ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Comparative Study On IEEE 802.11 Wireless Local Area Network Securities

Keshav Jindal
A.P., Dept of CSE
BPR College of Engineering, Gohana Sonipat, India
jindal.keshav43@gmail.com

Surjeet Dalal*
Research Scholar
Suresh Gyan Vihar University Jaipur, India
surjeetdalalcse@gmail.com

Vivek Jaglan
Research Scholar
Suresh Gyan Vihar University Jaipur, India
Jaglan.vivek@gmail.com

Abstract: The IEEE 802.11 Wireless Networks gains its popularity and fame by providing the users with several advantages in accessing information. WLANs provide true mobility and flexibility to users. Another advantage of wireless technology is installation. A physical or cable connection is no longer needed because a single connection to the access point via electromagnetic waves is all that is necessary. This both decreases installation costs and allows for wireless networks to be installed in locations where previously it would have been difficult or impossible to install wiring. Such benefits and advantages bring up some security and performance problems. Various researchers have proposed several solutions to improve WLAN security and to understand the impact of the security mechanisms on the performance of the network. However, the establishment of a tradeoff between security and network performance is often neglected. The aim of our research paper is to quantify the impact of the security mechanisms on the performance of the network.

Keywords: WLAN, WEP, WPA, WPA2, WPS, Wi-Fi protected setup

I. INTRODUCTION

The wireless LAN technology and industry were born in the mid 1980s when radio frequency (RF) spectrum was first made available by the Federal Communications Commission (FCC). When it was first introduced to the market, growth was considerably slow. Lately, wireless LAN technology is experiencing incredible growth. In addition to the flexibility it provides to the users, one of the key reasons that allows its growth is the increased bandwidth made possible by the IEEE 802.11 standard. Table 1.1 provides some key and important characteristics of the 802.11 standard.

WLANs are based on a set of IEEE standards named 802.11. 802.11-1997, which defines WEP security algorithm, was the first standard in the 802.11 standards family released in 1997. [1] The standard was clarified in 1999 under the name 802.11-1999. [2] In the same year were released amendments IEEE 802.11a-1999 and IEEE 802.11b- 1999. The former defines wireless transmission in a rate of 54 Mbps at 5 GHz frequency, and the latter in 11 Mbps at 2,4 GHz. In 2003 were released the amendment IEEE 802.11g- 2003, which defines 54Mbps data rate at 2.4 GHz frequencFy. The amendment IEEE 802.11i-2004 was published in 2004. [9] It defines new security mechanisms for WLANs, named WPA and WPA2.

Table 1.1: Characteristics of 802.11 Wireless LANs

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum, Frequency Hoping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11Mbps (11b), 54 Mbps (11a)
Data & Network Security	RC-4 based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for802.11i).
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.
Negative Aspects	Poor security in native mode: throughput decreases with distance and load.

WPA was released already in 2002, but not in a form of an official standard amendment. In 2007 the valid standard from the year 1999 and all the amendments published after it were combined in a new standard, named IEEE 802.11-2007, which is the valid version of the standard at the moment. [10] IEEE 802.11n is a proposed amendment to the 2007 standard, and it is expected to be approved in 2010. The amendment defines a new transmission mechanism for WLANs, which can reach data rate of 600 Mbps.

This paper analyses security of the WLANs primarily based on four important concepts in information security: confidentiality, integrity, availability and authenticity. Confidentiality is a property of keeping information secret, so that only authorized parties are allowed to get it. Integrity means that data cannot be modified without authorization, or any unauthorized data modifications are detected.

Availability means that data is available for its users. Authenticity means that each communicating party can be sure that other parties are who they claim they are. Designing a good security technique is mostly about balancing between these properties.

II. WIRELESS LAN SECURITY

Wireless Local Area Networks have gained a tremendous and incredible popularity across the computer network market over the years. However, the threats and security fears associated with them have caused some network managers and administrator to avoid installing wireless LAN, regardless of the numerous benefits that they provide. Several manufacturers understand the fears, uncertainties and doubts caused by the security problems of the Wireless Local Area Network. They realize that coming up with a security measure to make the WLAN more secure would be a great asset and source of profit for them. Thus, they invest in research with the goal of coming up with a solution that satisfies the needs of the buyers when it comes to the security of the IEEE 802.11 WLAN.

