情 報 保 護 學 會 誌
第 12 券 第 3 號, 2002. 6

3GPP 네트워크 도메인 보안에 관한 분석

김 건 우*, 류 희 수*

요 약

3GPP(3rd Generation Partnership Project) NDS(Network Domain Security)에 관한 표준화 제정은 특성상 IETF와의 협의를 통하여 최근에 비교적 활발히 이루어지고 있다. 차세대 이동통신의 등장과 인터넷의 발달로 인하여 여러 가지 형태의 네트워크가 존재하게 되고 또한 다양한 프로토콜과 메커니즘이 사용됨에 따라, 무선 구간에서의 안전한 액세스 외에도 유선구간에서의 정보보호 역시 중요한 문제로 대두되고 있다. 본 고에서는 3GPP 네트워크 도메인에서의 정보보호에 관하여 최신 릴리즈 5 버전을 중심으로 stage 2 수준으로 분석을 하였다.

1. 서 론

최근의 3GPP 표준안 중 보안에 관한 동향을 살펴보면 무선구간의 인증 및 암호화는 릴리즈 99는 물론이고 릴리즈 4, 릴리즈 5까지 거의 완성된 상태이다. 이를 위하여 사용자와 네트워크는 AKA(Authentication and Key Agreement) 절차를 수행하고 또한 무선구간에서의 데이터에 대한 무결성과 기밀성을 제공한다. 이에 반해, 유선 네트워크 영역에서의 보안에 관해서는 일부 표준이 확립된 것도 있고 아직 논의가 활발히 진행중인 부분도 있다. 이는 사업자 고유의 영역이었던 핵심망과 유선 네트워크 구간이 최근 이동통신 및 인터넷 환경의 변화에 따라 복잡하고 다양한 형태로 발전함으로서 보안 요구사항도 역시 다양하게 증가하게 됨을 의미한다. 예를 들면, SS7(Signaling System no. 7) 프로토콜을 사용하는 2세대 이동통신 시스템과는 달리 3세대 3GPP 시스템에서는 SS7 뿐만 아니라 IP, SIP (Session Initiation Protocol) 등의 다양한 프로토콜이 도입되었고 이에 따른 정보보호의 대책도 더욱 다양해지고 중요해졌다. 이는 IP를 기본으로 하는 시스템이 도입되면서 패킷 스위칭으로 향한 이동, 그리고, 개방되고 쉽게 접근할 수 있는 프로토콜로 전환이 되고 있음을 의미한다. 따라서, 정보보호도 이러한 관점에서 새로운 공격과 위협으로부터 보호되어야 하고, 사용되는 프로토콜에 따라 안전하고 다양한 보안 메커니즘이 개발되어 표준화 되어야 한다.

현재 3GPP는 네트워크 도메인 보안에 관해 크게 3가지로 분류해 표준을 제정하고 있다. SS7 MAP (Mobile Application Part)에서의 시그널링 보안, IP 프로토콜 네트워크 계층에서의 IP 보안, 그리고, IMS(IP Multimedia Subsystem) 네트워크에서의 SIP 보안에 관한 스펙이 각각 제정중에 있다. 이중 MAP 보안과 IP 보안에 관해서는 거의 표준화가 완료되었고, IMS 보안에 관한 논의가 SA3 WG(Working Group)와 IETF(Internet Engineering Task Force) SIP WG을 중심으로 활발히 진행중이다. 무선구간과 달리 유선구간에서는 새로운 메커니즘을 개발하기도 하지만 기존의 인터넷 및 네트워크 관련 프로토콜이나 검증받은 메커니즘을 수정하여 사용하기도 한다. 각 영역에서의 보안개념과 요구사항 정립, 그리고, 이들간의 인터페이스에 관해서는 3GPP가 표준안을 제정하지만, IP나 SIP 관련 보안 메커니즘에 관해서는 IETF와 협력하여 표준을 만들거나 경우에 따라서는 IETF 프로토콜을 그대로 사용하기도 한다.

본 고는 최근에 이슈화 되고 있는 3GPP 유선영역 네트워크 보안에 관해서 릴리즈 5 버전의 TS (Technical Specification)를 stage 2 수준으로

* 한국전자통신연구원 정보보호연구본부({wootopian, hsryu}@etri.re.kr)

정리한 것이다. 크게 세 부분으로 나누어 MAP 보안, IP 보안, 그리고, IMS 보안에 관하여 설명한다.

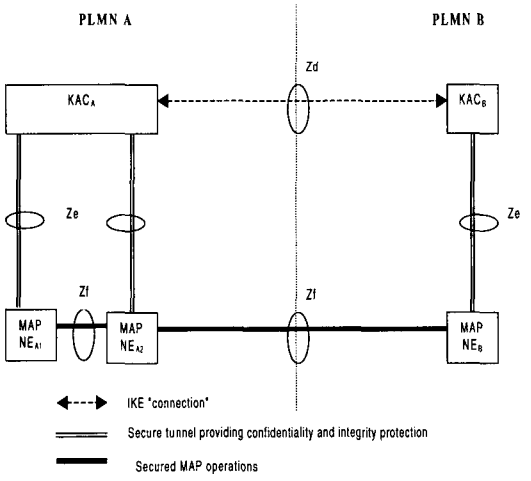
II. MAP 보안

2장에서는 MAP 시그널링을 보호하기 위해 필요한 MAP SA(Security Association) 설정 및 보안구조를 살펴본다. 또한, MAPsec 구조와 MAPsec 보안 프로파일에 관해서도 분석한다.

