3GPP-WLAN interworking 보안기술

신상욱 | 부경대학교 전자컴퓨터정보통신공학부
홍도원 | ETRI 정보보호연구단 정보보호기반그룹 정보보호기반연구팀

1. 서론

3GPP-WLAN(3rd Generation Partnership Project-Wireless Local Area Network) interworking[1]은 WLAN UE(User Equipment)에 의한 3GPP 시스템 내에서 자원이용과 서비스 접근을 의미한다. 3GPP-WLAN interworking의 목적은 3GPP 서비스와 기능을 WLAN 액세스 환경으로 확장함으로써, 3GPP 시스템에 무선 액세스 기술로 WLAN을 보완적으로 이용하는 것이다. 3GPP-WLAN interworking에서 3GPP 시스템의 기능들은 WLAN을 통해 또는 3GPP 액세스를 통해 사용되어질 수 있다. 3GPP-WLAN interworkg을 위해 다음의 6가지 시나리오를 고려한다.

(1) Common billing and customer care
(2) 3GPP system based access control and charging
(3) Access to 3GPP system PS based services
(4) Service continuity
(5) Seamless service provision
(6) Access to 3GPP CS services

이 중에서 시나리오 1~3은 Release 6에서 고려하고, 시나리오 4, 5는 향후에 고려될 것이다. 3GPP TS 23.234 Release 6에서는 3GPP-WLAN interworking을 위해 3GPP 시스템에서 다음 2가지 절차를 정의한다[1].

- 3GPP 시스템을 통해 인증되고 권한부여 되어지는 WLAN과 WLAN에 바로 연결된 로컬 IP 네트워크(인터넷)로의 액세스를 제공하는 WLAN 액세스, 인증, 권한부여
- WLAN UE가 3G 네트워크, 기업 인트라넷, 인터넷과 같은 외부 IP 네트워크로의 연결을 설정하도록 하는 외부 IP 네트워크 액세스

시나리오 3의 경우, 외부 IP 네트워크로의 액세스는 WLAN 액세스, 인증, 권한부여에 기술적으로 독립적이어야 한다. 그렇지만 3GPP WLAN interworking 시스템에서 외부 IP 네트워크로의 액세스는 WLAN 액세스, 인증, 권한부여가 먼저 완료된 이후에만 가능해야 한다. PDG(Packet Data Gateway)가 3GPP PS(Packet Switching) Domain 기반 서비스를 포함한 외부 IP 네트워크로의 액세스를 지원한다. 시나리오 2는 WLAN으로부터 인터넷/인트라넷으로의 직접적인 연결만을 제공한다.

본 고에서는 3GPP에서 표준 개발 중인 WLAN interworking에서의 보안기술을 분석한다. 먼저 3GPP-WLAN interworking을 위한 보안 요구사항

과 보안특성을 살펴본 후, 현재 고려 중인 3GPP-WLAN interworking을 위한 보안 메커니즘을 분석한다.

2. 3GPP-WLAN interworking 보안 요구사항과 보안특성

3GPP TS 23.234[1], TR 23.934[2] 문서에서는 그림 1, 그림 2, 그림 3의 3가지 3GPP-WLAN interworking 참조 모델을 제시하고 있다. 그림 1의 첫 번째 non-roaming 참조 모델에서 홈 네트워크가 액세스 제어와 터널 설정을 책임진다. 그림 2의 3GPP 홈 네트워크를 통해 제공되는 3GPP PS 기반 서비스 참조 모델 역시 홈 네트워크가 액세스 제어와 터널 설정을 책임지며, 트래픽은 방문 네트워크를 통해 라우트된다. 그림 3의 3GPP 방문 네트워크를 통해 제공되는 3GPP PS 기반 서비스 참조 모델에서 액세스 제어는 홈 네트워크에 의해 수행되지만 터널 설정의 권한 결정은 홈 네트워크로부터 수신된 정보를 이용하여 3GPP proxy AAA 서버에 의해 수행된다. 방문 네트워크의 PDG가 터널 설정에 참여한다.

