http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 6 (7): 1108-1113, 2007
ISSN 1812-5638

Perfect Forward Secrecy of Authentication and Key Exchange Protocols in Three Versions of WAPI

[1]Chun-Jie Cao, [1]Chao Yang, [1]Xing-Hua Li, [2]Yuan-Bo Guo and [1]Jian-Feng Ma
[1]Key Laboratory of Computer Networks and Information Security, Ministry of Education,
Xidian University, Xi'an 710071, China
[2]Institute of Electronic Technology, Information Engineering University of PLA,
Zhengzhou 450004, China

Abstract: Wireless Local Area Networks (WLAN) are now being widely deployed for many applications, but security remains one of the most critical challenges yet to be fully addressed. Recently, a basic solution to this problem namely WLAN Authentication and Privacy Infrastructure (WAPI) provided by China Broadband Wireless IP Standard Group are proposed, which consisted of three versions. Nevertheless, this solution has some drawbacks: the Authentication and Key Exchange (AKE) protocols in WAPI cannot provide perfect forward secrecy. Moreover, the AKE protocol based on pre-shared keys of the last version of WAPI can be subject to off-line dictionary attacks. In this study, we first analysis the security of WAPI, then improvements on AKE protocols of WAPI are proposed.

Key words: Authentication and key exchange, perfect forward secrecy, Diffie-Hellman, WAPI

INTRODUCTION

Wireless Local Area Networks (WLAN) are now being widely deployed for many applications, but security remains one of the most critical challenges yet to be fully addressed. Chinese WLAN standard GB 15629.11-2003 (Anonymous, 2003), the first issued Chinese standard in the field of WLAN, has been formally implemented since November 1, 2003. The security solution of it is known as WLAN Authentication and Privacy Infrastructure (WAPI). And in March 2004, China Broadband Wireless IP Standard (BWIPS) Group of National IT Standardization Technical Committee drafted out WAPI Implementation Plan (Anonymous, 2004b), which fixes some drawbacks (Zhang and Ma, 2005a) in the original standard WAPI and is more robust (Zhang and Ma, 2005b; Li and Ma, 2005). However, considering the compatibility with different WLAN security solutions, for example, IEEE 802.11i (Anonymous, 2004a), a new national standard WAPI-XG1 (Anonymous, 2006) is standardized and published by China BWIPS group in July 2006. Then, the context of GB 15629.11-2003 relating to WAPI is adaptively modified. And the Pre-Shared Key (PSK) is adopted in WAPI-XG1 as an alternative to certificate based Authentication and Key Exchange (AKE) which had been proven to be secure by Tang. (Http://eprint.iacr.org/2007/122.pjf) If a PSK is used, the PSK is the Base Key (BK) used to drive the unicast Key exchange protocol. The related national departments had also stated that the new national standard would be used at 2008 Olympic Games.

We will analyze the Perfect Forward Secrecy (PFS) of AKE protocols used in three versions of WAPI. A protocol is said to have PFS if compromise of long-term keys does not compromise past session keys. For an AKE protocol, PFS is a very important security property (Günther, 1990; Menezes, *et al*., 1996). PFS provides that the compromise of long-term keys does not affect the security of past session keys, which guarantees that previous traffic is locked securely in the past. The results show that all the AKE protocols in three versions of WAPI cannot provide PFS and the PSK-based AKE protocol of WAPI-XG1 is also very weak under an offline dictionary attack. Furthermore, some improvements are presented to overcome these security flaws.

AKE PROTOCOLS IN THREE VERSIONS OF WAPI AND THEIR SECURITY ANALYSIS

The AKE protocol in the original standard WAPI and its security analysis: The key exchange process of WAPI is shown in Fig. 1, where ENC(*) is the

Corresponding Author: Chun-Jie Cao, Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, China

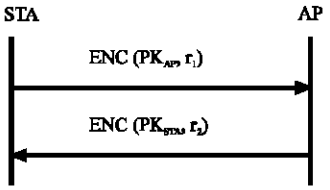

Fig. 1: The AKE protocol in the original standard WAPI

- The adversary selects the target STA and AP that he wants to compromise.
- The adversary captures all the exchanged messages by eavesdropping the communications between AP and STA. Two kinds of messages may be captured by the adversary: The AKE protocol interaction messages and encrypted messages by the session key established in the AKE protocol. Then the adversary can obtain ENC (PK_{AP}, r_1) and ENC (PK_{STA}, r_2) from the first kind of messages and some cipher-texts from the second kind of messages.
- At some stage, the adversary obtains long-term keys of STA and AP, i.e., SK_{AP} and SK_{STA}. (Recall the definition of PFS).
- With the help of SK_{AP} and SK_{STA}, the adversary can easily decrypt ENC (PK_{AP},r_1) and ENC (PK_{STA}, r_2) and extract r_1 and r_2, then the session key $K = r_1 \oplus r_2$ is exposed. Furthermore, all the captured cipher-tests are decrypted.