2.1. 보안구조 및 인터페이스

SS7 및 SS7/IP 기반 프로토콜에 대한 보안 메커니즘은 응용 계층에서 구현된다. IP 프로토콜이 사용되더라도 SS7 MAP 프로토콜만이 보호되고, 이때의 MAP 보안을 MAPsec 이라 한다. MAPsec에서는 데이터 무결성, 데이터 출처 인증, 재전송 방지, 기밀성과 같은 정보보호 서비스가 제공된다.

그림 1에서 MAP 보안구조와 인터페이스를 나타내었다.



〔그림 1〕 MAP 보안구조와 인터페이스

- **Zd 인터페이스 (KAC-KAC)**

PLMN(Public Land Mobile Network) 사이에서 MAPsec SA를 협상하기 위해 사용되는 인터페이스로, Zd에서의 트래픽은 오로지IKE(Internet Key Exchange)로만 구성되어 있다.

- **Ze 인터페이스 (KAC-NE)**

동일 PLMN 내의 MAP-NE와 KAC 사이의 인터페이스로, KAC로부터 MAP-NE에게 SA와 보안 정책 정보를 전송하기 위해 사용된다.

- **Zf 인터페이스 (NE-NE)**

MAP-NE와 MAP-NE 사이의 인터페이스로, 동일한 네트워크 NE 사이의 인터페이스일수도 있고, 서로다른 네트워크 NE 사이의 인터페이스일수도 있다. MAP-NE는 MAP 보안을 위해 자신이 속해있는 KAC로부터 MAPsec SA를 받아서 사용하고, 보안 프로파일에 의해서 선택적으로 보호된다.

MAP 보안이 적용되기 위해서는 MAP 네트워크 요소들 사이에 SA가 설정되어야 하고, 이SA에서는 MAP 시그널링을 보호하기 위한 키, 알고리즘, 보호 프로파일 등을 정의한다. 이때 MAPsec-SA는 각 네트워크의 KAC(Key Administration Center) 사이에서 협상되고, 협상된 SA는 네트워크 내의 MAP 응용 계층 보안을 필요로 하는 개체들에게 분배된다. 이러한 MAPsec-SA에는 다음과 같은 요소들이 필요하다.

- **Destination PLMN-Id**

수신 PLMN의 ID로서, MCC(Mobile Country Code)와 MNC(Mobile Network Code)로 구성된다.

- **SPI(Security Parameter Index)**

목적지의 PLMN-Id와 함께 MAPsec SA를 식별하기 위한 32비트 값

- **Sending PLMN-Id**

송신 PLMN의 ID로서, MCC와 MNC로 구성된다.

- **MEA**

암호화 알고리즘을 가리키는 값으로, 동작 모드는 알고리즘 식별자에 의해 정의된다.

- **MEK(MAP Encryption Key)**

암호화 키로서, 길이는 알고리즘 식별자에 의해 정의된다.

- **MIA**

무결성 알고리즘을 가리키는 값으로, 동작 모드는 알고리즘 식별자에 의해 정의된다.

- MIK(MAP Integrity Key)

무결성 키로서, 길이는 알고리즘 식별자에 의해 정의된다

- PPI(Protection Profile Identifier)

보안 프로파일에 관한 16비트 값

- SA Hard Expiry Time

SA의 실제 만료 시간을 정의하는 UTC time

- SA Soft Expiry Time

Outbound 트래픽에 대한 SA의 만료 시간을 정의하는 UTC time

만약, MAPsec이 적용되지 않는다면 위의 각 요소들은 NULL 값을 갖는다.

2.2. KAC의 역할과 특성

KAC는 MAP-NE가 사용할 MAPsec SA를 통신하고자 하는 상대방의 KAC와 협상하는 개체이다. MAP-Ns가 다른 MAP-NE로의 안전한 연결을 설정하고자 할 때, MAP-NE는 자신의 SAD (Security Association Database)안에 유용한 MAPsec-SA의 소유여부를 알아서 없다면 KAC에게 MAPsec SA를 요구한다. 그러면, KAC는 기존의 MAPsec SA를 MAP-NE에게 제공하거나, 새로운 MAPsec SA를 협상하는 절차를 거친다.

MAPsec SA는 협상되는 두 보호 도메인 사이의 모든 MAP 통신에 대해서 유효하다. 즉, PLMN B의 MAP-NE와 통신하는 PLMN A의 모든 MAP-NE에 대해서는 동일한 MAPsec SA가 적용된다. 각 PLMN은 하나 이상의 KAC를 가질수 있고, KAC는 다음과 같은 역할을 한다.

- 다른 망의 KAC와 MAPsec SA 협상
- NE에 의해 해석될 수 있도록 SA 파라메터 변형
- SA lifetime에 의한 MAP-SA 갱신
- 자신의 KAC와 동일한 보호 도메인에 속하는 NE에게 MAP-SA나 보호정책 분배

그리고, KAC의 정상적인 동작을 위해서 다음의 데이터베이스를 관리해야 한다.

