Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Encryption using DES of ANonce in 4-Way Handshake Protocol for Authentication in Wpa2

Pawan Kumar
Department of ECE
G.L Bajaj Institute of Tech. & Mgt.
Greater Noida, India

Gopal Prasad
Department of ECE
K. P. Engineering College
Agra, India

Atul Kumar Singh
Department of ECE
Kamla Nehru Inst. of Tech.
Sultanpur, India

Abstract— IEEE standard 802.11i is the latest standard for security in wireless LAN (WLAN). This standard provides data confidentiality as well as integrity. The 802.11i 4-way handshake and key management stays secure against any attack the key used for this purpose is secure. But, availability is main issue because 802.11i is subjected to denial of service (DoS) attacks. Since first Message in the 4-way handshake is not encrypted and protected by any method so counterfeiting these messages is possible. This paper presents a simple proposal to prevent DoS attacks against the 4-way handshake protocol.

Keywords— 802.11i, ANonce, WLAN Security, 4-way handshake protocol, DoS attack

I. INTRODUCTION

Now a day's Wireless LAN (WLAN) is becoming more popular among home users as well as enterprise users (big industries). The reason behind this is its mobility, wide availability of hardware and comparatively less price. IEEE has different standard and 802.11 is one of the standards for WLAN. Many amendments have been made in 802.11 [13] for the improvement of bandwidth, functionality, range and the most importantly its security. Wired Equivalent Privacy (WEP) protocol [4] is the earliest and simplest form of security adopted in the early stages of WLAN. but After few years, WEP was proved to be insecure and it was replaced by the Wi-Fi Protected Access (WPA) protocol.WPA uses TKIP the type of application in WPA: WPA Pre-shared Key (PSK) for home users and SOHO users and WPA Extensible Authentication Protocol (EAP) for enterprise users [4].the WPA is assumed to be a secure protocol until attackers and hackers finds many vulnerabilities inside the 4-way handshake protocol. An attacker can easily obtain a passphrase by capturing the 4-way handshake messages and then performing a dictionary attack on the captured packets [6, 4, 5]. The i task group was created in the IEEE In January 2001 to improve 802.11 for data authentication and encryption security. the final release of the 802.11i standard was adopted In June 2004,and received its commercial name WPA2 from the Wi-Fi Alliance[12]. WPA2 deploy a major improvement of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) [21], in which Advanced Encryption Standard (AES) [14] is used.

802.11i is quite able to protect the passphrase from being compromised but it is not completely secure. Regardless of the development of WLAN security protocols from WEP to WPA2,various denial of service (DoS) attacks such as radio frequency jamming, disassociation and deauthentication attacks [1] and flooding [11, 8] threats the WLAN to be vulnerable. Specially, the 802.11i 4-way handshake is proved to be vulnerable to denial of service attacks. This includes the reflection attack [7] and the 1 Message DoS attack. These results in an incomplete or failure of 4-way handshake. So in this situation the client station will not be able to authenticate itself to the server or the access point. Hence a new mechanism is needed to face these attacks to ensure availability of data and network connectivity continuously. The main focus made in this paper is to address the problem of DoS attacks in the 4-way handshake protocol. It also elaborates various studies and research done previously for proposed solutions [11, 8].

This paper is divided into segments according to the following arrangement. Section II gives an overview of 802.11i 4-way handshake protocol. Section III summarizes the previously related works done by researchers to defend 802.11i 4-way handshake protocol from DOS attacks. Section IV describes our proposed solution in detail, Section V concludes the paper.

II. IEEE 802.11I

The IEEE 802.11i introduces Cipher Block Chaining Message Authentication Protocol (CCMP) [12] which is based on strong block cipher, the Advanced Encryption Standard (AES) [12,14]. This wipes out the use of the weak RC4 stream cipher key [9] in WPA and enhances the strength of the key in IEEE 802.11i with the use of AES algorithm. The IEEE 802.11i standard introduced some primary changes such as separating user authentication from message integrity and privacy, in this way providing robust and scalable security architecture that is equally suitable for small networks (home) as well as large corporate systems. This new architecture used in wireless networks is called the Robust Security Network (RSN) and it uses 802.1X authentication i.e. RSNA, new integrity and privacy mechanisms and key distribution techniques.

