주 제

WCDMA에서의 IP Security 기술 동향 분석

LG전자 이상윤, 김형택, 연철흠

차 례

요 약

본 논문은 비동기 방식의 WCDMA 시스템에서 특히 IP Multimedia Subsystem의 도입과 함께 IP Security 기술이 어떤 형식으로 적용되어 표준화되고 있는지 기술동향을 알아보고자 한다. 현재 WCDMA 시스템에서의 IP Security 기술은 일반 네트워크 영역 보안 분야와 WLAN Inter-working 분야 그리고 IMS 보안 분야에 적용되고 있다. 가장 기본이 되는 네트워크 영역 보안은 3GPP 표준화 규격인 TS 33.210에 정의되어 있고, 이를 바탕으로 WLAN Inter-working 분야에서는 IKE version 2가 추가되었으며, IMS 보안 분야에서는 네트워크 영역 보안에서 정의된 Z 인터페이스를 이용하여 해당 트래픽에 대한 보안을 수행한다.

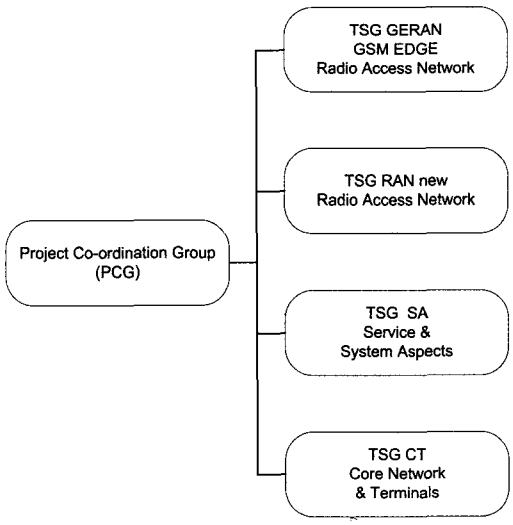
Ⅰ. 서 론

비동기 방식의 3세대 이동통신 시스템은 3GPP (3rd Generation Partnership Project)에 의해 표준화되고 있다. 3GPP는 Radio Access Network, Core Network, Terminal 그리고 관련 서비스와 시스템 규격 등 다양한 부분에 있어서 표준화를 정의하고 있고, 많은 부분 이미 기존에 표준화된 프로토콜들을 이용하고 있다. 특히, Core Network 분야의 기술발전으로 3GPP 이동통신망에서는 Internet 망에서 표준화된 다양한 프로토콜을 활용하여 3GPP 표준화 과정에 많이 활용하고 있다.

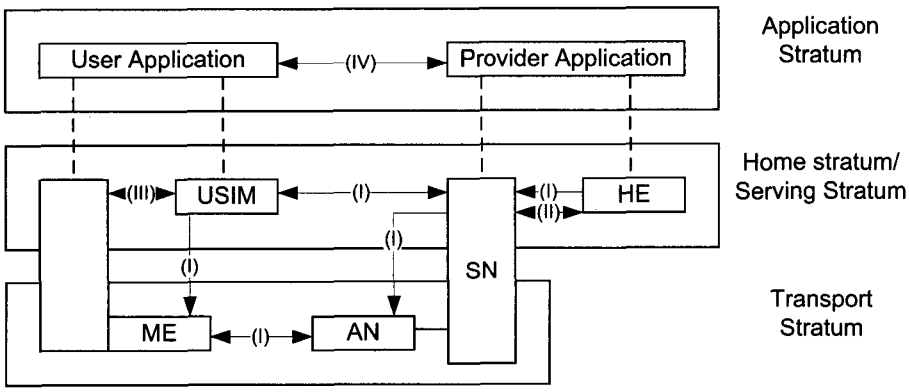
3GPP는 (그림 1)에 도시한 바와 같이 4개의 TSG(Technical Specific Group)로 구성된다.[1]. TSG GERAN은 GSM/EDGE의 무선 구간의 표준을 제정하고, TSG RAN은 FDD TDD 두 가지 모드에 대해서 UTRA(Universal Terrestrial Radio Access)

network의 인터페이스, 요구되는 사항, 그리고 기능 정의를 담당하고 있으며, TSG SA는 3GPP 표준에 기초하여 시스템이 지원 가능한 서비스와 전체적인 시스템 구조를 정의한다. 마지막으로 TSG CT에서는 3GPP 시스템의 Core Network 파트와 단말 인터페이스 및 단말 기능의 표준화를 담당하고 있다.

WCDMA 시스템의 표준화에서 중요한 특징 중의 하나는 통신보안의 강화다. 기존 GSM 시스템에서부터 통신보안은 중요한 이슈중의 하나였고, 표준화가 진행되면서 새로운 프로토콜들과 더 강화된 기술들이 포함되었다. 보안 분야의 표준화는 TSG SA에서 이루어지는데, 5개 WG 중 SA WG 3 Security 에서 표준작업이 진행 중이다.