- 협상될 MAP-SA의 범위나 보호정책, MAP-PP (Protection Profile), 알고리즘, SA-lifetime 등을 정의하는 데이터베이스인 KAC-SPDB-MAP
- NE에서 필요한 MAP 보호정책을 가지는 데이터베이스인 NE-SPB-MAP
- MAP-SA 정보를 포함하는 데이터베이스인 KAC-SADB-MAP

2.3. MAPsec 구조

MAPsec에서 제공되는 보호 서비스는 사용되는 보안모드에 따라 범위가 달라진다.

〔표 1〕 MAPsec 보안모드와 서비스

보호모드	서비스
0	-
1	무결성, 인증
2	기밀성, 무결성, 인증

MAPsec에 의해 보호되는 MAP operation은 Security Header와 Protected Payload로 구성되고, 세가지 보호모드 모두 Security Header는 cleartext로 전송된다.

- Security Header

보안모드 0에서의 Security Header는 SPI와 Original Component ID로 구성되어 있고, 보안모드 1과 2에서의 Security Header 구성은 다음과 같다.

SPI	Original Component ID	TVP	NE-ID	Prop

- Original component Id

MAP operation (operation 코드에 의한 operation, 에러코드에 의한 에러, 사용자 정보 등)의 Component Type (invoke, result, error)에 대한 식별자

- TVP

MAP operation의 재전송 방지를 위한 16비트 time-stamp로, 수신 NE는 time-stamp가 적당한 time window내에 있을 때에만 operation을 받아들인다. 수신 NE에서의 time window의 크기는 표준화되어 있지 않다.

- NE-Id
  동일 TVP 구간내의 서로 다른 NE에 대하여 각각 다른 IV를 생성하기 위해 사용되는 6 octet 값

- PROP(Proprietary field)
  하나의 NE에 대해서 동일 TVP 구간내의 서로 다른 보호된 MAP 메시지에 각각 다른 IV를 생성하기 위한 4 octet 값

• **Protected Payload**

- 보호모드 0

보호모드 0에서는, 어떤 보호 서비스도 제공되지 않고, Protected Payload는 원래 MAP operation의 payload와 동일하다.

- 보호모드 1

보호모드 1에서의 Protected payload는 다음과 같이 구성된다.

Cleartext || f7(Security Header || Cleartext)

cleartext는 original MAP 메시지의 payload이고, 데이터 출처 인증과 무결성은 "Security Header || Cleartext" 에 대하여 SA에서 정의된 무결성 키를 사용하여 32 비트 메시지 인증코드 함수 f7을 사용하여 이루어진다. 무결성 알고리즘으로는 128 비트 CBC MAC 모드의 AES를 사용하고, ISO/IEC 9797 Part 1의 padding method 2를 이용한

- 보호모드 2

보호모드 2에서의 Protected Payload의 구성은 다음과 같다.

f6(Cleartext) || f7(Security Header || f6(Cleartext))

기밀성은 SA에 의해 정의된 기밀성 키와 초기 벡터 IV를 이용한 암호화 함수 f6을 사용하여 cleartext를 암호화 함으로서 이루어진다. 이때 Block Cipher Mode에 관한 FIPS 800-38A 권고안에 따라 128 비트 counter mode AES를 기밀성 알고리즘으로 사용하고, IV는 TVP||NE-Id||Prop||Pad로 구성된다. Padding 필드는 TVP||NE-Id||Prop를 확장해서 IV 길이를 16 octet으로 맞추기 위해 사용되는데, 2 octet 모두 "0"으로 세팅된다.

2.4. 보안 프로파일

MAP 보안에서는 operation component에 따라 3가지 보안모드를 차등 적용함으로서 6개의 레벨로 나눌수 있다. 그래서, 주어진 어플리케이션에 대해 적용되는 보안레벨을 조정함으로서 16개의 보안그룹으로 분류하는데 이중 5개의 보안그룹만 정의되어 있다. MAPsec 보안 프로파일(Protection Profile)이란 바로 이 보안그룹의 결합으로 이루어진다.

〔표 2〕 보안 프로파일 인코딩

Protection profile bit	Protection Group
0	No protection
1	Reset
2	Authentication information except handover situations
3	Authentication information in handover situations
4	Non-location dependent HLR data
5 ~ 15	Reserved

〔표 3〕 보안 프로파일

Profile name	Profile group				
	PG(0)	PG(1)	PG(2)	PG(3)	PG(4)
A	O				
B		O	O		
C		O	O	O	
D		O	O	O	O
E		O	O		O

Ⅲ. IP 네트워크 계층 보안

3장에서는 IP에 기반한 네트워크 도메인에서의 보안구조에 관해서 살펴본다.

3.1. IP 네트워크의 보안 개요

IP 네트워크의 보호 도메인 사이는 SEG(Security Gateway)를 통하여 안전한 통신이 가능하다. SEG

는 IP 보호 도메인의 가장자리에 위치하는 개체로 IP에 기반을 둔 프로토콜을 보호하기 위해 사용되고, 현재 위치의 SEG는 목적지 보호 도메인에 존재하는 SEG에 대하여 보안정책을 설정하는 역할을 한다. SEG는 서로 다른 IP 보호 도메인 SEG 사이에서 정의되며, 모든 NDS/IP 트래픽은 SEG를 통하여 보호 도메인에 입출력된다.

