ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Multiple Packet System: A Security Approach for Wireless Networks

Richa Jani
College of Technology and Engineering, Udaipur
electronics &communication engineering department
Udaipur, India
richa2854@gmail.com

Shuchi Jani
Computer science & engineering department
Geetanjali institute of technical studies, Udaipur
Udaipur,India
janishuchi@gmail.com

Madhuri agrawal
Computer science & engineering department
College of Technology and Engineering, Udaipur
Udaipur,India
engr.madhuri@gmail.com

Abstract **-** The paper explores several types of security protocols that are used in wireless networks. Security protocols such as Wired Equivalent Privacy (WEP), WEP2, Wi-Fi Protected Access (WPA) and WPA2, the protocols developed mostly to work within the IEEE 802.11 standard, are presented. In accordance with the encryption and decryption the study of the protocols merits and demerits are introduced (vulnerabilities and problems). The number of procedures is proposed to improve against most of the known vulnerabilities that are faced by the wireless networks security in present. The proposed procedures can be used in a number of security related fields.

Keyword**:** WEP, WPA, Multiple packet system, Message integrity check

I. INTRODUCTION

Wireless security is the hindrance of unauthorized access or ruin to computers using wireless networks. Everyday a large number of security risks exposed associated with the existing wireless protocols .the remedy of these problems is to enhancing our design methodology in addition implementing and testing the protocols. New techniques are required to provide security. In this paper we have proposed and discussed a new method. The proposed method is compared with a number of existing working methods in wireless networks. The old methods are discussed and a number of its issues have been listed.

II. SECURITY ATTACKS

In this section, we describe the security attacks which are more susceptible for wireless networks security protocols.

A. Modification:

It is considered to be an active attack. The content of the message is modified by a third party. It involves the insertion, alteration, or deletion of information in an unauthorized manner that is proposed to appear authentic to the user. These attacks can be very hard to detect. This attack affects the integrity of the message the motivation of this type of attack may be to plant information, change grades in a class, alter credit card records, or something similar. A common form of modification attacks are Website defacements.

B. Eavesdropping:

Its generally a passive attack .This is the process of overhearing parts of a conversation. It also includes attackers listening in on your network traffic.

C. Interception:

This can be either an active or passive process. In a networked environment, in an Active interception a computer system is putting between sender and receiver to capture information as it is sent and a passive interception might involve someone who consistently monitors network traffic. From the interception point of view, this process is covert. The last thing a person on an intercept mission wants is to be discovered. Intercept missions can occur for years without the knowledge of the intercept parties.

D. Brute-force attack:

It is an attack on cipher text message, wherein the attacker attempts to use all possible permutations and combinations. This occurs over a long period. To make passwords trickier to guess, they should be longer than two or three characters, be complex and have password lockout policies

E. Fabrication:

This is also called as tampering attack: In this attack, a third party inserts forged messages into the organization network by posing as a valid user. A spiteful node do not interrupting or modifying any routing table thus the attacker fabricate its own packets and transmit it on the network to create anarchy to bring down the network. This attack affects the confidentiality, authenticity, and integrity of the message.

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

F. Maintainability

It is the ability of the protocol that maintains the security of the network after one or some of the encryption /decryption algorithm(s) was negotiated for any reason.

Static placement of Message Integrity Check (MIC) Keywords: it is measured as a problem because in this the contents of the decrypted message validate by any hacker which is combined with the brute force attack Since to decrypt the data in wireless networks the brute force attack is not a valid attack because the sent data has no specific type (like image, text, etc.) The time needed to cross comparison the decrypted data with a specific type is not valid. Since the MIC is a part of the sent encrypted packet. The hacker can decrypt the data is decrypted by a hacker using a key and can locate where the MIC bits are stored within the decrypted packet. The hacker can disengage MIC part from the packet and run a MIC on the rest of the packet .The hacker compares the obtained MIC from the decryption with the intended one, to validate the key used for decryption.[1]

G. Time Factor:

is a very important factor in which we measure how long will it take to brute force a protocol, currently this is done by calculating how many permutations are there in the encryption/decryption key.[1]

III. WIRELESS SECURITY PROTOCOLS

A. Wired Equivalent Privacy (WEP)

Algorithm issued to protect wireless communication from eavesdropping. A secondary function of WEP is to avert unauthorized access to a wireless network; WEP relies on a secret key that is shared between mobile stations (eg. A laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.[2]

a. Weakness

a) WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the cipher text yields the original plaintext. This makes stream ciphers susceptible to several attacks.[2]

b) The standard does not discuss how the shared key is established. In fact, most installations use a single key that is shared between all mobile stations and access points. More complicated key management techniques can be used to help defend from the attacks we describe.

