IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 4 Issue 2 February, 2016

A Comparative Analysis between Various Encryption Standards in Wireless LAN

S.Revathi[1]
Assistant Professor
Dr. N.G.P Arts and Science College, Coimbatore
revathisujendran86@gmail.com

Dr. A. Malathi[2]
Assistant Professor
Government Arts college, Coimbatore
malathi.arunachalam@yahoo.com

ABSTRACT

Wireless Local Area Network (WLAN) are become more popular as they are fast, flexible, scalable and relatively low price. WLAN enables users to access resources, Data are transferred via radio waves spreading throughout the space and thus, the information reaches anyone with the appropriate radio receiver. But there is a problem of the protection of information it was necessary to create mechanisms for the protection of the wireless networks in order to enable users to use wireless networks and feel sure about the accuracy of information and their privacy. This paper examined the comparison between the use of wired equivalent protocol (WEP), Wi-fi Protected Access (WPA) and Wi-fi Protected Access 2 (WPA2/802.11i). It discusses the security weakness of Wired Equivalent Privacy (WEP) and provides with the interim and ultimate solutions: Wi-Fi Protected Access (WPA) and WPA2/802.11i standards. The purpose of this paper is to give developers with little or no knowledge of cryptography the ability to understand the concept of various security protocols used to protect data.

Keywords: Wireless Security, WEP, WAP and WAP2/802.11i.

1. INTRODUCTION

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an **access point device [1]**. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even "roam" within a building or between buildings [11].

There are three major wireless network architectures implemented today: the basic service set, the extended service set, and the independent service set [2]. The basic service set (infrastructure mode) is a collection of wireless devices that are served by a single access point (AP). This configuration is used in small wireless network

implementations. The extended service set is composed of two or more basic service set networks. It is able to cover a much broader area and can offer roaming services for wireless clients. This is frequently used in large wireless network implementations. Finally, the independent service set (ad-hoc mode) does not utilize an access point, but instead is completely peer-to-peer, most organizational wireless implementations utilize the basic service set and extended service set architectures for transmitting data.

2. LITERATURE REVIEW

The constant increase in use of wireless infrastructure networks for business purposes created a need for strong safety mechanisms. In [6] it describes WEP (Wired Equivalent Privacy) protocol for the protection of wireless networks, its security deficiencies, as well as the various kinds of attacks that can jeopardize security goals of WEP protocol: authentication, confidentiality and integrity. It also gives a summary of security improvements of WEP protocol that can lead to a higher level of wireless network infrastructure protection. Comparative analysis shows the advantages of the new 802.11i standard in comparison to the previous security solutions.

The contribution is twofold in [5]. First, it presents a design and an implementation of a light weight application-level security solution for handheld devices in wireless LAN. Second, it analyzes the impact of the processing power, time, and memory on the performance of two of the widely known encryption algorithms—RC4 and AES—used by the lightweight handheld devices in the wireless network environment. The work in this paper uses pure Java components to provide end-to- end client authentication and data confidentiality and integrity

The evolution of wireless security in 802.11 networks discusses the security weakness of Wired Equivalent Privacy (WEP) and provides with the interim and ultimate solutions: Wi-Fi Protected Access (WPA) and 802.11i standards. It then covers various responses from vendors, IEEE and the Wi-Fi Alliances [7]. The Wi-Fi Alliances extracts the key features from 802.11i to establish WPA to satisfy the immediate needs for the wireless industry. Meanwhile, IEEE 802.11 Task Group "I" is working on the 802.11i standard to provide the ultimate robust security for the wireless infrastructure. A high level of key features used by WPA and 802.11i, such as 801.X EAP based authentication, TKIP encryption protocol, AES encryption protocol, are explained

Some experimental work was performed to illustrate the performance of RC4 algorithm based on changing some parameters [12]. The execution time as a function of the encryption key length and the file size was examined; this has been stated as complexity and security. Various data types were analyzed and the role of the data type was also emphasized. The results have been analyzed and interpreted as mathematical equations showing the relationship between the examined data and hence can be used to predict any future performance of the algorithm under different conditions. The order of the polynomial to approximate the execution time was justified.

