Prevention of DoS and Memory Attacks: Enhanced 3-Way Handshake

Paridhi Singhal
(Dept. Of CS &Technology)
FET, Mody
Institute of Technology and Science,
Lakshmangarh, Rajasthan, India

Manoj Diwakar
(Dept. Of CS &Technology)
FET, Mody
Institute of Technology and Science,
Lakshmangarh, Rajasthan, India

Mandeep Katre
(Dept. Of CS),
Inderprastha Engineering College,
63 Site IV, Surya Nagar Flyover Road,
Sahibabad, Ghaziabad, U.P.
India

ABSTRACT

In today's world most organizations are moving from wire-connected LAN to wireless LAN. The phenomenal popularity of the 802.11 network standards stems from the fact that they provide for wireless connections with ease and convenience. Recently, security holes have been identified in the operation of 802.11 networks, and the 802.11i protocol has been announced to protect such networks. However, there are still security issues that prevent the 802.11 network from becoming the best choice protocol for wireless LANs. We reviewed 802.11i security with a focus on a denial of service attack. This attack exhausts the client's memory using a vulnerability of the key derivation procedure in 802.11i. It is vulnerable to various Denial of Service attacks (DoS) which includes de-authentication and disassociation attacks including memory exhaustion attacks. For Dos and memory exhaustion attacks which are possible in 4-way handshake ,this paper provides an enhanced 3-way Handshake algorithm which is free from these attacks in comparison to original protocol and is more secure.

Keywords

3-way handshake; 4-Way Handshake; De-authentication; DoS Attacks; memory exhaustion attack; IEEE802.11; IEEE802.11i.

1. INTRODUCTION

Wireless Local Area Networks (WLAN) [1,2] used to provide flexibility for schools, hostels, college campuses, coffee shops, airports and other enterprises. Because this WLAN provide much higher transmission rates than any other current cellular systems, WLAN systems promise to be widely deployed in the coming years. Security is main concern for many networks and for wireless network it is very important because wireless medium is open for public access within certain range. Only authenticated users and computers can access this network to solve any type of WLAN issues related to security we should take care of two-way authentication between the communicating entities, method of dynamically allocating the encryption keys, use some kind of centralized Authentication mechanism, enhanced encryption algorithms and efficient key management techniques . Various services being offered by any security mechanism includes:

- Data Secrecy/Privacy: in this method data is preserved from the attacker so that only authorized person can read the data.
-
- Data Integrity Data Integrity in its broadest meaning refers to the trustworthiness of information over its entire life cycle.
- Access Control: Access control refers to exerting control over who can interact with a resource.

Wired Equivalent Privacy (WEP) [1] is a security protocol for wireless networks that encrypts transmitted data. It's easy to configure. Without any security your data can be intercepted without difficulty. However, WEP was an early attempt to secure wireless networks, and better security is now available such as DES, VPN, and WPA [2]. WEP is not difficult to crack, and using it reduces performance slightly. . In order to remove these vulnerabilities a technique called WPA(Wi-Fi Protected Access)[3] was developed.WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated in 2004 and is documented in the current standard. It is an interim solution that is used now until 802.11i comes out. It still using RC4, but the Key was changed to TKIP.TKIP basically works by generating a sequence of WEP keys based on a master key, and re-keying periodically before enough volume of information could be captured to allow recovery of the WEP key. The IEEE 802.11i amendment introduces a range of new security features that are designed to overcome the shortcomings of WEP. It introduces the concept of a Robust Security Network (RSN) [4], which is defined as a wireless security network that allows the creation of Robust Security Network Associations (RSNA) only which acts as a key management scheme in IEEE 802.11i framework and validates that Pairwise Master Key (PMK) has been established. It further helps in the synchronization of temporal keys which are installed for the process of authentication and encryption being carried out in 802.11i Framework that overcomes the WEP and WPA flaws.

In this paper we mainly concentrate on 2 types of attacks they are: Denial of Service attacks and memory exhaustion attacks which are present in 4-way handshake mechanism which makes IEEE802.11i amendment vulnerable to attacks and thus making the encryption and authentication process more secure This paper is organized as follows: Section 2 overview of IEEE 802.11i framework, various confidentiality and integrity protocols being used and the potential threats arising from them. Section 3 modified, enhanced and proposes authentication mechanism for key management. Section 4 results obtained. Section 5 conclusion and future work.