(그림 1) 3GPP TSG



HE : Home Environment
ME : Mobile Equipment
SN : Serving Network
USIM : User Services Identity Module

Network access security (I)
Network domain security (II)
User domain security (III)
Application domain security (IV)
Visibility and configurability of security (V)

(그림 2) 3GPP 보안 구조

보안 구조(Security Architecture)는 크게 5가지로 정의된다[2]. 3G 서비스에 대한 엑세스를 보호하거나 무선 구간에 대한 엑세스를 보호하기 위한 네트워크 엑세스 보안, 유선 네트워크상의 공격을 막거나 시그널링 데이터를 보호하기 위한 네트워크 도메인 보안, 단말에 대한 엑세스 보호를 위한 사용자 도메인 보안, 사용자와 서비스 제공자 사이에서 응용 프로그램들의 메시지 전달을 보호하기 위한 응용 도메인 보안, 마지막으로 보안 프로그램이 구동되고 있는지 아닌지 사용자에게 알려주는 보안의 설정 및 출력이 있다. 각 보안 구조가 상호 어떤 관계를 갖는지는 (그림 2)에서 살펴 볼 수 있다.

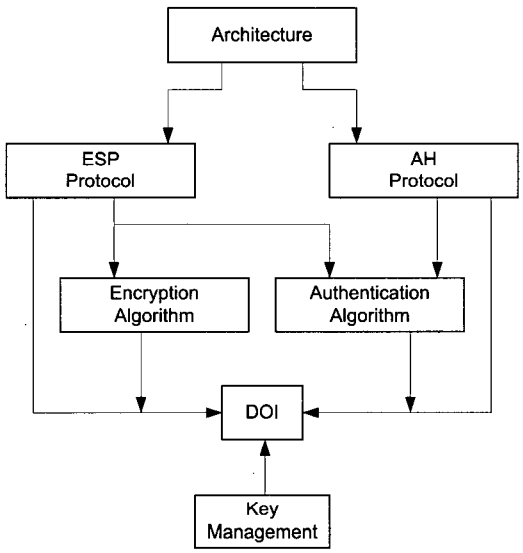
본 논문에서는 이러한 3GPP 보안 구조에서 많이 쓰이고 있는 IPSec architecture에 대한 표준화 동향을 알아보고, 3GPP에서 어떤 방식으로 적용되고 있는지 살펴보기로 한다.

현재 3GPP에서의 IP Security 기술은 네트워크 도메인 영역 보안 분야에서 주도적으로 활용되고 있으며, 이것을 바탕으로 IMS 보안 분야와 WLAN interworking 보안 분야로 확대되고 있다.

II. 네트워크 영역 보안

2세대 이동통신 시스템에서는 특히 취약부분으로 지적되었던 보안 부분이 핵심망의 보안 메커니즘 결여 때문인 것으로 나타났다[3]. 3세대 시스템에서는 이러한 취약성을 없애기 위하여 여러 보안 메카니즘들이 제안되었는데, 망 보안에 있어서는 IETF에서 제안된 IP Security 기술이 표준의 위치에 서게 되었다.

IP Security 기술은 IETF의 ipsec WG에서 표준화된 보안 구조로 총 4개의 프로토콜을 포함하고 있다. IPSec SA (Security Association)협상을 위해서는 IKE (Internet Key Exchange), ISAKMP (Internet Security Association and Key Management Protocol)가 쓰이고, 실제 트래픽에 암호화나 인증 서비스를 제공하기 위해서는 ESP (IP Encapsulating Security Payload), AH (IP Authentication Header) 가 쓰인다. 이러한 프로토콜들에 대한 표준화는 그림 3과 같은 구조를 가지고 진행되는데, 전체적인 보안 구조를 중심으로 ESP와 AH 프로토콜이 정의되어 있고, 두 프로토콜이 사용하는 암호화 알고리즘과 인증 알고리즘이 있으며, Key 교환을 위한 Key management 와 이들 간의 값을 변환해주는 DOI(Domain of Interpreter)가 있다.



(그림 3) IPSec document roadmap

3GPP에서는 IETF에서 정의된 IPSec을 이용하는데, 모든 범위의 표준을 적용하게 되면 선택 사항(Options)이 많아지기 때문에 상호 호환성에 문제가 발생하게 된다. 이러한 문제를 방지하기 위해 3GPP는 기 정의된 표준내용 중 꼭 필요한 부분만 선택적

으로 사용한다.