It based on the input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length (a bit is a binary digit, 0 or 1, while the term length describes the number of bits in a sequence). In general the length of the input and output

sequences can be any of the three allowed values but for the Advanced Encryption Standard (AES) the only length allowed is 128. However, both Rijndael and AES allow cipher keys of all three lengths [15].

3. WIRELESS SECURITY MEASURES

Wireless print servers are a convenient way to get access to printers without any cables. Wireless printing can provide the same level of privacy and security as wired printing, provided that the wireless devices are configured to use appropriate security [3]. The type of security chooses will depend on the wireless standards supported by the access point or wireless card used and the level of security required.

Basically, there are three security standards to be consider which are as follows (Figure 1) :

- WEP (Wired Equivalent Privacy)
- WPA (WiFi Protected Access)
- WPA2

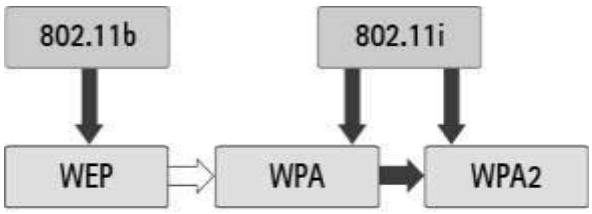

Figure1. Relations between WEP, WPA and WPA2

4. WIRED EQUIVALENT PRIVACY (WEP)

The basic function of WEP protocol is to provide data security in wireless networks in the same way as it is in the wired networks. Lack of physical connection among users and wireless networks enables all users within the network range to receive data if they have appropriate receivers. The only possible way to protect this kind of network was to create a protocol that would work on the second layer of OSI model and, in this way, provide the data protection during the transmission. In order to protect data transmitted among the communicating parties, WEP uses shared secret key of 40 to 140 bits [6].

WEP protocol is applied through the following three steps

- CRC (Cyclic Redundancy Code) message is calculated and added to the original message.
- The message is encrypted by RC4 algorithm. Encryption is the one in three phases. First, pseudo-random data sequence of three bytes is generated (IV – Initialization Vector) to extend the key. Then RC4 algorithm generates keystream based on the new key. Encryption ends with the application of exclusive or function (XOR) between keystream and message thus resulting in encrypted message.
- The last step is to transmit sequence IV and encrypted message.

4.1 The Vulnerabilities of WEP

WEP seemed like a good idea at the time when encryption schemes were under tough scrutiny due to export restrictions and few users had gone wireless, revealing few vulnerabilities, WEP seemed like just the thing to make wireless networks secure, or at least as secure as their wired counter parts [4].

The WEP's first vulnerabilities were revealed are

- Brute force attacks (with a 40-bit key, such an attack is feasible)

● Dictionary attacks (the key can be guessed if weak)
● Keystream attacks (keystream cracking allows eavesdropping & message injections)
● Statistical correlation attacks (FSM, KoReK, and PTW attacks allow key cracking)
● Man-in-the-middle attacks (due to one-way authentication)
● Denial of service attacks (through disassociation frames)
● Weak message authentication (the ICV can be modified, packet injections possible)
● Flawed shared-key authentication (keystream exposed)
● Poor key management (the use of a single key by many users)

5. WI-FI PROTECTED ACCESS (WPA)

WPA (Wi-Fi Protected Access) standard to improve the protection of wireless devices. WPA has contributed to the increased protection of wireless communications through the increased level of data protection and access control of current and future solutions to wireless networks. WPA is designed to be the software upgrade to the existing devices and is compatible with the new IEEE 802.11i standard [14].

WPA has several purposes:

- To be a strong protective mechanism for wireless networks,
- To be interoperable,
- To replace WEP,
- To enable the existing Wi-Fi wireless devices to be upgraded with the new software solution,
- To be applicable in small, as well as in large wireless networks, and
- To be applicable immediately.