2. IEEE802.11I SECURITY ANALYSIS

To analyze the possible DoS vulnerabilities, it is mandatory to GIVE BRIEF overview of IEEE802.11i amendment which is then followed by 4-Way Handshake and possible DoS attacks.

2.1 Overview of IEEE802.11i Standard

IEEE 802.11i [5] there are three data encryption algorithms defined by IEEE 802.11i[5] : CCMP, TKIP and WEP, where CCMP is the long-term solution requiring additional hardware capabilities, TKIP is the short-term solution to fix WEP problems, and WEP is included for backward compatibility. However, in this paper we mainly focused on the protocols authentication and do not investigate these data confidentiality protocols in any detail. The basic 3 elements of 802.1X authentication framework are:

- Supplicant/Client
- Access Point which serves as Authenticator
- Authentication Server(RADIUS)[10]

RSNA [6, 7] establishment use mainly 802.1x authentication protocols followed by protocols for key management. Like any other authentication procedure, firstly a shared key is generated between the client and the authenticator, then this key subsequent temporal keys are generated which is then followed by distribution of usable keys by the key managements protocols for the particular communication session. Figure1 shows the different stages involved in generation of a secure RSNA. There are 6 stages involved in generation of RSNA [8].

- Network Discovery Stage: The Access Point (AP) continuously broadcasts some special type of frames called Beacon frames which that indicate its security capabilities.
- Authentication and Association Stage: Supplicant chooses one of the available APs depending on its signal strength and tries to authenticate and get connect with that AP, then it starts sending the associated request frame to the AP
- EAP/802.1X/RADIUS Authentication Stage: RADIUS server comes into action which is the authenticator server used for providing AAA services.
- 4-Way Handshake Phase: This phase is executed in order to confirm that PMK has been successfully installed at both the client side and the authenticator side.
- Group-Key Handshake: This is an optional phase and is executed in case of multicast applications to generate a fresh GTK.
- Secure Data Communication: it indicates that all cipher suites and security capabilities of both the client and authenticator have been exchanged and PTK or GTK has been successfully installed.

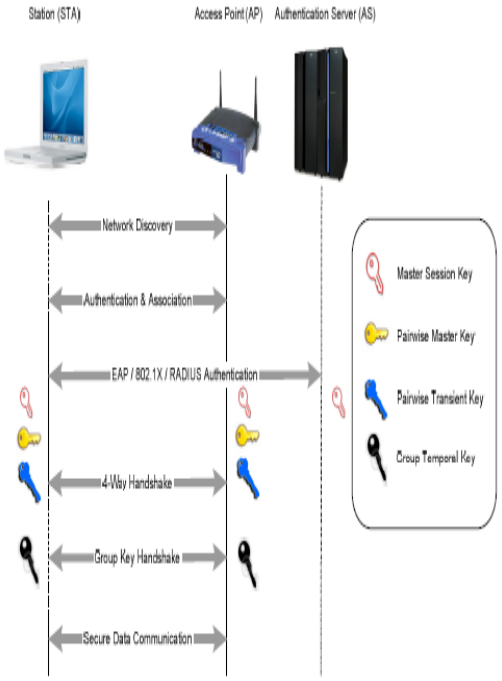

Figure 1 IEEE802.11i Authentication Procedure

We mainly focus here on 4-Way Handshake [9] procedure and various types of Dos Attacks against it.

