情報保護學會論文誌
第14券 第3號, 2004. 6

3GPP-WLAN interworking에서의 효율적인 보안 메커니즘*

신 상 욱†‡

부경대학교 전자컴퓨터정보통신공학부

Efficient security mechanism in 3GPP-WLAN interworking

Sang-Uk Shin†‡

Division of Electronic, Computer and Telecommunication Engineering,
Pukyong National University

요 약

3GPP-WLAN(3rd Generation Partnership Project-Wireless Local Area Network) interworking은 WLAN UE(user equipment)에 의한 3GPP 시스템내에서 자원 이용과 서비스 접근을 의미하며, 3GPP 서비스와 기능을 WLAN 액세스 환경으로 확장함으로써, 3GPP 시스템에 무선 액세스 기술로 WLAN을 보완적으로 이용하는 것을 목적으로 한다. 본 논문에서는 3GPP-WLAN interworking에서 UE 개시 터널 설정을 위한 효율적인 메커니즘을 제안한다. 제안된 메커니즘은 UE와 3GPP AAA(Authentication, Authorization, Accounting) 서버 사이의 인증과 키 일치 과정에서 미리 분배된 비밀키에 기반한다. 따라서 UE에서 많은 계산을 필요로 하는 모듈러 지수승 연산과 공개키 서명 연산을 피할 수 있다. 또한 제안된 기법은 UE와 PDGW(Packet Data Gateway) 사이에 상호 인증과 세션 키 설정을 제공한다.

ABSTRACT

3GPP(3rd Generation Project Partnership)-WLAN(Wireless Local Area Network) interworking refers to the utilisation of resources and access to services within the 3GPP system by the WLAN UE(User Equipment) and user respectively. The intent of 3GPP-WLAN Interworking is to extend 3GPP services and functionality to the WLAN access environment. We propose an efficient mechanism for the setup of UE-initiated tunnels in 3GPP-WLAN interworking. The proposed mechanism is based on a secret key which is pre-distributed in the process of authentication and key agreement between UE and 3GPP AAA(Authentication, Authorization, Accounting) server. Therefore it can avoid modular exponentiation and public key signature which need a large amount of computation in UE. Also the proposed scheme provides mutual authentication and session key establishment between UE and PDGW(Packet Data Gateway).

Keywords: *3GPP, WLAN, authentication, key agreement, AKA, EAP*

Ⅰ. 서 론

3GPP-WLAN(3rd Generation Project Partnership-Wireless Local Area Network) interworking[1]은 WLAN UE(User Equipment)에 의한 3GPP 시스템내에서 자원 이용과 서비스 접근을 의미한다. 3GPP-WLAN interwork-

접수일 : 2004년 4월 14일 ; 채택일 : 2004년 6월 2일
* 이 논문은 2003년도 부경대학교 기성회 학술연구비에 의하여 연구되었음.
† 주저자, ‡ 교신저자 : shinsu@pknu.ac.kr

ing의 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.

3GPP의 표준 문서[1]는 3GPP-WLAN interworking을 위해 3GPP 시스템에서 다음 2가지 절차를 정의한다.

(1) 3GPP 시스템을 통해 인증되고 권한 부여되어지는 WLAN과 WLAN에 바로 연결된 로컬 IP 네트워크(인터넷)로의 액세스를 제공하는 WLAN 액세스, 인증, 권한 부여
(2) WLAN UE가 3G 네트워크, 기업 인트라넷, 인터넷과 같은 외부 IP 네트워크로의 연결을 설정하도록 하는 외부 IP 네트워크 액세스

두 번째 시나리오의 경우, 외부 IP 네트워크로의 액세스는 WLAN 액세스, 인증, 권한 부여에 기술적으로 독립적이어야 한다. 그렇지만 3GPP WLAN interworking 시스템에서 외부 IP 네트워크로의 액세스는 WLAN 액세스, 인증, 권한 부여가 먼저 완료된 이후에만 가능해야 한다. PDGW(Packet Data Gateway)가 3GPP PS(Packet Switching) Domain 기반 서비스를 포함한 외부 IP 네트워크로의 액세스를 지원한다. 첫 번째 시나리오는 WLAN으로부터 인터넷/인트라넷으로의 직접적인 연결만을 제공한다.