한편, UMTS NDS는 user plane 까지는 포함하지 않는데, 이는 보호 도메인과 SEG가 UMTS 외부의 다른 IP 네트워크까지는 user plane Gi 인터페이스를 포함하지 않는다는 것을 의미한다. 그리고, IP 프로토콜은 네트워크 계층에서 보호되며, 이 계층에서 사용되는 보안 프로토콜은 RFC-2401에서 명시된 IPsec 프로토콜이다.

3.2. NDS/IP에 대한 키 관리와 보안구조

UMTS NDS에서 SEG 간의 키 관리와 분배는 IKE(Internet Key Exchange) 프로토콜에 의해서 수행된다. IKE를 수행하는 목적은 안전한 연결을 설정하려고하는 두 개체들 사이에서 SA를 협상, 설정, 관리하려는 것이다.

SA의 기본적인 개념은 IKE와 IPsec 이다. 두 호스트나 두 SEG 사이의 안전한 양방향 통신을 위해서는 하나의 ISAKMP SA와 두개의 IPsec SA가 필요하다. IPsec SA는 SPI, Destination IP Address, 그리고, Security protocol identifier (항상 ESP)와 같은 파라미터에 의해서 정의된다. 그리고, UMTS 핵심망 control plane 에서는 단지 터널 모드 SA와 ESP SA만 지원하고, 트랜스포트 모드 SA와 AH SA는 지원하지 않는다. 또한, ISAKMP SA는 Initiator's cookie와 Responders's cookie에 의해서 정의되고, NDS/IP는 단지 ISAKMP with pre-shared keys 만 지원한다. 다음은 Za 인터페이스에서의 보호 도메인간 SA 협상에 관해 ISAKMP SA와 IPsec SA에 대한 요구사항을 나타낸 것이다.

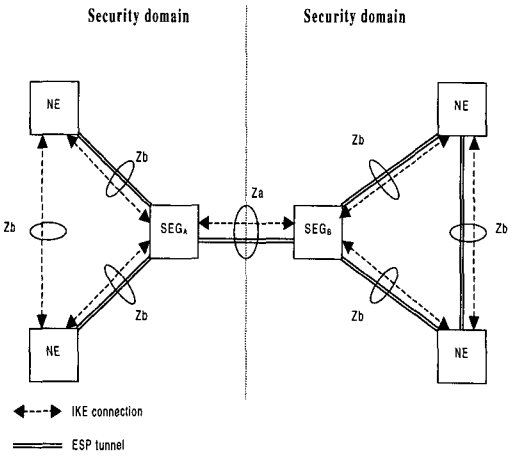
IKE phase-1 (ISAKMP SA)에 대해서,
- 인증을 위해 미리 공유된 비밀 데이터를 사용하는 것이 지원
- Main Mode만 사용
- FQDN(Fully Qualified Domain Names) 만 사용
- 기밀성을 위한 CBC 모드 AES 지원
- 무결성과 메시지 인증을 위한 SHA-1 지원

IKE phase-2 (IPsec SA)에 대해서,
- Perfect forward secrecy는 선택
- IP address와 subnet identity type 만이 필수적인 address type
- Notification의 지원은 필수

그리고, NDS/IP 구조의 기본적인 특징은 hop-by-hop 보안이다. 이것은 chained-tunnel이나 hub-and-spoke 모델과도 일치한다. hop-by-hop 보안의 사용은 내부적으로나 외부 보호 도메인에 대해서나 각각의 보호 정책을 쉽게 수립할 수 있도록 한다.

NE는 동일한 보호 도메인 내에서 SEG나 다른 NE와 필요에 따라 ESP SA를 설정하고 관리할 수 있다. 도메인 A의 NE가 도메인 B의 NE와 연결을 설정하고자 할 때에는, 반드시 SEG를 통하여 라우팅되고 최종 목적지까지 hop-by-hop으로 보호된다. 한편, 서로 다른 NE 사이에는 보호 인터페이스가 존재하지 않는데, 이는 서로 다른 보호 도메인 사이에는 보안 정책을 명확하게 분리하는 것이 중요하기 때문이고, 서로 다른 보안 정책을 가진 NE가 직접 통신하는 것은 바람직하지 않다.

그림 2는 IP 네트워크 도메인의 보안구조에 관해서 도식한 것이다.



〔그림 2〕 IP 네트워크 도메인 보안구조와 인터페이스

IP based 프로토콜에서 보안을 위한 인터페이스는 Za와 Zb 인터페이스가 있다. 최근의 TSG SA3 회의 결과, 동일한 보호 도메인내의 NE 사이의 인터페이스 Zc가 제외되고 Zb와 통합되었다.

• **Za 인터페이스 (SEG-SEG)**

이 인터페이스를 통해 두 보호 도메인 사이의 안전한 IP 연결이 설정된다. SEG는 그들 사이에 안전한 ESP 터널을 협상, 설정, 유지하기 위하여 IKE를 사용하고, ESP는 기밀성과 무결성/인증을 다 제공할 수 있지만 무결성/인증만이 필수적으로 제공되고 기밀성은 선택사항이다. Za는 모든 보호 도메인에서 필수적인 인터페이스이다

• **Zb 인터페이스 (NE-SEG / NE-NE)**

Zb는 동일한 도메인 내에서 NE와 SEG 사이, 그리고 NE와 NE 사이의 인터페이스이다. Zb는 실제 구현에서 반드시 필요한 인터페이스는 아니다. Zb 인터페이스에서는 Za와 마찬가지로 무결성/인증 서비스만 사용되고 기밀성 서비스는 선택사항이다.

