석 사 학 위 논 문

Master's Thesis

3GPP-WLAN 상호연동을 위한 인증 및 키 합의에 관한 연구

A Study on Authentication and Key Agreement for 3GPP-WLAN Interworking

문 혜 란 (文 惠 蘭 Mun, Hye-Ran)

정보통신공학과

Department of Information and Communication Engineering

한 국 과 학 기 술 원

Korea Advanced Institute of Science and Technology

2009

3GPP-WLAN 상호연동을 위한 인증 및 키 합의에 관한 연구

A Study on Authentication and Key Agreement for 3GPP-WLAN Interworking

A Study on Authentication and Key Agreement for 3GPP-WLAN Interworking

Advisor : Professor Kwangjo Kim

by

Mun, Hye-Ran
Department of Information and Communication Engineering
Korea Advanced Institute of Science and Technology

A thesis submitted to the faculty of the Korea Advanced Institute of Science and Technology in partial fulfillment of the requirements for the degree of Master of Engineering in the Department of Information and Communication Engineering

Daejeon, Korea
2009. 5. 15.
Approved by

Professor Kwangjo Kim
Advisor

3GPP-WLAN 상호연동을 위한 인증 및 키 합의에 관한 연구

문 혜 란

위 논문은 한국과학기술원 석사학위논문으로 학위논문심사 위원회에서 심사 통과하였음.

2009년 월 일

심사위원장 김 광 조 (인)

심사위원 이 영 희 (인)

심사위원 염 용 진 (인)

MICE 20074346 문 혜 란. Mun, Hye-Ran. A Study on Authentication and Key Agreement for 3GPP-WLAN Interworking. 3GPP-WLAN 상호연동을 위한 인증 및 키 합의에 관한 연구. Department of Information and Communication Engineering . 2009. 39p. Advisor Prof. Kwangjo Kim. Text in English.

Abstract

The 3rd Generation Partnership Project (3GPP) standard is developing System Architecture Evolution (SAE)/Long Term Evolution (LTE) architecture for the next generation mobile communication system. The SAE/LTE architecture provides secure service and accesses non-3GPP such as WLAN.

3GPP provides efficient charging management, nearly universal roaming, completed subscriber management, mobility, and wide service area. WLAN provides high bandwidth and data rate, compatibility of the Internet. However, WLAN provides narrower service area, lower mobility and roaming than 3GPP. If 3GPP can access non-3GPP such as WLAN, subscribers can have both 3GPP and WLAN advantages. In 3GPP-WLAN interworking, both networks require authentication for secure communication.

To provide secure access of non-3GPP such as WLAN in the SAE/LTE architecture, Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) is used. However, EAP-AKA has several vulnerabilities such as disclosure of user identity, man-in-the-middle attack, Sequence Number (SQN) synchronization, and additional bandwidth consumption.

This thesis analyzes threats and attacks in 3GPP-WLAN interworking and proposes a new authentication and key agreement protocol based on EAP-AKA. The proposed protocol combines Elliptic Curve Diffie-Hellman (ECDH) with symmetric key cryptosystem to overcome these vulnerabilities. Moreover, our protocol provides Perfect Forward Secrecy (PFS) to guarantee stronger security, mutual authentication, and resistance to replay attack. Compared with previous protocols which use public key cryptosystem with certificates, our protocol can reduce computational overhead. Therefore, our protocol can provide secure and efficient 3GPP-WLAN interworking.

Contents

List of Tables

List of Figures

1. Introduction

1.1 Overview

The next generation mobile communication system is being developed for secure and fast communication. The SAE/LTE architecture [17, 18] that is being developed by 3GPP provides more secure communication than Universal Mobile Telecommunication System (UMTS) which is described in [16]. Fig. 1.1 shows the overall of the SAE/LTE architecture [15]. Refer to Fig. 1.1 the SAE/LTE architecture can access non-3GPP such as WLAN and UMTS architecture. Therefore, several authentication and key agreement protocols were proposed for secure communication among each type [17, 18].

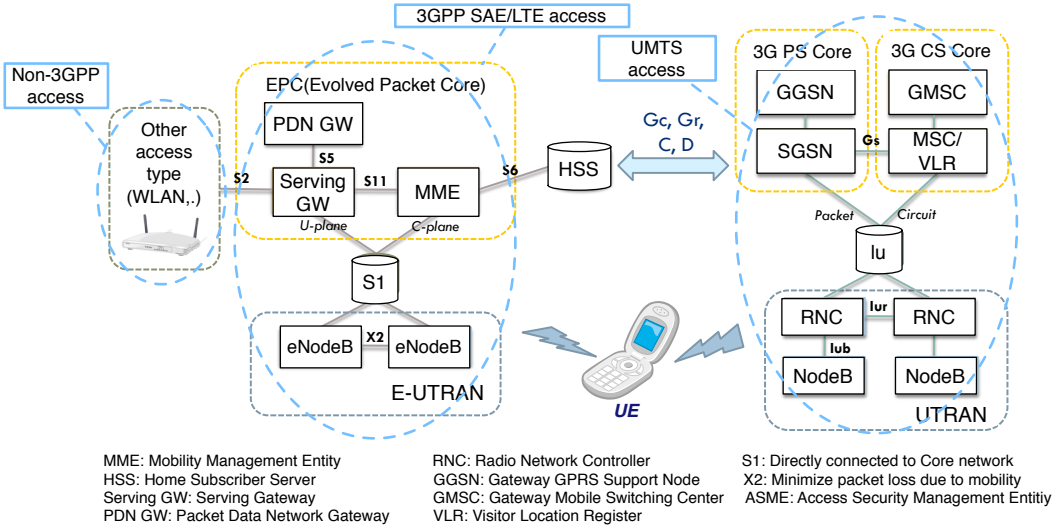


Figure 1.1: Overall of SAE/LTE architecture

To provide mutual authentication between User Equipment (UE) and Mobility Management Entity (MME) through E-UTRAN, the SAE/LTE architecture reuses UMTS-AKA which is described in [16]. This authentication and key agreement protocol is called Evolved Packet System-Authentication and Key Agreement (EPS-AKA) which generates intermediate key K_{ASME}. Refer to Fig. 1.2 the K_{ASME} can generate 5 keys for protect-

ing traffic between the UE and the MME, between the UE and the eNodeB, and between the UE and the Serving GW [17].

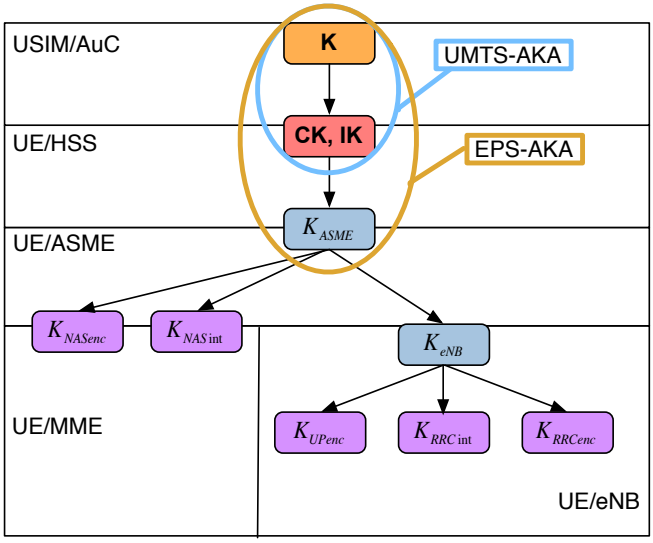


Figure 1.2: Key hierarchy in E-UTRAN

Moreover, the SAE/LTE architecture provides 3GPP-WLAN interworking. 3GPP provides efficient charging management, nearly universal roaming, completed subscriber management, mobility, and wide service area. WLAN provides high bandwidth and data rate, compatibility of the Internet. However, WLAN provides narrower service area, lower mobility and roaming than 3G networks. Therefore, many researchers have been studying 3GPP-WLAN interworking because 3GPP-WLAN interworking has both 3G and WLAN advantages. In 3GPP-WLAN interworking, both networks require authentication for secure communication.

1.2 Our contribution

The SAE/LTE architecture reuses EAP-AKA [9, 20] to provide secure 3GPP-WLAN interworking. When a subscriber attempts to access WLAN, he sends International Mobile Subscriber Identity (IMSI) through Network Access Identifier (NAI) to the Access Point (AP). Fig 1.3 shows an example of NAI coding. This identifier, which follows the IETF generic 'username@realm' format, is built using IMSI, and the MCC and MNC parts of it. '0' indicates the NAI corresponding to EAP-AKA and '1' indicates SIM-AKA, which is another authentication process allowing WLAN access to 2G/GSM SIM-based credentials. The MNC/MCC information is actually used by the WLAN to determine the relevant 3GPP Authentication, Authorization, Accounting (AAA) server which corresponds to the user [1]. EAP-AKA is based on UMTS-AKA. For this reason, EAP-AKA can have not only vulnerabilities of UMTS-AKA but also vulnerabilities in 3GPP-WLAN interworking.

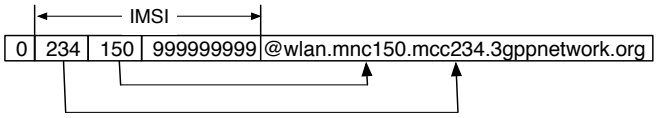


Figure 1.3: An example of NAI coding

This thesis shows overview of architecture for accesses to 3GPP and analyzes threats and attacks in 3GPP-WLAN interworking. Moreover, we explain several authentication protocols based on EAP and propose a new authentication and key agreement protocol based on EAP-AKA. Our protocol overcomes several vulnerabilities of EAP-AKA such as violated user's privacy owing to disclosure of IMSI, man-in-the middle attack, SQN synchronization, and additional bandwidth consumption. Furthermore, our protocol provides Perfect Forward Secrecy (PFS) to guarantee stronger security, mutual authentication between the UE and the AAA server and between the UE and the Home Subscriber Server (HSS), and resistance to replay attack. Compared with previous protocols which use public key cryptosystems with certificates, our protocol can reduce computational overhead.

