

Comparative Studies on Authentication and Key Exchange Methods for 802.11 Wireless LAN

Jun Lei¹, Xiaoming Fu¹, Dieter Hogrefe¹, Jianrong Tan²

¹Telematics Group, University of Goettingen

¹Lotzestrasse 16-18, D-37083 Goettingen, Germany

²State Key Lab of CAD&CG, Zhejiang University

²310027, Hangzhou, Zhejiang Province, China

Email: ¹{lei, fu, hogrefe}@cs.uni-goettingen.de, ²egi@zju.edu.cn

Corresponding author: Jun Lei, lei@cs.uni-goettingen.de

Abstract: IEEE 802.11 wireless LAN has become one of the hot topics on the design and development of network access technologies. In particular, its authentication and key exchange (AKE) aspects, which form a vital building block for modern security mechanisms, deserve further investigation. In this paper we first identify the general requirements used for WLAN authentication and key exchange (AKE) methods, and then classify them into three levels (mandatory, recommended, and additional operational requirements). We present a review of issues and proposed solutions for AKE in 802.11 WLANs. Three types of existing methods for addressing AKE issues are identified, namely, the legacy, layered and access control-based AKE methods. Then, we compare these methods against the identified requirements. Based on the analysis, a multi-layer AKE framework is proposed, together with a set of design guidelines, which aims at a flexible, extensible and efficient security as well as easy deployment.

Keywords: authentication, key exchange, WLAN, security, confidentiality

1 Introduction

IEEE 802.11, a set of Wireless LAN (WLAN) standards developed by the IEEE LAN/MAN standards committee's working group 11, including the original 802.11 and its extensions such as 802.11b, 802.11a, 802.11g, - sometimes denoted as 802.11x - was designed to offer reliable data transmission under diverse and adverse environmental conditions. Recently it has become one of the most popular wireless access technologies. In contrast to the 3G (third-generation) networks, WLAN can offer higher data transmission rate for users and lower cost despite its coverage limitation.

When a user wants to access an 802.11 wireless network, two key security aspects are involved: (1) authentication of the wireless user/device; (2) data confidentiality between the wireless device and the network, which is usually achieved by the encryption technique based on key exchange mechanisms. In this

paper, we mainly focus on the authentication and key exchange mechanisms, which form an important building block for modern security mechanisms.

In our view, there are three major issues with today's authentication mechanisms for wireless networks. The first issue is the lack of mutual authentication between user and network. For instance, the identity of a user is usually verified when he logs into a network, but the authentication of the network is often omitted. The second issue is caused by the wireless technology itself since the shared communication channel could be monitored by any malicious user. Thereafter, attackers can easily eavesdrop or even actively modify the message header and data. To ameliorate this issue, one method is to apply a challenge/response model via hiding password over the air [1]. However, this method causes a third issue - known as dictionary attacks - where an attacker might figure out the password by simply observing the pair of challenge and response messages.

To address the second issue as mentioned above, cryptographic algorithms are commonly used to protect the information transmitted between user and network. In order to control the operation of such cryptographic algorithms, some keys used for encryption and decryption need to be established between the communicating entities, thus various key exchange mechanisms have been proposed. For example, Public Key Infrastructure (PKI) [2] allows two parties to establish a secure channel for key exchange. The key exchange issue, however, has not been completely solved yet such as in the electronic commerce [3].

Recently, there have been a number of authentication and key exchange approaches proposed for WLANs. Examples include Shared Key Authentication (SKA) [4], EAP-TLS [5], PEAP [6], 802.1X [7], 802.11i [8]. However, these proposals still contain a number of security weaknesses. For

instance, “rouge” access points deployed by end users pose great security risks since Denial of Service (DoS) and Distributed DoS (DDoS) attacks may occur by flooding such access points. Therefore, it is useful to perform a systematic comparison among different approaches and an investigation of the overall design aspects in the long run. Among previous works, Baek et al [4] presented eight desired properties of WLAN authentication and reviewed some of recent WLAN authentication protocols. Interlink networks [9] identified the requirements that an authentication method must meet for wireless networks and discussed several EAP authentication methods. They did cover some of existing and emerging authentication and key exchange approaches and did propose some useful metrics for the comparison. However, most of these reviews were made rather from a high level perspective without providing details into the substantial properties of the authentication and key exchange (AKE) methods, in particular the distinction between their common features and scenario-specific purposes. Moreover, some other approaches have not been considered. The objective of this paper is to investigate and compare current AKE methods against their substantial properties, and accordingly, to pave the way towards developing the authentication and key exchange framework for 802.11 WLANs.