본 논문에서는 3GPP 시스템과 WLAN 사이의 interworking에서 보안에 대해 분석한다. 먼저 3GPP WLAN interworking 시스템에서 제공되는 보안 메커니즘을 분석한 후, 두 번째 시나리오에 초점을 맞추어 좀더 효율적인 보안 메커니즘을 제안한다. 3GPP 표준 문서[4]에 의하면, WLAN UE와 PDGW 사이의 보안을 위해 WLAN UE와 3GPP AAA(Authentication, Authorization, Accounting) 서버 사이의 인증 과정을 거친 후 WLAN UE와 PDGW간의 데이터 보호를 위해 IKEv2 (Internet Key Exchange version 2)[9] 프로토콜을 사용하여 WLAN UE와 PDGW 사이에 SA (Secuerity Association)을 설정하여 IPsec ESP(Encapsulating Security Payload)[8] 터널(tunnel)을 적용한다. 이 경우 WLAN UE와 PDGW 사이에 복잡한 IKEv2 프로토콜 수행을 필요로 한다. 따라서 본 논문에서는 복잡한 IKEv2 수행을 하지 않고 WLAN UE와 PDGW 사이에 SA를 설정할 수 있는 효율적인 기법을 제안한다.

먼저 2장에서는 3GPP-WLAN interworking을 위한 보안 아키텍쳐와 보안 요구 사항을 소개하고, 3장에서 3GPP 표준 문서에서 고려하고 있는 보안 메커니즘을 기술한 후, 두 번째 시나리오에서 WLAN UE 개시 터널 설정을 위한 효율적인 보안 메커니즘을 제안하고 분석한다. 마지막 4장은 결론이다.

II. 3GPP-WLAN interworking을 위한 보안 아키텍쳐와 보안 특성

3GPP 표준 문서에서는 그림 1, 그림 2, 그림 3의 3가지 3GPP-WLAN interworking 참조 모델을 제시하고 있다[1][2]. 첫 번째 non-roaming 참조