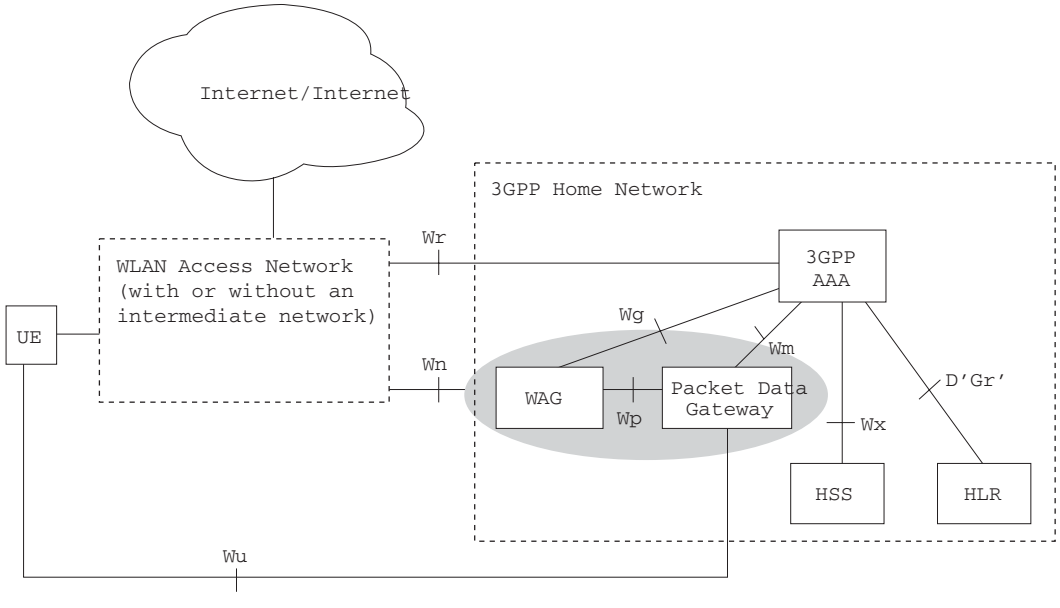


그림 1. Non roaming 참조 모델

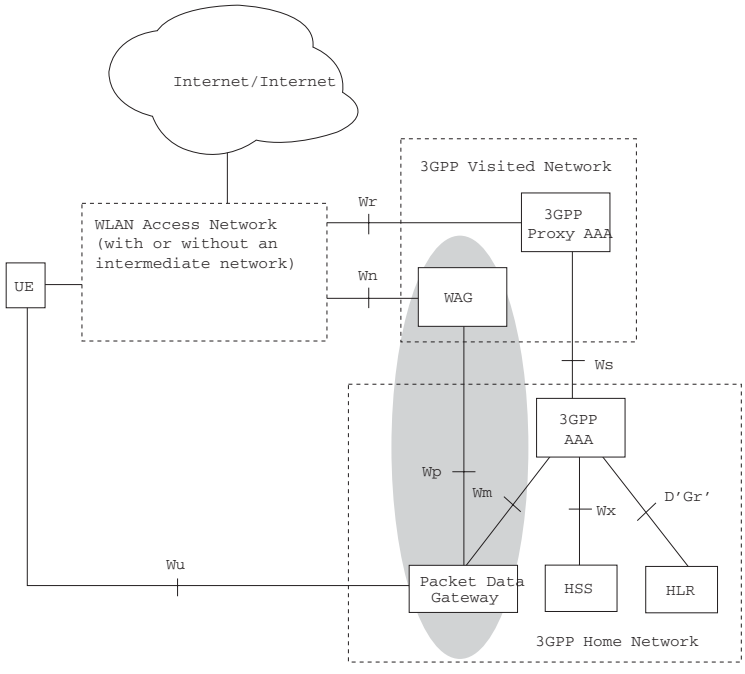


그림 2. roaming 참조 모델 – 3GPP 홈 네트워크를 통해 제공되는 3GPP PS 기반 서비스

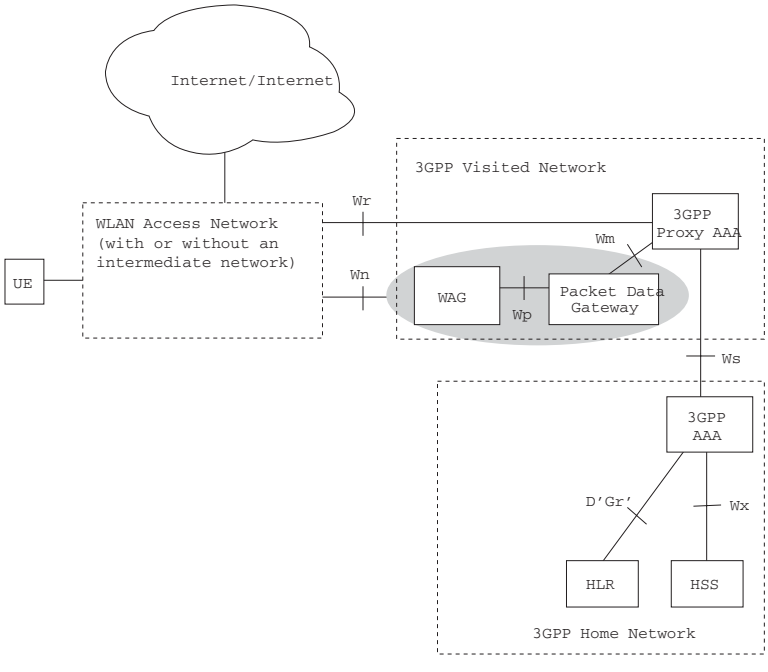


그림 3. roaming 참조 모델 – 3GPP 방문 네트워크를 통해 제공되는 3GPP PS 기반 서비스

3GPP-WLAN interworking에 관련되는 네트워크 개체는 다음과 같다[1][2].