The rest of this paper is organized as follows. In Section 2, we identify the general requirements used for WLAN AKE methods. Section 3 reviews an array of selected existing AKE methods by classifying them into three categories. In particular, we describe their properties according to the proposed requirements. In Section 4, we summarize the advantages and disadvantages introduced by these methods. We conclude that the existing solutions have different deficiencies, and so far there is no single perfect solution that fits all requirements. Based on the analysis, a plausible multi-layered framework that can be extracted from the result is presented, where several critical design guidelines are introduced for AKE method developments. Finally, this paper concludes in Section 6.

2 Authentication and Key exchange (AKE) method requirements for IEEE 802.11 WLANs

Today’s most 802.11 networks authenticate users rely on the Extensible Authentication Protocol (EAP), defined in [10]. EAP supports the exchange of

various authentication credentials such as digital certificates, user names and passwords. Based on [10], we identify the requirements for WLAN authentication and key exchange (AKE) methods, which are classified into three levels: Mandatory Requirements, Recommended/Desired Requirements and Additional Operational Requirements.

AKE methods used in 802.11 WLAN must satisfy the following requirements:

- (1) Mutual authentication [10] — any AKE method for wireless networks must provide mutual authentication. That is, the network must authenticate the user, but the user must be able to authenticate the network as well;
- (2) Credential security [11] — for the confidentiality and integrity protection of user’s data;
- (3) Resistance to dictionary attack [10] — this is to prevent easy sniffing onto 802.11 frames;
- (4) Man-in-the-middle attack protection [10] — 802.11 provides no authentication functionality to the access point, an attacker can easily fool the network via deploying a rogue access point;
- (5) Immune to forgery attacks — an attacker may forge the public key pair so that he could be validly verified
- (6) Anti-replay (packet forgery) protection — an AKE method needs to be able to protect the network from replaying previous packets by malicious users (thus limiting the amount of (D)DoS attacks);
- (7) Strong session key [11] — it is required to have a strong session key which offers the message authentication, the confidentiality, and the integrity protection for the sessions.

Besides, the following requirements are recommended:

- (1) Management message authentication — to authenticate all management messages, preventing denial of service (DoS) attacks;
- (2) Authenticate users — not only authenticating a user device, but also authenticating the user can improve the communication reliability;
- (3) Key integrity Check — to provide a key protection for key exchanges and session-key generation procedure;
- (4) Weak key protection — to address one of the vulnerabilities from WEP, avoiding weak key attacks.

Lastly, there are three Additional Operational Requirements:

- (1) No computational burden — the new requirement for current authentication and key exchange mechanisms because some devices may have

constrained power and limited hardware support (e.g. PDA);

(2) Ease implementation — one important criterion to evaluate the deployment of different methods;

(3) Fast reconnection [10] — the ability to create a new or a refreshed security association more efficiently if a security association has been established in the previous short time.

Actually, most of the mandatory requirements are motivated by Extensible Authentication Protocol (EAP) methods used for WLAN deployments. Other mandatory requirements mentioned in [11] are not included because they only associated with EAP methods, and do not apply to the general case. In addition, forgery key, key integrity and weak key protections are proposed to address the possible vulnerabilities in key exchange mechanisms. Considering the properties of wireless networks and some newly discovered security weaknesses (e.g., DDoS attacks), some recommended requirements are presented. Lastly, three operational considerations are illustrated as the realistic deployment issues of AKE methods are taken into considerations.