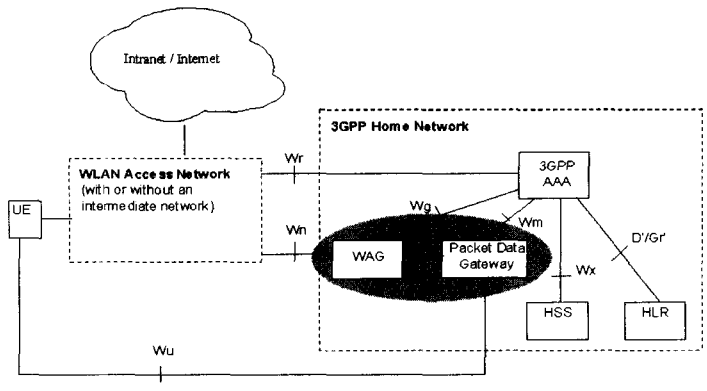


그림 1. Non roaming 참조 모델

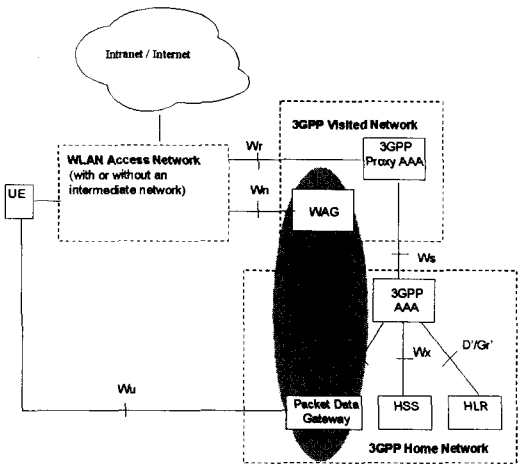


그림 2. roaming 참조 모델 - 3GPP 홈 네트워크를 통해 제공되는 3GPP PS 기반 서비스

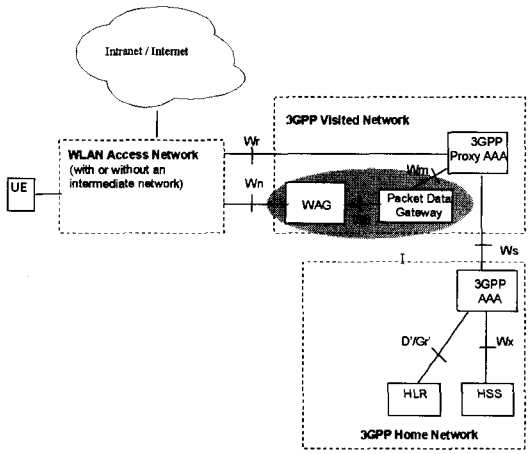


그림 3. roaming 참조 모델 - 3GPP 방문 네트워크를 통해 제공되는 3GPP PS 기반 서비스

모델에서는 홈 네트워크가 액세스 제어와 터널 설정을 책임진다. 3GPP 홈 네트워크를 통해 제공되는 3GPP PS 기반 서비스 참조 모델 역시 홈 네트워크가 액세스 제어와 터널 설정을 책임지며, 트래픽은 방문 네트워크를 통해 라우트된다. 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 PDGW가 터널 설정에 참여한다.

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 인증 정보를 조회하여 3GPP 가입자를 인증한 후 WLAN에게 권한 부여 정보를 전달한다.
- HLR/HSS : 3GPP 가입자의 홈 네트워크에 위치하며, 가입자에 대한 인증과 가입 데이터를 가진 개체이다.
- PDGW : 가입자가 3GPP PS 기반 서비스를 제공받기 위해 액세스하는 개체이다. 3GPP AAA로부터 수신된 정보를 가지고 권한 부여하고 터널을 설정한다.

3GPP-WLAN interworking에서 중요한 보안 요구 사항은 다음과 같다[4].

- 인증은 시도-응답(challenge-response) 프로토콜에 기반해야 하고, 상호 인증이 지원되어야 한다.
- 가입자와 네트워크 인증을 위한 long-term security credential은 UICC 또는 SIM (Subscriber Identity Module)에 안전하게 저장되어야 한다.
- 가입자는 적어도 WLAN 액세스와 같은 수준의 보안을 가져야 한다.
- 시그널링과 사용자 데이터를 보호해야 한다.
- 사용자 신분 프라이버시를 제공해야 한다.

3GPP 표준 문서에서는 WLAN과의 interworking 환경에서 다음의 보안 특성(security

feature)들이 제공되어야 한다고 정의하고 있다[4].

(1) 가입자와 네트워크의 인증 및 SA 관리
- IEEE 802.11i[10]와 같은 WLAN 무선 인터페이스 보안, EAP(Extensible Authentication Protocol)[7], DIAMETER[12] 또는 RADIUS[11] 프로토콜 등을 사용하여 WLAN-UE와 3GPP AAA 서버 사이의 상호 인증을 제공한다.

(2) 기밀성과 무결성 보호
- 네트워크 개체들 사이에 기밀성 보호가 제공되어야 하고, 첫 번째 시나리오에 대해서는 아직 정의되지 않았고, 두 번째 시나리오에 대해서는 UE와 PDGW 사이에 터널을 통해 전달되는 IP 패킷의 기밀성을 제공해야 하고, 이를 위해 IPsec ESP의 적용을 고려하고 있다.
- 무결성 보호 역시 기밀성 보호와 유사하게 제공되며, UE와 PDGW 사이에 터널을 통해 전달되는 IP 패킷에 IPsec ESP를 적용하여 무결성 보호를 제공할 것을 고려하고 있다.