- WLAN-UE : 3GPP interworking 목적을 위해 WLAN에 접근하는 3GPP 가입자에 의해 이용되는 USIM(Universial Subscriber Identity Module)을 포함한 UICC(USIM Integrated Circuit Card)를 가진 단말기이다. 예로 WLAN 카드와 UICC 카드 리더를 가진 노트북, PDA 등이 있다.
- 3GPP AAA proxy : WLAN과 3GPP AAA 서버 사이의 방문 네트워크에 위치하는 논리적인 proxy 기능 개체로, AAA 정보를 중계한다.
- 3GPP AAA 서버 : 3GPP 가입자의 홈 네트워크의 HLR(Home Location Register)/HSS (Home Subscriber Server)로부터 인증정보를 조회하여 3GPP 가입자를 인증한 후 WLAN에게 권한부여 정보를 전달한다.
- HLR/HSS : 3GPP 가입자의 홈 네트워크에 위치하며, 가입자에 대한 인증과 가입 데이터를 가진 개체이다.
- PDG(Packet Data Gateway) : 가입자가 3GPP PS 기반 서비스를 제공받기 위해 액세스하는 개체이다. 3GPP AAA로부터 수신된 정보를 가지고 권한부여하고 터널을 설정한다.

3GPP-WLAN interworking을 위한 보안 요구사항은 다음과 같다[4].

- 인증은 시도-응답(challenge-response) 프로토콜에 기반해야 하고, 상호인증이 지원되어야 한다.
- 가입자와 네트워크 인증을 위한 long-term security credential은 UICC 또는 SIM (Subscriber Identity Module) 카드에 안전하게 저장되어야 한다.
- EAP SIM[7]과 EAP AKA[6]가 AAA 서버와 WLAN UE 모두에 의해 지원되어야 한다.
- 시그널링과 사용자 데이터를 보호해야 한다.
- 사용자 신분 프라이버시를 제공해야 한다.
- 가입자는 적어도 WLAN 액세스와 같은 수준의 보안을 가져야 한다.
- 3GPP interworking을 위한 WLAN 인증 메커니즘은 적어도 USIM과 SIM 기반 액세스를 위한 인증과 같은 수준의 보안을 제공해야 한다.
- UE 개시 터널에 대해 데이터 출처 인증과 기밀성, 무결성이 제공되어야 한다.

3GPP TS 33.234 표준 문서에서는 WLAN과의 interworking 환경에서 다음의 보안특성(security feature)들이 제공되어야 한다고 정의하고 있다[4].

(1) 가입자와 네트워크의 인증 및 SA(Security Association) 관리

- WLAN-UE와 3GPP AAA 서버 사이의 WLAN 액세스 인증 시그널링은 EAP[5]에 기반해야 한다.
- WLAN 무선 인터페이스 상의 액세스 시그널링은 IEEE 802.11i 표준[8]을 따라야 한다.
- WLAN 액세스 네트워크와 3GPP AAA 서버 사이의 액세스 인증 시그널링은 DIAMETER[10], RADIUS[9] 프로토콜에 기반해야 한다.
- UE 개시 터널이 설정될 때 UE와 PDG의 두 종단은 상호인증해야 한다. 또한 터널 설정과정은 터널을 통해 전달되는 데이터의 기밀성과 무결성 보호를 사용되는 SA를 설정해야 한다.

(2) WLAN 액세스에서 재인증(re-authentication)

- WLAN 802.1x/AAA 재인증은 WLAN-UE와 AAA 서버 사이에서 수행된다.
- 3GPP AAA server는 특정 이벤트 또는 주기적으로 802.1x/AAA 재인증 과정을 개시할 수 있다.
- EAP SIM/AKA 재인증 과정이 네트워크와 WLAN UE 모두에서 구현되어야 한다.

(3) 사용자 신분 프라이버시

- 사용자 신분 프라이버시(익명성)은 영구 가입자 ID(IMSI(International Mobile Subscriber Identity) 또는 NAI(Network Access Identifier))를 평문으로 전송하는 것을 피하여 도청자가 현재의 통신 연결을 정당한 가입자와 연결시킬 수 없게 하는 것이다.
- AAA 서버가 생성하여 인증과정 중에 WLAN UE에게 분배한 임시 ID 또는 pseudonym의 사용에 기반하여 제공된다.