The first improvement offered [13] by WPA is data encryption by TKIP (Temporal Key Integrity Protocol). This protocol provides a strong encryption mechanism whose characteristics are:

- A unique stream for encryption of each of the packets,
- Message integrity check (MIC, Michael),
- IV extension, and
- Repeated key mechanism.

The second improvement is related to the strong security authentication of the users through 802.1x and EAP (Extensible Authentication Protocol). In large networks, WPA uses authentication server RADIUS to secure centralized management and control of the access. In small SOHO (Small Office/Home Office) networks, there is no centralized authentication server so that WPA is initiated by a special mode. This mode is also called Pre-Shared Key (PSK) and it enables users to authenticate by a password or a key. Users have to enter a password (or a key) to the access point; otherwise home network reaches each of the workstations included in the Wi-Fi wireless network [10]. Devices with appropriate password can be networked and thus protected from eavesdropping and other unauthorized users.

6. 802.11I: THE ULTIMATE WIRELESS SECURITY SOLUTION

IEEE 802.11i is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. WPA2 is a product of Wi-Fi alliance that guarantees that all the equipment with WPA2 installed can support the most important characteristics of 802.11i. Wi-Fi alliance enables AP usage supported only by

WPA2 mode and AP supported by mixed WPA2/WPA mode. This means that WPA2 equipment is compatible with WPA. Due to WEP security problems WPA2/WPA mode is not allowed in WPA2 equipment. WPAandWPA2/802.11i specifies new standards for authentication, encryption and message integrity.

Authentication: WPA and WPA2/802.11i use 802.1x/EAP for authentication and key exchange. 802.1 x authentication models require the existence of 802.1x client, authenticator (access point) and authentication server (RADIUS). WPA and WPA2 use 802.1 x for the authentication in large networks, while a shared key authentication is used in small networks. 802.11i introduces pre authentication [8] in order to escape re-authentication and reduce all late arrivals caused by 802.1x. Reduced lateness of 802.1x would enable faster roaming between wireless station and APs. This is very important for the application sensitive to lateness.

Key Management: The process of management and creation of the key is the same for the TKIP and AES-CCMP (Advanced Encryption Standard – Counter Mode with Cipher Block Chaining message Authentication Code Protocol). Both TKIP and AES-CCMP are defined by 802.11i standard, but there is a difference in the number of keys. AES-CCMP uses the same number of keys for message encryption and data integrity while TKIP uses two keys. This difference is the result of the fact that TKIP is based on RC4 encryption technique while AES-CCMP uses advanced encryption standard.

WPA and 802.11i encryption and integrity: TKIP and AES-CCMP solution are introduced to improve bad WEP encryption mechanisms. Wi-Fi alliance integrated TKIP into WPA in order to use it on the WLAN hardware. TKIP protocol contains RC4, but introduces changes in the area of message integrity, IV creation and key management, all that with the purpose of increasing WEP safety.

7. COMPARATIVE ANALYSIS OF WLAN SAFETY IMPROVEMENT

This section describes differences between WEP, WPA and WPA2/802.11i safety improvements. Table1 gives a comparison of these safety improvements in comparison to WEP as a first solution to achieve safety goals in WLAN networks [9]. Table also shows availability of safety solutions in improvements of all three safety goal

Table 1. Comparative analysis of WLAN safety improvements.

	WEP	**WPA**	**WPA/802.11i**
Authentication	Open authentication System and shared Key authentication (same key as for encryption) – Pre-RSN	Shared key authentication and strong authentication based on 802.1x and EAP (RADIUS Server)	Authentication based on 802.1x , EAP and Pre-authentication , RSNA
Encryption	Uses Initialization Vector – RC4 encryption algorithm		Does not use Initialization Vector – AES encryption algorithm
	Thoroughly researched and documented deficiencies	Removes all WEP Deficiencies	Removes WEP and WPA deficiencies
Key Management	40 bit Key	128 bit Key	128,192,256 bit keys
	Statistical key distribution - all network users use the same key	Dynamic key distribution – new keys for each user, session, packet	
	Manual key distribution – it is necessary to enter the key into each device	Dynamic key distribution	
Integrity	CRC	MIC (64 bit Key)	CBC-MAC (the same key as for encryption)