(3) 사용자 신분 프라이버시
- 사용자 신분 프라이버시(익명성)는 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 인증 과정 중에 WLAN UE에게 분배한 임시 ID 또는 pseudonym의 사용에 기반하여 제공된다.

III. 3GPP-WLAN interworking에서의 효율적인 보안 메커니즘 분석 및 개선

3.1 WLAN 액세스 인증과 키 일치, 그리고 UE 개시 터널 설정 메커니즘

앞에서 기술한 것처럼 3GPP WLAN interworking 시스템은 먼저 WLAN UE와 3GPP AAA 서버 사이의 상호 인증을 요구한다. 인증을 위한 long-term secret은 UICC 또는 SIM 카드에 저장될 것을 요구한다. 이 논문에서 UICC의 경우만을 고려한다(SIM의 경우도 비슷하게 동작 가능하다).

WLAN UE가 3GPP 서비스에 액세스하기 위해 인증과 키 일치 과정을 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 수행된다.

WLAN UE와 3GPP AAA 서버 사이의 상호 인증이 완료된 후, WLAN UE가 3GPP PS 기반 서비스를 이용할 경우(1장의 시나리오 2에 해당) WLAN UE는 PDGW에 액세스하여 서비스를 제공받는다. 이때 UE와 PDGW 사이에 전송되는 데이터는 기밀성과 무결성이 보호되어야 한다. 이를 위해 3GPP 표준 문서에서는 IPsec의 적용을 고려한다. 먼저 WLAN UE는 PDGW와 IKEv2 프로토콜을 수행하여 IPsec SA를 설정한다. 이때 PDGW를 인증하기 위해 공개키 서명 기반 인증이 사용되며, WLAN UE를 인증하기 위해 IKEv2내에 EAP-AKA가 사용된다.

3.2 효율적인 UE 개시 터널 설정 메커니즘

위에서 기술한처럼 WLAN UE와 PDGW 사이의 터널 설정을 위해 IKEv2 수행으로 인한 복잡한 공개키 연산이 WLAN UE에서 수행되어야 하고, IKEv2내에서 EAP-AKA 수행을 위해 6번의 메시지 교환이 필요로 하므로 WLAN UE와 PDGW 사이의 인증과 키 분배를 위해 많은 오버헤드가 부가된다.

본 논문에서는 이러한 복잡한 과정없이 WLAN UE와 3GPP AAA 서버 사이의 인증과 키 일치 과정에서 분배된 키를 이용한 효율적인 보안 메커니즘을 제안한다.

이를 위해 3GPP 표준 문서의 WLAN UE와 3GPP AAA 서버 사이의 인증 과정(그림 4)을 다음과 같이 수정한다.

먼저 그림 4의 세번째 단계에서 EAP Response/Identity 메시지에 UE가 3GPP PS 기반 서비스의 사용을 알리는 지시자 "Service"를 포함시킨다. 그림 4의 단계 6에서 추가적으로 "Service" 지시자를 검사한 후, 3GPP PS 기반 서비스를 위한 키 "PS_Key"를 생성한다. "PS_Key"는 다른 keying material인 IK, CK와 비슷하게 3GPP MILENAGE 알고리즘[5]을 사용하여 long-term secret과 RAND, AUTN에 기반하여 생성된다. 단계 11번에