The 4-way Handshake Protocol

In WPA2, The PMK (Pairwise Master Key) derivation depends on the authentication method used [6]: if a PSK (Pre-Shared Key) is used, PMK = PSK.

The PSK is generated from a passphrase ranging from 8 to 63 characters or a 256-bit string. This will provides a solution for home networks and small enterprises where no authentication server is used. for big enterprises where an authentication server is used, the PMK is derived from the 802.1X authentication Master Key.

PMK = PBKDF (passphrase, SSID, SSID length, 4096, 256)

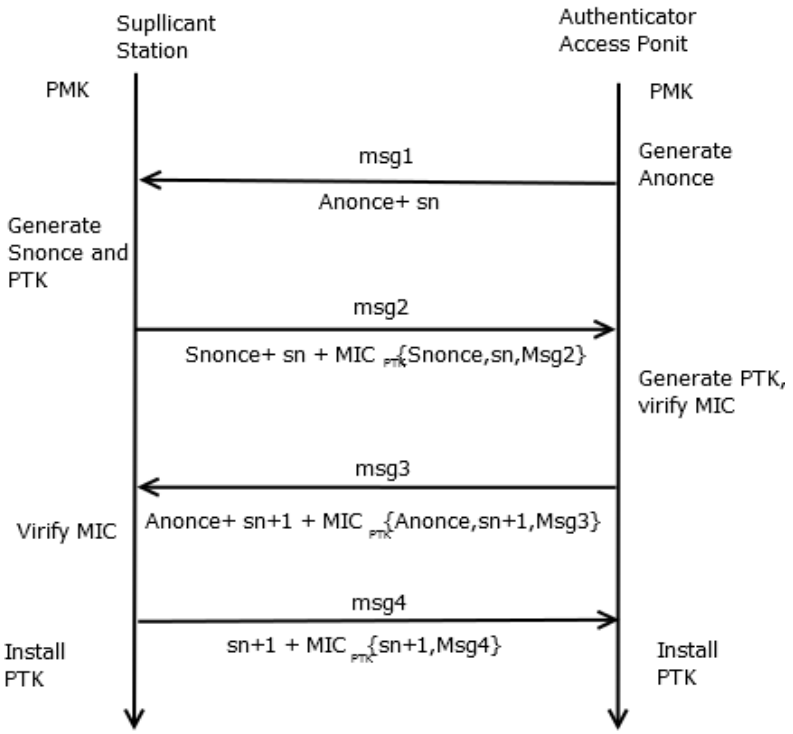

Fig 1 . 802.11i 4-way handshake protocol

This PMK is not used for the encryption or message integrity checking rather than it is used for generating another key (pairwise master key) PTK which encrypt the unicast traffic. The key length of PTK depends upon the encryption protocol used. It is of 384 bits for CCMP and 512 for TKIP.

Initially, the authenticator access point will generate a random number, ANonce. This nonce is then encapsulated inside Message 1 with a sequence number. This sequence number is used to prevent replay attacks [6, 4]. After receiving Message 1, the supplicant station will generate another random number Snonce and derive a pairwise transient key (PTK) using the PMK, the received ANonce and the generated SNonce. The PTK derivation can be expressed as in [6]:

PTK = PRF-X (PMK, Pairwise key expansion, Min (Authenticator_MAC, Supplicant_MAC) || Max(Aauthenticator_MAC, Supplicant_ MAC) || Min(ANonce, SNonce) || Max(ANonce, SNonce))

PTK contains 4 temporal keys KCK (Key Confirmation Key – 128 bits): Key for authenticating the message's MIC during the 4- Way Handshake and the Group Key Handshake,

• KEK (Key Encryption Key – 128 bits): this Key is used for ensuring data confidentiality during the 4-Way Handshake and Group Key Handshake,

• TK (Temporary Key – 128 bits): Key for data encryption for unicast (used by TKIP or CMMP),

• TMK (Temporary MIC Key – 128 bits): Key for data authentication (used only by Michael w i t h TKIP) [6, 4].