1.3 Organization

We briefly explain organization of this thesis as follows:

- **Chapter 2** presents architecture for accesses to non-3GPP. This chapter consists of two section: Security architecture for accesses to non-3GPP and architecture of

interworking between 3GPP and non-3GPP.

- **Chapter 3** analyzes threats and attacks in 3GPP-WLAN interworking.
- **Chapter 4** explains related work. In this chapter, we explain several authentication protocols based on EAP. EAP-AKA, EAP-SIM, and EAP-UTLS are used for 3GPP-WLAN interworking. EAP-TLS, EAP-TTLS, and EAP-PEAP are used for WLAN authentication.
- **Chapter 5** proposes a new authentication and key agreement protocol based on EAP-AKA. Our protocol overcomes several vulnerabilities of EAP-AKA and provides additional security properties such as PFS.
- **Chapter 6** presents analysis of our protocol and comparison with previous protocols.
- **Chapter 7** offers our conclusion.

2. Overview of Architecture for accesses to Non-3GPP

In this chapter, we briefly explain architecture for accesses to non-3GPP.

2.1 Security Architecture for accesses to Non-3GPP

In this section, we briefly explain security architecture for accesses to non-3GPP in SAE/LTE. The outline indicates the needed security features to access non-3GPP. Fig. 2.1 shows security architecture for accesses to non-3GPP [19].

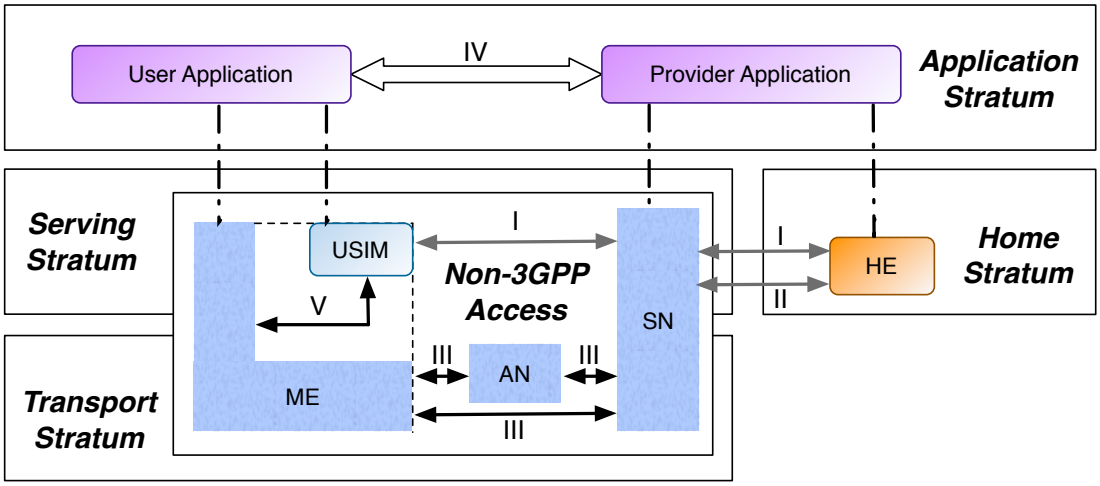


Figure 2.1: Security architecture for accesses to non-3GPP

The needed security fratures are as follows:

- **Network access security(I):** This security features provide users with secure access to services. Radio access protection is a non-3GPP access specific and outside the scope.
- **Network domain security(II):** This security features can enable nodes to securely exchange signaling data and protection against attacks on the wireline network.

- **Non-3GPP domain security(III):** This security features are a non-3GPP access specific and outside the scope.
- **Application domain security(IV):** This security features can enable applications in user and in provider domain to securely exchange messages.
- **User domain security(V):** This security features can securely access the mobile station.

2.2 Architecture of Interworking between 3GPP and Non-3GPP

Fig. 2.2 shows how the SAE/LTE architecture accesses non-3GPP. Refer to Fig. 2.2 non-3GPP consists of trusted non-3GPP such as WiMax and untrusted non-3GPP such as WLAN.

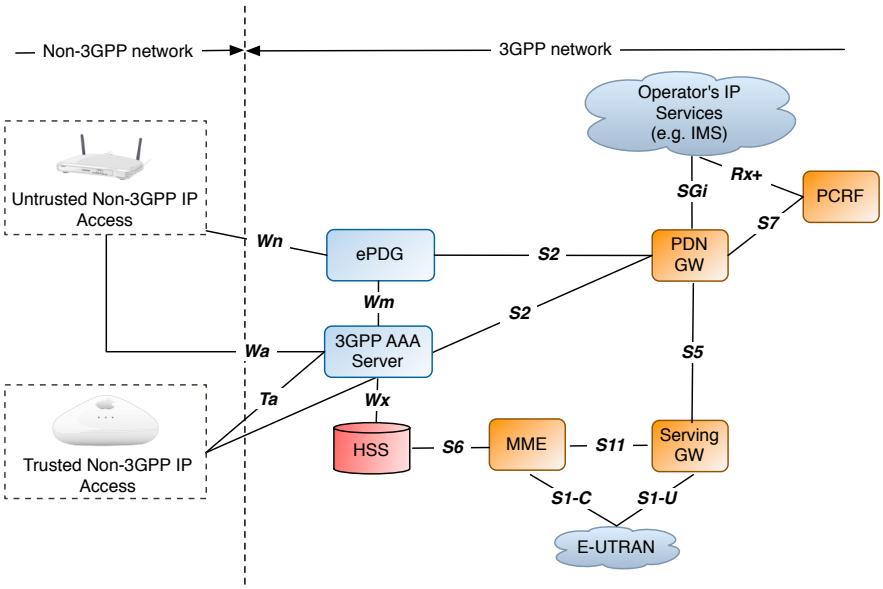


Figure 2.2: Architecture of interworking between 3GPP and non-3GPP

The AAA server performs mutual authentication between 3GPP and non-3GPP as well as accesses HSS through *Wx* interface to get subscriber's information such as IMSI and Authentication Vector (AV). Therefore, the AAA server performs important roles in in-

terworking between 3GPP and non-3GPP interworking. *Ta* interface which was connected with trusted non-3GPP transmits authentication, authorization, and accounting information to the AAA server. Trusted non-3GPP transmits subscriber's information to PDN GW through *S2* interface.

In order to access untrusted non-3GPP, evolved Packet Data Gateway (ePDU) is added in 3GPP network. All traffics which are generated by untrusted non-3GPP are concentrated on the ePDU. Therefore, the ePDU establishes secure tunnel using IPsec and then securely sends subscriber information. Moreover, *Wm* interface transmits subscriber-related information from AAA server to ePDU [15, 19].

3. Threats and Attacks in 3GPP-WLAN Interworking

3.1 Threats

To find threats in 3GPP-WLAN interworking, identification of trust relationship among participants is important. Fig. 3.1 shows a simplified trust relationship among three important participants in 3GPP-WLAN interworking. Details of the trust relationship among the participants are described in [20]. The threats related with each participant are as follows [20]:

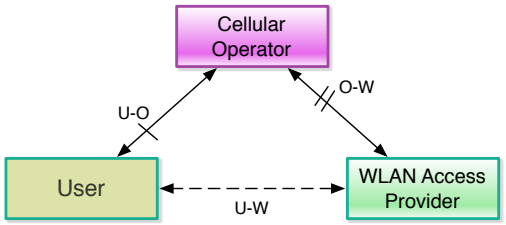


Figure 3.1: Trust relationship

3.1.1 Cellular Operator

The threats related with cellular operator are as follows [20]:

- An attacker bypasses the access control and authorization mechanisms to get the WLAN service for free.
- An attacker impersonates a legitimate WLAN user. Therefore, the attacker accesses WLAN service for free and then the legitimate user gets charge for the attacker's usage of the service.
- An attacker interferes with the charging mechanism for the WLAN service. As a result, legitimate user's bill is incorrect.

- An attacker may be a legitimate user and then interfere with the charging mechanism to reduce his own bill. In another case, the attacker may be a prepaid user. Therefore, the attacker interferes with the charging mechanism to avoid disconnection despite the expiration of his prepaid account.
- An attacker prevents the use of WLAN service through Denial of Service (DoS) attack. Therefore, users cannot use WLAN service.

3.1.2 User

The threats related with user are as follows:

- When a user accesses WLAN service, an attacker gets information which is either sent or received by the user. This information contains the user's information such as personals and credentials. As a result, the attacker can identify the user and modify the user's information.
- In order to derive a user's personal information, an attacker analyzes the information which is either sent or received by the user. As a result, the attacker can presume he is which service the user is using or where he is located at a given time.
- An attacker gets information about a user's permanent identity such as IMSI and then traces the user using IMSI.

3.1.3 WLAN Access Provider

The threats related with WLAN access provider are as follows:

- The WLAN user cannot usage of WLAN service due to DoS attack, which is against the network or specific user.
- The WLAN user cannot access the legitimate WLAN service and get illegitimate WLAN service set up by an attacker.

3.2 Attacks

Attackers setting up a rouge AP may attempt to get free access service, modify a legitimate user's traffic, or perform DoS attacks. Furthermore, attacks can be performed remotely over the Internet. Therefore, the attacks are classified according to where the attack is performed/launched [20].

3.2.1 Victim's WLAN UE

Open platform terminals can be infected by viruses, Trojan horses, or other malicious software. The software can be operated without the knowledge of the user on his terminal and used for performing different types of attacks.

- If the user uses Universal Subscriber Identity Module(USIM), which stores important information and connects with the user's terminal, Trojan horses residing in the terminal can send fake requests to the USIM and then transmit challenge-response results to another terminal. The owner of the latter terminal could get access with the stolen important information.
- Trojan horses may reside all the usual activities. Therefore, attackers monitor the user's keyboard or sensitive data and then forward the information to another machine using residing Trojan horses.
- Malicious software can be used to perform Distributed DoS(DDoS) attack. In other words, several instantiations of which software synchronize and start a DoS attack simultaneously against the target.
- Malicious software tries to connect with different WLAN for annoying the user.

3.2.2 Attacker's WLAN UE and/or AP

An attacker can perform several types of attacks during his access to the terminal and the AP. For example, DoS attack and eavesdropping can occur because control signaling is not protected. This type of attack can cause different threats.