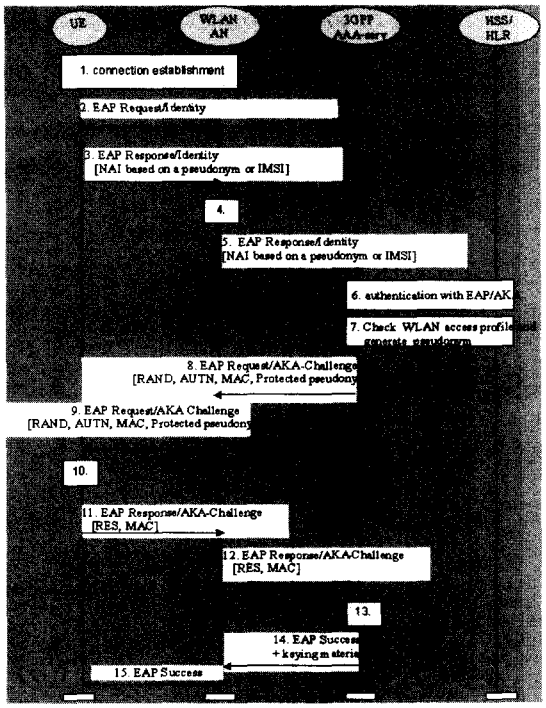


그림 4. EAP AKA에 기반한 인증

서 WLAN UE는 필요한 keying material인 IK, CK와 함께 "PS_Key"를 같은 방법으로 유도한다.

WLAN UE와 3GPP AAA 서버 사이의 인증과 키 일치 과정이 완료된 후, WLAN UE가 3GPP PS 기반 서비스를 제공받기 위해 PDGW에 액세스 한다. 이를 위한 효율적인 보안 메커니즘은 그림 5와 같다.

1. UE는 터널 설정을 위한 요청 메시지, "Tunnel Setup Request"를 전송한다. 이 메시지는 앞의 UE와 3GPP AAA 서버 사이의 인증 과정에서 할당된 pseudonym에 기반한 NAI와 UE에 의해 랜덤하게 생성된 nonce N_UE를 포함한다.
2. PDGW는 수신된 NAI의 realm 부분에 기반하여 적절한 3GPP AAA 서버를 찾아 "PS_Key Request" 메시지를 전달한다.
3. 3GPP AAA 서버는 WLAN 액세스 인증 과정에서 생성된 가입자의 PS_Key를 PDGW에게 전달한다.
4. PDGW는 PS_Key, NAI, N_UE 그리고 자신이 생성한 랜덤 nonce N_PDGW를 prf(pseudo-random function)에 적용하여 마스터 키 MK를 생성한다. 생성된 MK를 이용하여 암호화와 무결성 보호를 위한 키 MK_C와 MK_I를 유도한다.

$$MK = prf(PS\_Key, NAI \mid N\_UE \mid N\_PDGW)$$

$$(MK\_C, MK\_I) = prf+(MK, N\_PDGW \mid N\_UE \mid NAI)$$

여기서 prf는 암호학적으로 안전한 유사 랜덤 함수이고, prf+는 prf를 반복 적용하여 prf 알고리즘의 출력보다 더 큰 keying material을 생성한다. prf와 prf+ 함수는 IKEv2에 정의된 함수들을 적용하는 것이 가능하다. 또한 '|' 기호는 두 비트 스트링의 연결(concatenation)을 의미한다.

유도된 MK_I를 이용하여 인증 정보 Auth_PDGW를 생성하여 터널 설정 응답 메시지 "Tunnel Setup Response"를 UE에게 전송한다.

$$Auth\_PDGW = MAC(MK\_I, NAI \mid N\_UE \mid N\_PDGW)$$

여기서 MAC은 암호학적으로 안전한 메시지 인증 코드 알고리즘으로, HMAC-SHA1을 고려할 수 있다.

5. UE는 PDGW와 동일한 방법으로 마스터 키 MK를 생성한 후 암호화와 무결성을 위한 키 MK_C와 MK_I를 유도한다.

$$MK = prf(PS\_Key, NAI \mid N\_UE \mid N\_PDGW)$$

$$(MK\_C, MK\_I) = prf+(MK, N\_PDGW \mid N\_UE \mid NAI)$$

PDGW를 인증하기 위해 수신된 Auth_PDGW를 검증한다. 검증이 성공하면, MK_I를 이용하여 자신의 인증 정보 Auth_UE를 생성한 후, MK_C

