Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol

MOHD IZHAR[*], MOHD. SHAHID[**], DR. V.R.SINGH[***]

[*] HMR Inst. of Tech. & Mgt,& Ph.D. Scholar of Mewar University
[**] Ph.D. Scholar of Mewar University,
*** Recognised Supervisor of Mewar University

Abstract- IEEE 802.11-2007 Standard for wireless network classifies security algorithms into: RSNA and Pre-RSNA. Pre-RSNA algorithms are the algorithms used before RSNA. Pre-RSNA security comprises the algorithms; WEP (Wired Equivalent Privacy) and IEEE 802.11 entity authentication. RSNA security comprises the algorithms like TKIP, CCMP, RSNA establishment and termination procedures, including use of IEEE 802.1X authentication, key management procedures and providing mechanisms for protecting management frames. All Pre-RSNA Methods fail to meet their security goals and are deprecated except for Open System authentication after that RSNA comes in the picture. This Paper evaluates why pre-RSNA methods fail for providing security to wireless Networks. This analysis is necessary to migrate to RSNA and making more highly secure and reliable RSNA methods. Security features and capabilities associated with IEEE 802.11i through its framework for Robust Security Networks (RSN) are explained here and can be used as guidance on the planning and deployment of RSNs.

Index Terms- RSNA (Robust Security Network Association), Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), temporal key integrity protocol (TKIP), confidentiality, Wireless Local Area Network (WLAN) local area network, Medium Access Controller (MAC) and Physical (PHY).

I. INTRODUCTION

IEEE 802.11-2007, Revision of IEEE Std 802.11-1999 was approved on 08.03.2007 and published on 12 June 2007 by IEEE. This revision gives the IEEE 802.11 standard for wireless local area networks (WLANS) with all the amendments that have been published to date i.e.08.03.2007. The original standard was published in 1999 and reaffirmed in 2003. IEEE 802.11i, an IEEE standard ratified June 24, 2004, is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks[3]. The 802.11i specification defines two classes of security algorithms: Robust Security Network Association(RSNA), and Pre-RSNA. Pre-RSNA security consists of Wired Equivalent Privacy (WEP) and 802.11 entity authentication. RSNA provides two data confidentiality protocols, called the Temporal Key Integrity Protocol (TKIP) and the Counter-mode/CBC-MAC Protocol (CCMP), and the RSNA establishment procedure, including 802.1X authentication and key management protocols. This paper analyzes the Pre-RSNA and RSNA methods in order to migrate from pre-RSNA to RSNA methods and making more secure RSNA methods.

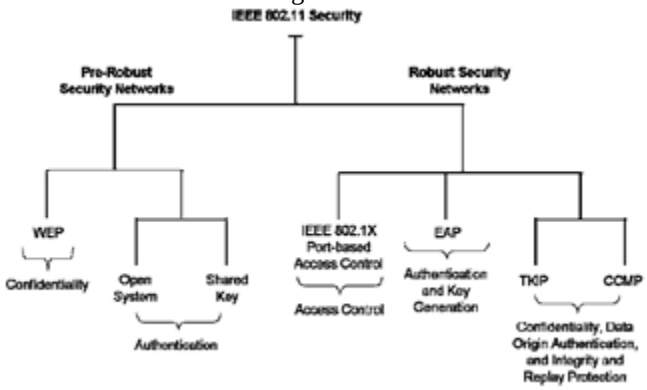

Fig 1 : Broad Classificaiton of Security Protocol

I. BACKGROUND

Wired equivalent Privacy

WEP-40(40-bit key) is defined as a means of protecting the confidentiality of data exchanged among authorized users of a WLAN from casual eavesdropping. The same algorithms have been widely used with a 104-bit key instead of a 40-bit key, this is called WEP-104. WEP security involves two parts, Authentication and Encryption. Authentication in WEP involves authenticating a device when it first joins the LAN. The authentication process in the wireless networks using WEP is to prevent devices/stations joining the network unless they know the WEP key[4].

Many Papers have been published relating to security methods of Pre-RSNA discussing the Wireless LAN 802.11 network security including the comparisons of SSIDs, MAC address filtering and the WEP key encryption. Various simulative platform of software and hardware is designed to crack WEP key based on these authentication methods and analyzing the weaknesses of WEP and RC4, It has been shown that WEP Key can be cracked including SSID enumeration, MAC address spoofing and WEP key cracking by FMS(Fluhrer, Mantin, Shamir) Attack[5].