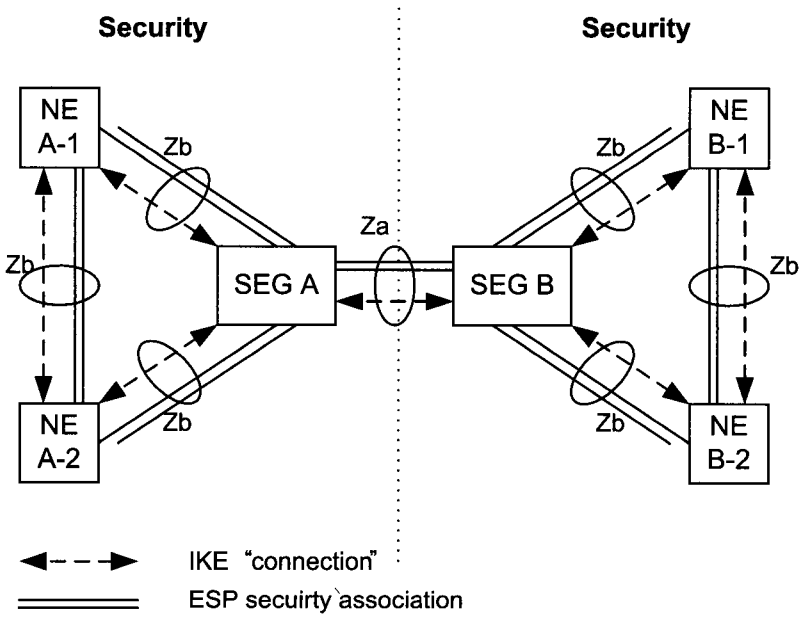
SA 설정을 위한 IKE 는 Phase 1 과 Phase 2 방식으로 나뉘고, Phase 1에는 Main mode와 Aggressive mode 방식으로 구상되는데, 3GPP에서는 Main mode만 사용하도록 표준을 정의하였다. 그리고 인증 방법으로서 전자 서명, 공개키 방식, 미리 공유된 키 방식 중 미리 공유된 키 방식을 사용토록 하였으며, 알고리즘 부분에서는 기밀성을 위해서 3DES CBC 방식을 사용하고, 인증을 위해서는 SHA1을 사용하는 것을 필수로 정의하였다. 또한 Identification을 위하여 사용되는 여러 Type 중에서는 IP 어드레스와 FQDN(Fully Qualified Domain Name)만 사용된다. Release 6에서는 이렇게 정의된 부분 외에 기밀성을 위한 암호화 알고리즘에 AES-CBC를 추가 하였고, 키 교환시에 Diffie-Hellman group 2를 지원토록 하였다.

Phase 2에서는 PFS(Perfect Forward Secrecy)는 필수가 아닌 선택사항으로 했고, Identification을 위해서는 IP 어드레스와 서브넷 타입을 필수로 정의하였으며, Notification을 필수로 지정하였다. 3GPP Release 6에서는 Phase 1과 마찬가지로 Diffie-Hellma group 2를 지원하는 것을 필수로 권고하고 있다.

SA 설정 후 트래픽 처리에 있어서 3GPP는 Tunnel mode만 지원하고, AH는 사용하지 않으며, ESP 프로토콜만 사용한다. 3GPP Release 6에서는 3DES-CBC외에 AES-CBC 암호화 알고리즘도 사용한다.

이렇게 정의된 IPSec을 바탕으로 네트워크 영역 보안의 구조는 (그림 4)와 같이 구성된다.

네트워크 영역 보안에서는 Za 와 Zb 두개의 인터페이스를 정의하고 있는데, Zb 인터페이스는 구현에 있어 선택적이다. Za 인터페이스는 서로 다른 보안 영역 사이에서 흐르는 모든 IP 패킷에 보안 서비스를 적용하고, Zb 인터페이스는 보안영역 안에서 네트워



(그림 4) NDS (Network Domain Security) 구조

크 개체와 Security Gateway 사이의 보안을 담당한다. Za 인터페이스는 ESP에서 인증/무결성 서비스와 암호화를 필수로 제공해야 하지만, Zb 인터페이스에서는 암호화는 선택사항이다.

네트워크 영역 보안은 GTP 프로토콜의 보안에 대해서도 언급하고 있다. GTP 프로토콜은 사용자 데이터 전송을 위한 GTP-U 와 제어 데이터 전송을 위한 GTP-C로 나뉘는데, GTP-C는 이동성 관리 메시지, 인증 데이터, 이동성 관리 설정(MM context) 데이터와 같은 민감한 데이터들을 전송하기 때문에 보안 서비스를 적용하는 것이 필요하지만, GTP-U는 네트워크 영역 보안 표준을 적용 받지 않는다.