2.2 4-Way Handshake

Figure2 depicts the 4 types of messages that are exchanged between the communicating entities i.e. Supplicant and the AP [11, 12].The Procedure begin by sending of Message1 from AP to Supplicant. The AP generates ANonce which is a random number, starts a Sequence Number and encapsulates these inside Message1. The Supplicant after receiving message1 generates other random value SNonce, MAC address of the supplicant that is SPA and derives a fresh temporal key Public Transient Key (PTK) which is a function of both SNonce and ANonce and stores both ANonce and SNonce in the memory. Than supplicant generates other message, Message2 which consist of SPA, SNonce, Sequence Number and MIC value which is a function of all other fields and is generated using calculated PTK as the key [7,13]. MIC is calculated in order to preserve the integrity of the send message as other fields are sent as plain text. On receiving Message2, AP generates PTK using the same method and verifies received MIC with the calculated one in order to guarantee its integrity [13]. Then again it constructs Message3 as shown in Figure2 which serves as an acknowledgement of message2 which is verified at supplicant side in order to confirm that correct PTK has been generated at other end, Message4 is again the acknowledgement by the supplicant.

PTK = PTK = PRF (PMK, SNonce, ANonce, AA, SPA)

Here :

a) AA: Access Point's MAC address.

b) ANonce: random number generated by AP.

c) SNonce: random value generated by Supplicant.

c) SN: Sequence Number.

d) MsgX: type of message.

e) SPA: supplicant's MAC address

f) MIC: message integrity code

g) PTK: pairwise transient key

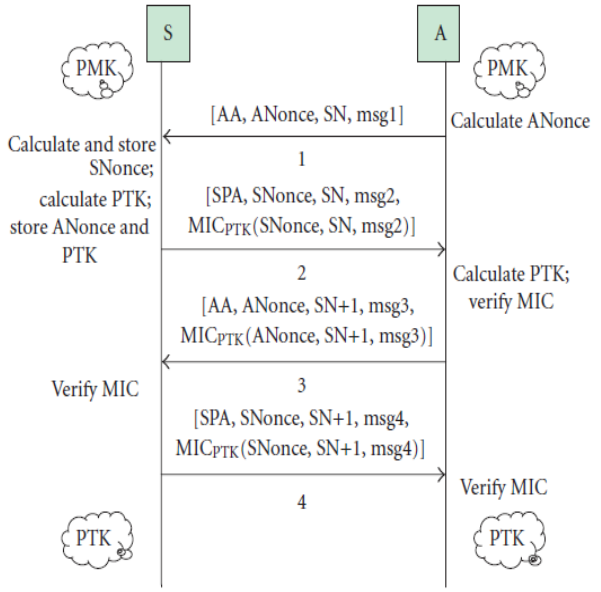

Figure2. 4-Way Handshake Process

2.3 DoS and Memory Exhaustion Attacks on 4-Way Handshake:

The mechanism defined by IEEE 802.11i is vulnerable to memory exhaustion attacks [11], [13], [14] and DoS flooding .So, to handle these types of attacks we need to develop some security mechanisms. The weakness of 4-way handshake phase of 802.11i standard is the first message that is Message1 because of not using any MIC field in order to guarantee the message integrity. That's why it can be easily eavesdrop by any hacker since it is broadcasted and all fields of it can easily be known to the hacker. As mentioned in above section, that supplicant side will have both of the random values SNonce and ANonce as stored and new key PTK is derived from function of these random values as shown in Figure3.

In next step Message 2 is generated and MIC field is calculated using this PTK as secret shared key to preserve the integrity of the message and is attached with the message. On the other hand PTK is again calculated with the help of same procedure and MIC is calculated and verified [7]. After sending of Message2 attacker plays its role and constructs a fake message Message1' which differs in ANonce field value only as it is random value generated by AP and sends it to the supplicant .Let the fake nonce value be ANonce'. Supplicant thinking it as genuine stores ANonce', calculates PTK which let be denoted as PTK' and updates the original PTK value to PTK'.

PTK' = PRF (PMF, ANonce', SNonce, AA, SPA)

If the attacker is able to send Message1' between Message 3 (from AP to Supplicant) and Message 2 (from Supplicant to AP), then this will lead to storage of ANonce' and PTK' at the supplicant side and sending of Message2' with appended MIC as a function of PTK'. Now the authenticator will send Message3 where attached MIC will be a function of ANonce value. This will lead to failure in integrity check since MICPTK is not equal to MICPTK' and hence the Message3 will be discarded without any notification to authenticator.