The station will then generate random number SNonce and compute the Message Integrity Code (MIC) using KCK [2,9] .this MIC ensures the integrity of Message 2 [2,6,9].before receiving Message 2 from the supplicant, the authenticator extract the SNonce, compute the PTK and derive the temporal keys. The KCK affirm MIC in Message 2. If the verification is successful the authenticator continues to send Message 3 that consist of GTK that is encrypted with KEK and the MIC [6].

Once the station receives Message 3, it verifies the MIC by following the same process. If it is successful, then the station installs the PTK and GTK. At last, Message 4 as an acknowledgement message is sent to the access point to verify that PTK and GTK have been installed and the handshake is completed successfully [6, 4].

Weaknesses in the 4-way Handshake Protocol

Lack of confidentiality and integrity of message 1 is the main factor for DoS attack in the 802.11i 4-way handshake protocol [6, 8]. In the 4-way handshake, the authenticator sends the ANonce to the supplicant is transmitted as plaintext [6].

It is also notable that at this time there is no method of authentication or privacy protection, so an attacker can easily capture and spoof this message [11, 3, 7, 8].

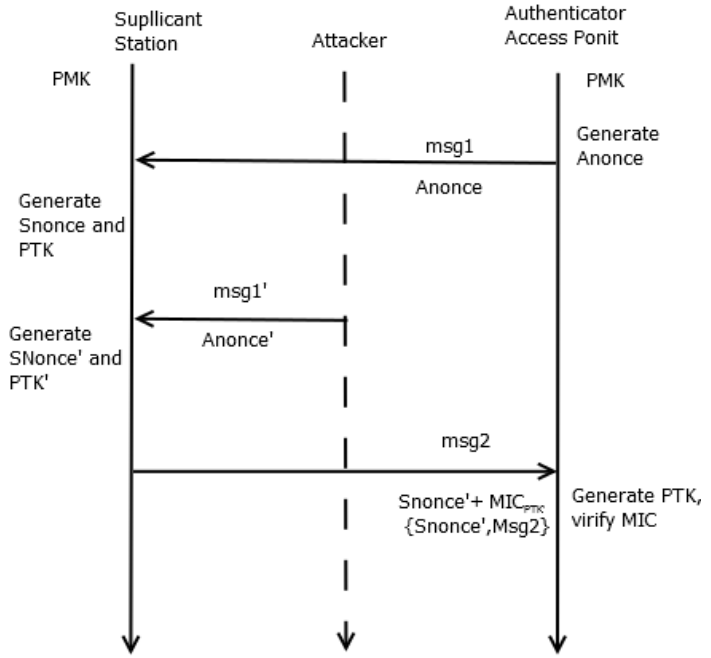

Fig 2. One message denial of service attack (situation 1)

Figure 2 show, the attacker sends a fake Message 1 which includes a new ANonce (says ANonce') value for the station before the station send Message 2 to the access point. This causes the station to re-generate a new SNonce (says SNonce') value and also derive a new Pairwise Transient Key (says PTK') depends on the ANonce received from the attacker [8]. When the station sends Message 2 to the access point, the MIC is computed and it becomes fail because PTK ≠ PTK' [3, 8]. Therefore, the handshake becomes incomplete.

In Another DoS attack (Figure 3) in which an attacker sends a forge Message 1, the station is forced to generate another new SNonce, derives a new PTK based on the new ANonce and SNonce, and at last install the new PTK [8]. Station receives Message 3 and verifies the MIC in Message 3 with its new PTK. However, since the new PTK value is different from the PTK used by the access point so the MIC verification fails, that results in incomplete handshake [8].