- An attacker can modify the user's traffic or divert the traffic to another network.
- An attacker can falsify a network or a commercial site to get access to credit card information.
- An attacker can perform man-in-the-middle attack and then get credentials of the legitimate user. After getting a legitimate user's information, the attacker can prevent access of the legitimate user.
- After getting a legitimate user's information, the attacker can prevent access of the legitimate user.
- An attacker can use fake configuration or control message to redirect a user's traffic.

- In order to interfere or gain access, an attacker performs simply eavesdropping on the traffic around an AP.

3.2.3 WLAN Access Network Infrastructure

- An attacker can perform attacks at WLAN access network infrastructure such as AP, LAN connecting APs, and Ethernet switches.
- If WLAN is partially a wired network, an attacker may hook up part of the network.
- An attacker can interfere with the charging functions, just to increase a user's bill.

3.2.4 Other Device on the Internet

- An attacker can perform a flooding attack sending garbage packets, just to increase the user's bill.

4. Related Work

4.1 EAP-AKA

When the UE attempts to access non-3GPP such as WLAN, the UMTS-AKA protocol cannot be used. Therefore, EAP-AKA [9] is used to support 3GPP-WLAN interworking. EAP-AKA protocol is based on UMTS-AKA. We will describe overview of EAP-AKA and its vulnerabilities in this section.

4.1.1 Generation of Temporary Identity

For hiding user's permanent identity, the AAA server can generate temporary identity such as pseudonyms or re-authentication identity by using Advanced Encryption Standard(AES) in Electronic Code Book(ECB) with 128 bit key sizes. The temporary identity has the same form with IMSI. Fig. 4.1 shows generation of temporary identity. Generated temporary identity will use next authentication procedure instead of IMSI [20].

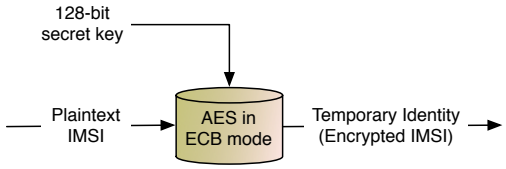


Figure 4.1: Generation of temporary identity

Fig. 4.2 shows structure of encrypted IMSI. The following fields are concatenated.

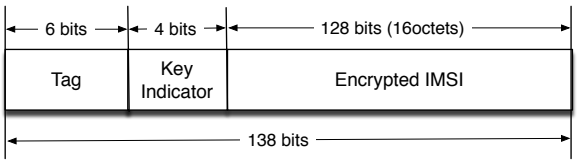


Figure 4.2: Structure of encrypted IMSI

- *Encrypted IMSI:* The AAA server can later obtain the IMSI from the temporary identity.
- *Key indicator:* The AAA server that received the temporary identity can locate the appropriate key to de-encrypt the Encrypted IMSI.
- *Temporary identity tag:* Temporary identity tag is used to mark the identity as temporary pseudonym of re-authentication identity.

4.1.2 Procedure of EAP-AKA

EAP-AKA provides mutual authentication between the UE and the AAA server. That is, EAP-AKA performs a procedure of authentication and key agreement between 3G and non-3GPP. Fig. 4.3 shows procedure of EAP-AKA.

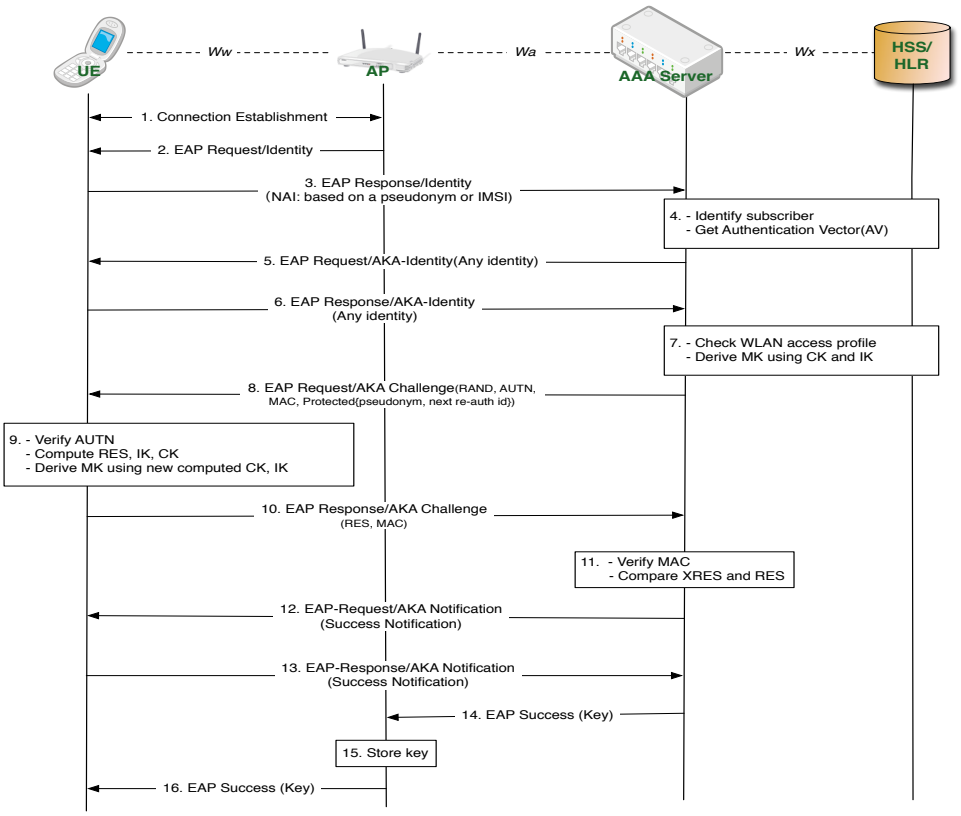


Figure 4.3: Procedure of EAP-AKA

From Step 5 to 6, the AAA server requests again the user identity because immediate nodes can modify user identity such as IMSI included in EAP Response/Identity message. Therefore, if the UE receives EAP Request/AKA-Identiy message, the UE should send EAP Response/AKA-Identity message which must contain the same user identity included in EAP Response/Identity message to the AAA server. The AAA server will use user identity received from EAP Response/AKA-Identity message in the rest of the authentication and key agreement procedure. In Step 7, the AAA server checks the WLAN access profile and verifies that the subscriber is authorized to use the WLAN service.

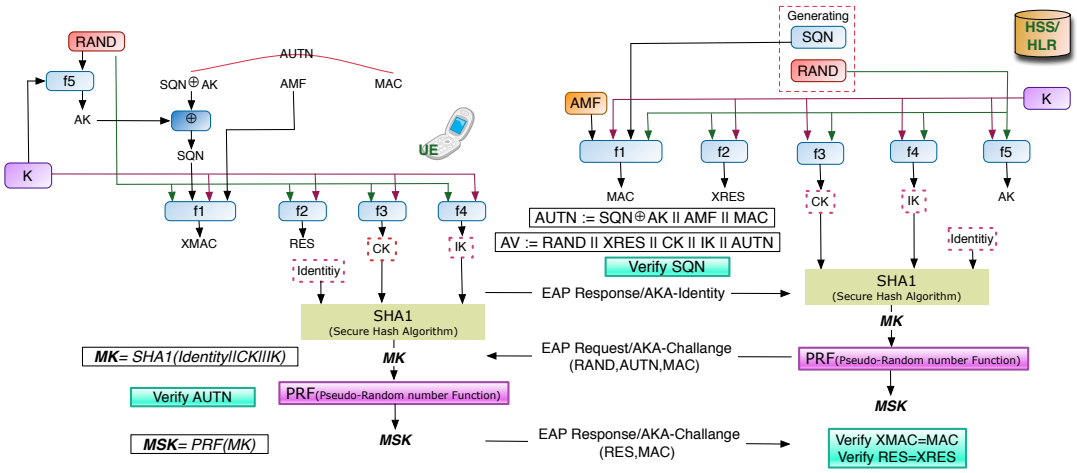


Figure 4.4: Generation of MK and MSK

Fig. 4.4 indicates the procedure of generation of MK and MSK. The AAA server retrieves AV through Wx interface. The UE receives EAP Request/AKA-Challenge message with three parameters (RAND, AUTN, and MAC). The UE verifies AUTN and SQN. If AUTN is incorrect, the UE terminates authentication. If SQN is in incorrect range, the UE occurs SQN synchronization procedure. Meanwhile, the AAA server should request again the AV to the HSS. If AUTN is in the correct range, the UE computes RES, Integrity Key (IK) and Cipher Key (CK) using symmetric key K shared between the UE and the HSS. Moreover, the UE computes new MAC value and then sends EAP Response/AKA-Challenge message containing calculated RES and new MAC value to the AAA server. Both CK and IK are used to derive the EAP Master Key (MK), from which EAP Master Session Key (MSK) is derived. Generated MSK is transmitted to the AP and used to protect further communication.

4.1.3 Vulnerabilities of EAP-AKA

EAP-AKA is based on UMTS-AKA. For this reason, EAP-AKA can have not only vulnerabilities of UMTS-AKA but also vulnerabilities of 3GPP-WLAN interworking. Vulnerabilities of EAP-AKA are as follows:

- **Disclosure of IMSI**: Although EAP-AKA uses a temporary identity such as pseudonyms or re-authentication identity, the UE must send a permanent identity such as IMSI to the AAA server on first connection. If an attacker gets IMSI, he can misuse IMSI and can trace subscriber.
- **Man-in-the-middle attack**: EAP-AKA has several factors which can cause man-in-the-middle attacks.
  - As mentioned earlier, IMSI is plaintext on the first connection between the UE and the AAA server. Therefore, an attacker may be waiting for transmission of IMSI and can modify IMSI.
  - Although the UE and the AAA server can be successfully authenticated each other, the AAA server sends EAP Success message with MSK to the AP and the UE without authentication. As a result, an attacker who impersonates the AP can receive EAP Success message with MSK, modify the received message and then send the modified message to the UE or another UE.
- **Perfect Forward Secrecy**: EAP-AKA uses symmetric key K shared between the UE and the HSS to perform authentication and key agreement. The CK, IK, MK, and MSK were generated using K. For this reasion, disclosure of K is equal to the disclosure of all procedure of EAP-AKA. That is, EAP-AKA does not provide Perfect Forward Secrecy(PFS).
- **Bandwidth consumption**: The AAA server requests again the user identity before the challenge/response procedure because immediate nodes can modify user identity. For this reason, EAP-AKA has additional bandwidth consumption.
- **SQN synchronization**: EAP-AKA also uses AV which was used in UMTS-AKA. If received SQN is in the incorrect range, the UE should perform SQN synchronization procedure. Meanwhile, the AAA server should request again AV to the HSS. As a result, bandwidth consumption between the AAA server and the HSS can occur.

