

Security analysis of newly ameliorated WAPI protocol

Pang Liaojun¹ Li Huixian² Wang Yumin¹

(¹Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)

(²School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Based on thorough researches on the Chinese wireless local area network (WLAN) security standard, i. e., WLAN authentication and privacy infrastructure (WAPI), the security of the authentication access process is analyzed with the CK (Canetti-Krawczyk) model and the BAN (Burrows-Abadi-Needham) logic. Results show that it can achieve the alleged authentication and key negotiation goals. Besides those alleged, further analyses indicate that the authentication access process can satisfy other security requirements, such as mutual identity authentication, mutual key control, key confirmation, message integrity check, etc. If the used elliptic curve encryption algorithm and the hash algorithm are secure enough, the protocol can efficiently realize mutual authentication between STAs (station) and APs (access point). Therefore, WAPI can be applied to replace the security mechanism used in the original WLAN international standard to enhance its security.

Key words: wireless local area network (WLAN); WLAN authentication and privacy infrastructure (WAPI); authentication; key negotiation; CK model

Due to its convenience and flexibility, wireless communication technology has found wider and wider applications around the world. But, with more attention being paid to the wireless communication technology, the security problems appear to be more prominent than ever before^[1-2]. Since the original wireless LAN (WLAN) international standard, ISO/IEC 8802. 11, has been found to have security defects, China has proposed a WLAN authentication and privacy infrastructure (WAPI)^[3-4] protocol to enhance its security, which is the first Chinese standard proposed in this field.

The defects in the protocol are always subtle and difficult to find out, and security analysis has become a necessary step in guaranteeing the security of protocols. There is no doubt that the degree of WAPI security should affect its application in China or even the whole world, so it is very significant and necessary to make a security analysis of the WAPI and offer a scientific judgment. From Refs. [3 – 4], we can see that WAPI is composed of a WLAN authentication infrastructure (WAI) and a WLAN privacy infrastructure (WPI). The WAI is the basis of the WPI, and WPI security depends on the WAI security and the security of the cryptographic algorithms and the encryption modes used.

Received 2007-04-26.

Biographies: Pang Liaojun (1978—), male, doctor; Wang Yumin (corresponding author), male, professor, ymwang@xidian.edu.cn.

Foundation items: The National Basic Research Program of China (973 Program) (No. G1999035805), the Natural Science Foundation of Shanxi Province (No. 2007F37), China Postdoctoral Science Foundation (No. 20060401008, 20070410376).

Citation: Pang Liaojun, Li Huixian, Wang Yumin. Security analysis of newly ameliorated WAPI protocol[J]. Journal of Southeast University (English Edition), 2008, 24(1): 25 – 28.

Assume that the cryptographic algorithms and the encryption mode are secure, and the security of the WPI completely depends on that of the WAI. Therefore, in this paper we shall only analyze WAI security. The WAI is also called the authentication access process, which mainly achieves mutual identity authentication and the establishment of session keys between STA and AP.

1 Constructing Two Security Protocols

To analyze the WAI protocol by the CK model, we first give two SK-secure key-exchange protocols, which will be used in the security analysis of the WAI. The details of the CK model can be found in Refs. [5 – 6].

1.1 Two SK-secure key-exchange protocols in AM

Let (G, E, D) be key-generation, encryption and decryption algorithms, respectively, of a public-key encryption scheme secure against chosen ciphertext attacks (CCA)^[7]. Let k be the security parameter. Assume that each party P_i has invoked $G(k)$ to obtain a pair (e_i, d_i) of encryption and decryption keys, and all the parties have the public encryption key e_j of the other parties. In addition, let $\{f_K\}_{K \in \{0, 1\}^k}$ be a pseudorandom function family.

Protocol 1^[5] ENC

Proceed as follows: given security parameter k .

Step 1 The initiator, P_i , on input (P_i, P_j, s) chooses $K \xleftarrow{R} \{0, 1\}^k$ and sends $(P_i, s, E(e_j; K))$ to P_j . Next, P_i outputs the session key $\sigma = f_K(P_i, P_j, s)$ under session-id s .