III. RELATED WORKS

Various solutions and implementations have been proposed to oppose the denial of service attacks on the 4- way handshake protocol [11, 3, 8, 1].

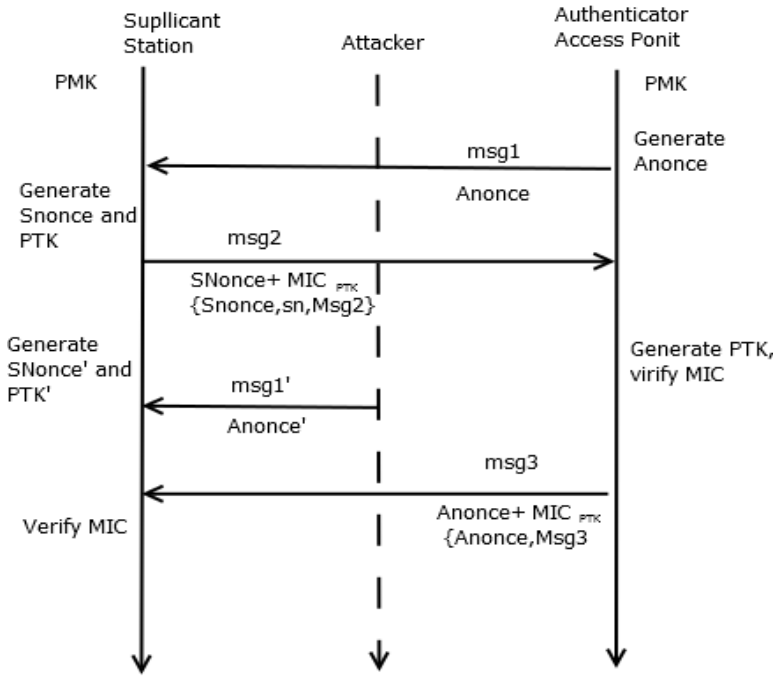

Fig 3. One message denial of service attack (situation 2)

Message 1 Authentication

The proposed solution is to use an authentication method in Message 1 to check its integrity [8]. MIC is added inside Message 1. Both station and access point should already have a preshared common secret key (PMK) before any message exchange in the 4- way handshake. This PMK is used by the access point to calculate the PTK, using PTK MIC is completed. When the station receives Message 1, the PTK is derived from the PMK and this PTK is used to verify the value of the MIC. If it is successful, the station will now calculate the SNonce. Message 3 and Message 1 are still distinguishable by the secure bit [8].