4.2 EAP-SIM (Subscriber Identity Module)

SIM based authentication is used for GSM (Global System for Mobile communications) subscribers that do not have USIM applications. Therefore, EAP-SIM is the standard to authenticate a user for WLAN access via the SIM card using GSM network. By combining GSM and EAP authentication techniques, a mobile user can be authenticated to the network via the SIM card. EAP-SIM provides mutual authentication which integrates GSM and WLAN [7].

For generation of strong keys, EAP-SIM combines n ($n = 2$ or $n = 3$) individual RANDs that result in the derivation of n session keys, K_C. These keys can be used for generating Master Key (MK) which is combined with NONCE. Generated MK can be used for generating Master Session Key (MSK) and K_auth key. Formula of MK is as follow:

MK=$SHA1$(Identity | n*K_C | $NONCE$ | $VersionList$ | $SelectedVersion$)

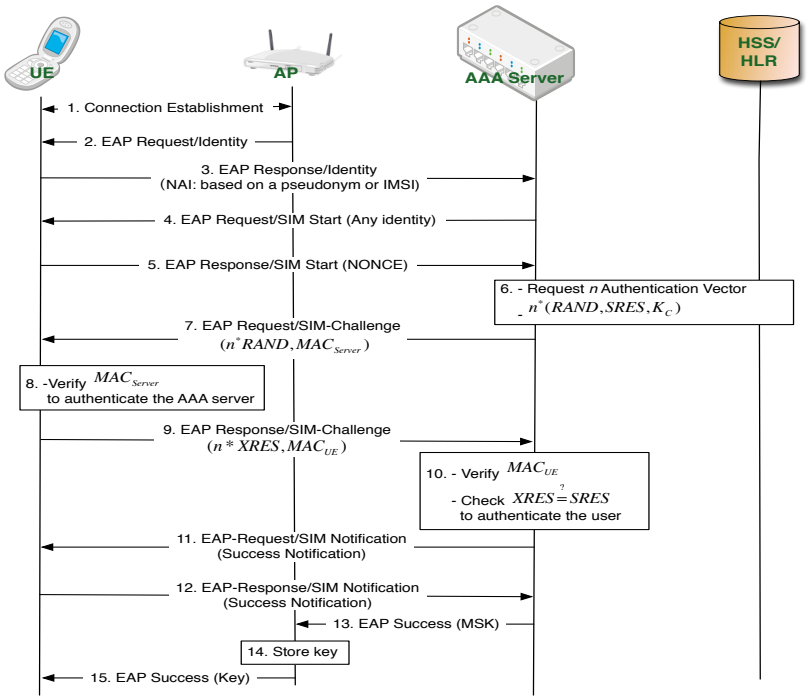


Figure 4.5: Procedure of EAP-SIM

Fig. 4.5 shows procedure of EAP-SIM. In Step 6, the AAA server can be communicated with HSS/Home Location Register (HLR) and obtain n GSM Authentication Vector (AV). The generated GSM AV (RAND, SRES, K_C) is based on secret key K_i shared between the user and the HSS/HLR. In step 7, the AAA server sends EAP Request/SIM-Challenge with n RANDs and MAC_{Server}. Formula of MAC_{Server} is as follow:

MAC_{Server} =HMAC_$SHA1_{K_auth}$(EAP Request/SIM-Challenge (n*RAND) | NONCE)[2]

The UE executes the GSM/GPRS authentication algorithms n times in order to generate n K_C keys and n XRES values. Then, the UE verifies MAC_{Server} using K_auth. Result of verifying K_{Server} is true, UE can authenticate AAA server. In step 9, the UE computes MAC_{UE}. Formula of MAC_{UE} is as follow:

MAC_{UE} =HMAC_$SHA1_{K_auth}$(EAP Response/SIM-Challenge (n*XRES) | n*XRES)[3]

In step 10, the AAA server verifies MAC_{UE}. Result of verifying MAC_{UE} is true, the AAA server sends EAP-Request/SIM Notification to UE. Result of EAP-SIM, the UE and AAA server can authenticate each other. Moreover, the UE and AP share the key MSK which is used for encryption.

EAP-SIM has several vulnerabilities as follows [12]:

- User's identity can be protected by using temporary identity during conversation. However, identity protection cannot be provided on the first connection because the UE must send user's permanent identity (IMSI) to the AAA server. In this case, the eavesdroppers can easily get IMSI.
- EAP-Request/SIM Notification which indicates result of "EAP-Success" or "EAP-Failure" are not protected. Therefore, attackers can send false notifications to other peers and execute DoS attack by spoofing this message.

4.3 EAP-UTLS (USIM-based EAP Authentication Protocol)

In [22], the authors proposed novel symmetric-key certificate distribution scheme based on USIM card in a cellular network. Furthermore, combining the proposed certificate distribution scheme with EAP-TLS, they present a new EAP authentication protocol called EAP-UTLS (USIM-based EAP authentication protocol). Therefore, EAP-UTLS is an extension of EAP-TLS and follows the EAP framework in the IEEE 802.1X standard.

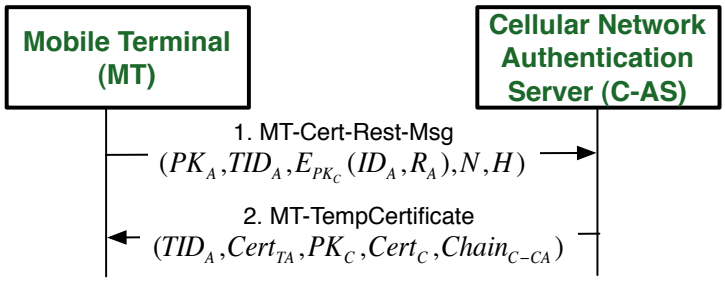


Figure 4.6: Certificate distribution scheme

Fig. 4.6 shows certificate distribution scheme. In this scheme, assume that the Mobile Terminal (MT) and Cellular Network Authentication Server (C-AS) share a symmetric key and the MT knows public key of the C-AS. Result of this scheme is that mobile subscribers can obtain temporary certificate from the corresponding cellular network. Because of the temporary certificate $Cert_{TA}$ issued by the C-AS, if other users attempt to verify $Cert_{TA}$ and does not know public key of C-AS PK_C, he may then verifies $Cert_C$ and $Chain_{C-CA}$ which is a certificate chain from the C-AS to the highest Certificate Authority (CA) before verifying $Cert_{TA}$. This case is called a certificate chain based on the X.509 [8].

Fig. 4.7 shows new EAP-UTLS protocol. Most steps of EAP-UTLS are the same as EAP-TLS [4, 5], but several steps are required to be modified. The main different from EAP-TLS, the MT sends a certificate request message to the W-AS, and the W-AS bypasses it to the C-AS and then receives the temporary certificate of MT from the C-AS.

EAP-UTLS provides identity protection achieved by the certificate distribution scheme. Moreover, EAP-UTLS prevent passive attack, guessing and dictionary attacks, and man-in-the-middle attack.

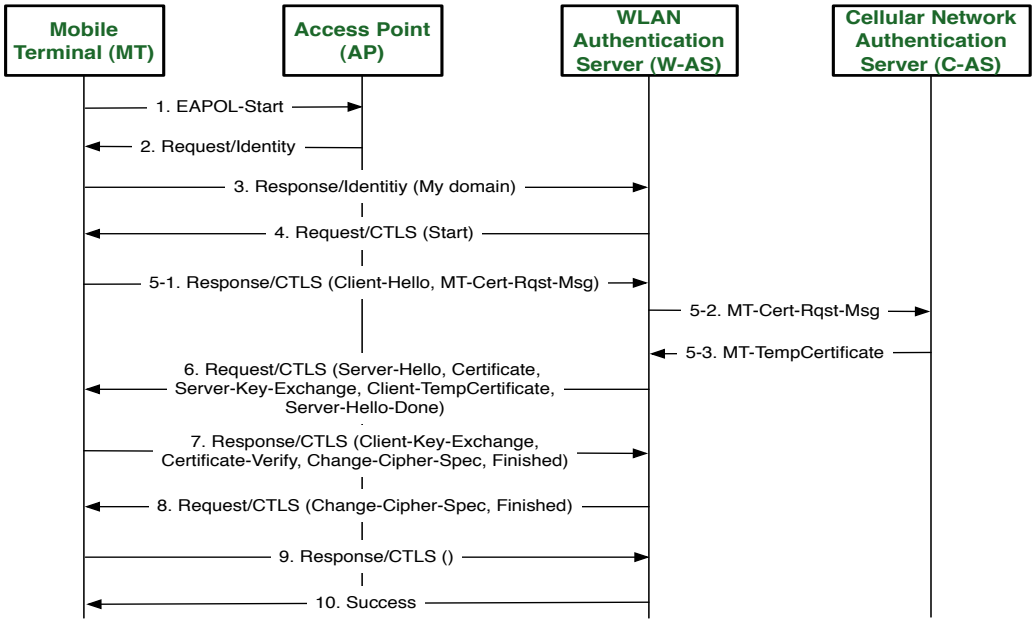


Figure 4.7: New EAP-UTLS protocol

4.4 EAP-TLS (Transport Layer Security)

EAP-TLS provides user protected cipher-suite negotiation, key management, and mutual authentication between user and WLAN authentication server based on X.509 certificates. Moreover, user can authenticate the network in EAP-TLS. After EAP-TLS negotiation is completed, the two end-points can securely communicate within the encrypted TLS tunnel. For this reason, disclosure of user's identity and password can not occur, and rogue APs can be detected. However, user's identity must be performed in the clear before the EAP-TLS negotiation.