Step 2 Upon receipt of (P_i, s, c) , the responder, P_j , computes $K' = D(d_j; c)$. If the decryption algorithm does not reject the ciphertext, then P_j outputs the session key $\sigma' = f_{K'}(P_i, P_j, s)$ under session-id s .

Theorem 1^[5] The protocol ENC is SK-secure without perfect forward secrecy (PFS) in AM.

Protocol 2 EKP_AM

Proceed as follows: given security parameter k .

Step 1 The initiator, P_i , on input (P_i, P_j, s) chooses $R_1 \xleftarrow{R} \{0, 1\}^k$ and sends $(P_i, s, E(e_j; R_1))$ to P_j .

Step 2 Upon receipt of (P_i, s, c_1) , the responder, P_j , computes $R'_1 = D(d_j; c_1)$. If the decryption algorithm does not reject the ciphertext, then P_j chooses $R_2 \xleftarrow{R} \{0, 1\}^k$ and sends $(P_j, s, E(e_i; R_2))$ to P_i . At the same time, P_j outputs the session key $\sigma = f_{R'_1 \oplus R_2}(P_i, P_j, s)$.

Step 3 Upon receipt of (P_j, s, c_2) , P_i computes $R'_2 = D(d_i; c_2)$. If the decryption algorithm does not reject the ciphertext, then P_i outputs the session key $\sigma' = f_{R_1 \oplus R'_2}(P_i, P_j, s)$.

Theorem 2 The protocol EKP_AM is SK-secure without PFS in AM.

1.2 Choosing two authenticators

Authenticator 1^[5-6] Signature-based MT-authenticator λ_{sig}

Given security parameter k , let sig and ver denote the signing and verification algorithms.

1) When activated, within party P_i and with an external request to send message m to party P_j , P_i sends “message: m ” to P_j first. P_i also outputs “ P_i sent message m to P_j ”.

2) Upon receipt of “message: m ” from P_i , party P_j chooses a random value $N_B \xleftarrow{R} \{0, 1\}^k$, and sends $\{m, N_B\}$ to P_i .

3) Upon receipt of $\{m, N_B\}$ from P_j , party P_i sends $\{m, \text{sig}(P_i; (m, N_B, P_j))\}$ to P_j .

4) Upon receipt of the response from P_i , party P_j accepts m if the signature is successfully verified, and then outputs “ P_j received m from P_i ”.

Theorem 3^[5-6] The protocol λ_{sig} emulates protocol MT in UM.

Authenticator 2^[5-6] MAC-based authenticator λ_{MAC}

Given security parameter k , let f denote a secure MAC function, and $K_{i,j}$ be a shared key between a pair of parties P_i and P_j . Let m denote a message that P_i wants to send to the recipient P_j .

1) P_j sends a challenge $r \xleftarrow{R} \{0, 1\}^{2k}$ to P_i .

2) P_i sends the message m together with the authentication tag $f_{K_{i,j}}(P_j, r, m)$ to P_j .

Theorem 4^[5-6] The protocol λ_{MAC} emulates protocol MT in UM.

1.3 Two SK-secure key-exchange protocols in UM

Here, we transform EKP_AM and ENC into SK-secure protocols in the UM, called EKP_UM and ENC_UM, respectively.

Protocol 3 EKP_UM

Let k be the security parameter. Assume that each party P_i has a pair (e_i, d_i) of public and private keys, and all the parties have the public key e_j of the other parties. CH_i is the challenge information of party P_i .

Step 1 The initiator, P_i , on input (P_i, P_j, s) chooses $R_1 \xleftarrow{R} \{0, 1\}^k$ and sends $(P_i, s, E(e_j; R_1))$ to P_j .

Step 2 Upon receipt of (P_i, s, c_1) , the responder, P_j , computes $R'_1 = D(d_j; c_1)$. If the decryption algorithm does not reject the ciphertext, then P_j chooses $R_2 \xleftarrow{R} \{0, 1\}^k$ and computes the session master key $\sigma = f_{R'_1 \oplus R_2}(P_i, P_j, s)$ under session-id s (Using the session master key σ , P_j can derive a session encryption key K_e and an integrity check key K_i). Then P_j computes $\text{MAC}_{K_i}(P_i, \text{CH}_i, P_j, s, E(e_i; R_2))$ and sends $(P_j, s, E(e_i; R_2))$ and $\text{MAC}_{K_i}(P_i, \text{CH}_i, P_j, s, E(e_i; R_2))$ to P_i .