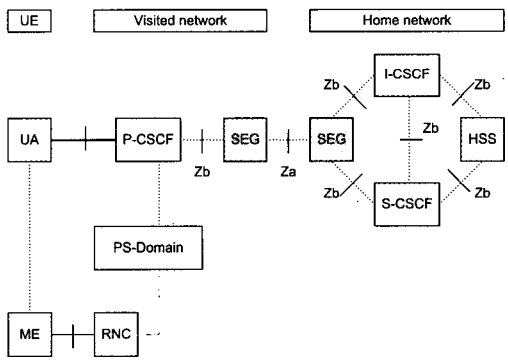
다음 장에서는 이와같이 정의된 네트워크 영역 보안이 다른 서비스들에 어떻게 적용되는지 살펴본다.

III. IPSec을 이용한 IMS 보안

IMS(IP Multimedia Subsystem)는 Release 5에서 제안된 기술로 IP 기반의 멀티미디어 서비스를 위하여 3GPP 표준에 포함되었다. 단말에서는 IMS 시그널링을 위하여 IETF의 SIP/SDP 프로토콜을 사용하며, 핵심망에서는 QoS 서비스를 위하여 GGSN이 COPS/COPS-PR를 기반으로 하는 Go 인터페이스를 지원해야 한다.

IMS에는 UA(User Agent), P-CSCF(Proxy Call Session Control Function), I-CSCF(Interrogating CSCF), S-CSCF(Serving CSCF), HSS(Home Subscriber Server)와 같이 5개의 네트워크 개체가 존재한다. IMS 서비스를 받기위해 SIP/SDP가 응용 프로그램들과 구동이 되는 부분이 UA이고, P-CSCF는 IP 멀티미디어 핵심망의 첫 번째 연결 포인트로 단말로부터 수신한 SIP 등록 요청 메시지를 I-CSCF로 전달하는 역할을 한다. 또한 단말로부터 수신한 SIP 메시지를 S-CSCF와 같은 SIP 서버로 전달하는 역할을 수행하며, SIP 응답 메시지를 단말로 전달하는 역할도 수행한다. I-CSCF는 단말의 SIP 등록 요청 메시지를 이용하여 S-CSCF를 할당하는 역할을 수행하고, 다른 네트워크에서 수신된 SIP 메시지를 S-CSCF로 라우팅 하는 역할을 수행한다. 해당 S-CSCF의 주소는 HSS로부터 얻어 온다. S-CSCF는 단말을 위한 호 제어 서비스를 제공하는데, 일반적인 SIP 서버역할을 수행한다[5].

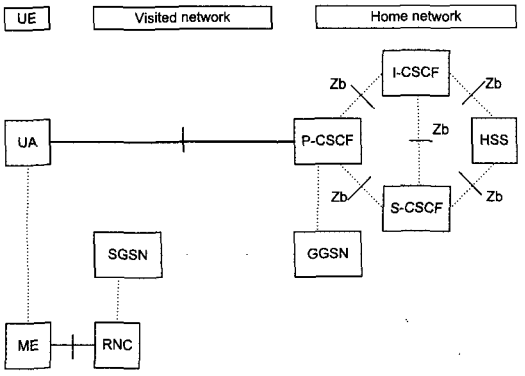
이와 같이 각 네트워크 개체들 간에는 다양한 SIP 메시지들을 주고받는데, 이를 보호하기 위하여 보안 서비스의 적용이 요구되었다. 3GPP에서는 IMS 보안 요구 사항을 만족시키기 위하여 앞 절에서 언급된 네트워크 영역 보안(NDS/IP) 방법을 사용한다.



(그림 5) 방문망의 P-CSCF

IMS 보안을 위한 망 구조는 크게 P-CSCF가 방문망에 있는 경우와 홈 망에 있는 경우로 나눌 수 있는데, P-CSCF가 방문 망에 있는 경우는 그림 5와 같은 망 구조를 가진다. P-CSCF에서 홈망의 I-CSCF나 S-CSCF로 메시지를 전달하기 위해서는 Za 인터페이스를 거치게 되어 있다. Za 인터페이스에서는 모든 IP 패킷에 보안 서비스를 적용하기 때문에 안전하게 홈망으로 메시지를 전달 할 수 있다. 나머지 네트워크

개체들 사이에서는 Zb 인터페이스를 통하여 메시지를 전달한다[6].



(그림 6) 홈 망의 P-CSCF

P-CSCF가 홈망에 있는 경우에는 (그림 6)과 같은 망구조를 가지는데, 홈 망에 있는 네트워크 개체들은 Zb 인터페이스를 사용하여 SIP 시그널링 패킷을 보호한다.