Fig. 4.8 shows procedure of EAP-TLS in WLAN [4, 5]. From Step 3 to 4, the AP receives the user's identity included in EAP-response/identity and then creates a RADIUS-access-request which also contains the user's identity. From Step 5 to 6, the WLAN authenticator server sends its certificate to the supplicant. Then, the supplicant verifies the server's certificate. If the server's certificate is valid, the supplicant provides its certificate to WLAN authentication server and also initiates the negotiation for cryptographic material. In Step 7, the WLAN authentication server sends a RADIUS-access-success to the AP and also responses the cryptographic material for the session, if the received user's

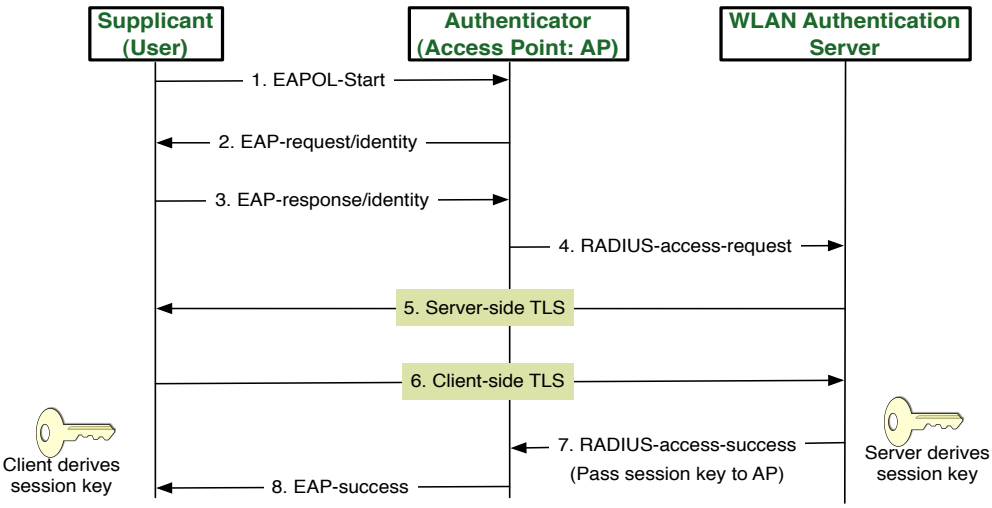


Figure 4.8: Procedure of EAP-TLS

certificate is valid. The generated session key can be used for data encryption.

Refer to [10] which is widely used and well tested, EAP-TLS is consider to be very secure. Therefore, EAP-TLS can prevent several attacks such as replay attack and man-in-the-middle attack. Table. 4.1 shows risk evaluation of EAP-TLS using the methodology described in [6]. In Table. 4.1, "occurrence Likelihood" and "Impact (evaluation of threat's consequences)" are estimated with values from 1 to 3. The larger the number is, the more likely a threat could happen and more critical its impact is. "Risk" is measurement for overall critical degree of a threat. Its value can be calculated by multiplying the corresponding "occurrence Likelihood" and "Impact" value [11].

Table 4.1: Risk evaluation of EAP-TLS

Threat	**Likelihood**	**Impact**	**Risk**
User Impersonation	1	1	1
AP impersonation	1	3	3
Data alteration	1	2	2
DoS attack	1	2	2
Dictionary Attack	1	3	3
Man-in-the-middle attack	1	3	3

4.5 EAP-TTLS (Tunneled Transport Layer Security)

EAP-TTLS extends EAP-TLS to exchange additional information such as accounting information through the secure TLS tunnel [13]. That is, EAP-TTLS are tunneled methods which can hide user's identity from eavesdropping in the secure tunnel. EAP-TTLS is divided into two phases: *the TLS handshake phase* and *the TLS tunnel phase*.

In first phase, the server is authenticated by client using an X.509 certificate. Optionally, the server can also authenticate the client. A secure TLS tunnel is established after the TLS handshake in first phase. Fig. 4.9 shows the TLS handshake phase.

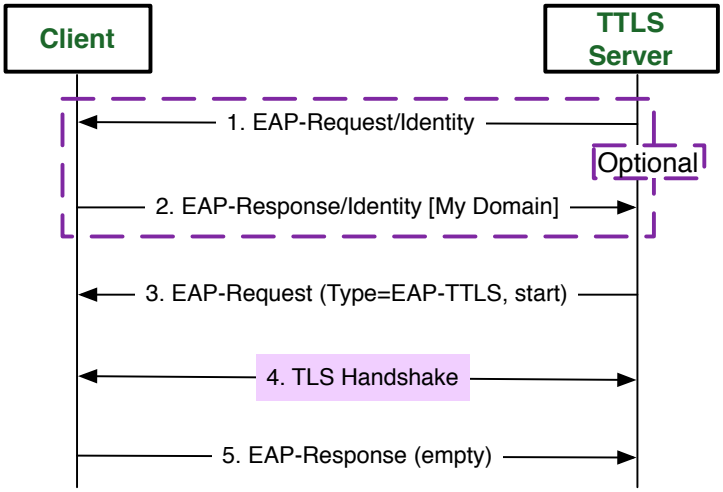


Figure 4.9: The TLS handshake phase

In second phase, the secure TLS tunnel can be used for additional information exchanges such as client's username, password, and accounting information. These information are included in the attribute-value pairs (AVPs) defined by the AAA server. Using these information, the AAA server can authenticate client. Fig. 4.10 shows the TLS tunnel phase.

EAP-TTLS allows the use of legacy password-based protocols with existing authentication databases, while protecting the security of these legacy protocols against eavesdropping and man-in-the-middle attack. Moreover, EAP-TTLS provides mutual authentication, key generation, client identity privacy, and data cipher suite negotiation.

Table. 4.2 shows risk evaluation of EAP-TLS using the methodology described in [6]. In Table. 4.2, "occurrence Likelihood" and "Impact (evaluation of threat's consequences)"

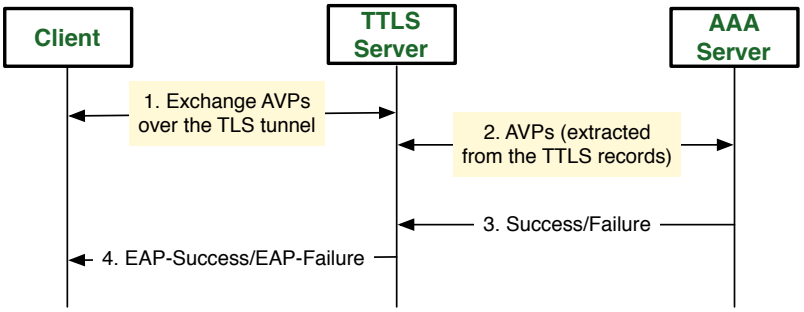


Figure 4.10: The TLS tunnel phase

are estimated with values from 1 to 3. The larger the number is, the more likely a threat could happen and more critical its impact is. "Risk" is measurement for overall critical degree of a threat. Its value can be calculated by multiplying the corresponding "occurrence Likelihood" and "Impact" value [11].

Table 4.2: Risk evaluation of EAP-TTLS

Threat	Likelihood	Impact	Risk
User Impersonation	1	1	1
AP impersonation	1	3	3
Data alteration	1	2	2
DoS attack	1	2	2
Dictionary Attack	1	3	3
Man-in-the-middle attack	1	3	3

4.6 EAP-PEAP (Protected EAP)

EAP-PEAP provides wrapping of the EAP methods within TLS [3]. Therefore, the EAP messages encapsulated inside the TLS tunnel are protected against various attacks. Therefore, EAP-PEAP is divided into two phrase.

In first phrase, EAP-PEAP performs TLS handshake in which the server is being authenticated to the client by using a certificate. Optionally, the PEAP server can also authenticate the client. Fig. 4.11 shows first phrase of EAP-PEAP.

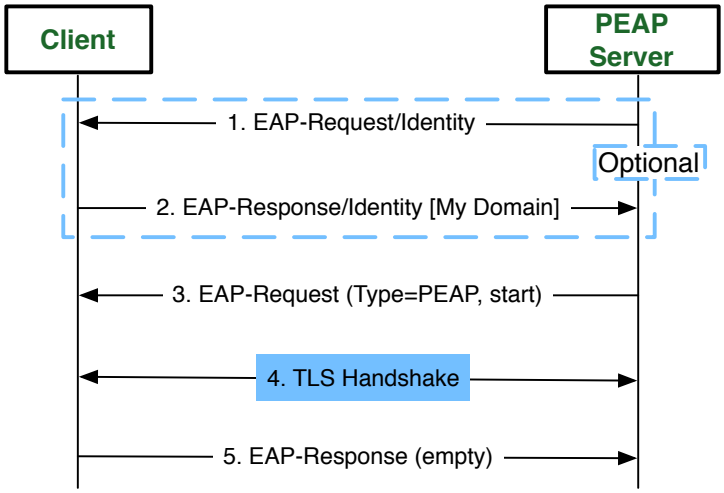


Figure 4.11: The first phrase of EAP-PEAP

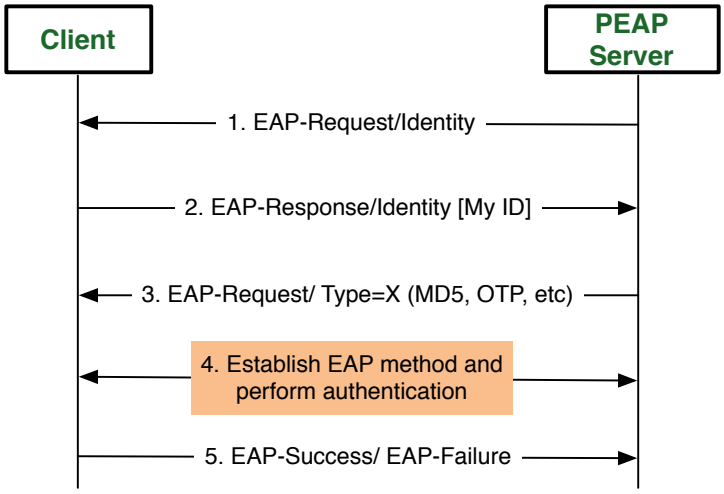


Figure 4.12: The second phrase of EAP-PEAP

In second phrase, EAP in the generated TLS tunnel are performed in order to authenticate the client using user name and passwords. Fig. 4.12 shows second phrase of EAP-PEAP. The basic idea of EAP-PEAP and EAP-TTLS are same. However, EAP-PEAP can only use EAP protocol in the second phrase, while EAP-TTLS can use EAP or non-EAP methods.

