3GPP NDS 표준안 분석

김건우*, 장구영*, 류희수*

*한국전자통신연구원 정보보호연구본부

Analysis about 3GPP network domain security

Keonwoo Kim*, Ku-Young Chang*, Heuisu Ryu*

*Electronic and Telecommunication Research Institute

요 약

3GPP NDS에 관한 연구나 표준화 제정 현황은 아직까지 활발히 이루어지고있는 것은 아니다. 하지만, 다양한 프로토콜이 사용되고 서비스 제공자의 핵심망에 대해 전적으로 신뢰를 할 수 없는 상황에서 유선구간에서의 정보보호도 역시 무선구간 만큼이나 중요한 문제로 대두되고 있다. 본 논문에서는 3GPP 유선구간에서의 정보보호를 위한 3GPP의 최신 표준안을 분석한 것이다. 아직 stage 3 스팩까지는 공개되지 않았지만 stage 2 수준의 표준은 현재 활발히 진행중이다.

I. 서론

W-CDMA 방식 IMT-2000의 표준을 제정하는 3GPP(3rd Generation Partnership Project)에서는 무선구간의 보안을 위하여 AKA 절차를 수행하고 또한 보안모드를 협상해서 데이터에 대한 무결성과 암호화를 제공한다. 하지만, 유선구간인 핵심망에서의 보안은 무선구간에 비해서 아직 연구가 활발이 진행되지 않고 있고, 자세한 스팩 역시 나와있지 않은 상태이다.

SS7(Signaling System no. 7) 프로토콜에 기반한 2세대 시스템과 비교해서, 3세대 3GPP 시스템에서는 정보보호에 관한 대책이 더욱 중요해졌다. GPRS 백본망으로 IP를 기본으로 하는 시스템이 도입되었고, 이것은 UMTS 네트워크에까지 확장하게 되었다. IP 프로토콜은 사용자 데이터 뿐만 아니라 시그널링 트래픽에 대해서도 사용되며, IP의 도입은 패킷 스위칭으로 향한 이동뿐만이 아니라 개방되고 쉽게 접근할 수 있는 프로토콜로의 전환을 의미한다. 따라서, 정보보호도 이러한 관점에서 다시 재고되어서 새로운 공격과 위협으로부터 보호되어야 한다. 즉, 3세대 시스템에서 SS7과 IP에 기초한 핵심망을 보호하는 것은 필수적이고, 이를 위해서 기밀성, 무결성, 인증, 부인봉쇄와 같은 암호학적 서비스가 제공되어야 한다.

본 논문에서는 3GPP에서의 핵심망 보호에 관한 내용을 살펴본다. 구체적으로 말하면, SS7에 기반을 둔 UMTS 네트워크 control plane 시그널링 프로토콜 뿐만 아니라 IP에 기반을 둔 control plane 시그널링 프로토콜에서의 정보보호 구조를 분석한다.

II. 3GPP 핵심망 보안 개요

이 장에서는 3GPP 핵심망 보안구조의 기본적인 개념에 관해서 살펴본다. 보호 도메인(Security Domain)이란 하나의 관리 주체에 의해서 보호되는 네트워크를 말하는데, 하나의 보호 도메인 내에서는 동일한 수준의 security를 가진 동일한 보안 서비스가 지원된다. 일반적으로 하나의 운영기관에 의해서 운영되는 네트워크는 하나의 보호 도메인만을 지원하지만, 네트워크가 여러 개의 서브 네트워크로 분할된다면 보호 도메인도 역시 여러 개로 나뉘어진다. IP 구조와 SS7 구조는 전송 메커니즘등의 기술적인 차이로 인하여, 이들을 사용하는 네트워크의 보호 방법도 달라질 수 밖에 없다.

● 순수한 IP에 기반을 둔 네트워크가 보호되기 위해서는, IPsec을 사용해서 네트워크 계층에서 보

호된다.

● SS7 프로토콜을 사용하는 네트워크가 보호된다면, MAP 수준에서 보호된다.

2.1 보호 도메인과 인터페이스

UMTS 네트워크는 논리적으로나 물리적으로 여러 개의 보호 도메인으로 나뉘어 진다. Control plane 보호 도메인은 SEG나 KAC에 의해서 서로 분리된다. 표 1에서는 NDS(Network Domain Security) 인터페이스를 나타내었다.

표 1 : 핵심망 보안 인터페이스

인터페이스	내용	네트워크 타입
Za	SEG와 SEG 사이의 보호 인터페이스	IP
Zb	동일한 네트워크 내에서 SEG와 NE 사이의 보호 인터페이스	IP
Zc	동일한 네트워크 내에서 NE와 NE 사이의 보호 인터페이스	IP
Zd	네트워크 사이의 보호 인터페이스	IP
Ze	동일한 네트워크 내에서 KAC와 MAP-NE 사이의 보호 인터페이스	IP
Zf	MAP-NE 사이의 보호 인터페이스	SS7/MAP

2.2 Security Gateway

SEG(Security Gateway)는 IP 보호 도메인의 가장자리에 위치하는 개체로, native IP에 기반을 둔 프로토콜을 보호하기 위해 사용된다. SEG는 서로 다른 IP 보호 도메인의 SEG 사이에서 사용되는 Za 인터페이스와, 동일한 보호 도메인 내에서 SEG와 NE 사이에서의 Zb 인터페이스에서 정의된다.