Fig. 2: The PFS property of the AKE protocol in the original standard WAPI

encryption function, PK_{AP} and PK_{STA} are the public keys of AP and STA, respectively.

STA and AP first negotiate a cryptography algorithm, i.e., ENC(*). Then, they respectively generate random value r_1 and r_2. These random values are encrypted with the peer's public key and sent to each other. Both parties decrypt the encrypted random value and derive the session key $K = r_1 \oplus r_2$.

Security analysis the AKE protocol in the original standard WAPI: The protocol does have a weakness: An adversary can easily computes the session key if he has already obtained the long-term keys of STA and AP. Fig. 2 shows the situation.

The AKE protocol in the WAPI implementation plan and its security analysis: The framework in the implementation plan of WAPI is the same as that of the original standard WAPI, which is composed of certificate authentication and key exchange. Compared with the original standard WAPI, the implementation plan remains unchanged in the certificate authentication, but makes a significant improvement in the key exchange. The new key

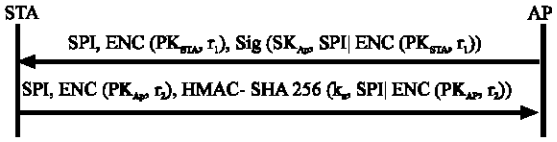

Fig. 3: The AKE protocol in the WAPI implementation plan

exchange protocol is shown in Fig. 3. It is different from the original one in the following aspects:

- In the implementation plan, AP should initiate the key exchange request which contains AP's signature on the encrypted random value and SPI, where the secure parameter index SPI = the MAC address of STA| the BSSID of AP| the time of authentication request and the signature algorithm is ECDSA.
- In the key exchange response, SPI and the STA's message authentication code on encrypted random and SPI are included. The message authentication code is computed through HMAC-SHA256 algorithm.
- The keys derivation method in the implementation plan is different. STA and AP first calculate the master key $k = r_1 \oplus r_2$, then extend k with KD-HMAC-SHA256 algorithm to get the session key k_d, the authentication key k_a and integrity check key.

Because the key exchange method used in the implementation plan is the same as in WAPI, an adversary can mount the same attack and then compute the session key as Fig. 2 illustrated.

The PAKE protocol in WAPI-XG1 and its security analysis: Compared with the original standard and the implementation plan, WAPI-XG1 made a rather big improvement in authentication and key exchange. Especially, a Pre-shared Key Authentication and Key Exchange (PAKE) mode is introduced, which provides an easily implemented alternative for the generation of the BK. The PAKE protocol in WAPI-XG1 is shown in Fig. 4.

- **Unicast key exchange request:** AP generates a random integer N_1 and sends (BKID, ADDID, N_1, $Param_1$) to STA, where BKID is the identifier of the current BK, ADDID is the concatenation of the MAC addresses of AP and STA, $Param_1$ are some other parameters such as flag, USKID and cipher suit.

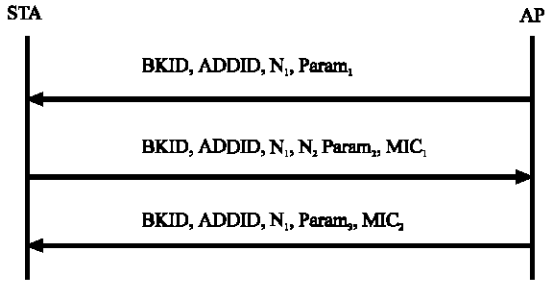

Fig. 4: The PAKE protocol in WAPI-XG1

- **Unicast key exchange response:** Upon receipt the unicast key exchange request, STA generates a random integer N_2 and computes Pair Transient Keys (PTKs) as Eq. 1:

$$UEK|\ UCK|\ MAK|\ KEK = KD\text{-}HMAC\text{-}SHA256\ (PSK, ADDID\ |\ N_1\ |\ N_2) \quad (1)$$

where:

A|B : The concatenation of A and B,
KD-HMAC-SHA256: Key derivation algorithm,
UEK : Unicast encryption key,
UCK : Unicast integration check key,
MAK : Message authentication key
KEK : Key encryption key used in group key announcement.