Table. 4.3 shows risk evaluation of EAP-PEAP using the methodology described in [6]. In Table. 4.3, "occurrence Likelihood" and "Impact (evaluation of threat's consequences)" are estimated with values from 1 to 3. The larger the number is, the more likely a threat could happen and more critical its impact is. "Risk" is measurement for overall critical degree of a threat. Its value can be calculated by multiplying the corresponding "occurrence Likelihood" and "Impact" value [11].

Table 4.3: Risk evaluation of EAP-PEAP

Threat	**Likelihood**	**Impact**	**Risk**
User Impersonation	1	1	1
AP impersonation	1	3	3
Data alteration	1	2	2
DoS attack	1	2	2
Dictionary Attack	1	3	3
Man-in-the-middle attack	1	3	3

5. Proposed Protocol

In this chapter, we propose a new authentication and key agreement protocol based on EAP-AKA.

5.1 Background

5.1.1 Perfect Forward Secrecy (PFS)

A protocol is said to have *Perfect Forward Secrecy* if compromise of long-term keys does not compromise past session key.

The idea of PFS (sometimes called *break-backward protection*) is that previous traffic is securely locked in the past. It may be provided by generating session keys by Diffie-Hellman key agreement, wherein the Diffie-Hellman exponentials are based on short-term keys. If long-term secret keys are compromised, future sessions are nonetheless subject to impersonation by an active adversary [2].

5.1.2 Elliptic Curve Diffie-Hellman (ECDH)

Using Elliptic Curve Diffie-Hellman (ECDH), two parties can establish session key. ECDH is public key cryptosystem. The ECDH provides same security properties and uses fewer resources than other public key cryptosystems that require certificates. Therefore, the overhead is less occurred using ECDH than other public key cryptosystems that require certificate. Fig. 5.1 shows procedure of ECDH. The procedure of ECDH is as follows:

- User A and B publicly agree on an elliptic curve E over a large finite field F and a point P on that curve.
- The user A and B each selects random number a and b, respectively. Two values a and b are private value.
- Using elliptic curve point-addition, user A and B each publicly compute aP and bP on E.
- User A and B each compute abP using private and public values.

As a result, solving ECDH is a computationally difficult problem [14].

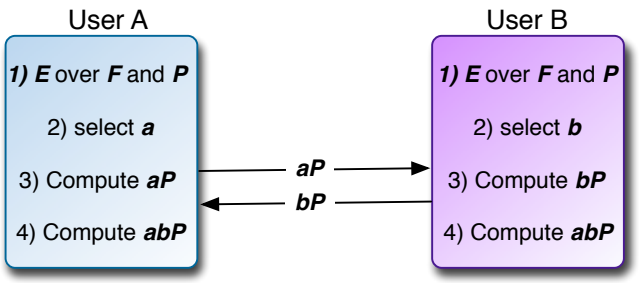


Figure 5.1: Elliptic Curve Diffie-Hellman

5.2 Notations

Table 5.1 shows notations.

Table 5.1: Notations of proposed protocol

Notation	Description
U, AP, A, H	Denote the UE, the AP, the AAA server, and the HSS, respectively
${}_cID_{UE}$	Current temporary ID of UE
ID_x	ID of entity x
T_x	Timestamp generated by entity x
g_K^i	Key generation function using the key K
f_K^1	MAC generation function using the key K
f_K^2	${}_cID_{UE}$ generation function using the key K
$RAND_x$	Random number by entity x
K_{xy}	Symmetric key shared between entity x and y
TK	Temporary Key

5.3 Assumption

In our proposed protocol, we assume the following:

- A secure channel is established between the AAA server and the HSS.

- The UE can identify the ID of AAA server and AP in which it is able to access now.

5.4 The Workflow of Our Protocol

Our protocol consists of four procedures which are shown in Fig. 5.2.

5.4.1 Initialization

- **Step 1.** A connection is established between the UE and the AP.
- **Step 2.** To get user identity, the AP sends EAP Request/Identity message to the UE.

5.4.2 Registration and Generation of TK

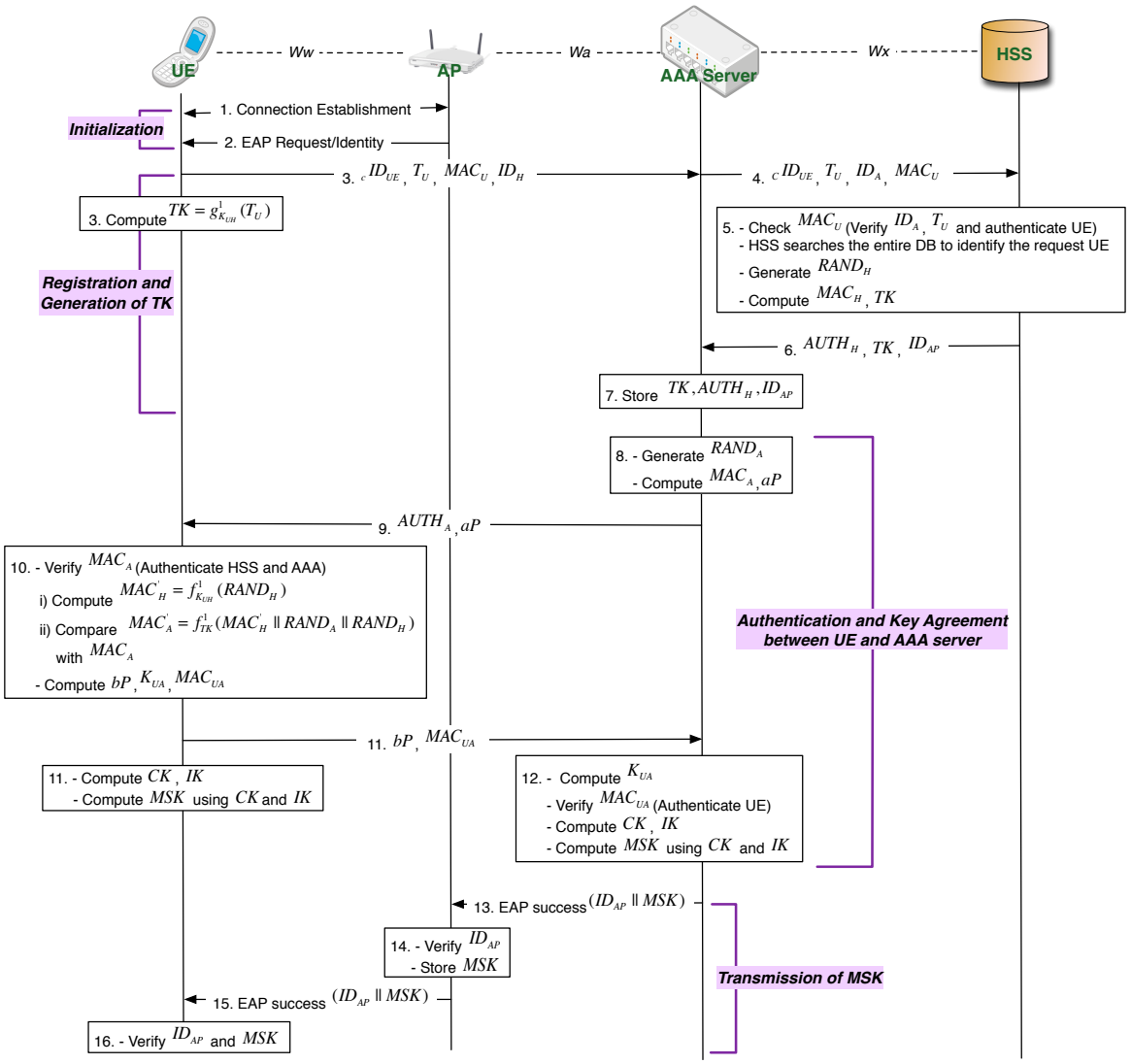
- **Step 3.** The UE generates T_U and computes MAC_U=$f^1_{K_{UH}}$ ($T_U||ID_A||ID_{AP}$) using the K_{UH}. In addition, the UE computes ${}_cID_{UE}$ to prevent the disclosure of IMSI. ${}_cID_{UE}$ can be computed as $f^2_{K_{UH}}(IMSI)$. Therefore, the UE sends ${}_cID_{UE}$, T_U, MAC_U, and ID_H to the AP. Meanwhile, the UE computes TK=$g^1_{K_{UH}}(T_U)$.
- **Step 4.** The AAA server transmits ${}_cID_{UE}$, T_U, MAC_U, and ID_A to the HSS using ID_H received from the UE in Step 3.
- **Step 5.** The HSS checks MAC_U. As a result, the UE can verify ID_A and T_U and authenticate the UE. The procedure of checking MAC_U is as follows:

  a) The HSS retrieves ID_{AP}, ID_A, and T_U from MAC_U.

  b) The HSS verifies whether or not ID_A retrieved from MAC_U equals ID_A which sent Step 4 message(${}_cID_{UE}$, T_U, MAC_U, ID_A) to the HSS.

  c) The HSS verifies whether T_U is in the correct range and then verifies whether T_U retrieved from MAC_U equals received T_U. If the result is correct, the HSS can authenticate the UE and prevent replay attack.