A. Goals of Wireless LAN Security:

The main goal of the wireless LAN security is to protect the privacy of the clients just to make sure that an attacker is not able to access the network without any permission and attack them. The following goals should be considered to implement effective wireless LAN security:

a. Maintain the confidentiality of data as it is stored, processed or transmitted on a wireless LAN.
b. Maintain the integrity of data as it is stored, processed or transmitted over a wireless local area network.
c. Maintain the availability of data stored on a wireless LAN, as well as the ability to process and transmit the data in a timely fashion.
d. Identify and ensure the identity of the sender and receiver of a message.

B. Wireless Security Threats and Attacks:

The security solutions decrease the chances or opportunities for an attacker to penetrate the WLAN but still most of them are vulnerable to attacks. The attacks that allow unauthorized users to get access to the system are divided into: active and passive attacks. Figure 1. Shows several types of attacks and security threats that can be used by an attacker to attack a wireless LAN.

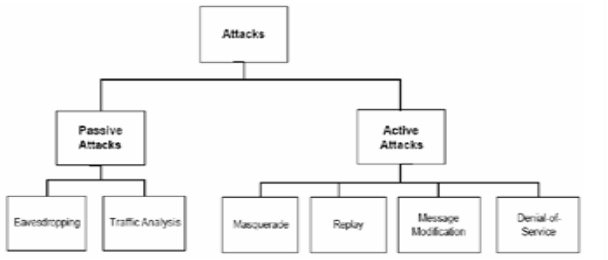

Figure 1: Security Threats and Attacks

III. 802.11 SECURITY ISSUES

This section identifies possible threats against wireless networks by classifying them into a six groups. It is actually hard to divide the attacks into separate categories because some overlapping always exists between the definitions. The attacks are collected from [5] and [6].

A. Eavesdropping:

Because radio waves propagate in every direction, wireless data traffic can always be sniffed and recorded by anyone near the transmitting stations. Eavesdropping is a threat to information confidentiality. It can be conducted passively, and so it is impossible to know whether the wirelessly transmitted. Information is captured by an adversary.

B. Message Modification:

An adversary may not only be able to passively listening to the wireless data traffic, but it can also send messages in the network. Message modification comprises all the operations to add, modify or delete packets in the wireless network. Adding means generating completely new packets. Modifying and deleting requires that the adversary has a control of the wireless channel, because the adversary must be able to prevent the original packets from reaching their destination.

One form of message modification attack is replay attack. In this case, an adversary records a valid transferred message and sends the same message later to the wireless channel. In a replay attack, the adversary does not have to be able to decrypt the message to be able send it again.

C. Masquerading:

An adversary can try to masquerade as a valid wireless station or an access point. For example, a valid wireless station can reveal its credentials to the fraud access point when it is trying to log into the network, if the wireless station is not able to detect the deception. Session hijacking is a special type of masquerading attack: in that case, an adversary takes over a valid session after the session initiation has been made.

D. Key Management:

Another type of key being used is the key management which is a static WEP key that can be either 40 bits or 128 bits of sizes. When this method is used, the static key has to be the same on every devices of the wireless LAN. The drawback of using it is that, if the static WEP key has been deciphered by an attacker, there is no way of knowing that.

E. Man-in-the-Middle:

In man-in-the-middle attack an adversary infiltrates itself between a wireless station and an access point. Both of the communicating parties believe they are connected to each other, but in reality both communicate with the adversary. Man-in-the-middle attack may resemble message modification but it is considered different type of attack, because in man-in-the-middle the adversary must participate in the communication continuously.

F. Denial-of-Service:

The purpose of denial-of-service attacks or DoS attacks is to hinder communication in the wireless network. This type of attack is the most difficult to prevent, because it is always possible to jam the radio link between the parties. On the other hand, denial-of-service attacks are the easiest ones to detect, when comparing to other attacks. Roughly two types of DoS attacks exists: so called brute methods can be used, where the wireless channel is continuously disturbed by an adversary.

