ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Integrating Enhanced Security Measures in WEP/WPA/WPA2-PSK (Review Paper)

BabitaDagar, Neha Goyal

M.Tech (pursuing), Dept. of Computer Science, Shri.Ram College of Engineering and Management, Palwal, Haryana under the Affiliation of Maharshi Dayanand University, Rohtak, India

Assistant Professor, Dept. of Computer Science, Shri.Ram College of Engineering and Management, Palwal, Haryana under the Affiliation of Maharshi Dayan and University, Rohtak, India

ABSTRACT: The focus of this work is to provide the solutions for WPA2/WEP/WPA2-PSK vulnerabilities by incorporating trusted computing in order to provide security for wireless networks. Trusted computing aims at addressing the workstation security issues by some software amendments and thus, establishing a trust relationship between clients connected to network. Trusted Computing enables binding of data to applications, users and workstations for secured communication. Therefore, in this paper the evolution of various security protocols for Wireless LANs has been discussed and a comparative study has been provided for these protocols in this paper. Also, since WPA2 is the most recommended protocol for wireless networks at present, so, various limitations of WPA2 have been examined and discussed, describes about the tools and programming language used for application implementation in this paper. The solutions for these shortcomings have been addressed by proposing/protocol an encryption algorithm which has been described in this paper the analysis of the results and details of application execution undertaken will also be presented in future work in this white paper.

KEYWORDS:Wireless Networks, Network Security ;Trusted Computing; Wi-fi Protected Access;Wired Equivalent Privacy; WPA-Group Temporal Key (GTK).

I. INTRODUCTION

Today, wireless networks are one of the rapidly emerging areas of growth and emphasises on the significance of providing ubiquitous network connectivity. Wireless networks can be classified on basis of service area range. IEEE 802.11 standard (Wi-Fi) provides wireless connectivity to users within campus, home or corporate premises. IEEE 802.16 (WiMAX) allows users high speed broadband Internet access within metropolitan area. IEEE 802.15 (Bluetooth) provides connectivity between mobile devices within a range of 10 meters. The focus of this work is on enhancing the security of most recommended protocol Wi-Fi Protected Access 2 (WPA2) at present for Wireless Local Area Networks (WLAN) by incorporating Trusted Computing. WLANs have gained rapid popularity due to easy deployment, mobility and reduced costs. It enables end users to access network without cable connectivity through hub or switch. But, WLAN still face several security risks like eavesdropping, data modification and replay attacks. WPA2 has implemented block cipher AES to provide stronger data encryption but it is still vulnerable to several attacks due to transmission of unencrypted management and control frames and sharing of Group Temporal Key (GTK) among peers connected to wireless network. Thus, it is essential to provide solution for WLAN security issues and protect the network from various attacks.

Various early access points were unable to verify if the end user was allowed to access the network or not. This problem was earlier prevalent in wired networks as well but became a major issue in wireless networks since it was possible for the attacker who was within geographical range of the network to sniff the transmitted data and in turn gain illicit access to network. Today, most laptops have built in wireless network capability without the need for a third

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

party or external adapter, thus enabling the wireless capability by default without the knowledge of possessor. This makes the machine prone to data sniffing and modification from other peers within the range.

Features

The security protocols WEP, WPA and WPA2 should encompass below security requirements for WLAN:

Data Integrity

Data integrity should be provided for every message that is transmitted over the network. This ensures that only authorized users are able to modify and access the messages. Also, the network must provide replay protection i.e. replay messages must be identified and discarded even if they comply with the integrity check criteria.

Confidentiality

Transmitted messages over the network must be protected from unauthorized access and thus, is a vital part of security. Protection should be provided against malicious software, spam, spyware and phishing attacks.

Data Availability

Data availability is a vital requirement for network security. The network should be able to avert the connection shutdown for an authorized individual or the complete system. Thus, eliminating or reducing the risk of denial of service (DoS) attacks.

Access Control

Access control refers to techniques and policies that ensure proper management of network resources and access is granted to various authorized users depending on permission level assigned to them.