마지막으로, NDS IPsec confidentiality transform은 ESP_AES를 사용하는 것이 mandatory이다. 또한, IPsec authentication transform을 위해서는 NDS/IP 트래픽 ESP가 항상 무결성과 데이터 출처 인증, 그리고 재전송 방지와 같은 보안 서비스를 제공해야 하기 때문에 ESP_HMAC_SHA-1과 AES MAC 알고리즘이 사용된다. 하지만, AES transform/mode는 아직 최종적으로 결정된 것이 아니기 때문에 추후에 업데이트될 가능성이 있다.

IV. IMS 보안

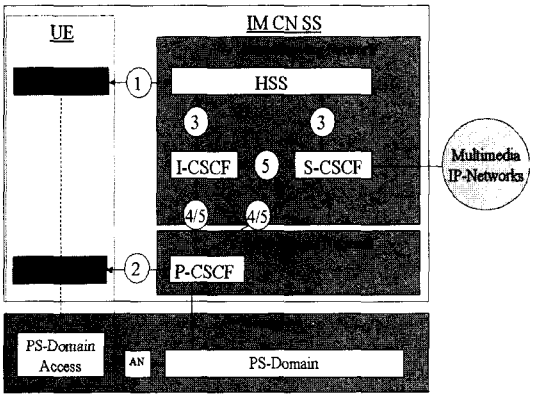
UMTS IMS는 비디오, 오디오, 실시간 화상회의 등의 IP 멀티미디어 어플리케이션을 지원한다. 그래서, 3GPP는 이러한 멀티미디어 세션을 생성, 종료하기 위한 시그널링 프로토콜로서 SIP(Session initiation Protocol)를 채택하였다.

4장에서는 이러한 IMS 네트워크에서의 보안 특성과 메커니즘에 관해서 설명한다. 즉, 사용자와 네트워크간의 인증 및 등록, 그리고 SIP 시그널링이 가입자와 IMS 사이에서 어떻게 보호되는지에 관해서 최근의 표준회의 결과를 바탕으로 분석한다.

4.1. IMS 보안 메커니즘 개요

PS 도메인에서는 단말기와 네트워크 사이에 SA가 설정되고 나서야 서비스가 제공된다. IMS는 PS 도메인과 오버레이 되는 부분도 있고, 어느 정도의 상관성은 있다. 하지만, IMS에서 멀티미디어 클라이언트가 멀티미디어 서비스를 제공받기 위해서는 IMSI(IM Service Identity module)와는 다른 별도의 사용자 IMPI(IM Private Identity)가 인증이 되어야 하고, 하나 이상의 IMPU(IM Public Identity)가 등록이 되어야 한다. 따라서, ISIM에서 저장, 관리하는 CK, IK, SQN 등은 USIM (UMTS Subscriber Identity Module)에서 사용되는 파라미터와는 별도로 생성이 되어야 한다.

그림 3은 IMS에 대한 보안구조를 나타낸 것이다. 이중 동일 보호 도메인 내에서나 서로 다른 보호 도메인 사이의 인터페이스와 레퍼런스 포인터에 관해서는 3장에서 설명한 방법을 이용한다.



〔그림 3〕 IMS 보안구조

그림 3에서 보는 바와 같이 IMS 보안을 위해서는 다섯 개의 서로 다른 보호연계를 필요로 한다.

1) 상호 인증 : HSS는 S-CSCF에게 가입자 인증에 관한 역할을 위임한다. HSS는 키와 challenge를 생성하는 역할을 하고, ISIM과 HSS에서의 long-term 키는 IMPI와 관계가 있다. 가입자는 하나의 IMPI와 하나 이상의 IMPU를 소유한다.
2) UE와 P-CSCF 사이에 보안링크와 보호연계가 제공된다.
3) Cx 인터페이스에 대한 내부 네트워크 도메인 보안
4) 서로 다른 망에서 SIP 기능이 있는 노드 사이의 보안
5) 동일망 내에서 SIP 기능이 있는 노드 사이의 보안

가입자와 네트워크의 상호 인증을 위해서는 IM 가입자는 홈 네트워의 HSS(Home Subscriber Server)

에 가입자 프로파일이 미리 저장되어 있어야 하고, 가입자가 IM 서비스를 요구하면 S-CSCF는 가입자 프로파일을 확인하여 Home Control (IM 서비스 인증) 여부를 결정한다. 이때 가입자 프로파일은 HSS로부터 Cx 인터페이스(Cx-Pull)를 통하여 S-CSCF에 전달된다. 이러한 상호인증은 등록 과정을 통해 이루어지고, S-CSCF는 이전의 등록과는 무관하게 언제던지 재등록을 요구하거나 시작할 수 있다. 하지만, 재등록 과정에서는 인증이 반드시 일어나는 것은 아니다.