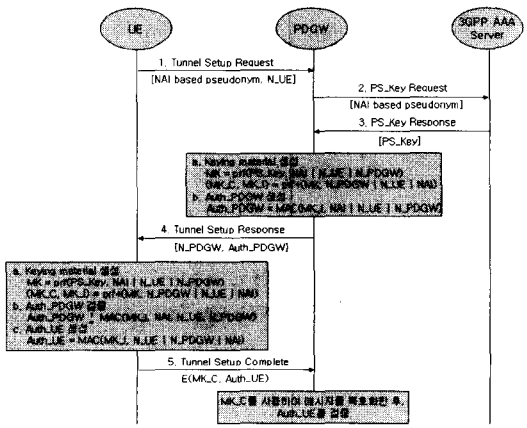


그림 5. UE 개시 터널 설정 메커니즘

로 암호화하여 "Tunnel Setup Complete" 메시지를 PDGW에게 전송한다.

Auth_UE = MAC(MK_I, N_UE | N_PDGW | NAI)

6. PDGW는 수신된 메시지를 MK_C로 복호화한 후, Auth_UE를 검증한다. 검증이 성공하면, UE의 액세스는 허가된다.

3.3 제안된 메커니즘 분석

제안된 프로토콜은 3GPP 표준 문서에서의 인증 및 키 일치 절차를 최소한으로 변경하여 수행된다. 그림 4의 EAP AKA 기반 인증 메커니즘에서 수정된 부분은 단계 3에서 파라메터 "Service"의 추가와 단계 6에서 "PS_Key"의 생성, 그리고 단계 11에서 UE가 "PS_Key"를 생성하는 부분으로, 최소한의 통신 오버헤드와 계산 오버헤드만을 부가한다.

인증 완료 후에 수행되는 UE 개시 터널 설정 메커니즘의 경우, 3GPP 표준 문서에서는 IKEv2를 이용하여 SA를 설정한 후 IPsec ESP의 적용을 고려한다. IKEv2 수행에서 Diffie-Hellman 키 교환을 위해 모듈러 지수 연산이 필요하며, 또한 계산량이 많은 공개키 서명 기반 인증이 요구된다. 또한 UE와 PDGW 사이의 6번의 메시지 교환을 요구한다.

제안된 프로토콜은 앞의 인증 과정에서 추가적으로 생성한 "PS_Key"에 기반하여 필요한 keying material을 유도한다. 따라서 계산량이 많은 모듈러 지수승과 공개키 서명 기반의 인증을 피할 수 있다. 제안된 프로토콜에서 keying material 유도를 위해 사용되는 prf와 prf+ 함수는 암호학적으로 안전한 임의의 유사 랜덤 함수로, IKEv2에 정의된 함수들을 적용할 수 있다. 제안된 프로토콜에서 UE 개시 터널 설정을 위해 5개의 메시지가 전달되며, 3개의 메시지만이 무선 인터페이스 상에 전달된다.

제안된 기법은 다음의 안전성 요구 사항을 만족한다.

(1) 사용자 프라이버시 보호 : 그림 5의 단계 1에서 pseudonym에 기반한 NAI를 전달함으로써 사용자 프라이버시를 제공한다. 사용되는 pseudonym에 기반한 NAI 정보는 WLAN UE와 3GPP AAA 서버 사이의 인증 과정에서 분배된 값이다.

(2) 상호 인증 : 단계 4에서 UE가 Auth_PDGW 검증을 통해 PDGW를 인증한다. Auth_PDGW 계산에 nonce N_UE가 포함됨으로써 freshness가 보장된다. 또한 NAI가 포함됨으로써 공유 비밀키 PS_Key와 사용자 신분간의 정확한 binding이 보장된다. PDGW는 단계 5에서 challenge N_PDGW에 대한 UE의 응답인 Auth_UE 검증을 통해 UE를 인증한다. Auth_UE의 freshness는 N_PDGW에 의해 보장된다.