Besides, $Param_2$ and $Param_3$ are parameters as $Param_1$. Then STA computes MIC_1 as Eq. 2:

$$MIC_1 = HMAC\text{-}SHA256\ (MAK, BKID|ADDID\ |\ N_1\ |\ N_2|\ Param_1|\ Param_2) \quad (2)$$

Finally, STA sends message (BKID, ADDID, N_1, N_2, $Param_2$, MIC_1) to AP as the unicast key exchange response.

- **Unicast key exchange acknowledgment:** Upon receipt the unicast key exchange response message, AP computes PTKs as above and verifies MIC_1 received from STA. If valid, AP computes MIC_2 as Eq. 3:

$$MIC_2 = HMAC\text{-}SHA256\ (MAK, BKID|ADDID\ |\ N_1\ |\ N_2|\ Param_1|\ Param_2|\ Param_3) \quad (3)$$

And then AP sends (BKID, ADDID, N_2, $Param_3$, MIC_1) to STA as the unicast key exchange acknowledgment; Otherwise, AP discards this response message.

- The adversary chooses the target STA and AP that he wants to attack.
- The adversary captures all the exchanged messages by eavesdropping the communications between AP and STA. Two kinds of messages can be captured by the adversary: The PAKE protocol interaction messages and the messages encrypted with the keys established in the PAKE protocol. Then the adversary can learn ADDID, N_1, N_2, MIC_1 and MIC_2 from the first kind of messages and some cipher texts from the second kind of messages.
- At some stage, the adversary knows the PSK between STA and AP (recall the definition of PFS).
- The adversary can easily compute the keys ever used according to the Eq. 1 for the parameters (PSK, ADDID, N_1, N_2) of the key-derivation function are all known to the adversary. Furthermore, the group key that is derived from KEK is also exposed.

Fig. 5: The PFS property of the AKE protocol in WAPI-XG1

- Upon receipt the unicast key exchange acknowledgment message, STA verifies MIC_2 received from AP. If valid, STA trusts in the AP and otherwise STA discards this acknowledgment message.

Security analysis the PAKE protocol in WAPI-XG1: The PAKE protocol also cannot provide PFS: It is subject to a passive attack described in Fig. 5.

As shown earlier, the main drawback of WAPI-XG1's PAKE protocol lies in the lack of PFS property. If PSK is compromised, either all messages previously sent or will be sent can be decrypted and bogus frames may be injected into current traffic.

However, if a passphrase is used as PSK, it is possible for an adversary to perform a dictionary attack using the above-eavesdropped information. This is a big problem because phrases over 20 characters are not really possible when humans are involved. In addition, random strings are difficult to remember and prone to misconfiguration. Therefore phrases are typically found in a dictionary. In current network deployment, a normal practice is to have a single PSK within an Extended Service Set (ESS). To generate any PTK, a device only needs to learn the two MAC addresses (ADDID) and nonces (N_1, N_2). All of this is available by a passive adversary from the message exchange. Any device can passively listen for these frames and then generate PTKs. Thus even though each unicast pairing in the ESS has unique keys there is nothing private about these keys to any other device in the ESS. Once the adversary learns the PSK, the whole ESS is compromised and then the adversary can read and forge any traffic in the ESS.

IMPROVEMENTS TO AKE PROTOCOLS IN THREE VERSIONS OF WAPI

PFS can be provided by generating session keys through Diffie-Hellman (DH) key exchange, wherein the DH exponentials are based on short-term keys. If long-term private keys are compromised, past sessions are also secure. For the implementation plan is the enhanced version of WAPI on security, we do not give the improvement to WAPI. Before the description of new protocols we first review the elliptical-curve computational Diffie-Hellman (ECCDH) assumption which is the security foundation of our protocols.

ECCDH Assumption: Let G_1 is an additive cyclic group of prime order q and P is an arbitrary generator of G_1. given $\{X = xP, Y = yP: x, y \in Z_q\}$, it is infeasible for any Probabilistic Polynomial-Time (PPT) adversary to compute $Z = xyP$.

Improvement to the AKE protocol of the implementation plan: We give two improvements to the AKE Protocol of the implementation plan: One is timestamp-based and the other is nonce-based. Both adopt the DH key exchange based on elliptical-curve.