c) As WEP uses one algorithm for encryption and decryption .if that algorithm is hacked by hacker then it will lead to the serious problem in wireless networks

d) MIC problem

B. Wired Equivalent Privacy 2:

WEP2 is an extension to Wired Equivalent Privacy (WEP), a wireless network security but was found to be inherently flawed. . WEP2 extended the IV and key values of WEP to 128 bits .it is a developed to fight against brute force attacks and IV deficiency.

a. Weakness:

a) Wep2 extended only WEP size but it faced same problems as WEP

C. Wi-Fi Protected Access:

Wi-Fi Alliance has developed a security protocol Wi-**Fi Protected Access** (**WPA**) to secure wireless networks.[3] WAP was developed in response to serious weaknesses had found in the previous system, WEP (Wired Equivalent Privacy). The WPA protocol implements most of the IEEE 802.11i standard. WPA introduced the Temporal Key Integrity Protocol (TKIP), TKIP is a per-packet key 128 bit key, and it is dynamically generated for each packet and thus removes weaknesses of the WEP. RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV) all three are concatenated in WPA.

In WPA payload integrity check is improved by using MAC (message authentication code) also known as MIC (message integrity check)[4]

a. Weakness:

a) Same as WEP, these are also not maintainable as WEP

b) MIC problem

D. Wi-Fi Protected Access 2:

As the name suggests, *WPA2* is a second, newer version of Wireless Protected Access (WPA) security and access control technology for Wi-Fi wireless networking.**WPA2** is changes to the original IEEE 802.11. It is designed to improve the security of Wi-Fi connections by requiring use of stronger wireless *encryption* than what WPA requires. Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes .WPA2 is strong security protocol then WPA. It introduces CCMP, a new AES-based strong security encryption mode WPA2 certification is compulsory for all new devices to have Wi-Fi trademark. CCMP is more secured MIC (message authentication code used in WAP). **WPA2** networks are also known as **RSN** (Robust Security Network).[2] More explanation of WPA2 and it's capability found in [4],[5],[6] .

a. Weakness:

a) WPA2 is not maintainable.

b) MIC problem.

IV. PROPOSED MECHANISMS

In this section, the proposed mechanism is described. The proposed mechanism is called Multiple Packet System (MPS).This system uses any one combination of five encryption/decryption algorithms RC4, Blowfish, IDEA, AES and RSA. MPS uses 256 packets in which one combination (excluding combination of

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

same algorithms) of the five algorithms is inserted randomly as shown in figure 1, where a 4-bit distinguish between the combinations of five algorithms instead of the actual name of the algorithm. Among 4 bit 2 bit correspond to one algorithm and another 2 bits correspond to other algorithm. MPS stores a key list for each one of the five algorithms. MPS encrypt each message with a different packet algorithm as well as different key that means that any hacker needs to go through 15^{256} possible combinations just to figure out the exact formation of the slots even before he starts to consider any key attacks (like brute force).

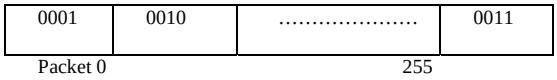
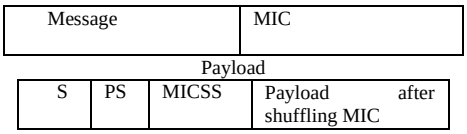


Figure 1. Packet System

Where

"0001" is RC4+AES,
"0010" is RC4+Blowfish
……
……
"0011" is RC4+RSA

MPS header consists of three parts. The first part is the key selector (KS), second part is packet selector (PS) and the third part is the MIC shuffle selector (MICSS) as shown in figure 2.message authentication code (also known as MAC, but The first part is 48-bit long to select between 2^{48} keys. the second part is 8bit long to select between the 256 slots that contain all the possible combinations of algorithms used for encryption/decryption. The third part is 8bit long to select between 256 shuffle tables. shuffle tables are generally used for shuffling or shamble the MIC bits with the original message .so that it can't be used as a lead in any king of attack as it was explained in section 2 (static placement of the MIC bits).