(4) 기밀성 보호

- 시나리오 2에서 기밀성 보호 : WLAN AN 링크 계층에서 기밀성 보호가 요구된다. 홈 네트워크는 WLAN AN에게 key material을 전송할 수 있어야 한다.
- 시나리오 3에서 기밀성 보호 : UE와 PDG 사이의 터널을 통해 전달되는 IP 패킷의 기밀성을 보호할 수 있어야 한다.

(5) 무결성 보호

- 시나리오 2에서 무결성 보호 : WLAN AN 링크 계층에서 무결성 보호가 요구된다. 홈 네트워크는 WLAN AN에게 key material을 전송할 수 있어야 한다.
- 시나리오 3에서 기밀성 보호 : UE와 PDG 사이의 터널을 통해 전달되는 IP 패킷의 무결성을 보호할 수 있어야 한다.

3. 3GPP-WLAN interworking 보안 메커니즘

3.1 인증과 키 일치

3GPP WLAN interworking 시스템은 먼저 WLAN UE와 3GPP AAA 서버 사이의 상호인증을 요구한다. 인증을 위한 long-term secret은 UICC 또는 SIM 카드에 저장될 것을 요구한다. 본 고에서 UICC의 경우만을 고려한다(SIM의 경우도 비슷하게 동작한다).

(1) USIM 기반 WLAN 액세스 인증

WLAN UE가 3GPP 서비스에 액세스하기 위해 인증과 키 일치과정을 먼저 완료해야 한다. 3GPP 표준 문서에서는 USIM 기반의 WLAN 액세스 인증을 그림 4와 같이 고려하고 있다. USIM 기반 인증은 EAP-AKA(Authentication and Key Agreement)[6]에 기반하여 다음과 같이 수행된다.

1. WLAN 기술을 사용하여 WLAN UE와 WLAN AN(Access Network) 사이에 연결을 설정한다(이 부분이 3GPP의 범위 밖이다).
2. WLAN AN은 WLAN UE에게 EAP Request/Identity 메시지를 전송한다. EAP 패킷은 WLAN 기술의 프로토콜 내에 캡슐화되어 WLAN 인터페이스 상으로 전송된다.

3. WLAN-UE는 EAP Response/Identity 메시지를 전송한다. WLAN-UE는 RFC 2486에 명시된 NAI(Network Access Identifier) 포맷을 따르는 자신의 ID(identifier) 정보를 전송한다. NAI는 이전의 인증과정에서 WLAN UE에게 할당된 임시 ID(pseudonym) 또는 첫 번째 인증의 경우 IMSI를 포함한다(IMSI로부터 NAI 포맷에 적합한 ID를 생성하는 것은 EAP/AKA에 정의되어 있다).
4. 메시지는 NAI의 realm 부분에 기반하여 적절한 3GPP AAA 서버로 라우트된다. 라우팅 경로는 하나 또는 여러 AAA 프락시(proxy)를 포함할 수도 있다.
5. 3GPP AAA 서버는 가입자 ID를 포함한 EAP Response/Identity 패킷을 수신한다.
6. 3GPP AAA 서버는 수신된 ID에 기반하여 EAP-AKA 인증을 위한 가입자를 식별한다. 그 후 3GPP AAA 서버는 가입자를 위해 활용가능한 사용하지 않은 인증 벡터(authentication vector)를 가지고 있는지 검사한다. 사용하지 않은 인증 벡터가 없는 경우, 새로운 인증 벡터들을 HSS/HLR로부터 가지고 온다. 임시 ID로부터 IMSI로의 매핑이 요구될 수도 있다.
7. 3GPP AAA 서버는 가입자의 WLAN 액세스 프로파일(profile)을 가지는지 검사한다. 가지지 않는다면, HSS로부터 프로파일을 검색한다. 3GPP AAA 서버는 가입자가 WLAN 서비스 사용권한을 가지는지 검증한다.
8. 새로운 keying material이 IK와 CK로부터 유도된다. 이 keying material은 EAP-AKA에 의해 요구된다. 다른 추가적인 keying material이 생성되어질 수도 있다. 새로운 pseudonym이 선택되어 생성된 keying material을 사용하여 보호되어질 수도 있다.
9. 3GPP AAA 서버는 RAND, AUTN, MAC (message authentication code), protected pseudonym, re-authentication ID를 WLAN-AN에게 EAP Request/AKA-Challenge 메시지로 전송한다. re-authentication ID의 전송은 3GPP 운영자 정책에 의존한다.
10. WLAN-AN은 EAP Request/AKA-Challenge 메시지를 WLAN-UE에게 전송한다.
11. WLAN-UE는 USIM에서 UMTS 알고리즘을 수행한다[3]. USIM은 AUTN이 정확한지 검증하여 네트워크를 인증한다. AUTN이 부정확하다면, 단말기는 인증을 거부한다. sequence number의 동기가 맞지 않다면, 단말기는 동기화 절차를 개시한다. AUTN이 정확하다면, USIM은 RES, IK, CK를 계산한다.