- The AKE protocol based on timestamp includes following two messages (Fig. 6):

- **Key exchange request:** First, AP randomly selects $y \in Z_q$ and computes yP, then creates a signature Sig (SK_{AP}, yP| SPI) with its long-term private key SK_{AP} and sends key exchange request (SPI, yP, Sig (SK_{AP}, yP| SPI)) to STA, where the SPI is computed as Eq. 4:

$$\text{SPI} = \text{the MAC address of STA| the BSSID of AP | the time of authentication request} \quad (4)$$

- **Key exchange response:** Upon receipt the key exchange request message, STA checks AP's signature. If valid, STA randomly selects $x \in Z_q$, computes xP and Pair Transient Keys (PTKs) as Eq. 5:

$$\text{UEK| UCK| MAK| KEK} = \text{KD-HMAC-SHA256}(xyP, \text{SPI}) \quad (5)$$

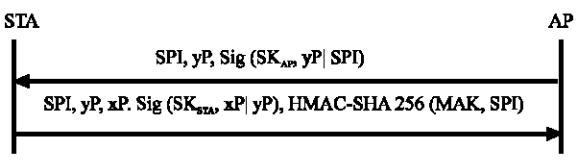

Fig. 6: The AKE protocol based on timestamp

Then STA sends the key exchange response message (SPI, yP, xP, Sig (SK_{STA}, xP| yP), HMAC-SHA256 (MAK, SPI)) to AP, where SK_{STA} is STA's long-term private key, Sig (SK_{STA}, xP|yP) is STA's signature with SK_{STA} and HMAC-SHA256 (MAK, SPI) is the message authentication code under MAK.

- Upon receipt the key exchange response message, AP checks yP and Sig (SK_{STA}, xP|yP). If valid, AP computes Pair Transient Keys (PTKs) as Eq. 5 and verifies the message authentication code HMAC-SHA256 (MAK, SPI). If the verification is passed, the secure channel between AP and STA is established.
- The AKE protocol based on nonce includes following two messages (Fig. 7):

- **Key exchange request:** First, AP randomly selects integer r_1, y and computes yP. Then AP sends key exchange request (SPI, r_1, yP) to STA, where the SPI is computed as Eq. 6:

$$\text{SPI} = \text{The MAC address of STA| the BSSID of AP} \quad (6)$$

- **Key exchange response:** Upon receipt the key exchange request message, STA randomly selects integer r_2, x, computes xP and Pair Transient Keys (PTKs) as Eq. 7:

$$\text{UEK| UCK| MAK| KEK} = \text{KD-HMAC-SHA256}(xyP, \text{SPI}| r_1| r_2) \quad (7)$$

And then sends the key exchange response message (SPI, r_1, r_2, xP, Sig (SK_{STA}, r_1| r_2| xP| yP), HMAC-SHA256 (MAK, SPI)) to AP.

- **Key exchange confirmation:** Upon receipt the key exchange request message, AP checks r_1 and Sig(SK_{STA}, $r_1|r_2|xP|yP$). If valid, AP computes the session key as Eq. 7 and verifies the message authentication code HMAC-SHA256 (MAK, SPI)). If the verification is passed, AP sends the key exchange confirmation message (SPI, r_2, Sig(SK_{AP}, $r_2|r_1|yP|xP$), HMAC-SHA256 (MAK, SPI)) to STA, where SK_{AP} is AP's long-term private key.

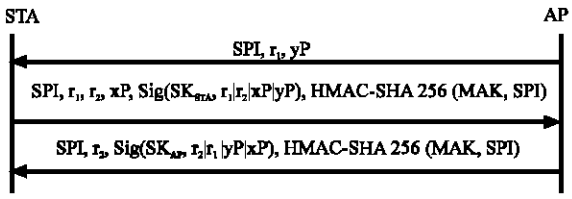

Fig. 7: The AKE protocol based on nonce

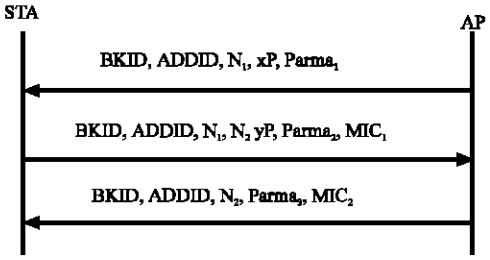

Fig. 8: The DH-based PAKE protocol

- Upon receipt the key exchange confirmation message, STA validates r_2, Sig (SK_{AP}, r_2| r_1| yP| xP) and HMAC-SHA256 (MAK, SPI)). If the validation is passed, the secure channel between AP and STA is established.