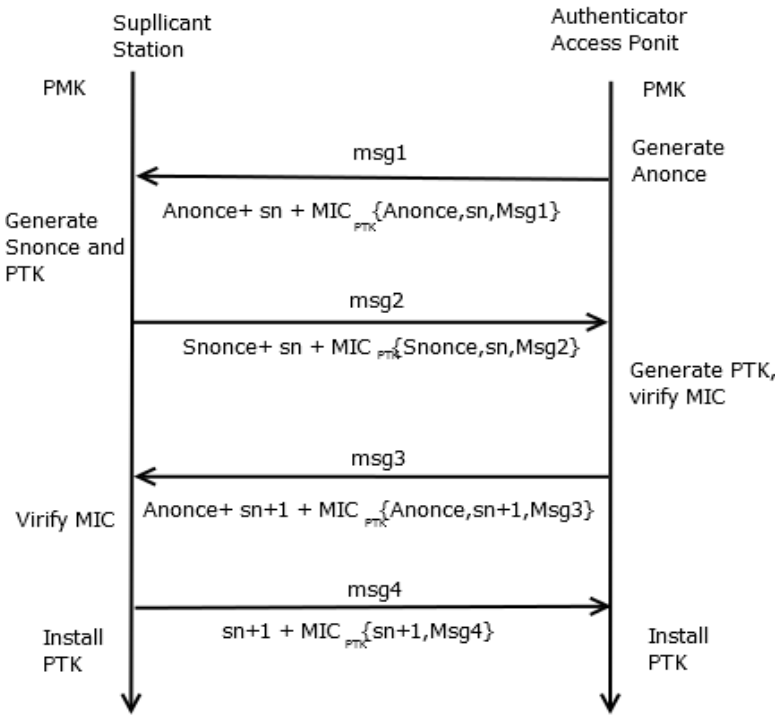

Fig 4. Message 1 authentication using MIC

Nonce Re-use

The station always re-uses the same values of SNonce until the legitimate handshake is completed and at the both sides, station and access point, the PTK is installed [8]. This requires the station to store the SNonce and derive a PTK based on the received ANonce and stored SNonce. When station receives Message 3 from the access point, the PTK is derived by the station again from the received ANonce and stored SNonce to verify the MIC in Message 3. The main benefit of this approach is that it eliminates memory but, more computational power is required at the station side because of the computation of PTK is done two times, so, if an attacker performs CPU exhaustion by Message 3 flooding on the station [8].

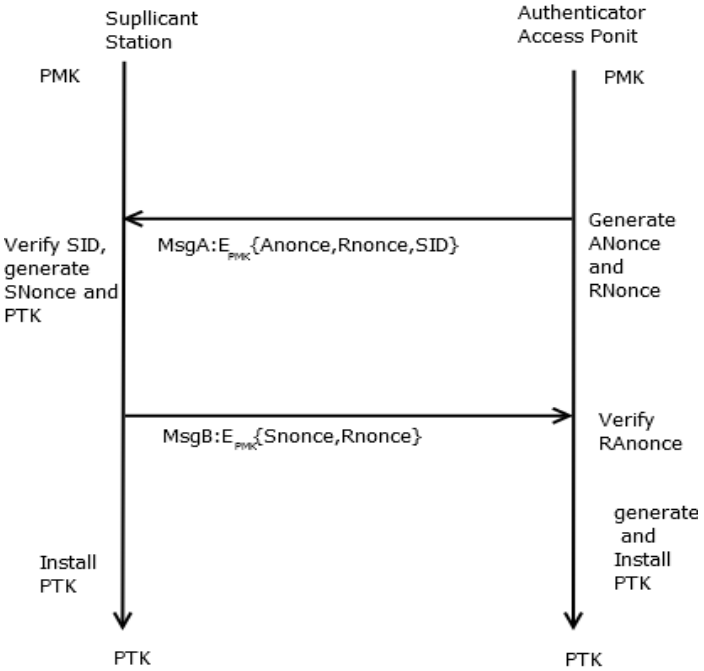

Fig 5. Enhanced 2-way handshake protocol

Enhanced 2-way Handshake Protocol

The proposed solution changes the authentication method, the WPA / WPA2 handshake into a 2-way handshake [11]. There are 2 messages; MsgA and MsgB. Figure 5 clarify the proposed solution. MsgA is sent by the access point, which is already encrypted with the PMK. this msg consist of RNonce, ANonce, and the SID (i.e. MAC address) [11]. supplicant station receives the MsgA, decrypt that packet and compare that SID value with its own SID value to verify if the authenticator access point is legitimate or not. If the authenticator is verified successfully then MsgB is sent to the authenticator. Both the values of RNonce in MsgB and the RNonce in MsgA will be the same [11].

The authenticator will have to verify the value of RNonce before it derives and install the PTK. There is not any involvement of MIC in the proposed 2-way handshake protocol, thus it uses less processing power [11]. This improvement also reduces the information exchange between the station and the access point. However, security only depends on the PMK because it is directly used as the key to encrypt both messages msgA and msgB. hence, the strength of the PMK must be very strong to resist against the dictionary or brute force attack.