    WLAN UE는 계산된 IK와 CK로부터 요구되는 추가적인 keying material을 유도한다. 새롭게 유도된 keying material로 수신된 MAC을 검증한다.

    protected pseudonym이 수신되었다면, WLAN-UE는 미래의 인증을 위해 pseudonym을 저장한다.
12. WLAN UE는 새로운 keying material로 EAP 메시지에 대한 새로운 MAC 값을 계산한다. WLAN-UE는 계산된 RES와 MAC을 포함한 EAP Response/AKA-Challenge 메시지를 WLAN-AN에게 전송한다.
13. WLAN-AN은 EAP Response/AKA-Challenge 패킷을 3GPP AAA 서버에게 전송한다.

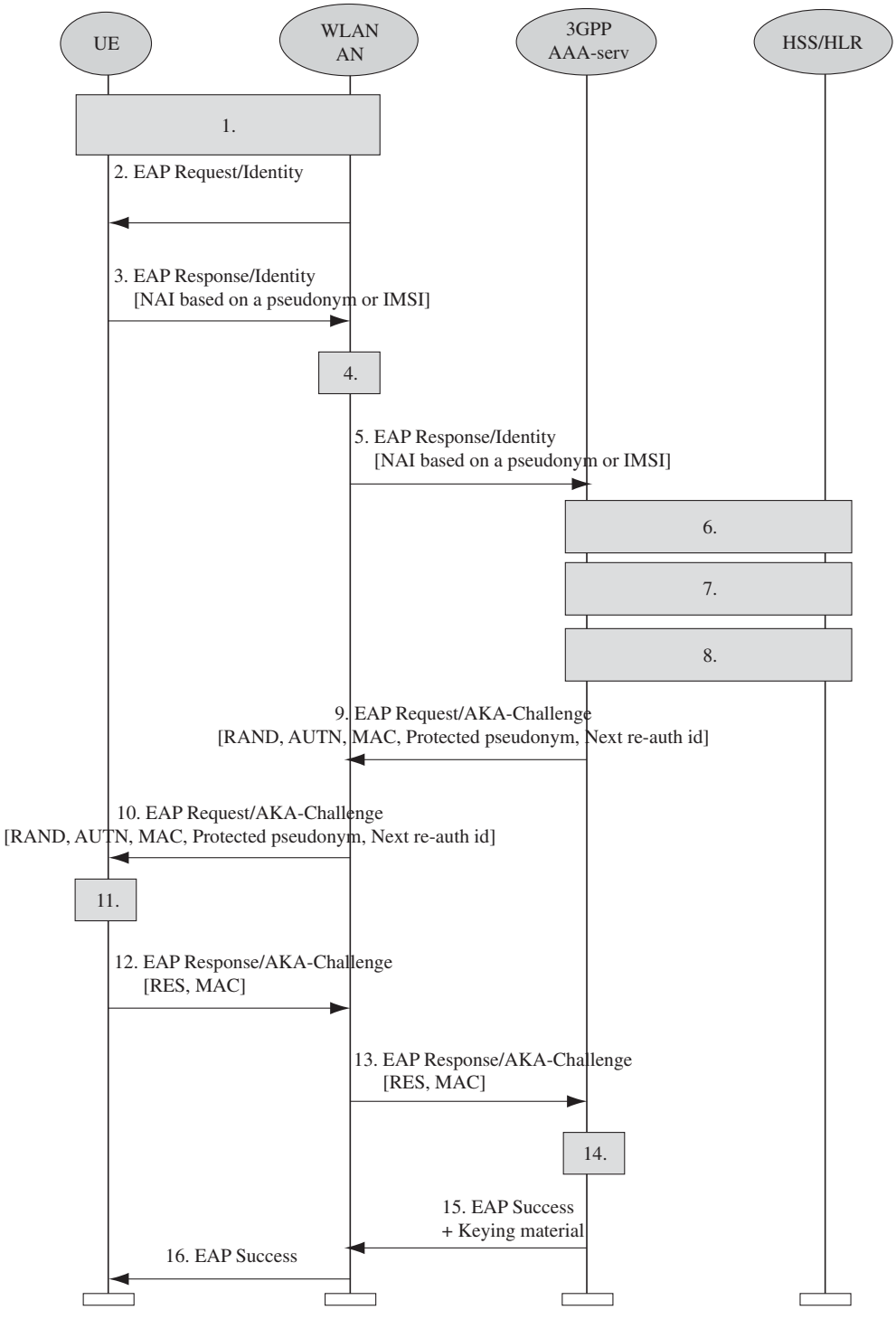


그림 4. EAP-AKA 기법에 기반한 인증

14. 3GPP AAA 서버는 수신된 MAC을 검사하고 수신된 RES를 XRES와 비교한다.
15. 모든 검사가 성공하면, 3GPP AAA 서버는 EAP Success 메시지를 WLAN-AN에게 전송한다. 다른 추가적인 keying material이 생성되었다면, 3GPP AAA 서버는 이 keying material을 기반이 되는 AAA 프로토콜 메시지에 포함시킨다. WLAN-AN은 인증된 WLAN-UE와 통신에 사용하기 위해 이 keying material을 저장한다.
16. WLAN-AN은 성공적인 인증을 EAP Success 메시지로 WLAN-UE에게 알린다. 이제 EAP AKA 교환이 성공적으로 완료되었고, WLAN-UE와 WLAN-AN은 keying material을 공유한다.

(2) WLAN 액세스에서 빠른 재인증 메커니즘

인증과정에 빈번하게 수행되어야 한다면 연결된 사용자 수가 많을 때 높은 네트워크 부하를 유발할 수 있으므로, 빠른 재인증(fast re-authentication)을 수행하는 것이 좀더 효율적이다. 따라서 재인증 과정은 이전의 완전한 인증(full authentication) 과정에서 유도된 키를 재사용함으로써 WLAN-AN이 완전한 인증을 수행하는 것보다 좀더 경량화된 과정으로 사용자를 인증하게 한다.