모든 NDS/IP(Network Domain Security over IP protocol) 트래픽은 SEG를 거쳐서 보호 도메인의 입력이 되거나 출력이 되고, 각각의 보호 도메인은 하나 이상의 SEG를 가질 수 있다.

2.3 Key Administration Center

SS7 또는 SS7/IP에 기반을 둔 프로토콜에서의 KAC(Key Administration Center)는 MAP-NE(Network Element)에 대한 MAPsec SA(Security Assocoation)를 협상하기 위해 사용되는 개체이다. 어떤 MAP-NE가 다른 MAP-NE와 안전한 연결의 설정을 원하면 KAC에게 MACsec을 요구한다. 그러면 KAC는 미리 협상된 MAPsec SA를 제공하거나, 새로운 MAPsec SA를 다시 협상하여 원하는 결과를 제공한다.

KAC에 관한 중요한 역할은 다음과 같다.

① 다른 네트워크에 속하는 KAC와 MAP-SA 협상

② MAP-SA의 유효기간이나 운영기관의 정책에 따라 MAP-SA 갱신

③ KAC와 동일한 네트워크에 속하는 노드에게 유효한 MAP-SA 분배

④ KAC와 자신의 네트워크에 존재하는 NE 사이에 ESP로 보호된 통신 설정

III. Native IP 프로토콜에서의 보안

3.1 보안구조

IP에 기반한 네트워크의 키 관리와 분배는 IKE 프로토콜을 기본으로 한다.

NDS/IP 구조의 기본적인 특징은 hop-by-hop 보안이다. 이것은 chained-tunnel/hub-and-spoke 모델과도 유사하다. hop-by-hop 보안의 사용은 내부적으로 보호 도메인을 분리하여 작동하는 것을 쉽게 하고, 외부의 보호 도메인을 대하여 보호 정책을 수립하는 것을 쉽게 한다.

NDS/IP에서는 단지 SEG만이 다른 보호 도메인의 개체와 직접적인 통신에 참여하는데, 이 때 SEG는 보호 도메인 사이에 ESP 터널을 설정하고 관리한다. 그리고, 각자의 인터페이스에 대해서 자신의 SAD(Security Association Database)와 SPD(Security Policy Database)를 관리한다. 그리고, NE는 동일한 보호 도메인 내에서 SEG나 다른 NE와 필요에 따라 ESP 터널을 설정하고 관리할 수 있다. 도메인 A의 NE가 도메인 B의 NE와 연결을 설정하고자 할때는 반드시 SEG를 통하여 연결되고, 최종 목적지까지 hop-by-hop으로 보호된다.

3.2 인터페이스

● Za 인터페이스 (SEG-SEG)

이 인터페이스를 통해 두 보호 도메인 사이의 안전한 IP 통신이 설정된다. SEG는 그들 사이의

안전한 터널을 협상, 설정, 유지하기 위하여 IKE를 이용한다. 하나의 SEG는 모든 로밍하는 상대 개체들 중에 단지 하나에게만 할당된다. 이것은 SA와 터널의 수를 제한하게 하는 이유가 되는데, 일반적으로 한 네트워크 내에서 SEG의 수는 BG(Border Gateway)의 수보다 많지 않다.

Za는 모든 보호 도메인에서 필수적인 인터페이스이다

● Zb 인터페이스 (NE-SEG)

Zb는 동일한 도메인 내에서 NE와 SEG 사이의 인터페이스이다. NE와 SEG는 그들 사이에 ESP 터널을 설정하고 관리해서 안전한 트래픽을 교환한다. 일반적으로 ESP는 암호화와 인증/무결성 둘 다를 위해서 사용되고, 도메인 외부로 나가는 모든 control plane 트래픽은 무조건 SEG를 거친다.

● Zc 인터페이스 (NE-NE)

Zc는 동일한 도메인 내에서 NE들 사이의 인터페이스이다. NE는 그들 사이에 ESP 터널을 설정하고 관리해서 안전한 트래픽을 교환한다. 서로 다른 도메인에 속하는 NE들 사이에는 NE-NE 인터페이스가 없다.

Zc 인터페이스의 구현 여부는 보호 도메인 관리 주체의 결정사항이다.