The other type of DoS attack exploits the flaws of wireless protocols by means of more subtle attack.

IV. WIRED EQUIVALENT PRIVACY

WEP is the first link-layer security standard of WLANs and it was included in the original IEEE 802.11 standard published in 1997. [7] It was soon found out that WEP has some major flaws in its design. In 2001 was published the first attack which was able to recover the pre-shared secret key and thus an adversary using that attack is able to decrypt all the traffic in the network. [4]. after that more and more efficient algorithms have been developed to break the encryption of WEP. At the moment the fastest ones are able to do it in less than a minute and require processor time only a few seconds.

WEP uses RC4 stream cipher for confidentiality and CRC-32 checksum for integrity. [8] WEP works as follows: Before a connection protected by WEP can be established, a pre shared secret key has to be divided between the communicating parties. First the CRC-32 checksum is calculated and added in the end of a packet. Together they form a plaintext. The plaintext is then encrypted with RC4 stream cipher. The pre-shared key is concatenated with a selected 24-bit size per packet initialization vector to form an RC4 traffic key. The traffic key is put into the RC4 algorithm to generate a key stream. The key stream and the plaintext are combined with exclusive-or operation (XOR) to produce a cipher text, which is sent through the wireless network. The initialization vector is transmitted unprotected with the packet.

A. Attacks Against Confidentiality:

WEP has several severe weaknesses and too short cipher keys are one of them. Standard WEP uses 40-bits long keys which are too short, because they can be broken by trying different key possibilities, i.e. using brute force technique. A new version of WEP with 104-bit keys has been implemented, which is more time consuming to break by brute force. Brute force techniques are not needed to break WEP, though. An attack named FMS was the first key recovery attack against WEP. [4] The attack works as follows: An adversary, who wants to get the pre-shared secret key to be able to decrypt the traffic, listens to the traffic in the wireless network and records a lot of encrypted packets. Because the first bytes of the plaintext are predictable in most packets, the adversary can recover the first bytes of the key stream. Because the initialization vector is transmitted unprotected, the adversary knows the first 24 bits of the RC4 traffic key. Thus, the adversary has part of the input for RC4 algorithm (initialization vector) and part of the output key stream (calculated from the first plaintext bits and the cipher text). With huge amount of valid packets the adversary is able guess the rest of the RC4 traffic key. Around 5,000,000 packets is needed to recover the key with 50 % probability. The attack is slow but still practical. In addition, the attack is passive, so the adversary does not have to reveal its existence.

In 2007 completely new type of attack against WEP was published named PTW. The attack required only about 40,000 encrypted packets with 50 % success probability, which means that only a minute is needed to gather needed packets in a fast network. Still, development of better attacks against WEP has not stopped: the Kore K attack has been improved further, and in 2008 was published a modified version of the attack requiring only 25,000 packets to 50 % success rate.

B. Attacks Against Integrity:

WEP uses CRC-32 checksum to calculate a message integrity code (MIC). Its purpose is to verify that packets do not get modified in transit. CRC-32 algorithm takes as an input an arbitrary length stream of bytes (in this case a packet) and produces as an output a 32-bit length integer value (the checksum). [8] CRC-32 algorithm popular, because it is very simple and computationally light. Bare MIC protects well against random transfer errors, but it is useless when contents of packets are changed on purpose, because an adversary is able to calculate the CRC-32 checksum again for the modified packet. To protect against intentional modification, message authentication code (MAC) is a common solution in cryptography. MAC differs from MIC that it also uses a secret key as an input in the checksum algorithm. By calculating the checksum again the receiver can also verify that the checksum in the packet has been calculated by someone who knows the secret key. WEP uses RC4 cipher to protect also the calculated MIC to achieve the same properties as in MAC. [8] According to Borisov et al. WEP unfortunately fails to do so. [2] They show that an adversary, who cannot decrypt packets, is still able made any changes to a packet without invalidating the checksum. Thus, the RC4 cipher does not provide any help in preventing intentional message modification.