Calculated payload and headers

Figure 2. MPS Headers and Payload

A. *MPS (Multiple Packet System) procedure:*

MPS uses a different configuration file for each user; MPS is going to operate on the Application layer, because as it was mentioned in the MIC problem the headers in each layer used as a lead combined with the brute force attack. The access point (AP) will contain all the configuration files for all the users and it will handle the decryption and the re-encryption of the transferred messages from one user configuration file to another. AP will act more like a conversion server.

a. *Sending segment:*

List of keys are assigned to each algorithm inside the slot.MIC is generated for the message and one of the shuffle column is chosen. The generated MIC is then shuffled with chosen column inside the message starting from the first bit until the last bit in MIC. The encrypter will encrypt the new payload with assigned combination of algorithms for each slot that it was chosen using the chosen key. Each time the key is used it is marked from the list so that it would not be used by other slot. The node will concatenate SS, KS and MICSS as a header to message and then send the message. The packet, key and shuffle data can be used methodically which means MPS will use first packet and the first pointed keys from the key list of both algorithms.

Column1		……	**Column N**
0	1	……	8
1	2	……	5
⋮	⋮ ⋮ ⋮	⋮ ⋮ ⋮	⋮ .
N	55	.....	57

Figure 3.Number of bits in MIC

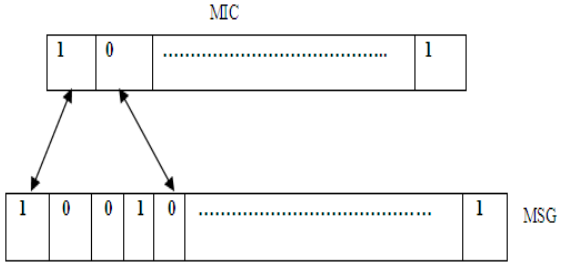


Figure 4 shuffling mechanism

b. *Receiving segment:*

PS, KS and MICSS is separated by receiver from the message.PS is used to identify the algorithm which is used to decrypt the message.The receiver decrypt the message by using assigned key lists of these algorithms and KS data. MICSS is used to get the shuffling column from the shuffled table.MIC for each message generated whether receiver and is compared with the received one to ensure the integrity of the message.

c. *Access Point and Control messages:*

AP(access point) acts as a conversion server. It has right to issue a refresh of configuration files for all users. For handling the conversion AP must have good processing power.MPS reissue control packets which is send by the user to AP,which is then delivered to the MPS control server.The MPS control server issue the new files and send them to AP.Copies of these files are kept by AP and send it to user.The configurations files are again received by the user and issue a control packet to AP so the old files are replaced with the new versions and reset all the counters.

V. CONCLUSION

The proposed mechanism can contradict most of vulnerabilities which was found in wireless network. By using the combination of five algorithms for encryption and decryption it's very difficult for intruder to identify the exact packet configuration, key lists and shuffling tables for each user in the network. The mechanism not only depends upon the permutation of the key list but also packets and shuffling tables. The static placement problem of MIC has been solved by MPS by using shuffle mechanism. The four combinations of algorithms have been used in each slot of MPS. If one

algorithm is found to be broken by any intruder the other one still remains in that packet so increases bandwidth but still provides better security as well with no losses in strength.

VI. REFERENCES

[1]. Prof. Dr. Gamal Selim et al., "New protocol design for wireless Networks security", ICA0T, 2006.

[2]. Nikita Borisov, Ian Goldberg, and David Wagner, Computer Science Division at the University of California, Berkeley, 01-Aug-2001,from http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[3]. Vandana Wekhande, "WI-FI Technology: Security Issues", Rivier Academic Journal, 2(2), FALL 2006, ISSN 1559-9388.

[4]. Wi-Fi Alliance, "Wi-Fi Protected Access: Strong, standards-based,interoperable security for today's Wi-Fi networks", Wi-Fi Alliance,(2003) Retrieved August 18, 2004 from http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf.

[5]. Wi-Fi Alliance (2004), "Wi-Fi Protected Access. security sees strong adoption: Wi-Fi Alliance takes strong position by requiring WPA security for product certification", Retrieved August 21, 2004 from http://www.wi-fi.org/opensection/releasedisplay.asp?TID=4&Item ID=165& Str Year=2004&str month=2

[6]. Wi-Fi Alliance (2004), "Press Release about new EAP types supportedunder WPA-Enterprise", Retrieved August 21, 2004 fromhttp://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID =205&StrYear=2005&strmonth=4.

[7]. Yonglei Liu, Zhigang Jin ; Ying Wang , "Survey on Security Scheme and Attacking Methods of WPA/WPA2", 6th International Conference on Wireless Communications Networking and Mobile Computing(WiCOM), Page(s): 1-4,2010