3 Authentication and Key Exchange (AKE) methods overview

The reason why WLAN security is difficult to accomplish is that WLANs can be deployed everywhere and generate different connection concepts from wired networks. In this section we group several AKE methods into three categories, namely, legacy AKE methods, layered AKE methods and access control-based AKE methods. The classification accords with the structural concerns, such as layered and access control-based features. Furthermore, we evaluate them according to the requirements proposed in the previous section.

3.1 Legacy AKE methods

The simplest and default authentication method for legacy 802.11 is Open System Authentication (OSA) which uses two steps to authenticate users. First, the client sends an authentication request with its identity to the access point. Second, the access point authenticates the client via validating the identity. The second legacy method is Shared Key Authentication (SKA) which uses a challenge/response mode with shared keys to provide the authentication [9]. The main difference between OSA and SKA is the latter provides mutual authentication.

Based on two presented methods, Wired Equivalent Privacy (WEP) protocol was introduced in 1997 to provide authentication and data encryption between a host and a wireless access point. It uses pre-shared key (PSK) that are manually exchanged at the both endpoints. However, WEP was found rather weak for the purpose of authentication and is no longer recommended for future use. Several papers have identified the weaknesses existed in WEP security issues [12, 13, 14]. These deficiencies can be summarized as follows.

1. WEP has no protection to forgery attacks
2. WEP provides no replay protection
3. WEP misusing RC4 algorithm for the encryption so that the protocol is extremely weak to key attacks
4. WEP has the security hole that attacker without the encryption key but reusing IV can decrypt the encrypted code.

In summary, legacy AKE methods for 802.11 networks have demonstrated many flaws of security protocol design, hence many of them are vanishing from today's deployment.

3.2 Layered AKE methods

It has been found that the security mechanisms offered in a single layer (mostly network layer) would not be sufficient in many deployment scenarios. Thus, some deployments of IEEE 802.11 WLANs use layered AKE methods to provide security, including EAP-TLS, EAP-TTLS [15], PEAP, EAP-SPEKE [16], EAP-FAST [17] and EAP-PSK [18]. EAP was standardized in 1998 [19], serving as a framework offering a basis for carrying other authentication methods. Its main advantage is the independence from any particular authentication algorithm and hence it can be highly extended.

Due to the space limitation, however, in this paper we only choose universal EAP-based methods to address the AKE issue. Some proprietary protocols (e.g. Lightweight EAP (LEAP) [20] developed by Cisco, which is created only to support the Cisco System Aironet products) will not be discussed here.

3.2.1 TLS embedded protocol

EAP-TLS, EAP-TTLS, PEAP and EAP-FAST all incorporate with TLS [21] to enable the secure communication between a client and a server, as well as to address inherent deficiencies (e.g. no protection of the user identity; no support for fast reconnections) when EAP is deployed into the WLAN alone. Figure 1 presents the layered model of TLS-embedded

protocols. They add a TLS layer on top of the EAP and the corresponding TLS session is established to protect the legacy EAP method.

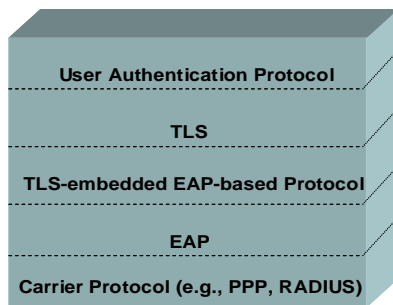


Figure 1 TLS-embedded Protocol Layered Model

In addition, EAP-TTLS and PEAP address the weaknesses of insecure authentication channel during the authentication phase, which is established by the TLS Handshake protocol allowing the server to authenticate the client [22]. Figure 2 shows the network architecture model for EAP-TTLS usage and the types of security it provides. The client and AAA server exchange a sequence of EAP messages which are encrypted and authenticated using TLS session keys. Therefore, EAP-TTLS is no longer venerable to dictionary attacks or the relay attack because the attackers have to break the secured EAP-TLS tunnel to mount these attacks on the client authentication if they want to sniff the tunneled session.