IMS 시스템의 망 보안 외에 단말과 P-CSCF 사이에도 보안이 필요한데, IP Security 의 IKE를 사용하지 않고, IMS AKA(Authentication Key Agreement)를 사용하여 key 값을 설정 한다. 이렇게 설정된 key값을 이용하여 IP Security의 ESP프로토콜을 사용하여 보안 서비스를 적용한다. 이때 적용되는 ESP는 기밀성을 제공하지 않고, 무결성 서비스만을 적용하고, 무결성 서비스를 위한 알고리즘으로 HMAC-MD5-96과 HMAC-SHA-1-96 중 하나를 사용 한다. 그리고 Tunnel 모드가 아닌 Transport 모드를 사용 하여 단말과 P-CSCF사이의 SIP 시그널링 메시지를 보호한다.

Release 6에서는 기본 망 보안에서 Za 인터페이스와 Zb 인터페이스를 사용하여 보안 서비스를 제공하는 것은 같지만, 단말과 P-CSCF간의 보안서비스에 기밀성 서비스가 제공된다는 것이 Release 5와 다른 점이다. 기밀성 서비스를 위해서 3GPP 에서는 암호화 알고리즘으로 DES-EDE3-CBC 와 AES-CBC를 사용하고 무결성 서비스를 위해서는 Release 5에서와 마찬가지로 HMAC-MD5-96와 HMAC-SHA-1-96를 사용한다.

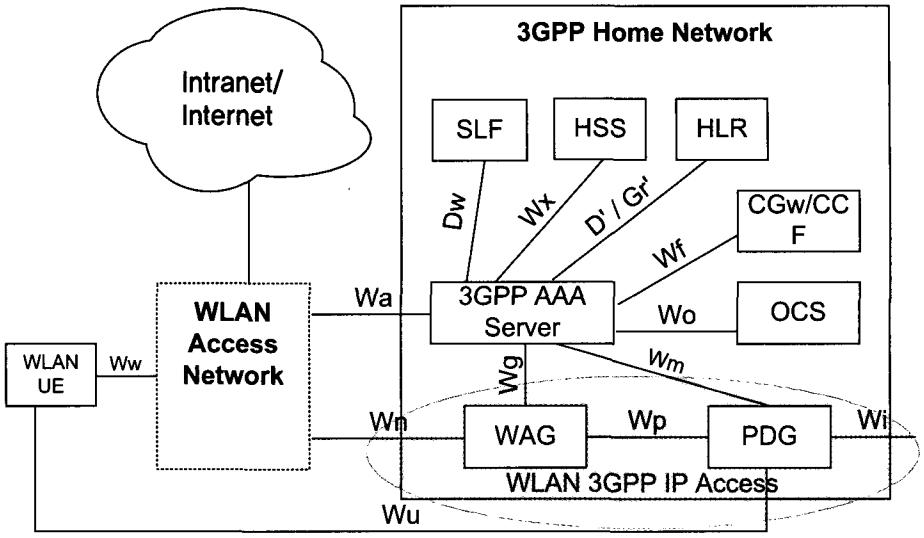
IV. 3GPP-WLAN interworking 보안

3GPP-WLAN inter-working은 Release 6에서 제안된 기술로 WLAN 단말이 3GPP 시스템에 접속하여 서비스를 받을 수 있도록 하는 것을 목적으로 한다. 이를 위하여 3GPP에서는 6단계로 시나리오를 정의하고 있다[7].

- Common billing and customer case
- 3GPP system based access control and charging
- Access to 3GPP system PS based services
- Service continuity
- Seamless service provision
- Access to 3GPP CS service

처음의 3가지는 Loose 연동 방식으로 WLAN과 WCDMA 망이 각각 독립적으로 운영되지만, 마지막 6단계에서는 서킷 서비스까지 지원하는 것을 목표로 한다.

6단계의 시나리오 외에 3GPP는 WLAN과의 연동을 위해 Non Roaming과 Roaming 의 두 가지 연동 모델을 정의하였고, Roaming 연동모델에는 홈 망을 통하여 연동되는 모델과 방문 망을 통하여 연동되는 모델로 두 가지로 분류하고 있다.