빠른 재인증 사용은 옵션이고 운영자의 정책에 의존하지만, EAP/AKA 구현은 빠른 재인증 메커니즘을 포함해야 한다. 빠른 재인증 과정은 [6]에 정의되어 있고, 3GPP-WLAN interworking에서의 동작 흐름은 그림 5와 같이 동작한다.

(3) UE 개시 터널 설정 메커니즘(시나리오 3)

- WLAN UE와 PDG는 IPsec SA(security association) 설정을 위해 IKEv2[11]를 사용한다.
- PDG 인증을 위해 인증서를 가진 공개키 서명기반 인증이 사용된다.
- IKEv2에서 EAP-AKA가 WLAN UE를 인증하기 위해 사용된다.
- IKEv2를 위해 다음의 프로파일이 사용되어야 한다.
  - 기밀성 : 128 비트 키를 이용한 AES CBC 모드
  - 유사 난수 발생기 : AES-XCBC-PRF-128
  - 무결성 : AES-XCBC-MAC-96

3.2 기밀성과 무결성 메커니즘

(1) 시나리오 2에서 기밀성과 무결성 메커니즘

링크 계층 기밀성 메커니즘과 무결성 메커니즘은 3GPP의 범위 밖이다. WLAN 링크계층이 IEEE 802.11을 사용하면, IEEE 802.11i의 기밀성 메커니즘과 무결성 메커니즘이 사용되어야 한다. 링크 계층 기밀성과 무결성 메커니즘을 위한 key material이 마스터 세션키 MSK로부터 어떻게 획득되는지는 [6]에 기술되어 있다. 또한 MSK의 생성 역시 [6]에 정의되어 있다.

(2) 시나리오 3에서 기밀성과 무결성 메커니즘

UE와 PDG 사이의 터널을 통해 전송되는 IP 패킷의 기밀성과 무결성은 IPsec ESP[12]에 의해 보호된다. IPsec ESP를 위해 다음의 프로파일이 사용되어야 한다.

- 기밀성 : 128 비트 키를 사용한 AES CBC 모드
- 무결성 : AES-XCBC-MAC-96
- 터널 모드가 사용되어야 한다.