IV. PROPOSED SOLUTION

Before the authentication process of the 4-way handshake, both the authenticator and the supplicant should have knowledge of the passphrase or PMK [11, 8]. This passphrase can be calculated as PMK = PBKDF2 (passphrase, SSID, SSID length, 4096, 256) [6], this key is used for the generation of another key named as PTK (pairwise transient key) which is used as a key for encryption process of the data communication between two entities. When the authenticator initially calculates the ANonce, this nonce will use the PMK as the key to encrypt the ANonce before it will be send to the supplicant. In this paper, the DES cipher block chaining (DES-CBC) [14] block cipher mode is chosen to encrypt the ANonce. After the supplicant receives Message 1, it will be able to decrypt the ciphertext to obtain the ANonce because of having preshared passphrase. If both passphrases that is being used by the authenticator and the supplicant are the same, then decrypted ciphertext will give a correct ANonce value. If different passphrases (in case of attacker) were used to encrypt or decrypt the ciphertext, the resulting ANonce will be invalid. This decrypted ANonce will be stored and used to compute PTK for the further process.proposed solution may be understood by the fig 6.

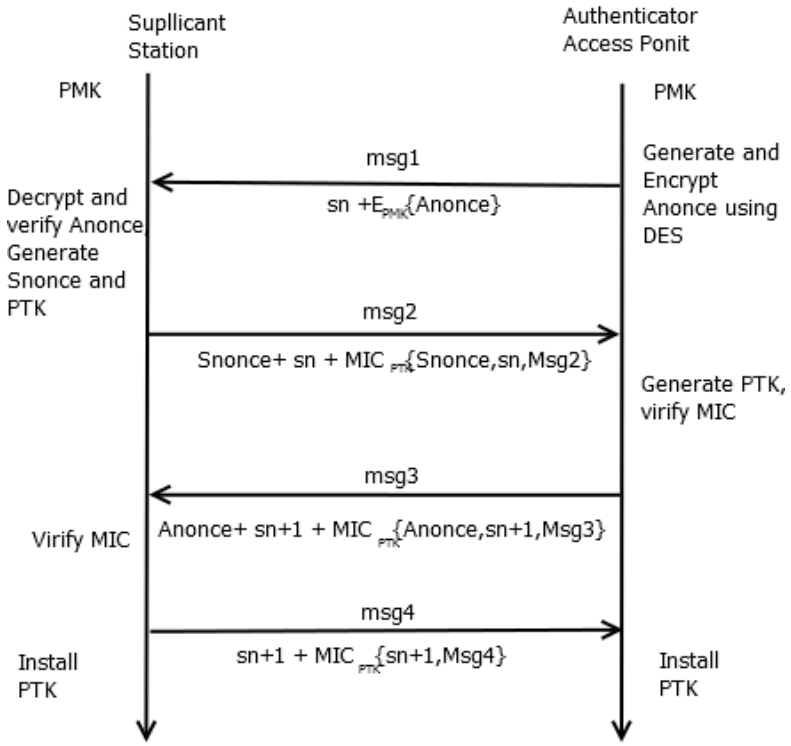

Fig 6. Proposed 4-way handshake protocol using DES encryption of ANonce

Still, the proposed solution in this paper brings outs a new vulnerability. Since the preshared PMK is computed from the passphrase, it is possible for attacker to obtain this PMK. If the attacker is able to capture first message of the 4-way handshake, the attacker can perform a brute-force or dictionary attack using the captured Message 1. Thus, the strength of key strongly depends upon the strength of the passphrase. However, some improvements can be made to the proposed solution in future work to obtain a more secure implementation of this solution. Further studies and analysis is needed to implement a better block cipher or encryption mechanism to anticipate this weakness. One of the possible improvement is by introducing the cryptographic hash function s that can be MD5 [19] or MD6 [16,17,18]. This improvement may be done by hashing the pairwise master key (PMK) before encryption of the ANonce. The results from this hash will be a 32-bit hexadecimal value which is believed to be a strong key. This process can be done at the sides, authenticator and supplicant to encrypt and decrypt the ANonce.