Step 3 Upon receipt of (P_j, s, c_2) and MAC_{K_i} , P_i computes $R'_2 = D(d_i; c_2)$. If the decryption algorithm does not reject the ciphertext, then P_i computes the session master key $\sigma' = f_{R_i \oplus R'_2}(P_i, P_j, s)$ under session-id s (Using the session master key σ' , P_i can derive a session encryption key K'_e and an integrity check key K'_i). Using the key K'_i , P_i can re-

compute $\text{MAC}_{K'_i}(P_i, \text{CH}_i, P_j, s, E(e_i; R_2))$ and compare it with the received MAC_{K_i} . If they are equal in value, P_i computes $\text{sig}(P_i; P_j, s, E(e_j; R_1), \text{CH}_j, P_j)$ and sends it to P_j . At the same time, P_i outputs the session key σ' under session-id s .

Step 4 Upon receipt of sig , P_j verifies the signature sig . If the signature is valid, P_j outputs the session key σ under session-id s .

Theorem 5 Assume that the signature scheme in use is secure against chosen message attack and the MAC function in use is secure, the protocol EKP_UM is SK-secure in the UM.

Proof From theorem 2, the protocol EKP_AM is SK-secure in AM. From theorems 3 and 4, both protocol λ_{sig} and protocol λ_{MAC} emulate protocol MT in UM; that is to say, both of them are MT-authenticators. Finally, from theorem 6 in Ref. [5], the protocol EKP_UM is SK-secure in UM.

Protocol 4 ENC_UM

Given security parameter k , let $K_{i,j}$ be a shared key between a pair of parties P_i and P_j . CH is the challenge information generated by P_j .

Step 1 The initiator, P_i , on input (P_i, P_j, s) chooses $K \xleftarrow{R} \{0, 1\}^k$ and sends $(P_i, s, E(e_j; K))$ to P_j . Next, P_i outputs the session master key $\sigma = f_K(P_i, P_j, s)$ (The session master key σ includes a session encryption key and an integrity check key) under session-id s . Then, P_i computes $\text{MAC}_{K_{i,j}}(P_j, \text{CH}, P_i, s, E(P_j; K))$ and sends $(P_i, s, E(P_j; K))$ and $\text{MAC}_{K_{i,j}}(P_j, \text{CH}, P_i, s, E(P_j; K))$ to P_j . At the same time, P_i outputs the session key σ under session-id s .

Step 2 Upon receipt of (P_i, s, c_2) and $\text{MAC}_{K_{i,j}}$, P_j recomputes $\text{MAC}_{K_{i,j}}(P_j, \text{CH}, P_i, s, c_2)$ and compares it with the received $\text{MAC}_{K_{i,j}}$. If they are equal in value, P_j computes $K' = D(d_j; c_2)$. If the decryption algorithm does not reject the ciphertext, then P_j computes and outputs the session master key $\sigma' = f_{K'}(P_i, P_j, s)$ under session-id s (The key σ' includes a session encryption key and an integrity check key too). At the same time, P_j outputs the session key σ' .

Theorem 6 Assume that the MAC function in use is secure, then the protocol ENC_UM is SK-secure in the UM.

Proof The proof is similar to that of theorem 5.

2 Security Analysis of WAI

In the CK model, the authenticator λ_{sig} assumes that each party P_i has a pair (s_i, v_i) of signing and verification keys, and all the parties have the verification key v_j of the other parties^[5-6]. But in WAI, this is not true. Therefore, we should prove this before we use the CK model, and here the proving method we will use is BAN.