V. WI-FI PROTECTED ACCESS

The Wi-Fi Alliance started to design a new security solution after WEP was found insecure. The new security technique, named Wi-Fi Protected Access (WPA), was published in the late 2002. WPA was included later an IEEE standard amendment 802.11i-2004. [9]

WPA was published primarily to fix the main problems of WEP. As a starting point in the designing was that the new technique could be introduced in existing WEP devices by a software update. That decision substantially restricted the freedom of action in the standard, because it was not possible to design the new technique from the outset. For example performance retrictions of WEP devices may not allow computationally more demanding algorithms.

A. Security Improvements:

WPA defines a new security protocol, Temporal Key Integrity Protocol (TKIP), which is used to protect the content of messages in terms of confidentiality and integrity. TKIP has several improvements compared to WEP:

a. Most attacks against WEP are based on the fact that the pre-shared secret key and the initialization vector was simply concatenated to form the RC4 traffic key. By contrast, TKIP has a more sophisticated key mixing function, so that the relationship between the keys is not so obvious. This change makes almost all the known key recovery attacks against WEP impossible.
b. TKIP has a 64-bit MIC named Mic Michael, which replaces the weak CRC-32 checksum used in WEP. The purpose of Michael is to detect if the message content has been changed between sender and receiver. In WEP the MIC algorithm takes as an input only the plaintext. To achieve additional level of security TKIP uses a separate MIC key as an input.
c. As a new feature, TKIP has a packet sequence counter and every packet contains a unique sequence number to indicate the packet order. The receiver monitors the sequence numbers and only allows packets to be received in order. WEP does not have this functionality, which enables simple replay attacks.

In addition, WPA uses 802.1X network access control mechanism to provide authentication and key management. In the start of the wireless connection 802.1X authenticates the parties for each other and derives a fresh master key for the both parties. The master key is used to derive two new keys: 128-bit temporal key (TK) for the key mixing function and 64-bit MIC key for Michael algorithm. The benefit is that a new key can be negotiated multiple times during the session, which considerably increases security. Rekey interval determines how ofter the negotiation process is done.

The key mixing function takes as an input the TK, transmitter's MAC address and an initialization vector, and the function outputs a 128-bit RC4 traffic key, which is used as in WEP. Because of the implementation constraints, the freely selectable initialization vector is actually also the sequence counter incrementing by one in every packet.

B. WPA Security Analysis:

Attacks against WEP are complete, fast and in practice they work in every case. [17] Completeness means that the encryption keys can be recovered and thus all the traffic can be unencrypted by an adversary. A review of recently published scientific articles related to WLAN link-layer security techniques reveal that no single complete attack against TKIP exists. Though, there is at least one practical attack, which has managed to uncover some parts of encrypted messages. In addition, TKIP has some weak spots, which are potential sources of attacks, but no practical attacks exploiting those has been developed.

Beck and Tews (2008) devised and implemented one type of an attack against TKIP [1]. If the rekey interval is long enough, for example one hour, it is possible to decrypt last bits of a packet without knowing the encryption key. In addition, the adversary is able to send new packets with any content to the network. The idea behind the Beck and Tews attack is not new, but it is based on a chopchop attack against WEP. The Beck and Tews attack is quite slow because it requires sending on average over one hundred packets to decrypt one byte of data. Besides, the attack can be prevented by using short rekeying times, for example two minutes should be enough for making the attack unfeasible. Also some simple changes to the operation of TKIP protocol could prevent this attack, as proposed by Beck and Tews.

TKIP has been showed to have other intrinsic deficiencies, but no practical attacks exploiting those have been developed. In addition, given two packet keys with the same initialization vector, it is possible to calculate the TK. If TK is known by an adversary, it is able to decrypt all the traffic, until the TK is renegotiated.

Michael algorithm has turned out to be invertible, which enables an adversary to calculate the secret MIC key if certain information is available. [3] To make the calculation, an adversary needs to know a single plaintext message and a corresponding MIC value. The adversary may be able to guess the plaintext value of a message in certain situation. Thus, security of Michael MIC relies on the fact that the MIC value is encrypted. Although this vulnerability challenges the protection of TKIP, no known practical attacks exploiting it have been devised.