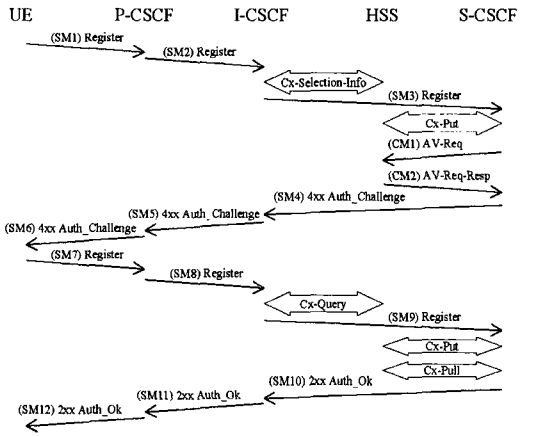
그리고, 무결성이나 기밀성 같은 IM 보안 서비스를 위해서는 SA가 설정되어야 한다. IMS에서의 무결성은 UE와 P-CSCF 사이에서 필요하고, 무결성 메커니즘으로는 IPsec을 사용하거나 SIP 레벨에서 HTTP Digest 메커니즘을 사용하는 두 가지 방법이 있었다. 하지만, 22차 SA3 회의 결과 두 가지 후보 중에 IPsec을 채택하기로 결정하였다. 한편, UE와 P-CSCF 사이의 기밀성을 위해서 SA를 협상하기는 하지만 무결성과는 달리 mandatory 가 아니라 선택사항이다. 그리고, IMS에서는 P-CSCF 이후의 네트워크 도메인 보안에 관해서 3장에서 설명한 메커니즘을 그대로 따른다.

4.2. IMS에서의 인증과 키 일치(IMS AKA)

IMS에서의 인증과 키 일치를 IMS AKA라고 하는데, IMS AKA는 ISIM과 S-CSCF 사이의 상호인증이다. 3GPP는 IMS AKA를 위해 Digest AKA를 사용하기로 하였는데, 이것은 HTPP Digest 인증 메커니즘을 AKA 파라메터를 사용하여 확장한 것으로 볼 수 있다. 그래서, 현재 HTTP Digest 인증 메커니즘 자체의 보안 결함을 수정하고 AKA와의 연동을 위해 IETF SIP WG과 3GPP SA3는 "HTTP Digest Authentication Using AKA"에 관한 표준화 작업을 진행중이고 internet draft가 나와있는 상황이다. IMS AKA 과정에서 생성된 보안 파라메터는 SIP에 의해서 전송되며, RAND, XRES, CK, IK, AUTN과 같은 인증벡터의 생성과 SQN 관리는 UMTS AKA와 동일하다.

또한, UE와 P-CSCF 사이에는 SA가 설정되어야 하고, 새로운 인증이 발생할 때 마다 업데이트된다. 한명의 사용자에 대한 각각의 IMPU에 대해서 모두 인증이 필요한지는 네트워크 관리자의 정책사항이다.

그림 4는 IMS에서 하나의 IMPU가 등록되고, 인증 및 키 일치에 관한 절차를 나타낸 그림이다. 사용자가 IM 서비스를 엑세스 하기 전에 적어도 하나의 IMPU는 등록되어야 하고, IMPI는 어플리케이션 레벨에서 IMS에 인증되어야 한다.



〔그림 4〕 IMS 인증과 키 일치 메커니즘

SIP 메시지 n을 SMn이라 하고 Cx 메시지m을 CMm 이라 표기하였다. 등록하기 위하여 UE는 SM1 (SIP REGISTER 메시지)를 SIP registrar server (S-CSCF)로 전송해서 가입자의 인증 메커니즘을 수행한다.

SM1:

REGISTER(IMPI, IMPU)

SM1 메시지는 S-CSCF까지 포워딩되고, S-CSCF는 HSS에게 registration flag를 보낸다. Registration flag는 S-CSCF name과 함께 HSS에 저장되는데, 이것은 어떤 사용자의 특정한 IMPU가 다른 S-CSCF에 이미 등록이 되었는지를 확인하거나, 어떤 S-CSCF에서 초기등록이 진행중인지의 여부를 확인하기 위해서 사용된다. HSS는 S-CSCF로부터 이러한 state(S-CSCF name + user identity)를 받고, Cx-Put 메시지가 S-CSCF로부터 HSS로 전송되고 나서야 비로서 사용자 등록을 수행한다.

SIP REGISTER를 받으면 S-CSCF는 사용자와의 인증과 키 일치를 위해 AV를 필요로 한다. 만약, S-CSCF가 유효한 AV를 가지고 있지 않다면 HSS에게 CM1에서 AVn을 요구한다. 물론, HSS는 IMPI와 IMPU가 동일한 사용자의 것인지를 확인한다.

CM1:
Cx-AV-Req(IMPI, n)

CM2:
Cx-AV-Req-esp(IMPI,RAND1//AUTN1/|XRES1||CK1||IK1,……,RANDn||AUTNn||XRESn||CKn||IKn)

그리고나서, S-CSCF는 SM4 메시지인 SIP 4xx Auth_Challenge를 보내는데, CK는 선택사항이다.

SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, (CK))
P-CSCF는 SM4 메시지에서 RAND와 AUTN만 UE에 전송하는데, Digest AKA에서는 challenge인 "nonce"에 해당한다.

SM6:
4xx Auth_Challenge(IMPI, RAND, AUTN)

SM6을 받은 UE는 MAC, SQN 등을 검증하고 둘다 성공하면 RES를 SM7에서 전송하고 CK, IK 등을 계산한다. 이때 SM7은 Digest AKA에서 response인 "password"에 해당한다.