Entity authentication

An access point must authenticate a station before the station communicates with the network. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key**.** There are two other mechanisms: the Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address—are also commonly used. Open System Authentication allows any device to join the network. The 802.11

client **authentication process** consists of the following transactions:

1. Probe request: Client broadcasts a probe request frame on every channel.
2. Probe Response: Access points within range respond with a probe response frame.
Open and shared key Authentication: Once the client determines the optimal access point to connect to, it moves to the authentication phase of 802.11 network access which is of two types Open Authentication and Shared key Authentication.
3. Authentication request: The client decides which access point (AP) is the best for access and sends an authentication request
4. Authentication Response: The access point will send an authentication reply
5. Association request: Upon successful authentication, the client will send an association request frame to the access point
6. Association response: The access point will reply with an association response
7. The client is now able to pass traffic to the access point

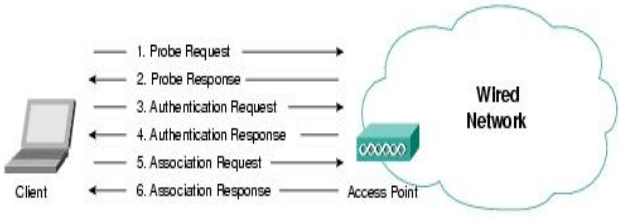

Fig 2 : 802.11 Client Authentication Process

Shared Key Authentication requires that the station and the access point have the same WEP key to authenticate. Turn on the wireless station. The station listens for messages from any access points that are in range. The station finds a message from an access point that has a matching SSID.

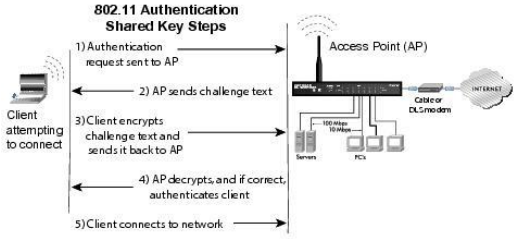

Fig 3 : WEP Shared Authentication

1. The station sends an authentication request to the access point.
2. Wireless access point sends 128 bit random challenge in text to the requesting station.
3. The station sends an association request to the access point. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the access point
4. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key, and the access point authenticates the station. The access point associates with the station.
5. The station can now communicate with the Ethernet network through the access point.

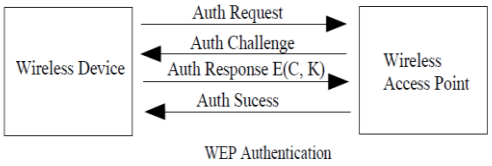

Fig 4 :WEP Authentication

Temporal Key Integrity Protocol

Wired Equivalent Privacy (WEP) was developed in order to secure wireless networks and provide security equivalent to the one that could be expected from a wired network. When WEP failed miserably to deliver the required security, the Temporal Key Integrity Protocol (TKIP) was built around WEP to fix its flaws and provide backwards compatibility with older equipment. Much resources and money were invested into upgrading old WEP networks to TKIP[7]. The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP.

IEEE Std 802.11i-2004, it was an amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999,802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g-2003, and 802.11h-2003], amendment 6: Medium Access Control (MAC) Security Enhancements, 23 July 2004. This amendment defines TKIP and CCMP, which provide more robust data protection mechanisms than WEP affords. It introduces the concept of a security association into IEEE 802.11 and defines security association management protocols called the 4-Way Handshake and the Group Key Handshake. Also, it specifies how IEEE 802.1X may be utilized by IEEE 802.11 LANs to effect authentication[8].

Counter Mode with Cipher Block Chaining(CBC) Message Authentication Code(MAC) Protocol (CCMP)

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology. CCMP was the second security protocol introduced as a replacement for WEP in the 802.11i amendment CCMP made from scratch using the modern AES block cipher. CCMP is based on the CCM of the AES encryption algorithm. CCM combines CTR for confidentiality and CBC-MAC for authentication and integrity. CCM protects the integrity of both the MPDU Data field and selected portions of the IEEE 802.11 MPDU header.

CCM is a generic authenticate-and-encrypt block cipher mode. CCM is only defined for use with 128-bit block ciphers, such as AES. For the generic CCM mode there are two parameter choices. The first choice is M, the size of the authentication field. The choice of the value for M involves a trade-off between message expansion and the probability that an attacker can undetectably modify a message. Valid values are 4, 6, 8, 10, 12, 14, and 16 octets. The second choice is L, the size of the length field. This value requires a trade-off between the maximum message size and the size of the Nonce[10].

II. Services and Methods

Network security is mostly achieved through the use of cryptography, a science based on abstract algebra. But here the term is used to refer to the science and art of transforming messages to make them secure and immune to attacks from the point of view of security of Wireless Technology[11]. There are different kinds of security algorithm or cryptography techniques broadly, classified as symmetric & asymmetric key cryptography algorithms. They are further classified as stream cipher and block cipher. DES(Data Encryption Standard) and AES (Advanced Encryption Standard) ciphers are referred to as block ciphers because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks.