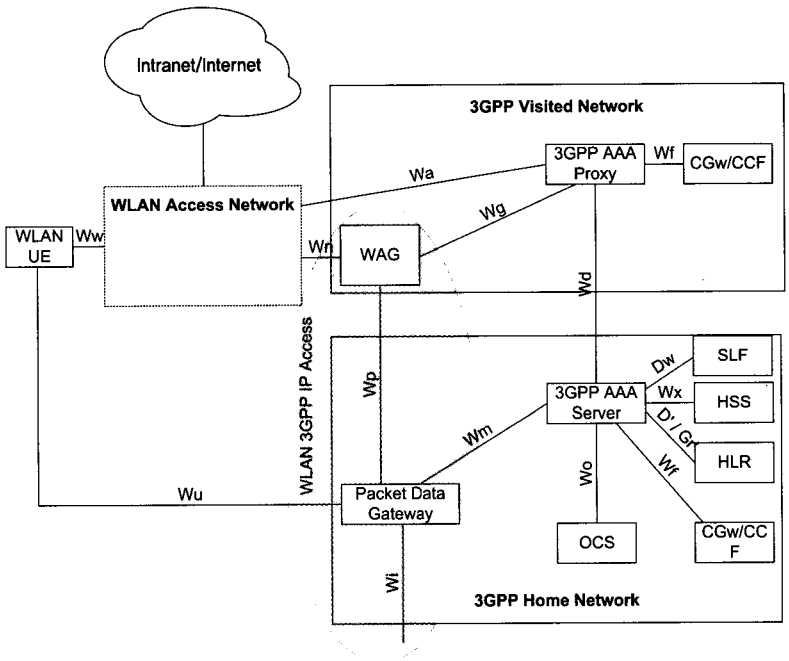
(그림 7) Non Roaming 연동 모델

(그림 7)은 Non Roaming 연동 모델로서 홈 망을 통해서 WLAN이 연동이 된다. (그림 8)은 방문망을 통한 Roaming WLAN 연동모델로, 홈 망이 접근 제어와 터널 설정을 책임지고 트래픽은 방문망을 통하여 수신된다. (그림 9)는 홈망을 통한 Roaming WLAN 연동모델로, 홈 망이 접근 제어를 책임진다. 하지만 터널 설정에 대한 권한 부여는 3GPP proxy AAA에 의해 결정된다.

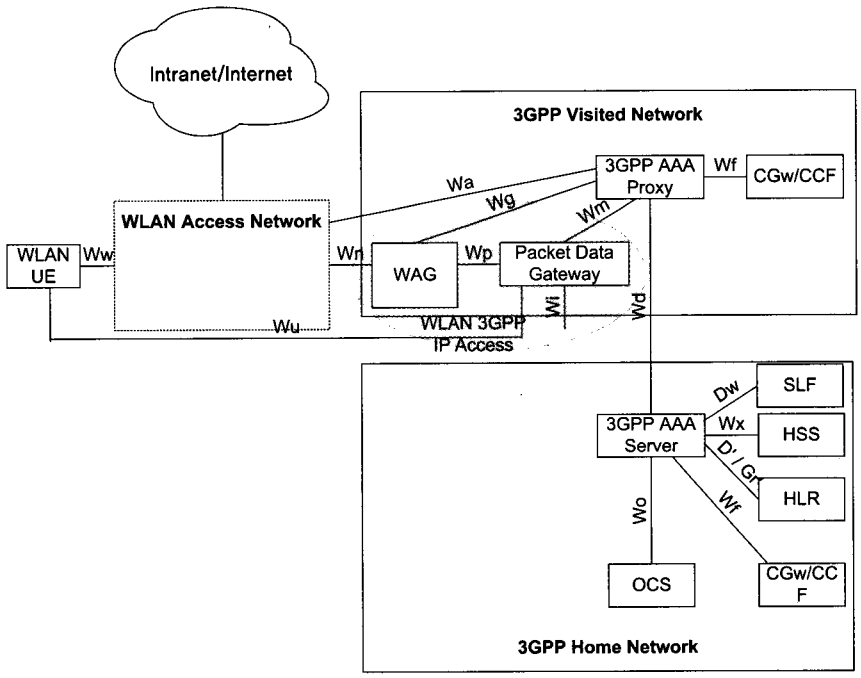
이러한 모델을 바탕으로 WLAN과 3GPP 시스템이 연동됨에 따라 보안 기준의 마련이 필요하게 되었다. 앞서 살펴봤듯이 각 연동 모델별로 접근 제어와 터널 설정이 있고, 각각에 대하여 보안 메카니즘이 존재한다. 이 중에 IP Security가 쓰이는 곳은 터널 설정이고, WLAN UE와 PDG(Packet Data Gateway) 사이에 존재하는 Wu 인터페이스에 의하여 사용된다.

UE에 의하여 터널 생성이 이루어 지는 경우 UE와 PDG는 IKE version 2를 사용하게 되어 있다. IKE version 2를 사용하여 UE와 PDG사이에 SA(Security Association)를 설정하는데, 터널 인증과 권한을 위해서 IKEv2의 EAP method[9]를 이용한다. (그림 10)은 이 과정을 나타낸 것이다.