8. CONCLUSION

In this paper, various encryption methods namely WEP, WPA and WPA2. WEP is the first protocol for data protection in wireless networks. This mechanism is designed to achieve three safety goals: authentication, confidentiality and message integrity. Basic WEP deficiencies come from unsafe authentication, repeated use and open transfer of IV, key management system and a mechanism for the protection of message integrity that is not applied properly. WPA contributes to the increase of wireless communication protection by Wi-Fi standard through increased level of data protection, access control and integrity. 802.11i defines Robust Security Network Association (RSNA) procedure to provide mutually strong authentication and key management procedure. AES counter encryption contributes significantly to the increase of data protection during communication transmission, while CBC-MAC contributes to integrity preservation by mixing encrypted and non-encrypted data blocks.

The comparative analysis shows that 802.11i standard provides a high level of protection from the attacks, but cannot solve all the problems caused by some DoS attacks. One of these attacks is jamming, whereas an attacker can disable communications among wireless networks users by using some devices. So the future work is focused on these sorts of attacks to save the wireless environment.

9. REFERENCES:

1. William Stallings, "Cryptography and network security: Principles and practice", Prentice Hall, Upper Saddle River, New Jersey, 2003.
2. Radomir prodanovi and dejan simi. "A Survey Of Wireless Security", journal of computing and information technology - cit 15, 2007
3. Sans institute reading room site "The Evolution of Wireless Security in 802.11 Networks: WEP, WPA and 802.11 Standards".
4. G. Rupinde, s. Jason, c. Andrew, "Specification-Based Intrusion Detection In WLAN". 22nd annual computer security applications conference, Miami Beach, florida, (2006).
5. J. Welch, s. D. Lathrop, "A Survey Of 802.11a Wireless Security Threats And Security Mechanisms". United States military academy west point, New York, (2003). Http://www.itoc.usma.edu/documents/itoc tr-2003-101 (g6).pdf.
6. Borisov, nikita, goldberg, ian wagner and david, "Security Of The WEP Algorithm". February 02, 2001. Http://www.isaac.cs.berkeley.edu/issac/wep-faq.html
7. Auscertaa, "Denial of Service Vulnerability In IEEE 802.11 Wireless Devices". (2004). Http://www.auscert.org.au/render.html?it=4091.
8. Karen scafone, derrick dicoi matthew sexton & cyrus tibbs, "Guide To Security Legacy IEEE 802.11 Wireless Networks" NIST special publication 800-48, Revision 1, July 2008.
9. Vipin Poddar, Hitesh Choudhary "A Comparative Analysis of Wireless Security Protocols (WEP and WPA2)", International Journal on Adhoc Networking Systems (IJANS) vol. 4, no. 3, july 2014.
10. Sebastin Bohn and Stephan Grob. "An Automated System Interoperability Test Bed For WPA and WPA2" in IEEE Explore, 2006.
11. Ezedin S. Barka, Emad Eldin Mohamed, "End-To- End Security Solutions for WLAN: A Performance Analysis for the Underlying

Encryption Algorithms in the Lightweight Devices".

12. Allam Mousa and Ahmad Hamad "Evaluation of the RC4 Algorithm for Data Encryption"
13. White paper: Testing for Wi-Fi Protected Access (WPA) inWLAN Access Points. Net-O2 Technologies (2004). http://whitepapers.zdnet.co.uk/0,39025942,60152756p,00.htm
14. Wi-Fi Alliance. "Wi-Fi Protected Access – Overview". URL: http://www.wi-fi.com/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf.
15. J. Daemen, L.R. Knudsen and V. Rijmen, "The block cipher Square," Fast Software Encryption, LNCS 1267., Springer-Verlag, 1997, pp. 149-165. http://www.esat.kuleuven.ac.be/rijmen/square/fse.ps.gz.