VI. DISCUSSION AND CONCLUSIONS

WEP encryption is easily breakable by means of ordinary computers and widely available software. That is why the method should definitely be abandoned and adopt newer technologies. Although the existing breaking methods are very fast, new ones are still being developed in recent years. Analysing WEP may be useful for the WLAN security research, because WPA is based on WEP and all the attacks against WEP can possibly be valid attacks against WPA. WPA provides a considerably more secure connection than WEP, but at least one attack towards it exists which has partly managed to break the protection and is also practical. It is possible that the recently found attack is just a beginning in searching for new breaking techniques for WPA. Thus, we think that this is the most important area of further study related to WLAN security. Taking into account the severity of the recently found vulnerability, WPA can still be considered adequately safe in many purposes, but in a few years it may end up in the same category of useless security algorithms with WEP.

WPA2 with its CCMP algorithm has been unbreakable so far providing excellent data confidentiality and integrity. The weakest point of WPA2 is vulnerability to denial-of-service attacks, which threatens only availability of wireless service. We do not consider the found DoS attacks, which exploit the design flaws of WPA2, very alarming because DoS attacks are always possible in wireless data links: jamming the wireless channel is effective regardless of the security protocol used. Still, the existence of smart DoS attacks has some significance, because they are harder to detect than arbitrary jamming. In information security the weakest point has sometimes turned out to be the user. For example, even the strongest security algorithm is possible to make useless by selecting too short encryption keys or use keys that are easy to guess. In that case an adversary is able recover the key by doing a large amount of random guesses or by using natural language dictionaries.

VII. REFERENCES

[1]. ANSI/IEEE "Std 802.11 1999 Edition" 20 September 2001 P: 59-69.

[2]. Adam Stubblefield, John Ioannidis, Aviel D. Rubin "Using the Fluhrer, Martin, and Shamir Attack to Break WEP" Revision 2. 21 August 2001.

[1]. William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan "Your 802.11 Wireless Network has No Clothes 30 March 2001

[2]. Anderson, Gustave, "A Secure Wireless Agent-based Testbed," Proceedings of the Second IEEE International Information Assurance Workshop, 2004.

[3]. Baghaei, Nilufar and Hunt, Ray, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients," Proceedings of the 12th IEEE International Conference on Networks, 2004.

[4]. Bargh, Mortaza, "Fast Authentication Methods for Handovers Between IEEE 802.11 Wireless LANs," Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, 2004.

[5]. Becker, Bernd, Eisinger, Jochen, and Winterer, Peter, "Securing Wireless Networks in a University Environment," Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, 2005.

[6]. Carli, Marco, Neri, A., and Rossetti, A., "Integrated Security Architecture for WLAN," Proceedings of the IEEE 10th International Conference on Telecommunications, 2003.

[7]. Chen, Jyh-Cheng, Jiang, Ming-Chia, and Liu, Yi-Wen, "Wireless LAN Security and IEEE 802.11i," IEEE Wireless Communications, February 2005.

[8]. Chen, Jyh-Cheng, Liu, Yi-Wen, and Wang, Yu-Ping, "Design and Implementation of WIRE1x." Proceedings of Taiwan Area Network Conference, 2003.

[9]. Edney, Jon and Arbaugh, William A., Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2004.

[10]. Fluhrer, Scott, Mantin, Itsik, and Shamir, Adi, "Weaknesses in the Key Schedule Algorithm of RC4," Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography, 2001.

[11]. Gast, Matthew S., 802.11® Wireless Networks: The Definitive Guide (2nd Edition), O'Reilly Media, 2005.

[12]. Changhua, and Mitchell, John, "Analysis of the 802.11i 4-Way Handshake," Proceedings of the 2004 ACM Workshop on Wireless Security, 2004.

[13]. IEEE Standard 802.11, 1999 Edition.

[14]. IEEE Standard 802.11i, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[15]. IEEE Standard 802.1X, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.1X-2004.pdf

[16]. IEEE Standard 802.11, 2007 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[17]. Arbaugh, W.A. Wireless security is different. Computer, Volume: 36, 9 – 101, Issue: 8, Aug. 2003.