SM7:
REGISTER(IMPI, RES)

SM7은 S-CSCF까지 포워딩되어서 S-CSCF는 XRES를 확인한다. 검증이 성공하면 사용자는 인증이 되고 IMPU는 S-CSCF에 등록이 된다. 이때 Cx 과정에서 등록 플래그가 업데이트되고, 그리고나서 UE에게 인증 성공 메시지를 보낸다.
지금까지는 인증이 성공하는 경우를 설명하였는데, 사용자나 네트워크 측에서 인증이 실패하는 경우는 UMTS AKA의 경우와 마찬가지이다. 여기에서는 간단히 각각에 대한 메시지 구성만 살펴보도록 한다.
사용자 인증 실패인 경우는 P-CSCF가 SM7을 삭제하고 인증절차는 종료된다.
네트워 인증 실패인 경우,

SM7:
REGISTER(Failure = AuthenticationFailure, IMPI)

CM3:
Cx-AV-Put(IMPI, Clear S-CSCF name)

SM10:
SIP/2.0 4xx Auth_Failure

동기 실패인 경우,

SM7:
REGISTER (Failure(Synchronization Failure, AUTS, IMPI)

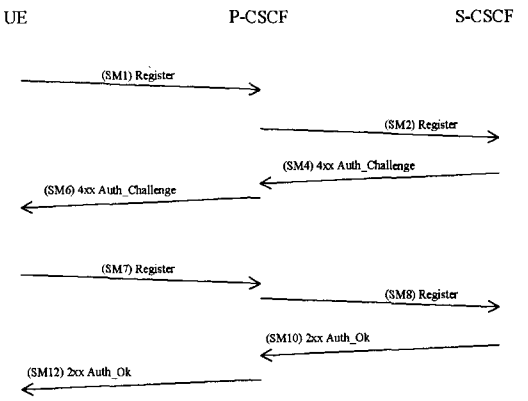
CM3:
Cx-AV-Req(IMPI, RAND,AUTS, n)

CM4:
Cx-AV-Req-esp(IMPI,RAND1//AUTN1/|XRES1||CK1||IK1,……,RANDn||AUTNn||XRESn||CKn||IKn)

한편, UE와 P-CSCF 사이의 SIP 시그널링의 무결성을 IP 계층에서 보호하기 위해서는 IPsec ESP가 transport mode로 사용된다. IPsec에 기반한 보안 설정에 관해서는 다음 절에서 설명한다.

4.3. IMS SA 설정 절차

IMS에서 SA 설정은 어떤 보안 서비스가 적용되어야 하고, 또, 언제 보안 서비스가 시작되어야 하는지를 결정하기 위해서 필요하다. 이 절에서는 UE와 P-CSCF 사이에서 IMS 시그널링을 보호하기 위한 보호 방법과 보안 파라메터 설정에 관해서 설명한다.



〔그림 5〕 SA 설정 절차

그림 5는 SA 설정 과정을 설명하기 위해 그림 4를 좀더 간략화 시킨 것이다.

UE는 자신의 위치를 등록하고 보안모드 설정을 위해 S-CSCF에게 SM1 Register 메시지를 보낸다. 등록절차는 4.2 절에서 설명하였다. 그리고, 보안모드 설정을 시작하기 위해 UE는 SM1 메시지는 Security-Setup 메시지를 포함한다.

SM1:
REGISTER(Security-setup = integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info]), IMPI, IMPU)

SA_ID_U는 UE에서 inbound (unidirectional) SA를 유일하게 식별하기 위해 사용된다. 그리고, Info 필드는 특별한 목적을 위해 reserve 되는데, 보안보드 설정에서 info 필드를 사용할지의 여부와 사용한다면 어떻게 사용할지를 명시해야한다.

P-CSCF는 제안된 메커니즘과 알고리즘들 중에서 각각 하나씩 선택하고 선택된 것들을 UE에 전송한다. SA_ID_P는 P-CSCF에서 (unidirectional) inbound SA를 유일하게 식별하기 위해 선택된다.

SM6:
4xxAuth_Challenge(Security-setup = integrity mechanism, [confidentiality mechanism], integrity algorithm, [confidentiality algorithm], SA_ID_P, [info], IMPI)

UE는 SM1과 SM6에서 협상된 파라메터와 메커니즘에 의해 SA를 설정하고 SIP 메시지에 대해서 해당되는 보호 방법을 적용한다. 즉, SM7에서 무결성을 제공한다. (선택적으로 기밀성 제공)

SM7:
REGISTER(Security-setup = integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info], IMPI)

UE로부터 SM7을 받은뒤에, P-CSCF는 이 메시지의 Security-setup과 SM1에서 받은 Security-setup을 비교한다. P-CSCF가 S-CSCF에게 보내는 SM8 메시지에는 UE로부터 받은 메시지가 무결성이 보장된 메시지라는 정보를 포함한다.

SM8:
REGISTER(Integrity-Protection = Successful, IMPI))

마지막으로 P-CSCF는 UE에게 SM12를 보냄으로서 보안모드 설정이 에러없이 성공적으로 완료되었다는 것을 알린다.

지금까지는 보안모드 설정이 성공하는 경우를 설명한 것이다. 하지만, 역시 보안모드 설정에서도 에러가 발생할 수도 있다.