2.1 Certificate and public-key verification

We use BAN to simply analyze the WAPI certificate authentication process which is composed of messages 1 to 4. In the WAPI-based WLAN, STA's and AP's identities are represented by their digital certificates, so the mutual identity authentication is practically achieved by authenticating their certificates. The task of authenticating certificates is due to authentication service unit (ASU) that is completely trusted by STA and AP, so STA and AP should believe the certifi-

cate authentication results generated by ASU. There is no secret information in each message of this process, and all that is required for security is to guarantee the freshness and integrity of each message. The usage of the timestamp “Ta” in messages 2 to 4 can protect them against replay attacks, and the digital signature in these three messages can protect them against forgery attacks. Although the usage of the timestamp “Ta” in message 1 can ensure its freshness, its integrity is not guaranteed because anyone can steal the certificate of a legitimate STA to arbitrarily construct a correct message 1 with an appropriate timestamp. Anyone can easily steal an arbitrary STA’s certificate to successfully cheat an AP in this process, but this cannot compromise the security because it can be detected in the following processes. An alternative method suggested here is to add the STA’s signature in message 1 to protect its integrity, and this can make the cheating be detected immediately.

2.2 Security analysis of the unicast key negotiation protocol

The WAI unicast key negotiation process is composed of message 5 and message 6. It is easy to see that the WAI unicast key negotiation protocol is the protocol EKP_UM in essence. In the protocol EKP_UM, if we let AP and STA replace P_i and P_j , respectively, let the session-id $s = (\text{algIdentifier}, \text{ukeyIdx}, \text{SPI})$ (here SPI includes their identity information), and let mIDap and nextmIDsta replace the challenge CH_i and CH_j , respectively. At the same time, move the signature in step 3 to step 1 with the repetitious information deleted. Then we can obtain the WAI unicast key negotiation protocol immediately. That is to say that the WAI unicast key negotiation process is essentially the protocol EKP_UM except for the difference in symbols. Because we have proven the fact that the protocol EKP_UM is SK-secure in the UM model in the foregoing section, we can conclude that the WAI unicast key negotiation process is also SK-secure in the UM model.

2.3 Security analysis of the multicast key announcement protocol

The multicast key announcement process is composed of message 7 and message 8. This process cannot be started until the former two processes have been completed successfully, so now STA and AP have a shared unicast encryption key and a unicast integrity check key. In fact, only message 7 can achieve the multicast key announcement, because it is easy to see that the protocol composed of only message 7 is in essence the protocol ENC_UM. In the protocol ENC_UM, if we let the unicast integrity check key be the MAC key $K_{i,j}$, let AP and STA replace P_i and P_j , respectively, let the session-id $s = (\text{gkeyIdx}, \text{ukeyIdx}, \text{gsn})$, and let gNonce replace the challenge CH. At the same time, deleting the repetitious information, we can then obtain the protocol composed of only message 7 immediately. That is to say that the protocol composed of only message 7 is essentially the protocol ENC_UM except for the difference in symbols. Because we have proven the fact that the protocol ENC_UM is SK-secure in the UM model in the foregoing section, we can conclude that the protocol composed of only message 7 is al-

so SK-secure in the UM model. Message 8 appears to be redundant, but it can directly achieve the unicast session key confirmation and indirectly achieve the private-key confirmation rather than only the response of the multicast key announcement.

2.4 Other security properties

Through further analyses, the WAI protocol also meets the following security demands of the authentication and key agreement protocol of the WLAN:

1) Privacy protection The secret information in each message of the WAI protocol is encrypted by the public-key algorithm, which protects the secret information from getting by the vicious attacker or an unexpected recipient.

2) Integrity protection During the certificate authentication process, the unicast key negotiation process or the multicast key announcement process, the digital signature and the message integrity code (MIC) are used to protect the message integrity.

3) Mutual identity authentication The digital certificate is used to represent the entity’s identity. Both the STA and the AP certificates are authenticated by the ASU, which are completely trusted by the STA and the AP.

4) Mutual key control^[8] The unicast master key is determined by relevant safe parameters, R_1 and R_2 , provided by the AP and the STA, respectively. By the security of the protocol EKP_UM, the unicast master key is only shared between the AP and the STA; no other party can calculate it. Moreover, the safe parameters, R_1 and R_2 , are chosen randomly by the AP and the STA, respectively, each time, so neither the AP nor the STA is able to control the establishment of the key alone.