Non Repudiation

Non repudiation ensures that validity of contract cannot be challenged by the sender or recipient. This can be achieved by implementing timestamps or digital signatures hence, ensuring that sender cannot deny having sent the message and recipient cannot deny the message receipt.

Authentication

Authentication assists in individual identification who tries to access the network and this can be achieved through the use of passwords, biometrics and digital certificates.

II. LITERATURE REVIEW

This section provides a review of the literature on evolution of security protocols for Wireless LAN in order to achieve requirements of confidentiality, data integrity and authentication. The encryption/decryption process, limitations and the vulnerability of each protocol to various attacks have been provided in this section.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) was the first protocol for securing wireless network and was introduced in September 1999 as part of IEEE 802.11 security standard. The purpose of Wired Equivalent Privacy (WEP) was to provide security comparable to that of wired networks. RC4 stream cipher is used by WEP to provide confidentiality and CRC-32 for data integrity. The standard specified for WEP provides support for 40 bit key only but non-standard extensions have been provided by various vendors which provide support for key length of 128 and 256 bits as well. A 24 bit value known as initialization vector is also used by WEP for initialization of the cryptographic key stream.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

1) WEP Encryption/Decryption Process

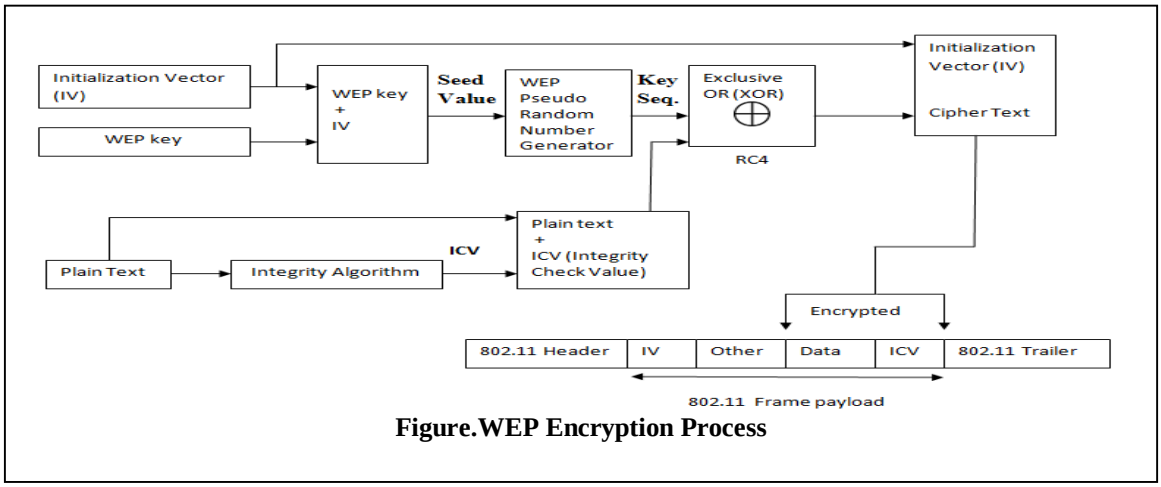

Figure.WEP Encryption Process

WEP Encryption process consists of following steps:

i. 24 bit initialization vector is concatenated with 40 bit WEP key.
ii. The resultant concatenated key acts as seed value for Pseudo random number generator.
iii. Integrity Algorithm CRC-32 is performed on plain text to generate Integrity Check Value (ICV) which is concatenated with plain text.
iv. RC4 algorithm is applied on Plain text + ICV and Key sequence to generate cipher text.
v. The payload for the wireless MAC frame is created by adding the IV to front of the encrypted combination of data and ICV along with other fields.

WEP Decryption Process consists of following steps:

i. Initialization vector from 802.11 frame payload is concatenated with WEP key. This acts as seed value for Pseudo Random Number Generator.
ii. CR4 algorithm is applied to cipher text of frame payload and key sequence to get plain text.
iii. Plain text and original ICV are obtained.
iv. Plain text is input to Integrity algorithm to generate new ICV.
v. New ICV is compared with original ICV to get the result.