P-CSCF가 UE에 의한 SM1의 보안모드 설정 요구를 수용할 수 없을 때, SM6에서 4xx Unacceptable_ Proposal로 응답함으로서 실패을 알리고 등록 과정은 종료된다. 또, UE에서 P-CSCF로 보내는 SM7의 security-setup line이 검증될수 없을 때, 즉, 보호되지 않은 SM1 security-setup line과 보호된 SM7 security-setup line이 일치하지 않을 때에도 에러가 발생한다. 그러면, S-CSCF가 SM10과 SM12에서 4xx Unacceptable_ Proposal 메시지를 보내서 등록절차를 끝내며, SM8 메시지는 다음과 같이 구성된다.

SM8:
REGISTER(Security-setup = integrity mechanisms list, [confidentiality mechanisms list], integrity algorithms list, [confidentiality algorithms list], SA_ID_U, [info], Failure =NoCommonIntegrityAlgorithm, IMPI, IMPU)

한편, IPsec ESP를 이용한 SIP 무결성이 적용될 때, 보호되지 않거나 보호되더라도 잘못 사용된 IP 패킷을 가진 SIP 메시지는 IP 계층에서 삭제되어서 SIP 계층까지 전달되지 않는다. 하지만 초기 REGISTER 메시지, 네트워크 인증 실패를 지시하는 REGISTER 메시지, 동기 실패를 지시하는 REGISTER 메시지는 보호되지 않더라도 P-CSCF에 의해서 받아들여져서 S-CSCF에 까지 전송이 되어야 한다. 그러므로, 이러한 메시지들은 IP 계층에서 삭제되지 않아야 하는데, 이것은 P-CSCF에서 보호되지 않

은 메시지에 대해 고정된 포트를 사용함으로서 가능하다. UE는 P-CSCF discovery 과정에서 P-CSCF의 IP 어드레스와 포트를 알 수 있으며, UE는 이 주소와 포트를 사용하여 초기 REGISTER 메시지를 보낸다. 그러면, 보호되지 않은 메시지라도 P-CSCF의 IP 계층에서 삭제되지 않는다. 인증 실패를 지시하는 REGISTER 메시지나 동기 실패를 지시하는 REGISTER 메시지도 마찬가지로 적용한다.

또한, 보호된 패킷에 사용되는 포트는 P-CSCF에 의해서 고정되고, 보안모드 설정 절차의 SM6 메시지의 info 필드를 이용하여 UE로 전송된다. 이러한 IP와 포트 정보는 SIP 메시지의 IMPU에 관련된 inbound SA가 올바른가를 검증하는데도 사용된다.

V. 결 론

본 고에서는 3GPP 네트워크 영역에서의 MAP 보안, IP 보안, 그리고, IMS 보안에 관하여 분석하였다. 다양한 네트워크와 프로토콜이 사용되는 3세대 이동통신 시스템에서는 무선구간 뿐만 아니라 유선구간에서의 정보보호 역시 중요한 문제로 등장하였다. 이에 3GPP SA3와 IETF security WG는 계속해서 보안 메커니즘을 수정, 보완하고 있다. 하지만, 아직까지 보안에 관해 명확한 해결책을 제시할 수 없는 부분도 많아서, 신뢰할 수 있고 효율적인 네트워크 보안을 위해서는 더욱더 많은 연구가 필요하다.

참 고 문 헌

[1] 3GPP TS 33.200 Network Domain Security : MAP application layer security

[2] 3GPP TS 33.210 Network Domain Security : IP network layer security

[3] 3GPP TS 33.203 Access security for IP-based services

[4] 3GPP TS 33.102 Security architecture

[5] 3GPP TS 23.228 IM Multimedia Subsystem(IMS)

[6] 3GPP TS 23.002 Network architecture

[7] IETF RFC2617 HTTP authentication: Basic and Digest Access Authentication

[8] IETF RFC2543bis SIP: Session Initiation Protocol

[9] IETF RFC2617 HTTP authentication: Basic and Digest Access Authentication

[10] IETF RFC2406 IP Encapsulating Security Protocol(ESP)

[11] IETF RFC2408 Internet Security Association and Key Management Protocol(ISAKMP)

[12] IETF RFC2409 Internet Key Exchange (IKE)

[13] IETF internet draft HTTP Digest Authentication using AKA (draft-ietf-sip-digest-aka-00)

[14] 3GPP TSG SA WG3 #22bis aSIP ad hoc S3z020051

[15] 3GPP TSG SA WG3 #22bis aSIP ad hoc S3z020052

[16] 3GPP TSG SA WG3 #22bis aSIP ad hoc S3z020053

[17] 3GPP TSG SA WG3 #22bis aSIP ad hoc S3z020055

[18] 3GPP TSG SA WG3 #22bis aSIP ad hoc S3z020056

〈著者紹介〉

김 건 우 (Keonwoo Kim)
정회원

1999년 2월 : 경북대학교 전자공학과(학사)
2001년 2월 : 경북대학교 전자공학과(석사)
2001년 1월~현재 : 한국전자통신연구원 연구원
관심분야 : 이동통신, 암호학, 네트워크 보안

류 희 수 (Heuisu Ryu)
정회원

1990년 2월 : 고려대학교 수학과(학사)
1992년 2월 : 고려대학교 수학과(석사)
1999년 5월 : Johns Hopkins University 수학과(박사)
2000년 7월~현재 : 한국전자통신연구원 선임연구원
관심분야 : 타원곡선 암호, 대수학, 이동통신 정보보호