Improvement to the PAKE Protocol of WAPI-XG1: In the improvement protocol described in Fig. 8, STA and AP execute the same operations as the PAKE protocol except that:

- AP sends the temporary DH public key xP within a unicast key exchange request message.
- STA sends the temporary DH public key yP within a unicast key response message and session keys are computed as Eq. 8.

$$PTKs = UEK| UCK| MAK| KEK = KD\text{-}HMAC\text{-}SHA256 (PSK, ADDID| N_1| N_2| xyP) \quad (8)$$

The message authentication code is computed as Eq. 9:

$$MIC_1 = HMAC\text{-}SHA256 (MAK, BKID|ADDID | N_1 | N_2| xP| yP| Param_1| Param_2) \quad (9)$$

Finally, STA sends (BKID, ADDID, N_1, N_2, $Param_2$, MIC_1) to AP as the key exchange response message.

- AP computes PTKs as STA and validates the message authentication code MIC_1. If the validation is successful, then AP computes the message authentication code MIC_2 as Eq. 10:

$$MIC_2 = HMAC\text{-}SHA256(MAK, BKID | ADDID| N_1| N_2| xP| yP| Param_1| Param_2| Param_3) \quad (10)$$

Security Analysis of The Improvements: In the improvement protocols, the session keys are computed as follows, respectively.

The AKE protocol : K= KD-HMAC-
based on timestamp : SHA256 (xyP, SPI)

The AKE protocol : $K_{STA}| K_{AP}$ = KD-HMAC-SHA256
based on nonce : (xyP, SPI| r_1| r_2)
The DH-based : PTK = KD-HMAC-SHA256
PAKE Protocol : (PSK, ADDID| N_1| N_2| xyP).

From the equations above, we know that the long-term keys of STA and AP are not involved in the computation of different session keys, so the losses of long-term keys do not affect the security of past session keys. Furthermore, according to the definition of ECCDH assumption, the adversary can not compute xyP even through he has obtained long-term keys, SPI, N_1, N_2, r_1, r_2, xP, yP. Namely, the adversary can not compute the session keys. Hence, all the improvement protocols can provide PFS.

CONCLUSIONS

We analyzed the authentication and key exchange protocols in three versions of WAPI and found that they all could not provide PFS. In WAPI and its implement plan, the adversary can easily decrypt random numbers r_1, r_2 and retrieve the session key $r_1 \oplus r_2$ if he has obtained the long-term private keys of STA and AP. And in the PAKE protocol of WAPI-XG1, the adversary can directly calculate the session key through the equation PTKs = KD-HMAC-SHA256 (PSK, ADDID | N_1 | N_2) if he has obtained ADDID, N_1, N_2 (sent by plaintext) and the shared key between STA and AP. Moreover, the PAKE protocol is weak under an offline dictionary attack when the passphrase is used as PSK. We proposed improvements to AKE protocols of the implement plan and WAPI-XG1, in which perfect forward secrecy was provided by Diffie-Hellman key exchange (the Diffie-Hellman exponentials are based on short-term keys). Even long-term private keys are compromised, past sessions are also secure. Furthermore, the offline dictionary attack to the PAKE protocol is avoided.

ACKNOWLEDGMENT

This work was supported by National Nature Science Foundation of China (No. 60633020, No. 60503012, No. 60573036).

REFERENCES

Anonymous, 2003. 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 National Standard of the PRC GB 15629.11-2003.

Anonymous, 2004a. Supplement to standard for telecommunications and information exchange between systems-LAN/MAN specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Enhanced Security IEEE Standard 802.11i.

Anonymous, 2004b. 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.»and GB 15629.1102-2003.

Anonymous, 2006. 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 National Standard of the PRC GB 15629.11-2003/XG1-2006.

Günther, C.G., 1990. An Identity-Based Key Exchange Protocol. In: Proceedings of EUROCRYPT '89, LNCS 434, 10-13 April, 1989, Houthalen, Belgium. Quisquater, J.J. and J. Vandewalle (Eds.), Springer-Verlag, pp: 29-37.

Li, X.H. and J.F. Ma, 2005. On the security of the key-agreement protocol of Chinese WLAN Standard Implementation Plan. Chinese J. Comp., 4: 576-580.

Menezes, A.J., C.P. Oorschot and A.S. Vanstone, 1996. Handbook of Applied Cryptography. CRC Press, NewYork.

Zhang, F. and J.F. Ma, 2005a. On the security and performance of WAPI. J. Xidian Univ., 2: 210-215.

Zhang, F. and J.F. Ma, 2005b. Security analysis of the Chinese wireless LAN standard implementation plan. J. Xidian Univ., 4: 545-548.