Now after the timer expire at Authenticator and it has still not received Message4, it will again send Message3 predicting it of being lost during communication but it will again be discarded by Supplicant S due to MIC mismatch. Now after nth attempt by authenticator and still not getting Message4 it will de-authenticate the supplicant and hence S will be disassociated and hacker is successful in launching DoS attack. Also attacker is able to launch memory exhaustion attack since sending of each of the fake Message1' result in storing of ANonce' and PTK' value at supplicant side leading to memory exhaustion if continuous flooding of Message1' is done.

According to 802.11i standard, in order to stop the attacker from updating the PTK value to PTK', a mechanism called Temporal PTK (TPTK) was developed in which TPTK represents PTK value until Message3 is received and verified. When supplicant receives Message1 it will generate a TPTK where TPTK = PTK and on all subsequent receiving of Message1' it will update only TPTK value and store them till Message3 is received and verified. It will not update the value of PTK. But this solution is acceptable only when supplicant has successfully installed PTK and receives Message1' after Message3 has been verified but here they are send before Message3, therefore it is not helpful in preventing the attacks.

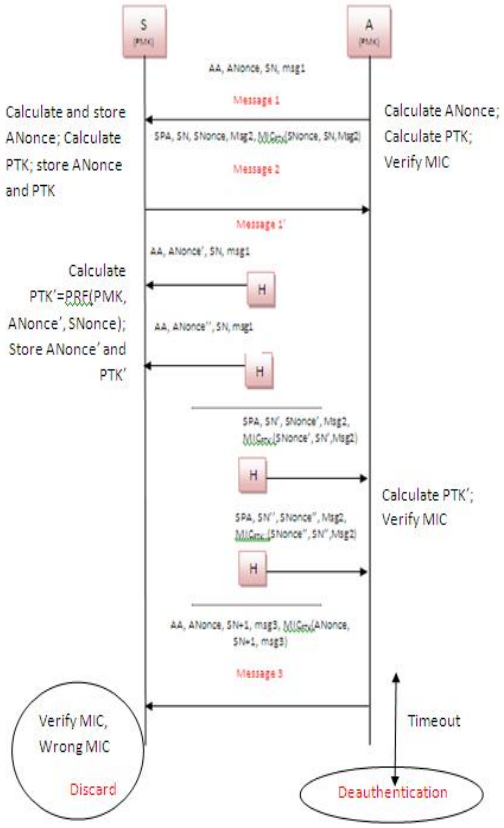

Figure3. DoS Flooding Attack in 4-Way Handshake

2.4 Related Work

According to Mitchell [11], if we add MIC in Message1 then we can easily prevent possible DoS attack because the 4-Way Handshake phase begins both Authenticator and Supplicant shares a common secret key PMK. As we know that PMK is used for adding the MIC value and it is the basic and mandatory element in deriving the series of other keys, so using of it directly in communicating any of the messages over the network

is risky and should be avoided as it becomes vulnerable to attacks.

Second method given by him, were of reusing the SNonce value, that is, as supplicant receives Message1 it will generate and store the value of SNonce, it will not store ANonce and the calculated PTK. Now in case S receives Message1' , in that case S should not update its SNonce value till it will receives message 3 which is verified and then PTK is installed. That's why we can say that S will store single SNonce value and re-calculate PTK whenever it receives Message3, this method will solves the problem of memory exhaustion but in case Message3 is flooded than we have to re-calculate the value of PTK again and again but this will again lead to CPU exhaustion attack.

Xiaodong Zha and Maode Ma [7] presented an enhanced 2-Way handshake protocol, according to which AP will generate 2 random numbers ANonce and BNonce, and encrypt these numbers and supplicant MAC address with PMK. AP then encapsulate this inside Message1 and sends it to the supplicant. Supplicant after receiving Message1 decrypts it with PMK and calculates PTK as stated in standard protocol. After this it encrypts the BNonce and generated SNonce with same PMK and encapsulates this inside Message2 and sends it to AP. After receiving Message2, AP again decrypts it with PMK and verifies BNonce value and once verified calculates PTK with the help of same method. It prevents DoS attacks since ANonce value is encrypted but it increases computation power and it is vulnerable to chosen plaintext attacks since PMK is used directly for providing confidentiality services.