The purpose of the paper is to evaluate these different security algorithms, RSNA and Pre-RSNA algorithms. However the RSA(named for its inventors Rivest, Shamir, and Adleman) is the most common asymmetric key(Public Key) algorithm is used, while the research activity may include EIGamal another asymmetric-key algorithm and its difference with the RSA. There are different software development kit available used for developing & evaluating such algorithms such as C++, java & matlab.

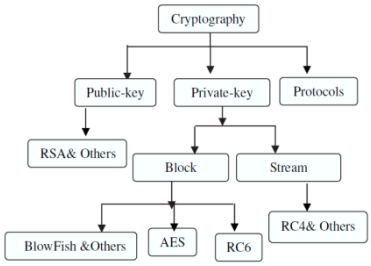

Fig 5 : Encryption Algorithms Classification

Cryptography Services

Cryptography has several applications in network security. Cryptography can provide five services. Four of these are related to the message exchange. The fifth is related to the entity trying to access a system for using its resources. IEEE Std 802.11 provides the ability to protect the contents of messages. This functionality is provided by the data confidentiality service. IEEE Std 802.11 provides three cryptographic algorithms to protect data traffic: WEP, TKIP, and CCMP. That means one can use the devices conforming this IEEE standard or WPA2 devices for security evaluation purpose.

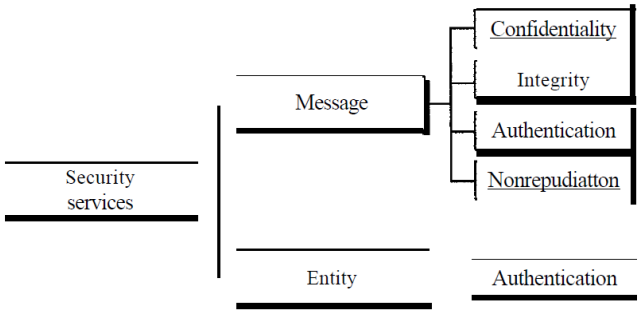

Fig 6 : Cryptography Services

Security Services

Cisco, netgear devices are available for such conformity one can create scenario and can check the security practically as per requirement. Besides the security methods may include the simulator such as NS2, Matlab, Qualnet and/or Opnet for evaluation purpose. The specific aspects of this paper is to investigate earlier security aspect called pre-RSNA within the framework of main objectives i.e. RSNA in order to develop a Secure Model for Wireless Local Area Network.

III. Results and Discussions

Earlier various attacks have been shown at WEP. When WEP failed to deliver the Security, the Temporal Key Integrity Protocol (TKIP) was built around WEP to fix its flaws and provide backwards compatibility with older equipment. On November 8, 2008, German researchers released a paper demonstrating a practical attack against the Temporal Key Integrity Protocol (TKIP) encryption algorithm used to secure Wi-Fi networks that are certified for Wi-Fi Protected Access (WPA). Motoral inc 2008 analyzed and recommends that enterprises must use AES-CCMP encryption with their WPA or WPA2 deployments. Motorola WLAN infrastructure is fully certified for AES-CCMP. [16] Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology. Various Papers has been published for analyzing CCMP.

Wireless LAN deployments should be made as secure as possible. Standard 802.11 securities are weak and vulnerable to numerous network attacks. CERT-In Monthly Security Bulletin-February 2012 reports that 95 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 7, 44% incidents related to Phishing were reported in this month. Other reported incidents include 22 % Virus/Malicious Code ,03 % unauthorized scanning , 31 % incidents related to technical help under the Others category. 2460 Indian websites were defaced during February 2012[24].

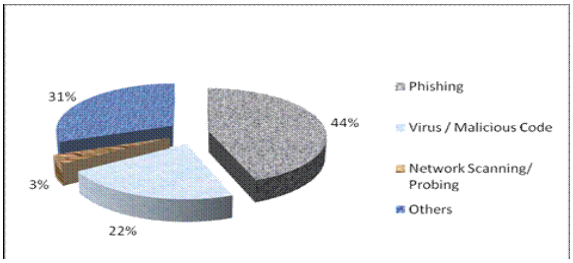

Fig 7 : Security Threats shown by CERT-In

CERT-In Website Intrusion and Malware Propagation : is tracking malicious URLs on regular basis. In the month, February 2012, CERT-In tracked 475 websites infected with malicious contents. A user visiting these URLs is redirected to malicious sites which downloading malicious code such as virus, worm, trojan. keylogger, rootkit on to the user's computer[24].