(3) 세션 키 설정 : UE와 PDGW는 세션 마스터 키 MK를 생성한다. 이 키를 사용하여 두 개체 사이의 보안 터널을 위한 세션키들을 유도한다. MK는 무선 구간으로 전달되지 않고, UE와 PDGW에 의해 공유된 비밀키 PS_Key와 nonce에 기반하여 유도된다. 따라서 PS_Key를 알지 못하는 공격자가 MK를 획득하기 위한 최선의 방법은 랜덤한 추측 공격이다. MK의 freshness와 랜덤성은 nonce N_UE와 N_PDGW의 freshness 그리고 적용된 prf의 암호학적 성질에 의해 보장된다.

(4) Known-Key 공격에 대한 안전성 : Known-Key 공격은 과거의 세션키를 아는 공격자가 사용자의 long-term 비밀키 또는 현재 세션키를 알아내기 위해 시도하는 공격이다. 제안된 기법에서는 과거 세션에 대한 키들 (MK_{old}, MK_I_{old}, MK_C_{old})이 노출되더라도, 적용된 prf의 성질에 의해 공격자는 PS_Key에 관한 어떠한 정보도 얻지 못한다. 또한 PS_Key와 랜덤한 nonce 값들을 prf에 적용하여 각 세션에 대한 세션키를 유도하기 때문에 과거 세션키들을 통해 현재 세션키들에 관해 어떤 정보도 얻지 못한다. 따라서 제안된 기법은 Known-Key 공격에 관해 안전하다.

(5) Forward secrecy : forward secrecy는 공격자가 사용자의 long-term 비밀키를 알게되더라도 이를 통해 과거의 세션키를 구하는 것이 불가능하다는 것을 말한다. 일반적으로 forward secrecy를 제공하는 대칭키 기반 키 설정 프로토콜을 설계하는 것은 매우 어려운 문제이다. 제안된 UE 개시 터널 설정 메커니즘에서 PS_Key의 노출은 모든 세션키들을 손상시킨다. 하지만 3GPP-WLAN interworking에서 WLAN 액세스 인증마다 서로 다른 랜덤한

PS_Key들이 생성되므로 하나의 PS_Key 노출에 의한 과거 세션키들의 손상은 그 PS_Key가 사용된 세션들로만 제한된다. 따라서 제안된 UE 개시 터널 설정 메커니즘은 제한적인 forward secrecy를 제공한다.

(6) interleaving 공격 : interleaving 공격은 공격자의 조정 하에서 다수의 프로토콜이 중첩되어 수행되는 공격으로, 병렬 세션들로부터 정보들의 선택적인 조합을 수반하는 위장 또는 다른 속임이다. interleaving 공격을 성공적으로 수행하기 위해서는 공격자가 다른 프로토콜 수행에서 메시지들간에 순차적으로 의존적인 관계를 이용해야 한다. 제안된 방식은 기존의 방식에 비해 WLAN 액세스 인증과 매우 밀접하게 연관되어 수행된다. WLAN 액세스 인증 과정에서 분배된 PS_Key에 기반하여 UE 개시 터널을 설정한다. 하지만 공격자는 WLAN 액세스 인증 과정에서 제안된 UE 개시 터널 설정 메커니즘을 수행하기 위해 필요한 어떠한 정보도 얻을 수 없다. UE 개시 터널 설정 메커니즘에서 사용자 신분 확인을 위해 필요한 NAI based pseudonym은 WLAN 액세스 인증 과정(그림 4)의 단계 9에서 암호화되어 전송되며, 또한 인증과 세션키 유도를 위해 필요한 PS_Key 값은 무선 인터페이스 상으로 전송되지 않고 UE에서 계산된다. 그리고 두 프로토콜에서 인증을 위해 사용되는 인증값들은 다른 키에 의존하여 계산된다. 즉, 첫 번째 프로토콜에서 MAC과 RES는 UICC에 저장된 long-term 비밀키에 의존하여 계산되며, 두 번째 프로토콜에서 Auth_UE와 Auth_PDGW는 PS_Key에 기반하여 계산된다. 따라서 공격자가 두 프로토콜 수행에서 메시지들의 적절한 조합이나 메시지들 사이의 어떤 관계를 이용한 공격을 수행하는 것이 불가능하다.