3. PROPOSED SOLUTION

As we have discussed above, DoS attack is mainly caused due to unprotect Message1 in 4-way handshake phase. Here we propose a modified handshake process that is 3-Way Handshake as shown in Figure4 which is free from DoS attacks and memory exhaustion attacks. The message flows are:

(i) Message 1: [AA, EncTPMK[ANonce], SN, Msg1];

(ii) Message 2: [SPA, SN, SNonce, Msg2, MICPTK(SNonce, SN,Msg2)];

(iii) Message 3: [AA, SN + 1, SNonce, Msg3, MICPTK(SNonce, SN + 1, Msg3)]

PTK = PRF-n(PMK, AA,SPA, ANonce, SNonce)

Here n=384 for CCMP or n=512 for TKIP

The major difference between 3-way Handshake and proposed 4-way Handshake are as follows: firstly to secure Message1, secondly ANonce value is encrypted by means of Temporal PMK(TPMK). As PMK is known to both authenticator and the supplicant before the Handshake process begins, it can be used to generate other secret key in order to protect message1 as securing message1 by means of PMK directly make the whole 802.11i standard vulnerable to attack by the attackers. Also there is no need of storing the ANonce value at the supplicant side and message1 now becomes secure from attacker.

Steps to be followed are:

(i) Receiving of Message1 by Supplicant:

- Decrypts the ANonce value
- Generates SNonce, calculates PTK
- Store PTK and SNonce
- Create and send Message2

(ii) Receiving of Messag2 by AP:

- Calculation of PTK by same mechanism
- Verify MIC
- Create and send Message 3

(iii) After receiving Message 3, firstly supplicant verifies MIC and then this validates the successful installation of PTK at the authenticator.

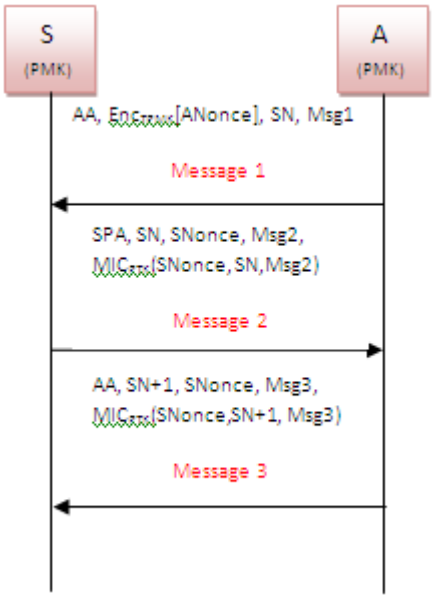

Figure4. Enhanced 3-Way Handshake

As we have seen in 3-Way Handshake process, Message4 is not required because of successful verification of MIC at the supplicant site indicates that PTK has been successfully calculated and installed at the Authenticator site. Hacker can't mount DoS attack by sending any type of fake Messages or Message1 since they are encrypted by TPMK which is known by supplicant and authenticator only, before this process actually started and Memory exhaustion attacks is also prevented because of ANonce value is not stored at the supplicant side.

Generation of TPMK:

TPMK is a temporary key used to secure Message1 of the 3-Way Handshake Phase only ,it can be generated as follows:

- Apply Permuted Choice1 to 64 most significant bits of PMK .
- After that, Divide the resultant bits into 2 halves; let it be L1 and R1.
- Then, apply 2 circular left shift operations to both L1 and R1. Let the result be L2 and R2.
- Now exchange L2 and R2 position and combine them to form TPMK.

Here Permuted Choice1 (PC1) is same as used in key generation process of DES algorithm [5].

4. RESULT AND DISCUSSION

The proposed solution was implemented using Java to simulate the 4-Way Handshake process between the supplicant, authenticator and an attacker. The size of the memory was fixed to 5 Mb. Table1 shows the results obtained from the DoS Flooding attack on standard 4-Way Handshake process and on proposed Solution.