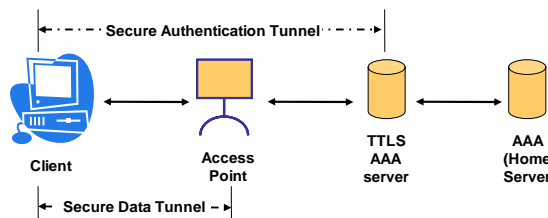


Figure 2 EAP-TTLS Architectural Model

It is noted that EAP-TLS has been widely deployed and can provide a well-formed and reliable mechanism to perform mutual authentication between EAP peer and EAP server. Besides, EAP-TTLS and PEAP augment the security of legacy EAP methods in terms of credential security, anti-relay protection. However, all tunneled authentication protocols are potentially venerable to the Man-in-the-Middle attack, which is discovered by Asokan et al [23]. The paper identified that the attack can be launched either when the client is authenticated based on the same identity and the same authentication token in different environments, or when the client fails to properly authenticate the server while building the tunnel. Therefore, they proposed a cryptographic binding between the client authentication protocol and the

protection protocol, which allows the flexible and secure usage of the authentication protocol in multiple authentication environments.

3.2.2 Layered method with cryptographic design

Incorporating with cryptographic algorithms strengthens the mutual authentication and provides more protections for WLANs. Different from PEAP or EAP-TTLS, EAP-FAST employs a symmetric cryptography and accordingly provides an enhancement to mutually authenticate the client and the server during the secure channel establishment phase. EAP-PSK is another AKE layered method with cryptographic design, which alleviates computational burden via not using asymmetric cryptography, but using a single cryptographic algorithm AES-128. The basic cryptographic design of EAP-PSK is formulated as Figure 3. Because of its particular key design, EAP-PSK has attracted several attentions, mainly in the scope of IEEE 802.1e (WiMAX). The WiMAX forum has suggested EAP-PSK to perform device authentication between the user's device and the base station of the access network [24].

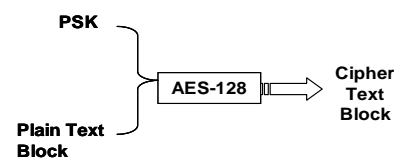


Figure 3 Cryptographic design of EAP-PSK

Besides, EAP-SPEKE is a simple password authentication method without performing public key or certificate mechanisms. It utilizes a series random-shape messages which are exchanged between devices. Upon the message exchange SPEKE modules compute these received messages to determine whether the password used at the other device is correct. Because of this, EAP-SPEKE can further address the issue of Man-in-the-Middle and off-line dictionary attacks.

In summary, the significant difference between the legacy methods and the layered AKE methods is that the layered methods separate the authentication process from the message protection. This separation is achieved by EAP which acts as the basis for higher layer authentication protocols (such as TLS, TTLS, FAST, and SPEKE). Although layered design appears as a highly efficient, easily deployable authentication framework over 802.11 WLANs, it also contains certain vulnerabilities, e.g. no identity protection; no protected ciphersuite negotiation; no

fast reconnection capability. To further address these weaknesses, some researchers have proposed access control-based layered AKE methods which are described as below.

3.3 Access control-based layered AKE method

The advent of 802.1X [25] provides a port-based network access control as a part of the IEEE 802 group of protocols. Only when the authentication server authorizes the supplicant, the 802.1X port will be kept connected and the supplicant will be granted access to the network.

3.2.1 Transitional solution

WPA [4] is the transitional security solution for 802.11 wireless networks until 802.11i can be widely supported by the common hardware, and is developed in conjunction with the IEEE. It takes basis on 802.1X and EAP for authentication and Temporal Key Integrity Protocol (TKIP) for traffic encryption. TKIP addresses all WEP's well-known vulnerabilities but doesn't guarantee them completely. Counter Code CBC/MAC (CCMP) is then recommended to replace TKIP. However, TKIP is still in use because most legacy hardware offers no capability of supporting the Advanced Encryption Standard (AES) algorithm, the basis of CCMP.