2) WEP Shortcomings

The WEP limitations are as follows: Weak Cryptography, Absence of Key Management, Small key size, Reuse initialization vector, Lack of Replay protection, Authentication issues, Jamming, Packet Forgery, Flooding.

3) WEP Attacks

Chopchop Attack, Bittau's fragmentation Attack, Fluhrer, Mantin and Shamir (FMS) Attack, Pyshkin, Tews and Weimann (PTW) Attack

Wi-Fi Protected Access

In order to overcome the flaws of WEP, **Wi-Fi Protected Access (WPA)** was introduced in 2003 by the Wi-Fi (Wireless Fidelity) alliance. WPA implements majority of the IEEE 802.11i standard, thus it is an intermediate solution. WPA was intended to address the WEP cryptographic problems without requiring new hardware.

1) WPA Encryption Process

WPA uses Temporal Key Integrity Protocol (TKIP) for encryption. A new key is dynamically generated for every packet; 128 bit per packet key is used. Michael algorithm is used by TKIP to generate Message Integrity Code (MIC) which provides enhanced data integrity as compared to CRC-32 used in WEP. Also, TKIP provides replay protection. MSDU is Medium Access Control Service Data Unit and MPDU is Medium Access Control Protocol Data Unit.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

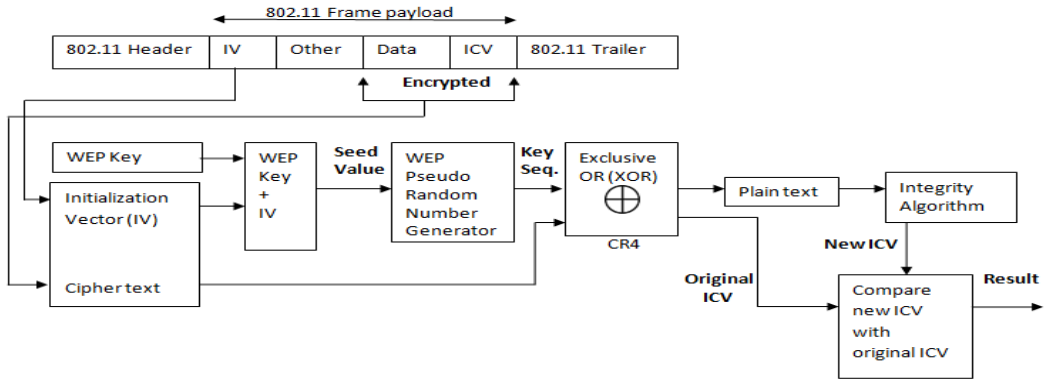

Figure.WEP Decryption Process

2) WPA Authentication Mechanism

The two authentication mechanisms provided by WPA are:

i. WPA-Personal or WPA-PSK (Pre-Shared Key)
ii. WPA-Enterprise

3) WPA Shortcomings

i. WPA uses old cryptography algorithm RC4 instead of superior Advanced Encryption Standard (AES).
ii. WPA is vulnerable to brute force attacks in case of weak passphrase for pre shared key mode.
iii. Prone to threats during Hash collisions due to use of hash functions for TKIP key mixing.
iv. Also, WPA remains vulnerable to availability attacks like Denial of Service.
v. WPA has greater performance overhead unlike WEP.
vi. Complicated setup is required for WPA-enterprise.

4) WPA Attacks

TKIP used in WPA is prone to Chopchop, Ohigashi-Morii, WPA-PSK and Beck-Tews attack

III. RELATED WORK

Comparison of Wireless LAN Security Protocols: WEP, WPA And WPA2

	WEP	WPA	WPA2
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Michael (generates Message Integrity	Cipher block chaining message authentication