Table1: Comparison of DoS Flooding Attack

Delay between packets (millisec)	Average time until Memory exhaustion in 4-Way Handshake (millisec)	Average time until Memory exhaustion in Proposed Solution (millisec)	Packets send by the attacker
50	870	---------	20
30	630	---------	35
10	410	----------	50

It states that in 4-Way Handshake process as the packets send by the attacker increases, the time taken until memory gets exhausted decreases. But in proposed solution memory never gets exhausted as when Message1' packets were send by the attacker after sending of Message2 by supplicant, ANonce' value is never stored at the supplicant side and PTK is also calculated and installed only once in the whole process. Also PTK is calculated after receiving Message 1 which is protected by encrypting the ANonce value with Temporal Pairwise Master Key (TPMK).

The proposed 3-way handshake mechanism is free from DoS Message flooding attacks from very start of the process till it ends and Temporal PMK can also be used for protecting other control frames which are send in plain text over the network and thus provide a means for protecting them before the 4-Way Handshake phase begins. Also it only needs modification in first message of the 4-way Handshake process, rest of the messages being same containing the respective MIC field and other parameters, thereby preserving the authentication and integrity of the messages as in original 4-way handshake process.

5. CONCLUSION

IEEE 802.11i standard was defined in order to overcome the vulnerabilities in WEP and WPA but still it is not secure against DoS attacks and memory exhaustion attacks in 4-Way Handshake phase. So here we proposed an enhanced 3 –Way Handshake procedure which provides a mean to secure the 4-Way Handshake phase of IEEE802.11i standard against Denial of Service (DoS), Denial of Service Flooding attacks and memory exhaustion attacks. The most vulnerable part of this phase is message1 which is the first step in this procedure, because this message is send unencrypted over the network. 3-Way Handshake procedure will resolves this problem by encrypting the ANonce value field by some temporal key TPMK which is a function of Pairwise Master Key (PMK) and thus can be decrypted by only the supplicant. However the solution becomes little complex due to calculation of one more key and using encryption to protect Message1, but it succeeds in providing security against DoS and DoS flooding attacks. This algorithm is also safe for memory exhaustion attacks because ANonce is never stored at the supplicant side since it can be decrypted only by the supplicant. Also Public Transient key (PTK) is stored once at the client side that make it secure for memory exhaustion attacks. Similarly the proposed modified 4-way handshake is secure against DoS and DoS flooding attacks.

6. REFERENCES

[1] IEEE Standard 802.11-1999. Information technology – Telecommunications and information exchange between Systems – Local and metropolitan area networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications. 1999. IEEE Standard 802.11b-1999. Higher-Speed Physical Layer Extension in the 2.4 GHz Band, Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. September, 1999.

[2] Guide to Internet Security

[3] What's New in Security: WPA (Wi-Fi Protected Access).

[4] Seung-Jo HanHeang-Soo Oh JonganPark Dept. of Electron. Eng., Chosun Univ." The improved data encryption standard (DES) algorithm., Spread Spectrum Techniques and Applications Proceedings, 1996.

[5] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1X standard," Tech. Rep. CS-TR-4328, University of Maryland, College Park, Md, USA, February 2002

[6] Xiaodong Zha ; Maode Ma ," Security improvements of IEEE 802.11i 4-way handshake scheme",IEEE International Conference on Communication Systems(ICCS) 2010.

[7] Xinyu Xing; Shakshuki, E.; Benoit, D.; Sheltami, T.; "Security Analysis and Authentication Improvementfor IE E802.11i Specification",Global Telecommunications Conference, 2008.

[8] http://wwwvs.informatik.uniulm.de/de/intra/bib/2008/ICC/DATA/S04S07P05.PDF

[9] http://www.massey.ac.nz/~dpparson/004.pdf

[10] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-Way Handshake," in Proceedings of the 3rd ACM workshop on Wireless security, Philadelphia, PA, USA, 2004, pp. 43 - 50.

[11] V.Moen, H. Raddum, and K. J. Hole, "Weaknesses in the temporal key hash of WPA," ACMSIGMOBILEMobile Computing and Communications Review, vol. 8, no. 2, pp. 76–83, 2004

[12] F. D. Rango, D. C. Lentini, and S. Marano, "Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi protected

[13] D. B. Faria and D. R. Cheriton, "DoS and authentication in wireless public access networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe '02), pp. 47–56, Atlanta, Ga, USA, September 2002.