Specifically, WPA utilizes a key mixing function to avoid the weak key attack. If we set

$$\begin{aligned} \text{Temporal Key} &= T; \\ \text{Intermediate Key} &= I; \\ \text{Per-packet Key} &= K; \end{aligned}$$

802 MAC address of the local wireless interface= A .

Step 1: $T \oplus A = I$. This way, combing with MAC address causes different results of I even though it generates from the same temporal key T ;

Step 2: $b \oplus I = K$, where b is a tiny cipher to encrypt the packet sequence number;

Step 3: streamkey = RC4 (IV , K), to overcome the one of the vulnerabilities in RC4 cryptography and protecting from the weak key attack.

Since 2004, the second generation of WPA (WPA2) has been standardized to provide a scalable and long-term wireless security system. WPA2 uses the Advanced Encryption Standard (AES) for data encryption. However, new hardware is necessary for running in the WPA2 mode [26].

3.2.2 Long-term scheme

The 802.11 architecture consists of three parts: 802.1X for authentication; Robust Security Network (RSN) for keeping the track of associations; and Advanced Encryption Standard-based Counter Mode CBC-MAC Protocol (AES-CCMP) to provide integrity, replay protection and confidentiality [27]. The important element of 802.11i authentication process consists of 4-way handshake as depicted in Figure 4. Upon a successful handshake, a secure communication channel will be established to protect the subsequent data transmission.

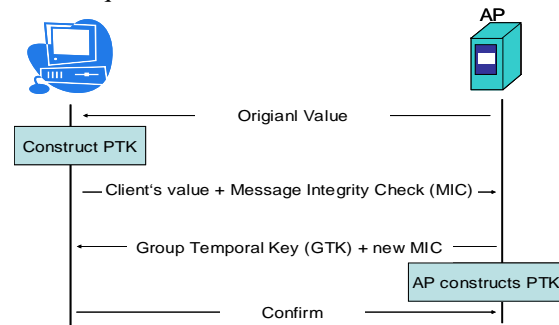


Figure 4 Four-way Handshake in 802.11i

802.11i offers crucial security enhancements to 802.11, including a complete protection of the Layer 2 packet, i.e. both header and payload and also prepares the framework with strong, mutual authentication between the Client and the Access Point (security server). Besides, 802.11i can provide a complicated authentication based on 802.1X and the AES-CCMP encryption protocol which is seen as the long-term solution for data transfer over WLANs. On the one side, CCMP provides confidentiality and privacy by encoding the plaintext before encrypting it. On the other side, AES has been proven to be an extremely solid encryption algorithm [27]. Unfortunately, 802.11i still contains unavoidably weaknesses and is complicated to implement in a certain extent [28].

4 Comparison results

Table 1 gives a comparison of aforementioned methods against the proposed requirements in the three levels as discussed in Section 2. Firstly, WEP can satisfy few of them; whereas most EAP layered methods can satisfy all mandatory requirements. Secondly, TLS embedded protocols (e.g. EAP-TLS, PEAP etc.) can be immune to forgery attacks and protect themselves from the anti-relay attack because TLS provides a secured tunnel for the communication between the wireless client and the server. Once incorporated with cryptographic techniques, some

Table 1: Comparison of AKE methods against requirements

	WEP	EAP-TLS	EAP-PEAP, TTLS	EAP-FAST	EAP-SPEKE	EAP-PSK	WPA	802.11i (WPA2)
Mandatory Requirements								
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓	✓
Credential security		Strong	Strong	Strong	Strong	Strong	Weak	Strong
Dictionary-attack protection		✓	✓	Passive type	Off-line type	✓	Vulnerable to external	✓
Man-in-the-middle attack protection		✓		✓	✓	✓	Passive type	✓
Immune to forgery attacks		✓	✓	✓	✓		Forge message via TK	Possible by inside attack
Anti-replay		✓	✓	✓	✓	✓	✓	✓
Strong session key		✓	✓	✓	✓	✓	✓	✓
Recommended Requirements								
Management messages authentication							✓	✓
Authenticate users	✓	Not, if certificate is store on disk	Not, if certificate is store on disk	✓	✓	✓	✓	✓
Integrity check		✓	✓	✓	✓	✓	✓	✓
Weak keys protection		✓	✓	✓	✓	✓	✓	✓
Additional Requirements								
No computational burden	✓	At the edge devices for asymmetric cryptography	At the edge devices for asymmetric cryptography	✓	✓	✓	For 802.1X support	For 802.1X and new hardware support
Ease implementation	✓	if certificate is store on disk	if certificate is store on disk	✓	✓	✓		
Fast reconnection	Dynamic keying	✓	✓	✓			✓	✓