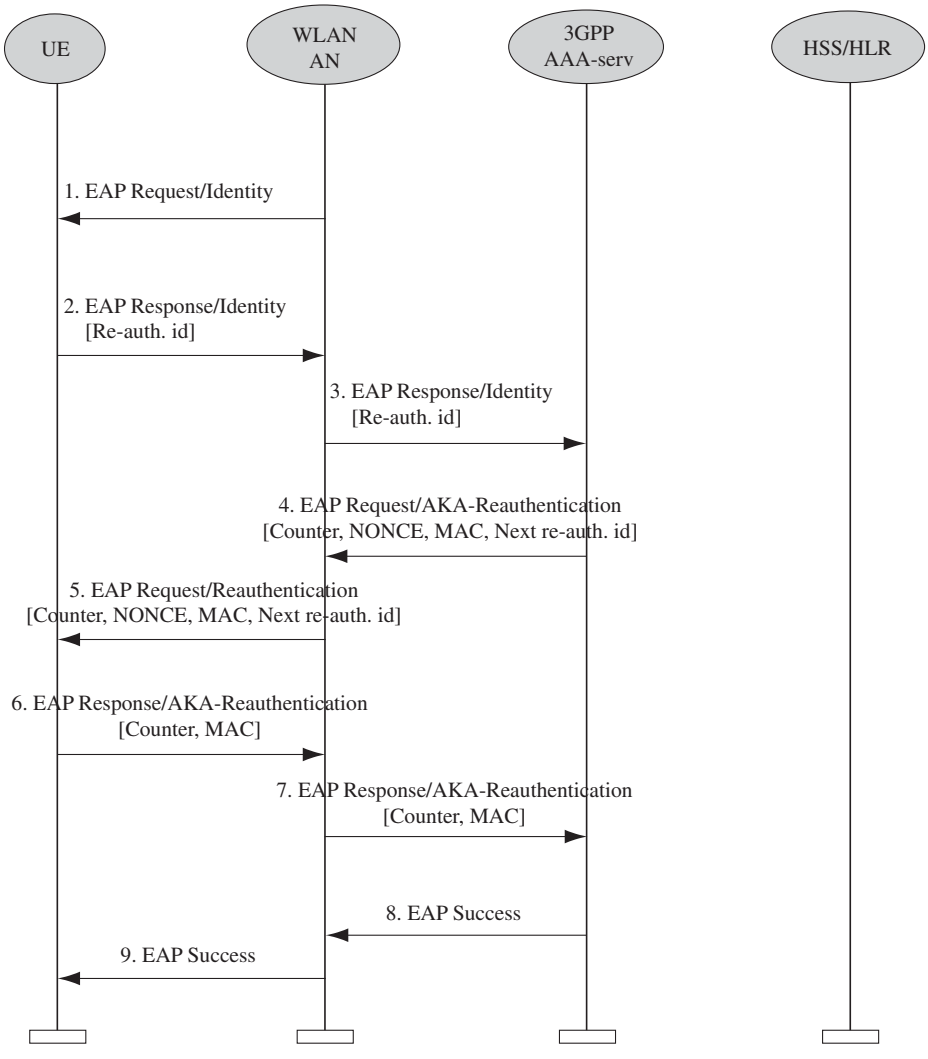


그림 5. EAP AKA 빠른 재인증

3.3 임시 ID(temporary identifier) 관리

임시 ID 또는 Pseudonym은 암호화된 IMSI 형태로 생성된다. 이를 위해 128비트 키를 가진 AES (Advanced Encryption Standard) ECB(Electronic Codebook) 모드가 사용된다. AES ECB 모드 암호화를 위해 평문의 길이는 16 바이트의 배수가 될 필요가 있다. 평문은 다음과 같이 형성된다.

1. IMSI의 각 digit를 표현하기 위해 4비트를 이용하여 Compressed IMSI가 생성된다. IMSI의 길이는 15 digit를 넘지 않는다. Compressed IMSI의 길이는 64비트이고 MSB들을 모두 1로 셋팅하여 채워진다. 즉,

   IMSI = 214070123456789(MCC = 214 ; MNC = 07 ; MSIN = 0123456789)

   Compressed IMSI = 0xF2 0x14 0x07 0x01

0x23 0x45 0x67 0x89

2. Compressed IMSI에 8 바이트의 난수를 연결함으로써 Padded IMSI가 생성된다.

128-비트 비밀키, Kpseu가 암호화를 위해 사용된다. 임의의 WLAN AAA 서버가 생성한 임시 ID로부터 임의의 WLAN AAA 서버가 영구 ID를 획득할 수 있도록 운영자 네트워크에서 모든 WLAN AAA 서버들이 동일한 비밀키를 가지도록 구성해야 한다. 그림 6은 Encrypted IMSI 생성과정을 보여준다.

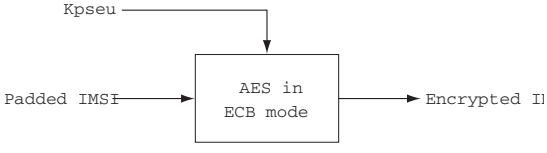
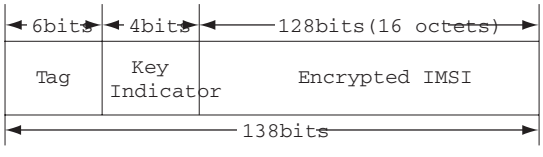


그림 6. Encrypted IMSI 생성

Encrypted IMSI가 생성되면, 다음의 필드들이 연결된다.