(그림 10)의 IKE v2의 IKE_SA_INIT라고 알려져 있는 initial exchange 과정을 통해 암호화 알고리즘과 Key 교환을 위한 Diffie Hellman 교환이 일어난다. IKE_SA_INIT 후에는 IKE_AUTH 단계의 협상이 일어나는데, Child SA를 교환하고 유저와 W-APN정보를 IDi 와 IDr 에 담아 전송하게 된다. 이를 수신한 PDG는 유저와 W-APN정보를 EAP AVP에 실어 Access Request 메시지를 3GPP AAA로 전송하게 되고, AAA로부터 EAP 메시지(challenge 값)를 수신하게 되면 IKE_AUTH response 에 실어 단말로 전송한다. 단말은 관련 파라미터들을 체크하고 IKEv2에 EAP 메시지만 담아 다시 PDG로 전송하게 된다. PDG는 IKEv2 메시지에서 EAP 메시지를 얻은 다음 이를 3GPP AAA로 보내주게 된다. EAP 메시지가 성공으로 판단되게 되면 AAA로부터 EAP



(그림 8) 방문망을 통한 Roaming WLAN 연동 모델



(그림 9) 홈망을 통한 Roaming WLAN 연동 모델

success 메시지가 수신되는데, 이를 IKEv2메시지에 실어 단말로 전해주면 과정이 완료된다[8].

WLAN inter-working에서 쓰는 IKEv2에도 네트워크 영역 보안과 마찬가지로 호환성을 위해 제한을 가했는데 내용은 다음과 같다.

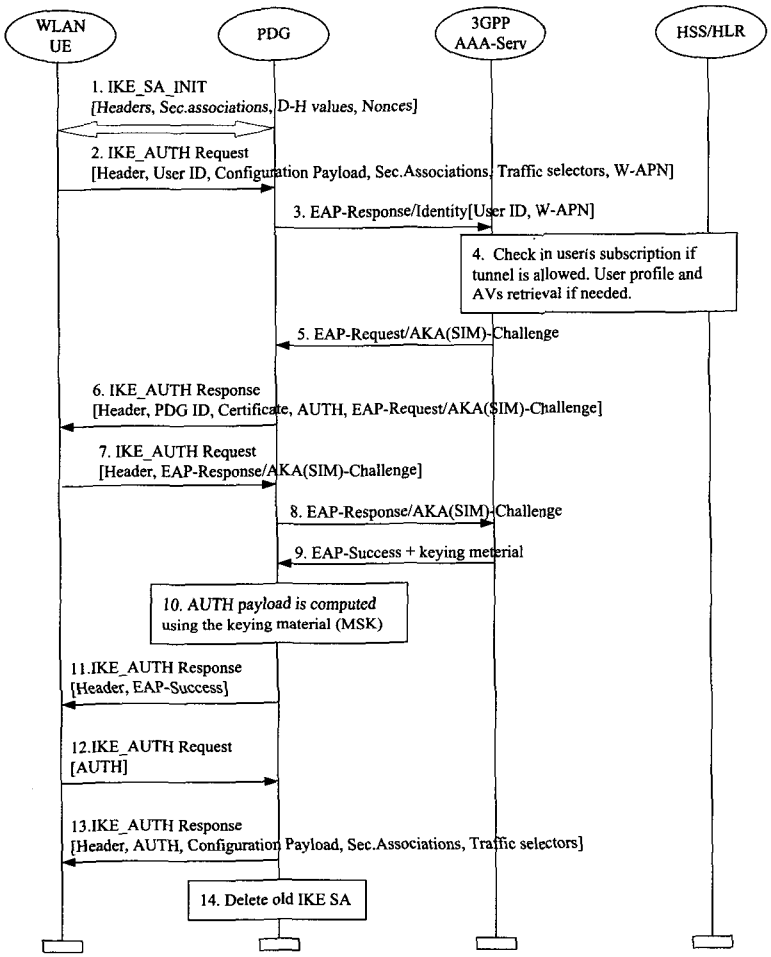
◆첫 번째 암호화 협상
- 기밀성 : 3DES in CBC mode
- 랜덤함수 : HMAC-SHA1
- 무결성 : HMAC-SHA1-96
- Diffie Hellman group 2 (1024bit)

◆두 번째 암호화 협상
- 기밀성 : AES in CBC mode (128 bit)
- 랜덤함수 : AES-XCBC-PRF-128
- 무결성 : AES-XCBC-MAC-96
- Diffie Hellman group 2 (1024bit)

또한 실제 트래픽을 위해 사용되는 ESP 또한 다음과 같은 제한사항을 두고 있다.

◆첫 번째 암호화 협상
- 기밀성 : 3DES in CBC mode
- 무결성 : HMAC-SHA1-96 (160 bit)
- 터널 모드

◆두 번째 암호화 협상
- 기밀성 : AES in CBC mode (128 bit)
- 무결성 : AES-XCBC-MAC-96
- 터널 모드



(그림 10) 터널 설정 및 인증

V. 결 론

본 논문에서는 IP Security 기술이 비동기 방식의 WCDMA 시스템에서 어떻게 적용되고 있고, 어떤 형태로 표준화되고 있는지 알아보았다. IP Security 기술은 Release 5의 IP Multimedia

Subsystem (IMS)에서 네트워크 영역 보안 부분과 IMS 보안 부분 그리고 3GPP-WLAN 연동 보안 부분에서 널리 사용되고 있으며, TSG SA WG3에서 세부적인 사항들의 표준화를 주도하고 있다.