layered AKE methods (e.g., EAP-FAST) have some indications of vulnerabilities, such as the dictionary attack, which is understandable because password-based methods are suffering from the weaknesses of numeric decryptions. Moreover, access control-based AKE methods (e.g., WPA, 802.11i) rely on a layered model which takes EAP as the basis for authentication, and some complicated cryptographic mechanisms for encryption. As a result, they have elementary capability of defending common attacks despite their complicated and costly implementation. We can further conclude that mutual authentication is not equal to simply authenticate a user and a server since the concept of “a user” includes “a client” and “a device” (e.g. telephone, PDA). For example, EAP-TTLS and PEAP show a strong capability of mutual authentication. Nevertheless, they cannot completely satisfy the requirement of authenticating users. Only after authenticating both the client and the access device, the authentication for a user is successful. Based on the table of comparison, we conclude that there is no existing solution immune to any attack

and it is hard to identify which is the most appropriate method for any 802.11 WLAN.

5 Towards a multi-layer AKE framework and its architectural considerations

Upon the above analysis, we propose a multi-layered AKE framework for 802.11 WLANs. As shown in Figure 5, it comprises three components: 802.1X for access control, the combination of EAP and TLS for mutual authentication and key distribution, and other high-layer protocols based on TLS/EAP for other new functionalities, such as PSK [19].

We argue this multi-layer framework is advantageous over existing systems. First, it allows an EAP peer to take advantage of the protected ciphersuite negotiation, mutual authentication and key management capabilities of the TLS protocol [5]. Note that EAP-TLS has been one of only available EAP methods for a long time. EAP-TLS-PSK [29] is currently being standardized, which takes advantages from both the EAP-TLS and TLS-PSK. Second, 802.1X is a framework for the user authentication

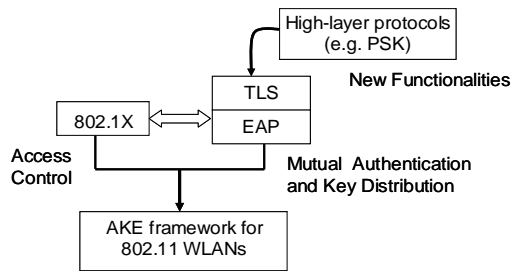


Figure 5 A multi-layered AKE framework for 802.11 WLANs

and key distribution. It utilizes many authentication methods, including passwords, certificates and smart cards to control the network access. Therefore, the multi-layered AKE framework is flexible and extensible due to its intrinsic support from EAP and 802.1X. As having considered today's AKE requirements, the proposed framework intends to be applicable for future deployment scenarios. Fourth, new functionalities could be easily incorporated into the framework, and hence the framework can be augmented to address threats caused new security concerns or development challenges of wireless technologies. It is also noted tradeoffs within this framework can be made between the security assurance level, high efficiency and the required implementation and development costs.

This framework implies a set of key design guidelines to improve the efficiency of AKE methods, and also to meet the security requirements identified in Section 2. They are identified as follows.

- ♦ To select a proper method for a certain security purpose is a good choice. Generally, we should conduct a risk analysis to determine the level of protection a certain WLAN requires and then find the most cost-effective protection against attacks. For instance, the EAP-SPEKE method especially fits for SOHO users and public hot spots where client distribution can be controlled and managed. The advantages of easy implementation and low cost as well as flexible infrastructure are the main reasons why EAP-SPEKE is chosen.
- ♦ AKE methods should consider preventing from some types of (D)DoS attacks. First, wireless networks are extremely vulnerable to (D)DoS attacks since its data transmission happens in the open air. Second, (D)DoS attacks may result in other attacks. However, today's methods involve little in (D)DoS attacks protection. Wan

et al. [30] propose a new Public Key Cryptosystem (PKC)-based protocol to provide the DoS resistance as well as the identity anonymity for the users.