V. CONCLUSIONS

The 802.11i security protocol is quite able to defend any attack or attempts to compromise the Pairwise Master Key or the passphrase. It provides both data encryption as well as data authentication. But it fails to defend against certain DoS attacks like 1 Message DoS attack on the 4-way handshake because at the handshaking process the messages exchange are not encrypted so they can be captured. After defining the handshaking problem and having reviewing other defence mechanisms, a new solution is proposed. However, the proposed solution might open the possibility for an attacker to perform a dictionary or brute-force attack and if successful, attacker obtains the passphrase and compromise the overall security of the WLAN. Accordingly, enhancements will be made to the proposed solution in future work.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[1] Cagalj, M., Capkun, S., Rengaswamy, R., Tsigkogiannis, I., Srivastava, M., Hubaux, J. P. 2006. Integrity (I) Codes: Message Integrity Protection and Authentication Over Insecure Channels. In IEEE Symposium on Security and Privacy. Oakland, California, USA.

[2] De Rango, F., Lentini, D.C., and Marano, S. 2006. Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack inWi-Fi Protected Access and IEEE 802.11i. In EURASIP Journal on Wireless Communications and Networking, 1-19.

[3] Edney, J., and William, A. A. 2003. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. Addison-Wesley. Boston.

[4] Fluhrer, S., Mantin, I., and Shamir. 2001. A.Weaknesses in the Key Scheduling Algorithm of RC4. In Proceedings of the 8th Annual International Workshop on Selected Areas in Cryptography.1-24.

[5] Guillaume, L. June 2005. Wi-Fi security – WEP, WPA and WPA2. In Hackin9. Available at http://www.hakin9.org.

[6] He, C., and Mitchell, J. C. 2005. Security Analysis and Improvements for IEEE 802.11i. In NDSS.

[7] He, C., and Mitchell, J. C. 2004. Analysis of the 802.11i 4-Way Handshake. In WiSe'04. 43-50.

[8] Huang, J., Susilo, W., Seberry, J. December 2004. Observations on the Message Integrity Code in IEEE 802.11 Wireless LANs. In WITSP'04. Adelaide, Australia.328-332.

[9] Liu,J., Ye,X., Zhang, J., and Li, J. 2008. Security Verification of 802.11i 4-way Handshake Protocol. In ICC 2008.1642-1647.

[10] IEEE Standard 802.11i-2004. 2004. Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[11] IEEE Standard 802.11-1999. 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.

[12] National Institute of Standards and Technology. November, 2001. Announcing the Advanced Encryption Standard (AES). In Federal Information Processing Standards Publication 197.

[13] Shim, J.H., Kwon, T. W., Kim, D. W., Suk, J. H., Choi, Y.H., and Choi, J.R. 2003.Compatible Design of CCMP and OCB AES Cipher for Wireless LAN Security. In SOC Conference, 2003. Proceedings IEEE International [Systems-on-Chip].

[14] DES_ FIPS 46-3: The official document describing the DES standard; csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[15] Rivest, R. L. The MD6 hash function - A proposal to NIST for SHA-3.

[16] Rivest, R. L. The MD6 Hash Algorithm. Available at http://groups.csail.mit.edu/cis/md6/

[17] Rivest, R. L., Agre, B., Bailey D.V., Crutchfield C., Dodis, Y., Fleming, K.E., Khan, A., Krishnamuthy, J.,Lin, Y., Reyzin, L., Shen, E., Sukha, J., Sutherland, D., Tromer, E. and Yin, Y.L. October 2008. The MD6 Hash Function-A proposal to NIST for SHA-3. Rivest's CRYPTO'08. Available at http://groups.csail. mit.edu/cis/md6/submitted-2008-10-27/ Supporting_Documentation/md6_report.pdf

[18] Robshaw, M. J. B. November 1996.On Recent Results forMD2, MD4 and MD5",In RSA Laboratories' Bulletin.