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

		Code (MIC))	code (CBC-MAC)
Key Management	Lack of key management	Provides robust key management and keys are generated through four way handshake	Provides robust key management and keys are generated through four way handshake
Hardware Compatibility	Works on existing hardware	Works on existing hardware through firmware upgrades on NIC	Supported in Wi-Fi devices certified since 2006, Does not work with older NIC
Attacks/ Vulnerabilities	Chopchop, Bittau's fragmentation, FMS and PTW attack, DoS attacks	Chopchop, Ohigashi-Morii, WPA-PSK, Beck-Tews and Michael Reset Attack and Hole 196 vulnerability, DoS attacks	Hole 196 vulnerability, DoS attacks due to unencrypted management and control frames, MAC address spoofing due to Deauthentication, Offline dictionary attacks in WPA2-Personal
Deployment complexity	Easy to setup and configure	Complicated setup required for WPA-enterprise	Complicated setup required for WPA2-enterprise
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	48 bit packet number prevents replay attacks

IV.CONCLUSION

The solutions for these shortcomings have been addressed by proposing/protocol an encryption algorithm which will be described in final paper the analysis of the results and details of application execution undertaken will also be presented in future work in this white paper.

REFERENCES

[1] Sung Jin-Cho, Un-Sook Choi, Yoon –Hee Hwang, Han –Doo Kim,"Design of New XOR based hash functions for cache memories",International Journal of computers and mathematics,Received 12 April 2006,Accepted 27 July 2007.
[2] Halil Ibrahim Bulbul, IhsanBatmaz, Mesut Ozel, "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols"; in Proceedings of the 1st international conference on Forensic applications and techniques, information, and multimedia and workshop, (Adelaide, Australia, January 21-23, 2008), ICST, Brussels, Belgium, 2008.
[3] Alexander Gutjahr, Albert Ludwigs University, Freiburg. "Wired Equivalent Privacy (WEP) Functionality, Weak Points, Attacks".
[4]JianquiangLou,Lihao Xu and James S.Plank,"An efficient XOR –Scheduling Algorithm for Erasure codes Encoding",University of Tennessee
[5] Martin Beck, Erik Tews, "Practical attacks against WEP and WPA", in WiSec '09: Proceedings of the second ACM conference on Wireless network security, New York, USA, ACM (2009).
[6] Andrea Bittau, Mark Handley, Joshua Lackey. The final nail in WEP's coffin, IEEE Symposium on Security and Privacy, pages 386-400. IEEE Computer Society, 2006.
[7] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds. Cryptology ePrint Archive, Report 2007/120 (2007).
[8] National Institute of Standards and Technology NIST 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
[9] Shadi R. Masadeh, NidalTurab, "A Formal Evaluation of the Security Schemes for Wireless Networks", Research Journal of Applied Sciences, Engineering and Technology 3(9): 910-913, 2011
[10] Marko Ihonen, AnssiSalo, Tuomo Timonen, Laboratory of Communications Software, Lappeenranta University of Technology, 802.11 Security Protocols, Seminar Report
[11] Arunesh Mishra, William, A. Arbaugh, "An Initial Security Analysis of The IEEE 802.1X Standard", University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Technical Report CS-T R-4328 and UMIACS-TR-2002-10 6 February 2002

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

[12] Jyh-Cheng Chen, Ming-Chia Jiang, Yi-Wen Liu, "Wireless LAN Security and IEEE 802.11i", IEEE Wireless Communications, vol. 12, no. 1, pp. 27–36, Feb. 2005
[13] N. Joukov, A. M. Krishnakumar, C. Patti, A. Rai, S. Satnur,A. Traeger, and E. Zadok. RAIF: Redundant Array of Independent Filesystems. In *MSST '07: Proc. of the 24th IEEE Conference on Mass Storage Systems and Technologies*,pages 199–212, September 2007.
[14] A. Chiornita, L. Gheorghe, and D. Rosner. A practical analysis of EAP authentication methods. In Roedunet International Conference (RoEduNet), 2010 9th, pages 31 - 35, June 2010.
[15] Jeng-An Lin and Chiou-ShannFuh. Research Article on 2-D Barcode Image Decoding.Hindawi Publishing Corporation,Mathematical problems in engineering,Volume 2013,Received 17 June 2013,Accepted 16 November 2013.