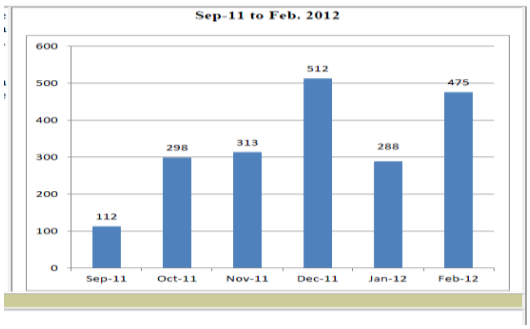

Fig 8 : CERT-In shows WIMP attack Tracking Sep-11 to Feb-12

IV. Conclusion

This paper has highlighted WLAN vulnerabilities and concluded that Wireless Security is always major issue. The purpose of this paper is to educate the public at large and protecting them from several serious attacks. However it is impossible in this paper to cover all the risks and vulnerabilities pertaining to wireless LANs. The most severe and most common vulnerabilities have been covered. Protecting a wireless network requires best planning considering the big or small size of network. The main point of considerations are : Not relying on WEP to provide security for the network, Limiting, as much as is possible, who can attach to a network , Surveying the interference and jamming likelihood for a planned wireless LAN before it is installed. Practical approaches have also been necessary to be secure from such attacks.

References

[1] IEEE Std 802.11™-2007, Revision of IEEE Std 802.11-1999,IEEE 3 Park Avenue New York, NY 10016-5997, USA 12 June 2007.
[2] IEEE Std. 2009 Revision of IEEE Std 802.11™-2007, 30 sept. 2009.
[3] Changhua He & John C Mitchell "Security Analysis and Improvements for IEEE 802.11i", Network and Distributed System Security Symposium, San Diego, California, 3-4 February 2005.
[4] Shivaputrappa Vibhuti, "IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability" , San Jose State University, CA, USA, *CS265 Spring 2005* (26.03.2005)
[5] NETGEAR, Inc. "Wireless Networking Basics", October 2005.
[6] Lu Zhengqiu; Tian Si; Wang Ming; Ye Peisong; Chen Qingzhang; "Security analysis and recommendations for Wireless LAN 802.11b network", Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on 16-18 April 2011.
[7] Finn Michael Halvorsen & Olav Haugen "Cryptanalysis of IEEE 802.11i TKIP", Norwegian University of Science and Technology, June 2009.
[8] IEEE Std 802.11i-2004, Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999,802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g-2003, and 802.11h-2003] Amendment 6: Medium Access Control (MAC) Security Enhancements, 23 July 2004.
[9] Back and Tews "Practical attacks against WEP and WPA", November 8, 2008.
[10] Paul Arana, "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", INFS 612 – Fall 2006
[11] Behrouz A. Forouzan "DATA COMMUNICATIONS AND NETWORKING", McGraw-Hill Forouzan Networking Series, Fourth Edition Copyright © 2007.
[12] NIST Special Publication 800-97, " Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", February 2007.
[13] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213{219, May 2010
[14] A.K.M. Nazmus Sakib et al"Security Improvement of WPA 2 (Wi-Fi Protected Access 2)" (IJEST), Vol. 3 No. 1 Jan 2011
[15] Vijay Chandramouli, "A Detailed Study on Wireless LAN Technologies", 23.10.2002
[16] "Understanding the New WPA TKIP Attack Vulnerabilities & Motorola WLAN Countermeasures", Motorola, Inc. 2008.
[17] Dajiang He, Charles. Q. Shen. "Simulation study of IEEE 802.11e EDCF" 2003
[18] ISMAHANSI BINTI ISMAIL, "Study of Enhanced DCF(EDCF) in Multimedia Application", 2005
[19] Preeti Venkateswaran, "Experiments to Develop Configurable Protocols", 2005
[20] Mark Greis, Tutorial for the Network Simulator "ns" 2008
[21] Lecture notes 2003-2004 University de Los Andes, Merida, Venezula and ESSI Sophia-Antipols, France.
[22] Guillermo Alonso Pequeño Javier Rocha Rivera, "Extension to MAC 802.11 for performance improvement in MANET", 2007
[23] Sam De Silva, Using TCP "Effectively in Mobile Ad-hoc Wireless Networks with Rate Adaptation", 2007
[24] CERT-In Monthly Security Bulletin- February 2012, website : http://www.cert-in.org.in

Authors

First Author MOHD. IZHAR, Associate Professor, HMR Inst. of Tech. & Mgt, GGSIP University, Delhi, Ph.D. Scholar of Mewar , University, NH-79, Gangrar, Chittorgarh (Rajasthan) India, email : mohd.izhar.delhi@gmail.com
Second Author – MOHD. SHAHID, Ph.D. Scholar of Mewar University, NH-79, Gangrar, Chittorgarh (Rajasthan) India email : shahidpdmce@gmail.com
Third Author – DR. V.R.SINGH, Director, PDM College of Engg., Bahadurgarh, MDU University, recognized supervisor of Mewar University, NH-79, Gangrar, Chittorgarh (Rajasthan) India-312901, email : vrsingh@ieee.org.

Correspondence Author – MOHD. IZHAR. email : mohd.izhar.delhi@gmail.com