- Encrypted IMSI : AAA 서버가 임시 ID로부터 영구 ID를 얻을 수 있도록
- Key Indicator : 임시 ID를 수신한 AAA 서버가 Encrypted IMSI를 복호화하기 위한 적절한 키를 찾을 수 있도록
- Temporary identity Tag : ID를 임시 pseudonym 또는 재인증 ID로 표시하기 위해 사용된다. 태그는 EAP-SIM과 EAP-AKA를 위한 ID에 대해 달라야 한다.



임시 ID 생성에서 마지막 단계는 위에서 연결된 스트링을 BASE64 방법으로 프린터 가능한 스트링으로 변환하는 것이다. 연결된 스트링의 길이가 138비트이므로 결과적인 임시 ID의 길이는 23 문자이고 채워넣기는 필요없다.

4. 결론 및 향후 표준화 동향

3GPP-WLAN interworking은 3GPP 서비스와 기능을 WLAN 액세스 환경으로 확장함으로써, 3GPP 시스템에 무선 액세스 기술로 WLAN을 보완적으로 이용하는 것이다. 3GPP-WLAN interworking 보안에 관련된 표준화 작업은 3GPP TSG SA(Service & System Aspects) WG3에서 TS 33.234 문서를 중심으로 수행하고 있다. 현재 V6.0.0 문서가 작성되어 기본적인 보안 요구사항과 보안특성 그리고 세부적인 보안 메커니즘들을 정의하고 있으며, 본 고에서 이를 자세히 소개하였다.

향후 3GPP-WLAN interworking 보안에 관련하여 주로 다음의 사항들에 관해 표준화 작업이 이루어질 것으로 예상된다.

- Wa 인터페이스(WLAN 액세스 네트워크와 3GPP 네트워크 사이의 인터페이스)에 관한 위협요소들이 명확히 정의되지 않은 상태이므로 이 인터페이스 보호는 향후 계속적으로 연구되어질 것이다.
- 대부분의 WLAN 기술은 사용자 데이터에 대한 링크계층 보호를 제공하므로, 3GPP-WLAN interworking은 WLAN 기술에 의해 제공되는 링크계층 보호를 이용해야 한다. 따라서 링크계층 보호 요구사항이 정의되어야 한다.
- WLAN interworking 서비스에 액세스하기 위

해 UICC를 장착한 WLAN UE는 여러 물리적인 장치들로부터 카드를 소유한 장치와 WLAN 액세스를 제공하는 장치를 기능적으로 분리하는 WLAN-UE 기능적 분리(Functional Split)에 관련된 여러 가지 문제(기존의 UICC를 재사용 등)는 향후 지속적으로 연구되어질 것이다.

- UE 개시 터널 설정을 위한 보안 메커니즘은 여전히 작업 중이다. IKEv2의 사용, legacy VPN 클라이언트에 관련된 이슈들, 키 관리 등에 관한 사항들은 계속 연구 중이며, 특히 EAP-AKA의 사용에 대해서도 연구될 것이다. 이와 관련하여 ETRI 정보보호기반연구팀에서는 IKEv2의 사용 없이 효율적으로 UE 개시 터널을 설정할 수 있는 기법을 3GPP SA WG3 33차 회의에 기고하였다.

참고문헌

[1] 3GPP TS 23.234 "3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3GPP system to Wireless Local Area Network(WLAN) Interworking; System Description".

[2] 3GPP TR 23.934 "3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3GPP system to Wireless Local Area Network(WLAN) Interworking; Functional and architectural definition".

[3] 3GPP TS 33.102 "3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3G Security ; Security Architecture".

[4] 3GPP TS 33.234 "3rd Generation Partnership Project ; Technical Specification Group Services and System Aspects ; 3G Security ; Wireless Local Area Network(WLAN) Interworking security(Release 6)".

[5] draft-ietf-eap-rfc2284bis-06.txt, October 2003 : " PPP Extensible Authentication Protocol(EAP)".

[6] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication".

[7] draft-haverinen-pppext-eap-sim-12, October 2003 : "EAP SIM Authentication".

[8] IEEE802.11i/D7.0, October 2003 : "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11 : Wireless MediumAccess Control(MAC) and physical layer(PHY) specifications : Specification for Enhanced Security".

[9] RFC June 2000: "Remote Authentication Dial In User Service(RADIUS)".

[10] RFC September 2003 : "Diameter base protocol".

[11] draft-ietf-ipsec-ikev2-12.txt, January 2004, "Internet Key Exchange(IKEv2) Protocol".

[12] RFC 2406, November 1998, " IP Encapsulating Security Payload(ESP)".