먼저 네트워크 영역 보안 부분에서는 IP Security의 다양한 선택 사항들이 어떻게 적용되어 사용되는지를 살펴보았다. IETF에서 정의된 IP Security의 경우 다양한 선택 사항들을 제시하고 있어 호환성에 문제가 발생될 수 있기 때문에, 많은 부분 제한을 두어 3GPP 시스템에 용이하게 적용될 수 있도록 하였다. 터널 설정을 위한 IKE프로토콜에서는 Main mode와 미리 공유된 키 방식을 사용토록 하였고, 트래픽 처리를 위해서는 ESP만 사용하게 하였으며, 터널 모드로만 작동하게 하였다.

암호화 알고리즘의 경우에는 Release 5에서는 주로 3DES를 사용하지만 Release 6에서는 보안이 한층 강화된 AES를 사용토록 하였다. 이를 바탕으로 IMS 보안 부분에서는 Za와 Zb 인터페이스를 정의하여 IMS 네트워크 개체들 사이에 정의된 인터페이스를 적용하여 보안 서비스가 제동되도록 하였고, 3GPP-WLAN 연동 부분에서는 IKEv2를 이용하여 UE와 PDG 사이의 터널 설정과 인증 서비스를 제공토록 하였다.

현재 3GPP 보안 관련 표준화 작업에서는 이동가입자의 접근 제어나 Key 관리와 같은 엑세스 제어쪽에 이슈가 많아지고 있고, 핵심망 보안과 관련된 사항은 IETF의 표준화에 준해 선택적으로 채택하여 활용하고 있다. 그리고 IP Security 기술 표준화를 담당했던 IETF의 ipsec WG은 2005년 4월 해산되었다. 가장 큰 이슈중의 하나였던 IKEv2도 거의 마무리 단계에 있어, 전체적인 RFC들의 변화가 있을 것으로 보인다.

ipsec WG은 해산되었지만, 이동성과 Multihoming에 IKEv2를 적용하기 위한 표준화를 mobike WG에서 주도하고 있으며, IPSec에서 PKI 적용을 위한 표준화를 pki4ipsec WG이 담당하고 있다.

결과적으로 WCDMA 이동통신망에서 IP Security 기술은 Release 5 이후 IP Multimedia Subsystem 도입과 함께 그 중요성과 필요성이 더욱 강화될 것으로 기대된다.

[참 고 문 헌]

[1] http://www.3gpp.org

[2] 3GPP TS 33.102 : 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture

[3] 3GPP TS 33.210 : 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security

[4] R. Thayer, N. Doraswamy, R. Glenn, "IP Security Document Roadmap" RFC 2411, November 1998

[5] 3GPP TS 23.228 : 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS)

[6] 3GPP TS 33.203 : 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services

[7] 3GPP TS 22.934 : 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area;

Network (WLAN) interworking

[8] 3GPP TS 33.234 : 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) interworking security

[9] Charlie Kaufman, "Internet Key Exchange (IKEv2) Protocol" draft-ietf-ipsec-ikev2-17, September 2004

이상윤

1999년 숭실대학교 정보 통신공학과 졸업 (학사)
2001년 숭실대학교 정보 통신공학과 (석사)
2001년 ~ 현재 LG전자 네트워크 연구소 근무
관심분야 : 정보통신공학, 이동통신, 네트워크보안

김형택

1987년 광운대학교 전자계산기공학 졸업 (학사)
1997년 KAIST 정보통신공학 졸업 (석사)
1987년 ~ 현재 LG전자 네트워크 연구소 근무
관심분야 : IP Multimedia, Mobile Packet Core Network, 이동통신 시스템 설계 등

연철흠

1981년 서강대학교 전자공학과 졸업 (학사)
1987년 KAIST 전기전자공학과 졸업 (석사)
1993년 KAIST 전기전자공학과 졸업 (박사)
1980년 ~ 1987년 (주)금성전기(현LG전자기술연구소) 선임연구원
1987년 ~ 1995년 (주)디지콤 정보통신연구소 책임연구원
1997년 ~ 2001년 LG전자 차세대통신연구소 연구위원(상무)
2001년 ~ 2003년 LG전자 UMTS 시스템연구소 소장
2003년 ~ 현재 LG전자 네트워크 연구소
관심분야 : Network Evolution, Wireless Access Technology, IMT-2000, 모뎀, All IP