5) Private-key confirmation Message 8 of the WAI protocol can achieve this confirmation, which has been discussed above.

6) KKS (known key security)^[9] Each unicast key or multicast key is established independently of the others; thus, the protocol satisfies the attribute of KKS.

7) Non-KCI (key compromise impersonation), Non-UKS (unknown key share) The key agreement protocol of the WAPI is proved SK-secure with the CK model, so it can offer such attributes as Non-KCI and Non-UKS^[6].

8) PFS Through the analyses above, we can see that the WAPI cannot offer the attribute of PFS. But (if keys are erased from memory when the session is expired) the only way to recover a past key is to attempt to obtain the private keys of both the AP and the STA. In the WLAN, the AP is more secure than the STA, and it is much more difficult to obtain the private key of the AP than to obtain the private key of the STA^[5,10]. In this case, it is of no use to obtain only the STA private key because the session keys are controlled by both the STA and the AP.

3 Conclusion

Based on the thorough researches on the WAPI, this paper analyzes its authentication access process with the CK model and BAN. Results show that the WAPI can meet the security demands in the WLAN, and thus it can be applied to replace the security mechanisms in the original international standards.

References

- [1] Branch J, Petroni N, van Doorn L, et al. Autonomic 802.11 wireless LAN security auditing [J]. *IEEE Security and Privacy*, 2004, 2(3): 56–65.
- [2] Johnston D, Walker J. Overview of IEEE 802.16 security [J]. *IEEE Security and Privacy*, 2004, 2(3): 40–48.
- [3] GB 15629.11—2003 Information technology-local and metropolitan area networks-specific requirements—part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications [S]. Beijing: Standards Press of China, 2003. (in Chinese)
- [4] GB 15629.11—2003/XG1 [S]. Beijing: Standards Press of China, 2006. (in Chinese)
- [5] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels [C]//*Proc of Advances in Cryptology—EUROCRYPT'01*, LNCS 2045. Berlin: Springer-Verlag, 2001: 453–474.
- [6] Canetti R, Krawczyk H. Universally composable notions of key exchange and secure channels [C]//*Proc of Advances in Cryptology—EUROCRYPT'02*, LNCS 2332. Berlin: Springer-Verlag, 2002: 337–351.
- [7] Cramer R, Shoup V. A practical public-key cryptosystem provably secure against adaptive chosen ciphertext attack [C]//*Proc of Advances in Cryptology—CRYPTO'98*, LNCS 1462. Berlin: Springer-Verlag, 1998: 13–25.
- [8] Mitchell C J, Ward M, Wilson P. Key control in key agreement protocols [J]. *Electronics Letters*, 1998, 34(10): 980–981.
- [9] Boyd C, Mao W, Paterson K. Key agreement using statically keyed authenticators [C]//*Proc of the 2nd International Conference on Applied Cryptography and Network Security*, LNCS 3089. Berlin: Springer-Verlag, 2004: 248–262.
- [10] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key-exchange protocols [C]//*Proc of the 30th Annual Symposium on Theory of Computing*. New York: ACM Press, 1998: 419–428.

新完善的 WAPI 协议安全性分析

庞辽军¹ 李慧贤² 王育民¹

(¹ 西安电子科技大学计算机网络与信息安全教育部重点实验室, 西安 710071)

(² 西北工业大学计算机学院, 西安 710072)

摘要: 在深入研究中国无线局域网安全标准 WAPI 接入鉴别过程的基础上, 利用 CK 模型并结合 BAN 逻辑, 对其认证和密钥协商过程安全性进行了形式化分析, 证明其能够实现所声称的各种认证及密钥协商目标. 进一步的分析结果表明, WAPI 不仅具有所声称的各种安全属性, 同时还能够有效地实现实体间相互认证、密钥的相互控制、密钥确认、消息完整性校验等安全属性. 如果协议中所采用的椭圆曲线加密算法和杂凑算法足够安全, 则该协议能够实现 STA 和 AP 之间的相互身份认证, 可以用于替代原来的无线局域网国际标准中的安全机制, 以增强无线局域网的安全性.

关键词: 无线局域网; WAPI; 认证; 密钥协商; CK 模型

中图分类号: TP309