- ♦ Decision on how to find the tradeoff between easy implementation and strong security is another consideration for AKE methods. Users prefer an easy and efficient AKE implementation, while service providers pay more attention to the stability and reliability. One example is that the widespread deployment of 802.11i has been cumbered until now because the use of AES requires new firmware and driver supports which are both expensive and time consuming.
- ♦ A combination of existing mechanisms or with some new technique together to overcome existing problems may be a feasible solution, since deploying a new security protocol is expensive and time-consumable. For instance, Mobile IPv6 [31] combines AAA architecture. IPsec operates at the IP layer, which can support the system authentication and authorization. But if using IPsec alone to protect the wireless LAN, the structure will fall under a weak environment. Just using AAA for a wireless environment, the part of wireless may also cause a loophole [32]. In this case, the use of Secure Sockets Layer (SSL) may overcome the problem. Currently, a Diameter AAA architecture for Mobile IP users has been implemented at the University of Stuttgart [33].

With the continuous development of wireless technologies, new attacks and security concerns will increase. As a result, the extensibility property for future developments should be taken into account when designing new AKE solutions. It is therefore necessary to devise an efficient and strong AKE framework, The development of this framework may follow the above-mentioned design guidelines, which we believe will result in a compromised solution being both practical and secure in the near future.

6 Conclusion

In this paper we have identified the AKE requirements for 802.11 WLAN. We reviewed eleven

desired 802.11 WLAN authentication and key exchange methods, and compared most of them: WEP, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-FAST, EAP-SPEKE, EAP-PSK, WPA and 802.11i (WPA2) against the identified requirements. It seems that among them EAP-based layered AKE methods are more promising since they can provide the strong security by EAP-TLS as well as some complementary features, e.g. high efficiency and easy deployment. In particular, WPA2 and 802.11i provide the fundamental capability of defending common attacks despite their complicated and costly implementation. Based on the analysis, we proposed a multi-layered AKE framework, and as well as a set of design guidelines.

The framework proposed in this paper has a reasonable set of features; fairly strong security,

flexibility and extensibility. In the following steps, we will continue to work on evaluation of such a design, and detailed analysis of each component in terms of its supposed functionalities. However, there are many other areas for interesting future work, for instance, the investigation on new functionalities provided by other high-layer protocols, and possible extensions to the proposed framework for the purpose of efficiency. Moreover, it is not sure whether these mentioned AKE methods can support sufficiently fast handovers among access points since their fast connection feature is not specifically discussed in this paper. It will be, therefore, interesting and useful to characterize how to handle fast-roaming users by these AKE methods.

