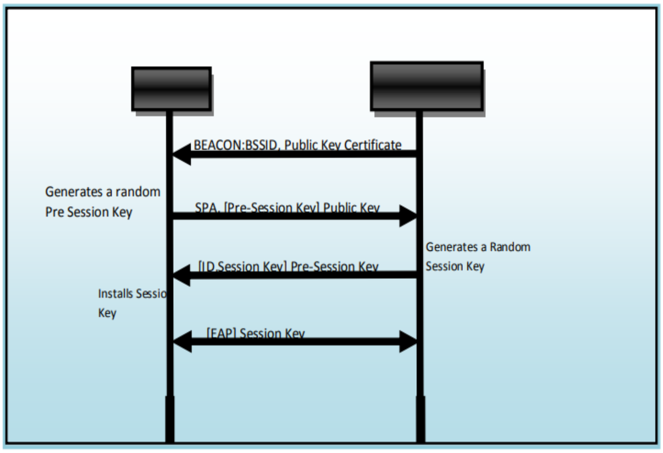
BEACON:BSSID, Public Key Certificate
Generates a random
Pre Session Key
SPA, [Pre-Session Key] Public Key
Generates a Random
Session Key
[ID,Session Key] Pre-Session Key
Installs Sessio
Key
[EAP] Session Key

Figure-2 Asymmetric-Key Authentication Mechanism

The access point can broadcast its public key in its BEACON frame and in the probe e frame. The public key can either be accompanied by a certificate or its authenticity can be verified offline.

Once the public key of the Access Point is known to the client rest of the authentication procedure is autonomous and secure. The messages exchanged are as follows:

[Frame 1: AP-> STA] BEACON
BSS1D, Public Key, Certificate
[Frame 2: STA-> AP] Association
[Pre-Session Key]Public Key
[Frame 3: AP -> STA] ACK
[ID, Session Key]Pre-Session Key
[AP -> STA]
EAP [EAP] Session Key

The complete procedure ensures that clients first establish a secure Session Key and then authenticate themselves to the server. Attackers can neither sniff the session key nor launch DOS attacks by blocking the authentication procedure.

B. Mitigation of Attacks

The proposed asymmetric authentication procedure mitigates most of the attacks as follows:

- ➢ Protection for Management Frames

In 802.11i there is no provision for protection of management frames. But using asymmetric authentication scheme all management frames that are sent before any session key is established are signed by the public key of the AP and thus protected from any modification.

- ➢ More Key Exchange Mechanism Secure

The proposed key-exchange mechanism is more secure than the earlier 4-way handshake. The vulnerable 4-way handshake is completely removed, so DOS attacks on it will not be possible. In the proposed mechanism all messages are protected.

FRAME-l is protected by the certificate. This protects it against modification.

FRAME-2 is protected by the public-key of the Access Point. Hence only the Access Point can read it.

FRAME-3 is protected by the pre-session key, which only the client knows. Thus only the concerned client can decrypt it

- Protection Against Insider Attacks

In the asymmetric-key mechanism proposed all clients get a random session key chosen and securely sent to the clients by the AP. Hence all session keys are secure.

- Mitigation of Denial of Service Attacks

The asymmetric-key authentication mechanism protects the network from de-authentication attacks by protecting management frames. The protection of management frames has been described earlier. Now attackers cannot send forged de-Authentication frames. Hence de-Authentication denial-of-service attacks are not possible. , DOS attacks were also possible since FRAME-I of the 4-way handshake was not protected. This enabled attackers to continuously send forged FRAME-I blocking a client from authentication procedure. In the proposed mechanism the 4-way Handshake is replaced y an asymmetric key session key establishment mechanism h which all messages are authenticated. This mitigates denial of service attacks on the 4-way handshake.

VI. CONCLUSION

Various solutions are proposed for many problems, but some issues still remain unsolved. Security is very important in Wireless LANs since they operate in a broadcast medium. Network and frequency jamming are still exist which can be cause of DoS attacks. Due to backward compatibility, open system authentication is also present due to which various attacks like man in the middle attack and message forgery etc are also possible. For removing the DoS attacks in 4-way handshake protocol, a 2-way handshake protocol has been proposed, but it is solely dependent on secrecy of PMK. However, PMK can be cracked using tools like aircrack which are based on dictionary attack. Therefore, key distribution also suffers from the DoS attacks. We conclude on the note that authentication mechanism is still vulnerable to DoS attacks.

VII. FUTURE SCOPE

There is obviously scope for improvement and future work. The possible improvements to our work can be:

- The proposed authentication scheme has been shown to mitigate existing attacks, it should be evaluated by formal evaluation method and predicate logic for the sake of completeness.
- It was shown that public-key cryptosystem is feasible in Wireless LANs by simulating it on machine with CPU speed comparable to Access Points. As future work the mechanism should be implemented on an actual Access Point and tested form feasibility.
- The RAP detection system only detects Rogue Access Points. A counter attack system can be incorporated into the Rogue Access Point system to block detected RAPs in the future. This can be done using SNMP to block the port where the Rogue Access Points are connected.

REFERENCES

[1] William A. Arbaugh, “Wireless security is different” Computer, Vol.1, pp.99-101, April 2003.

[2] William A. Arbaugh and Shankar, “Your 802.11 Wireless Network has No Cloths,” Wireless Communication, IEEE, vol.9, pp.44-51, December 2002..

[3] Ellingson, Jorgen. “Layers One & Two of 802.11 WLAN Security”August3,2001 http://rr.sans.org/wireless/WLAN_sec.php

[4] Edney, J. and Arbaugh, W. (2003). “Real 802.11 Security: WiFi Protected Access and 802.11i”. ISBN: 0-321-13620-9.

[5] Stubblefield, A., Ioannidis, J. and Rubin, D. (2001). Using the Fluhrer, Mantin, and Shamir Attack. to Break WEP.

[6] Junaid, M., Muid M. and Umar, M. I. (2007). Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol. World Academy of Science, Engineering and Technology, 11(200), pp. 910-915.

[7] Zhimin , Y., Adam, C ., Boxuan, G., Xiaole, B. and Dong, X. (2009). “Link-Layer Protection in 802.11i WLANs with Dummy Authentication.” WiSec ’09 proceding of the second ACM conference on Wireless network security.

[8] Sriram, V.S.S.;, “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN-a multi-agent sourcing Methodology,”Advance Computing Conference 2010 IEEE 2nd International, pp.256-260, 19-20 Feb 2010.

[9] ANSI/IEEE. Std 802.11 (1999). Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. New York. First Edition. Institute of Electrical and Electronics Engineers, Inc. ISBN 0-7381-1658-0. 20 August.

[10] Konsgen, A., Zakir Hossain, and Carmelita Gorg. "Transmit power control algorithms in ieee 802.11 h based networks." Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on. Vol.3. IEEE,2005.