부정한 네트워크 개체에 의한 재연 공격(replay attack)은 UE와 PDGW에 의해 매 세션마다 새롭게 생성되는 nonce에 의해 방지된다. 또한 위장 방지는 위의 안전성 요구 사항으로부터 쉽게 유도된다. 네트워크 개체에 대한 honesty 가정이 성립하면, UE의 인증은 서비스 제공자에게 정당한 사용자가 서비스를 제공받는다는 것을 보장한다. 또한 PS_Key의 비밀성은 불법적인 사용자가 기존의 세션을 하이재킹할 수 없다는 것을 보장한다.

제안된 프로토콜의 안전성은 사용된 prf, prf+, MAC 함수의 성질에 의존한다. 이들 함수들은 인증, 세션의 freshness, 세션 키의 freshness와 랜덤성을 보장하도록 선택되어야 한다. prf와 prf+ 함수로 IKEv2에 정의된 함수들을 고려할 수 있으며, MAC 함수로 HMAC-SHA1을 고려할 수 있다.

IV. 결 론

본 논문에서는 3GPP 시스템과 WLAN 사이의 interworking에서 보안에 대해 분석한 후, WLAN UE가 3GPP PS 기반 서비스에 액세스하는 경우에 초점을 맞추어 좀더 효율적인 보안 메커니즘을 제안하였다. 3GPP 표준 문서에 의하면, WLAN UE와 PDGW 사이의 보안을 위해 WLAN UE와 3GPP AAA 서버 사이의 인증 과정을 거친 후 WLAN UE와 PDGW간의 데이터 보호를 위해 IKEv2 프로토콜 사용하여 WLAN UE와 PDGW 사이에 SA을 설정하여 IPsec ESP tunnel을 적용한다. 이 경우 WLAN UE와 PDGW 사이에 복잡한 IKEv2 프로토콜 수행을 필요로 한다. 따라서 본 논문에서는 복잡한 IKEv2 수행을 하지 않고 WLAN UE와 3GPP AAA 서버 사이의 인증과 키 일치 과정에서 분배된 키를 이용하여 WLAN UE와 PDGW 사이의 상호 인증과 키 일치를 제공하는 효율적인 보안 메커니즘을 제안하였다.

참 고 문 헌

[1] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description"

[2] 3GPP TR 23.934: "3GPP system to WLAN Interworking; Functional and architectural definition"

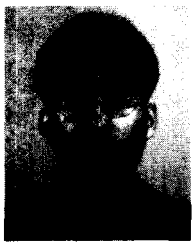
[3] 3GPP TS 33.102: "3G Security; Security Architecture"

[4] 3GPP TS 33.234: "WLAN Interworking Security"

[5] 3GPP TR 35.205: "3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key

generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General"
[6] draft-arkko-pppext-eap-aka-11, October 2003: "EAP AKA Authentication"
[7] draft-ietf-eap-rfc2284bis-06.txt, October 2003: "PPP Extensible Authentication Protocol (EAP)"
[8] draft-ietf-ipsec-esp-v3-06.txt, July 2003: "IP Encapsulating Security Payload (ESP)"
[9] draft-ietf-ipsec-ikev2-12.txt, January 2004: "Internet Key Exchange (IKEv2) Protocol"
[10] IEEE Std 802.11i/D2.0, March 2002: "Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security"
[11] RFC 2865, June 2000: "Remote Authentication Dial In User Service (RADIUS)"
[12] RFC 3588, September 2003: "Diameter base protocol".

〈著者紹介〉



신 상 욱 (Sang-Uk Shin) 정회원
1995년 2월 : 부경대학교 전자계산학과(학사)
1997년 2월 : 부경대학교 전자계산학과(석사)
2000년 2월 : 부경대학교 전자계산학과(박사)
2000년 4월~2003년 8월 : 한국전자통신연구원 선임연구원
2003년 9월~현재 : 부경대학교 전자컴퓨터정보통신공학부 전임강사
〈관심분야〉 암호 이론, 정보보호, 이동통신 정보보호