Reference

- [1] M. Falk, "Fast and secure roaming in WLAN", Department of Computer and Information Science, final thesis, Dec. 2004.
- [2] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X. 509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, April 2002.
- [3] S. Garfinkel, G. Spafford, "Web Security, Privacy and Commerce. Security for Users, Administrators and ISPs", O'Reilly Media, Jan. 2002.
- [4] K.-H. Baek, S. W. Smith, D. Kotz, "A survey of WPA and 802.11i RSN Authentication Protocols", TR2004-524, Dartmouth College, Department of Computer Science, Nov. 2004.
- [5] B. Aboba, D. Simon. "PPP EAP TLS Authentication Protocol." RFC 2716. Oct. 1999.
- [6] H. Anderson, S. Josefsson. "Protected EAP Protocol (PEAP)." draft-josefsson-pppext-eap-tls-eap-07.txt, Internet draft (work in progress), Nov. 2003.
- [7] IEEE Std 802.1X, "Port-based Network Access Control", 2001.
- [8] C.H. He, J.C. Mitchell. "Analysis of the 802.11i 4-way Handshake." Proc. of the 2004 ACM workshop on Wireless security. Pages 43-50. 2004.
- [9] Interlink Network, "EAP Methods for Wireless Authentication", April 2003.
- [10] B. Aboba, L. Blunk, J. Vollbrecht, et al. "Extensible Authentication Protocol (EAP)." RFC 3748. June 2004.
- [11] D. Stanley, J. Walker, B. Aboba. "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs." RFC 4017. Mar. 2005.
- [12] J. R. Walker. "Unsafe at any key size: an analysis of the WEP encapsulation." IEEE P802.11 Wireless LANs. Oct. 2000.
- [13] S. R. Fluhrer, I. Mantin, A. Shamir. "Weaknesses in the key scheduling algorithm of RC4." 8th Annual Workshop on Selected Areas in Cryptography. Aug. 2001.
- [14] A. Stubblefield, J. Ioannidis, A.D. Rubin. "Using the Fluhrer, Mantin, and Shamir attack to break WEP." TR TD-4ZCPZZ, AT&T Labs Research. Aug. 2001.
- [15] P. Funk, S. Blake-Wilson. EAP tunneled TLS authentication protocol (EAP-TTLS). draft-ietf-pppext-eap-ttls-05.txt. Jul. 2004.
- [16] Jablon, "Strong Password-only Authenticated Key Exchange." draft-jablon-speke-00.txt. Mar. 1997.
- [17] N. Cam-Winget, D. McGrew, J. Salowey, et al. EAP Flexible Authentication via Secure Tunneling (EAP-FAST). internet draft. Apr. 2005.
- [18] F. Bersani, H. Tschofenig. "The EAP-PSK Protocol: a Pres-Shared Key EAP Method." draft-bersani-eap-psk-07.txt. Feb. 2005.
- [19] L. Blunk, J. Vollbrecht. "PPP Extensible Authentication Protocol (EAP)." RFC 2284. Mar. 1998.
- [20] M. Banan, "The Lightweight & Efficient Application Protocols (LEAP) Manifesto." Mobile & Wireless Applications Industry. V- 0.7, Dec. 2000.
- [21] T. Dierks, C. Allen. "The TLS Protocol Version 1.0." RFC 2246. Jan. 1999.
- [22] C. Rigney, S. Willens, A. Rubens. "Remote Authentication Dial In User Service (RADIUS)." RFC 2865. June 2000.
- [23] N. Asokan, V. Niemi and K. Nyberg, "Man-in-the-middle in tunneled authentication protocols", in the 11th Security Protocols Workshop, Cambridge(UK), April 2003, Springer-Verlag, 2003.

- [24] WiMAX Forum. "WiMAX End-to-end Network Systems Architecture – Stage 2: Architecture Tenets, Reference Model and Reference Points", Dec. 2005.
- [25] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2004, December 2004.
- [26] Wi-Fi Alliance. "Deploying Wi-Fi Protected Access (WPA2TM) and WPA2TM in the Enterprise." Mar. 2005.
- [27] A. R. Prasad, P. Schoo. "IP Security for Beyond 3G towards 4G." Proc. of WWRF 7, Eindhoven, Netherlands, December 2002.
- [28] C. H. He, J. C. Mitchell. "Security Analysis and Improvements for IEEE 802.11i." Whitepaper. 2005.
- [29] T. Otto, H. Tschofenig, "The EAP-TLS-PSK Authentication Protocol", draft-otto-emu-eap-tls-psk-00, internet draft, April 2006.
- [30] Z. Wan, R.H. Deng, E. Bao and A. L. Ananda, "DoS-Resistant Access Control Protocol with Identity Confidentiality for Wireless Networks", WCNC' 05, 13-17 March 2005, New Orleans, LA, USA.
- [31] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6", RFC 3775, IETF, June 2004.
- [32] P. Engelstad, T. Haslestad, F. Paint. "Authenticated Access for IPv6 Supported Mobility." Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03). 2003.
- [33] Wenhui Zhang. "Interworking Security in Heterogeneous Wireless IP Networks". Proceedings of 3rd International Conference on Networking (ICN'04), Guadeloupe, 2004.