  After checking MAC_U, the HSS derives IMSI from ${}_cID_{UE}$ using K_{UH}. The HSS searches the entire DB which stored user identity such as IMSI to identify the requested UE. The HSS computes TK=$g^1_{K_{UH}}(T_U)$ and generate $RAND_H$. Using $RAND_H$ the HSS computes MAC_H=$f^1_{K_{UH}}(RAND_H)$.



$$_cID_{UE} = f^2_{K_{UH}}(IMSI) \qquad MAC_U = f^1_{K_{UH}}(T_U \| ID_A \| ID_{AP}) \qquad TK = g^1_{K_{UH}}(T_U)$$

$$MAC_H = f^1_{K_{UH}}(RAND_H) \qquad AUTH_H = (MAC_H \| RAND_H) \qquad MAC_A = f^1_{TK}(MAC_H \| RAND_A \| RAND_H)$$

$$AUTH_A = (MAC_A \| RAND_A \| RAND_H) \qquad K_{UA} = g^2_{TK}(abP) \qquad MAC_{UA} = f^1_{K_{UA}}(RAND_A \| bP)$$

$$CK = g^3_{K_{UA}}(RAND_A) \qquad IK = g^4_{K_{UA}}(RAND_A)$$

Figure 5.2: Proposed protocol

- **Step 6.** The HSS sends $AUTH_H$, TK, and ID_{AP} to the AAA server. ID_{AP} was obtain from MAC_U. We already assumed that a secure channel was established between the HSS and the AAA server. As a result, TK is secure against attackers although TK is plaintext on the air.

- **Step 7.** The AAA server stores TK, $AUTH_H$, and ID_{AP}.

5.4.3 Authentication and Key Agreement

- **Step 8.** The AAA server generates $RAND_A$ and computes MAC_A. Afterward, the AAA server selects random number a and computes aP on E.

- **Step 9.** The AAA server sends $AUTH_A$=($MAC_A||RAND_A||RAND_H$) and aP to the UE.

- **Step 10.** The UE verifies MAC_A. The procedure of verifying MAC_A is as follows:

  a) The UE computes $MAC_H^{'}$=$f^1_{K_{UH}}(RNAD_H)$. The $RAND_H$ is derived from $AUTH_A$ in Step 9.

  b) The UE computes $MAC_A^{'}$=$f^1_{TK}(MAC_H^{'}||RAND_A||RAND_H)$. The $RAND_H$ and $RAND_A$ are derived from $AUTH_A$.

  c) The UE verifies whether $MAC_A^{'}$ equals MAC_A or not. If $MAC_A^{'}$ is not same MAC_A, the HSS or the AAA server is not valid. Therefore, the UE terminates the procedure.

  The UE can authenticate the HSS and the AAA server by verifying MAC_A. As a result, verifying MAC_A prevents replay attack and man-in-the-middle attack. The UE selects random number b and computes bP on E. Subsequently, using aP received from the AAA server in Step 9, the UE can compute symmetric key $K_{UA} = g^2_{TK}(abP)$. Finally, the UE computes $MAC_{UA} = f^1_{K_{UA}}(RAND_A||bP)$ using K_{UA} shared between the UE ad the AAA server.

- **Step 11.** The UE transmits bP and MAC_{UA} to the AAA server and concurrently computes CK and IK. Afterward, the UE computes MSK using CK and IK as EAP-AKA.

- **Step 12.** Using bP received from the UE in Step 11, the AAA server can compute K_{UA}. Then the AAA server verifies MAC_{UA}. In other words, the AAA server verifies whether or not $RAND_A$ included in MAC_{UA} equals $RAND_A$ generated from

the AAA server in Step 8. If two values are same, the AAA server can authenticate the UE. The AAA server computes CK and IK. Finally, the UE computes MSK using CK and IK as EAP-AKA.

5.4.4 Transmission of MSK

- **Step 13.** The AAA server sends $ID_{AP}||MSK$ with EAP Success message to the AP. ID_{AP} was received from the HSS in Step 6.
- **Step 14.** The AP verifies whether received ID_{AP} equals AP's own ID or not. If the result is correct, the AP stores MSK. Otherwise the AP does not store MSK and then terminates the execution.
- **Step 15.** The AP sends $ID_{AP}||MSK$ with EAP Success message to the UE.
- **Step 16.** The UE verifies whether or not ID_{AP} received from the AP in Step 15 equals ID_{AP} used in Step 3 to compute MAC_U, and then verifies whether or not MSK received from the AP in Step 15 equals MSK generated in Step 11. If the result is correct, the procedure of authentication and key agreement is successful. Consequently, the UE can securely use WLAN service using MSK.

6. Analysis and Comparison

In this chapter, we analyze our protocol and then compare our protocol with the previous protocols.

6.1 Security Analysis

Our protocol has several security properties as follows:

6.1.1 Protect user identity (IMSI)

In our protocol, IMSI is not exposed by attackers. The UE generates the ${}_cID_{UE}$ using the K_{UH} and then sends ${}_cID_{UE}$ to the HSS. For this reason, the UE and the HSS can only retrieve user identity such as IMSI included in ${}_cID_{UE}$ using K_{UH}. Therefore, our protocol provides strong user identity protection.

6.1.2 Secure against man-in-the-middle attack

- The UE and the HSS can only retrieve IMSI from ${}_cID_{UE}$. Therefore, attackers cannot derive the IMSI and cannot modify IMSI.
- The AAA server sends the EAP Success message with $ID_{AP}||MSK$ to the AP. The AP then verifies whether or not received ID_{AP} equals AP's own ID. If two values are not same, procedure of authentication and key agreement fails. Therefore, our protocol prevents man-in-the middle attack compared with EAP-AKA, which sends the EAP Success message with MSK to the AP and the UE without authentication.
- The UE can certainly confirm that MAC_H is generated by the correct HSS by verifying MAC_A. As a result, our protocol can prevent man-in-the-middle attack.

6.1.3 Provide Perfect Forward Secrecy (PFS)

To provide PFS between the UE and the AAA server, our protocol uses ECDH. While generating K_{UA}, our protocol uses aP and bP that are not related with K_{UH}. Therefore, if disclosure of K_{UH} occurs, attackers cannot guess K_{UA}. In other words, guessing K_{UA} is a computationally difficult problem.

6.1.4 Provide mutual authentication

- **Between the UE and the AAA server:** The UE can authenticate the AAA server by verifying MAC_A in Step 10. Similarly, the AAA server can authenticate the UE by verifying MAC_{UA} in Step 12.
- **Between the UE and the HSS:** The UE can authenticate the HSS by verifying MAC_A in Step 10. Similarly, the HSS can authenticate the UE by verifying MAC_U in Step 5.

6.1.5 Secure against replay attack

Before generating TK, the HSS must verify whether T_U is in the correct range or not. Moreover, our protocol verifies $RAND_A$ and $RAND_H$ included in MAC_A. Therefore, our protocol can prevent replay attack.

6.2 Performance Analysis

6.2.1 Reduce bandwidth consumption

Our protocol uses ${}_cID_{UE}$ to prevent disclosure of user identity. As a result, disclosure of user identity does not occur by immediate nodes or attackers despite requesting user identity once. Thus, compared with EAP-AKA which requests again user identity in Step 5, our protocol can reduce bandwidth consumption.

6.2.2 Do not occur SQN synchronization

Our protocol does not occur SQN synchronization as well as does not consume bandwidth between the AAA server and the HSS, because it does not use SQN mechanism and AV. As a result, our protocol can reduce bandwidth consumption.

6.2.3 Use Elliptic Curve Diffie-Hellman (ECDH)

Generally, most of the previous protocols do not use any kind of public key cryptosystem because UEs have power limitation, low-level computational power, and less storage space. However, technology is significantly improving. For this reason, previous protocols consider use of public key cryptosystems with certificates [4, 13, 3, 11]. Therefore, our protocol combines ECDH with symmetric key cryptosystem to provide secure communication between 3GPP and non-3GPP. ECDH provides the same security properties and

uses fewer resources than other public key cryptosystems with certificates. In [21], authors used the OpenSSL speed program to measure RSA and ECDH operation for different key sizes. Table. 6.1 highlights the performance advantage of ECDH over RSA for different security levels. The performance advantage of ECDH gets even better than its key-size advantage as security needs increase.

Table 6.1: Measured performance of public key cryptosystem

	ECDH-160	**RSA-1024**	**ECDH-192**	**RSA-1536**	**ECDH-224**	**RSA-2048**
Time(ms)	3.69	8.75	3.87	27.47	5.12	56.18
Ops/sec	271.3	114.3	258.1	36.4	195.5	17.8
Performance ratio	2.4:1		7.1:1		11:1	
Key-size ratio	1:6.4		1:8		1:9.1	

Therefore, our protocol has less overhead than previous protocols which are based on public key cryptosystems with certificates. In our protocol, the UE and the AAA server only store and manage a, b, aP, and bP.

6.2.4 Communication overhead

UE always want to more efficient authentication protocols because UE has less storage space and limited battery power.

Table 6.2: Communication overhead

	UE-AAA AKA		**UE-HSS authentication**	
Our Protocol	UE AAA	2 1	UE HSS	1 1
EAP-AKA [9]	UE AAA	3 2	UE HSS	- -

Table 6.2 shows communication overhead. Compared with EAP-AKA, to perform mutual authentication and key agreement between the UE and the AAA server, the UE and the AAA server in our protocol require only two times and one time of conversation, respectively. More-

over, the UE and the HSS in our protocol require only one time to authenticate each other. As a result, our protocol is highly efficient in regard to communication overhead.

6.3 Comparison

To authenticate WLAN, IEEE 802.1x provides authentication framework based on Extensible Authentication Protocol(EAP). The EAP supports several authentication protocols and each protocol has advantages and disadvantages, respectively. Table 6.3 shows comparison of our protocol with previous protocols [11]. Refer to Table 6.3 our protocol supports 3GPP-WLAN interworking and provides strong user identity protection. Moreover, our protocol has less overhead than other protocols(EAP-TTLS, PEAP, and EAP-UTLS) because of using a symmetric key cryptosystem and ECDH. Moreover, our protocol prevents man-in-the middle attack and replay attack. In addition, our protocol provides PFS and does not occur SQN synchronization which occurs in EAP-AKA. Therefore, our protocol provide more efficient and secure 3GPP-WLAN interworking than previous protocols.

Table 6.3: Comparison of our protocol with previous protocols

	Our protocol	**EAP-TLS [4]**	**EAP-TTLS [13]**	**PEAP [3]**	**EAP-AKA [9]**	**EAP-SIM [7]**	**EAP-UTLS [11]**
Type of cryptosystem	Symmetric and ECDH	Public (Certificate)	Public (Certificate)	Public (Certificate)	Symmetric	Symmetric	Public (Certificate)
Subscriber management	3GPP network provider	WLAN provider	WLAN provider	WLAN provider	3GPP network provider	3GPP network provider	3GPP network provider
Protection of user identity (IMSI)	Yes	No	Yes	Yes	No	No	Yes
3GPP-WLAN interworking	Yes	No	No	No	Yes	Yes	Yes
Secure against man-in-the middle attack	Yes	Yes	No	No	No	No	Yes
Secure against replay attack	Yes	Yes	Yes	Yes	Yes	Yes	No
Provide PFS	Yes	No	No	No	No	No	No
Not need for SQN synchronization	Yes	-	-	-	No	-	-

7. Conclusion

In this thesis, we show overview of architecture for accesses for non-3GPP and analyze threats and attacks in 3GPP-WLAN interworking. Moreover, we explain several authentication protocols based on EAP and propose a new authentication and key agreement protocol based on EAP-AKA. The proposed protocol combines ECDH with symmetric key cryptosystem to overcome several vulnerabilities of EAP-AKA such as disclosure of user identity, man-in-the-middle attack, SQN synchronization, and additional bandwidth consumption. Moreover, our protocol provides Perfect Forward Secrecy (PFS) to guarantee stronger security, mutual authentication between the UE and the AAA server and between the UE and the HSS, and resistance to replay attack. Compared with previous protocols which use public key cryptosystem with certificates, our protocol can reduce computational overhead. Therefore, our protocol can provide secure and efficient 3GPP-WLAN interworking.

요 약 문

3GPP-WLAN 상호연동을 위한 인증 및 키 합의에 관한 연구

3GPP (3rd Generation Partnership Project) 표준은 차세대 모바일 통신 시스템을 위해 SAE (System Architecture Evolution)/LTE (Long Term Evolution)구조를 개발하고 있다. SAE/LTE 구조는 안전한 서비스를 제공하며 WLAN과 같은 non-3GPP에 접근 할 수 있다.

3GPP는 효과적인 과금 관리, 로밍, 완벽한 가입자 관리 및 넓은 서비스 지역을 제공하며 WLAN은 높은 대역폭과 데이터 전송률, 인터넷과의 높은 호환성을 제공한다. 하지만 WLAN은 3GPP에 비해 좁은 서비스 지역과 낮은 이동성 및 로밍을 제공한다. 따라서, 3GPP가 WLAN과 같은 non-3GPP에 접근하면 가입자는 3GPP와 WLAN의 모든 장점을 가질 수 있으며 안전한 3GPP-WLAN 상호연동을 위해서는 두 네트워크는 인증과정을 필요로 한다.

SAE/LTE 구조에서 안전한 non-3GPP에 접근하기 위해서는 EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement)가 사용된다. 하지만, EAP-AKA는 사용자 신원 노출, 중재자 공격, 시퀀스 넘버 동기화 그리고 추가적인 대역폭 소비와 같은 취약점들을 가지고 있다. 따라서, 이 논문에서는 3GPP과 non-3GPP의 상호연동 시 발생 가능한 위협들 및 공격들에 대해 분석하며 EAP-AKA에 기반한 새로운 인증 및 키 합의 프로토콜을 제안한다. 제안된 프로토콜은 EAP-AKA가 가진 취약성들을 해결하기 위해 ECDH (Elliptic Curve Diffie-Hellman)와 대칭키 기반 암호 시스템을 사용한다. 또한, 우리의 프로토콜은 더 높은 안전성을 제공하기 위해 완전 순방향 비밀성 및 상호 인증을 제공하며 재전송 공격에 안전하다. 인증서를 사용하는 공개키 기반 암호 시스템을 사용하는 기존 프로토콜들에 비해, 우리의 프로토콜은 계산적인 오버헤드도 줄일 수 있다. 따라서 우리의 프로토콜은 효율적이고 안전한 3GPP-WLAN 상호연동을 제공할 수 있다.

References

[1] Aboba B., Beadles M., The network access identifier *RFC 2486, Jan. 1996*

[2] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, *CRC Press, 1996*

[3] A. Palekar, D. Simon, S. Josefsson, H. Zhou, G. Zorn, Protected EAP Protocol (PEAP) Version 2, draft-josefsson-pppext-eap-tls-10, *IETF, October 2004*

[4] B. Aboba, S.Simon, PPP EAP TLS Authentication Protocol, RFC 2716, *IETE, October 1999*

[5] Ciscon Systems, "White paper: EAP-TLS Deployment Guide for Wireless LAN Networks, "2004, available at *http://www.cisco.com*

[6] ETSI. Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis. *Technical Specification ETSI TS 102 165-1 V4.1.1, 2003*

[7] H. Haverinen, J.Salowey, EAP SIM Authentication, draft-arkko-pppext-eap-sim-12, *IETE, October 2003*

[8] ITU-T recommendation X.509, Information technology-open system interconnection- the directory: authentication framework, *June 1997*

[9] J. Arkko, H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), *IETF RFC 4187, January 2006*

[10] Jim Burns, "Selecting an Appropriate EAP Method for Your Wireless LAN", 2003

[11] L. Han, A Threat Analysis of the Extensible Authentication Protocol, *Honors Project Report, April 2006*

[12] Ntantogian, C., Xenakis, C., Merakos, L., An Enhanced EAP-SIM Authentication Scheme for Securing WLAN, *15tg IST Mobile Wireless Communications, Myconos, Greece, Jun. 2006*

[13] P. Funk, S.Blake-Wilson, EAP Tunneled TLS Authentication Protocol, draft-ietf-pppext-eap-ttls-05, *IETF, July 2004*

[14] PlanetMath-Elliptic Curve Diffie-Hellman key exchange, *http://planetmath.org/encyclopedia/DiffieHellmanKeyExchange.html*

[15] P.Lescuyer, T.Lucidarme," Evolved Packet System (EPS): The LTE and SAE Evolution of 3G " , *J.Wiley & Sons, 2008*

[16] Third Generation Partnership Project (3GPP), 3GPP TS 33.102 v8.0.0 " 3G Security: Security Architecture (Release 8)" , *June 2008*

[17] Third Generation Partnership Project (3GPP), 3GPP TS 33.401 v8.1.1 " 3G System Architecture Evolution (SAE): Security architecture (Release 8)" , *October 2008*

[18] Third Generation Partnership Project (3GPP), 3GPP TS 33.821 v1.0.0 " Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE) (Release 8)" , *December 2007*

[19] Third Generation Partnership Project (3GPP), 3GPP TS 33.402 v8.3.0 " Architecture Enhancements for non-3GPP accesses (Release 8)" , *September 2008*

[20] Third Generation Partnership Project (3GPP), 3GPP TS 23.234 v8.1.0 " 3G security: Wireless Local Area Network (WLAN) Interworking Security (Release 8)" , *March 2008*

[21] V. Gupta, D. Stebila, S. Fung, S. Chang Shantz, N. Gura, H. Eberle, Speeding up Secure Web Transactions Using El liptic Curve Cryptography, *11th Network and Distributed System Security Symposium, February 5-6, 2004, San Diego, CA, pp. 231-239.*

[22] Yuh-Min Tseng, USIM-based EAP-TLS authentication protocol for wireless local area networks, *Computer Standards & Interfaces, November 2007*

감 사 의 글

이 논문을 완성하기까지 주위의 모든 분들로부터 수많은 도움을 받았습니다. 우선 오늘의 제가 있을 수 있게 해 준 우리 가족들에게 감사드립니다. 또한, 2년 동안 저에게 많은 관심과 지도를 주신 김광조 교수님께 감사드리며 우리 CAIS lab 모든 분들께 (현록오빠, 진이오빠, 규석오빠, DuC, Divyan, 장성오빠, 그리고 유일한 동기 혜원이, 승목오빠, 명한이, 임성이, 준현이) 감사합니다. 여러분들 덕분에 2년동안 무사히 석사 졸업을 맞이할 수 있었습니다. 그리고 연구활동에 많은 도움을 준 사랑하는 규석오빠 고마워! 오빠 덕분에 석사 생활 잘 마칠 수 있었어! 마지막으로 논문 심사에 참여해 주신 이영희 교수님과 국가보안연구소의 염용진 박사님께 감사드립니다. 저의 이 작은 결실이 그분들께 조금이나마 보답이 되기를 바랍니다.

이 력 서

이 름 : 문 혜 란

생 년 월 일 : 1983년 12월 18일

본 적 지 : 전라남도 해남군 황산면 관춘리 311번지

주 소 : 경기도 광주시 쌍령동 108-13 이스트빌 3동 402호

E-mail 주 소 : smartran@kaist.ac.kr

학 력

1999. 3. – 2002. 2. 경기여자고등학교

2003. 3. – 2007. 2. 서울여자대학교 정보보호공학 (B.S.)

1997. 3. – 1999. 2. 한국과학기술원 정보통신공학 (M.S.)

경 력

2005. 3. – 2005. 8. 한국정보보호진흥원 (KISA) 보안성평가 센터 평가 1팀 인턴

2008. 11. – 2009. 2. 한국전자통신연구원 (ETRI) 서비스융합표준팀 위촉연구원

학 회 활 동

1. **Hye-Ran Mun**, Kyu-Suk Han, and Kwang-Jo Kim, *Yet Another Intrusion Detection System against Insider Attacks*, Proc. of SCIS 2008, Jan. 22-25, 2008, Miyajaki, Japan
2. **문 혜 란**, 한 규 석, 김 광 조, *3G-WLAN 상호연동: EAP-AKA에 기반을 둔 새로운 인증 및 키 합의 프로토콜*, CISC-W'08 Proceedings, Dec. 6, 2008 고려대학교, 서울
3. **Hye-Ran Mun**, Kyu-Suk Han, and Kwang-Jo Kim, *3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA*, 2009 IEEE Wireless Telecommunication Symposium (WTS 2009), Apr. 22-25, 2009, Prague, Czech Republic

연 구 업 적

1. **문 혜 란**, *안전한 서비스 사업자 식별체계 요구사항 (표준안)*, 통합번호체계 (FoN) 포럼, Jan. 2009
2. 안 재 영, 박 웅, 심 은 석, **문 혜 란** 등, *NGN 식별체계 표준개발*, 한국전자통신연구소, 2009