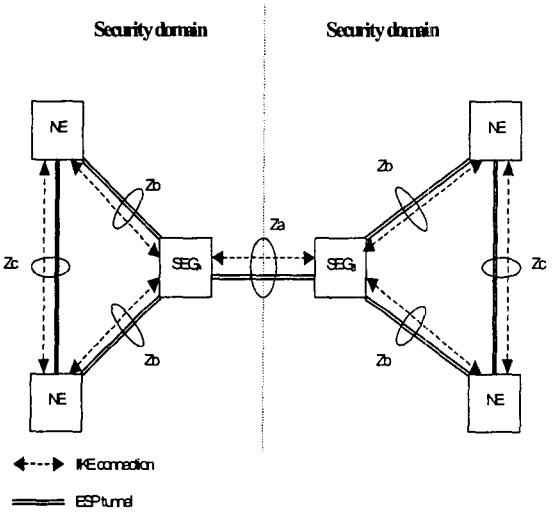


그림 1 : NDP/IP 구조와 인터페이스

IV. MAPsec

4.1 보안구조 및 인터페이스

SS7 및 SS7/IP based 프로토콜에 대한 보호 메커니즘은 응용 계층에서 구현된다. 단지 SS7 MAP 프로토콜만이 보호되고, 이때의 MAP 보안을 MAPsec이라 한다. MAPsec에서는 데이터 무결성, 데이터 출처 인증, 재전송 방지, 기밀성과 같은 보호 서비스가 제공된다.

다음은 SS7 기반 프로토콜에서의 보안을 위한 인터페이스이다.

● Zd 인터페이스 (KAC-KAC)

Zd는 MAP 보호 도메인 사이에서 MAPsec SA를 협상하기 위해 사용된다.

● Ze 인터페이스 (KAC-NE)

Ze는 동일한 MAP 도메인 내에서 MAP-NE와 KAC 사이에서의 인터페이스이다. KAC와 NE는 그들 사이에서 ESP 터널을 설정하고 관리할 수 있는데, 이 터널은 KAC로부터 목적지의 MAP-NE에 까지 MAPsec SA를 전송하기 위해 사용된다.

● Zf 인터페이스 (NE-NE)

Zf 인터페이스는 동일하거나 서로 다른 도메인의 NE들 사이에 위치한다. MAP-NE는 MAP 동작을 보호하기 위해 KAC로부터 받은 SA를 사용하고, MAP 동작은 적용된 MAPsec 보호 프로파일에 의해서 선택적으로 보호된다.

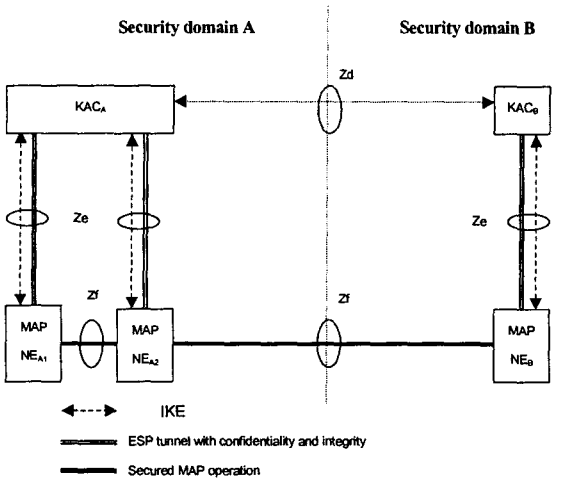


그림 2 : NDS/SS7 구조와 인터페이스

4.2 MAPsec 구조

MAPsec에서 제공되는 보호 서비스는 사용되는 보안모드에 따라 달라진다.

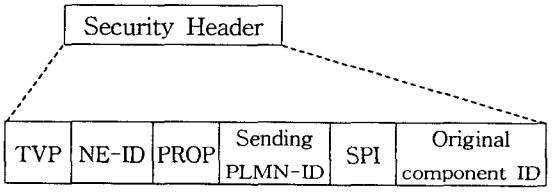
표 2 : MAPsec 보안모드와 서비스

보호모드	서비스
0	-
1	무결성, 인증
2	기밀성, 무결성, 인증

MAPsec에 의해 보호되는 MAP operation은 Security Header와 Protected Payload로 구성된다. 세가지 보호모드에서 Security Header는 cleartext로 전송된다.

1) Security Header

Security Header는 다음과 같이 구성된다.



● TVP

안전한 MAP operation의 재전송 방지에 사용되는 16비트 time-stamp로서, 수신 NE는 time-stamp가 적당한 time window 내에 있을 때에만 operation을 인정한다. 하지만, 아직 time window의 크기는 표준화되어 있지 않다.

● NE-ID

동일한 TVP 구간내에서 다른 NE에 대해 다른 IV를 생성하기 위해 사용되는 6 octet 값으로, PLMN 마다 다른 값을 가져와 한다. 그리고, NE-ID는 MCC(Mobile Country Code)와 MNC(Mobile Network Code)가 없는 NE의 E.164 global title 이다.

● Proprietary field (PROP)

하나의 NE에 대해 같은 TVP 구간 내에 있는 다른 보호된 MAP 메시지에 대해 다른 IV를 생성하기 위한 4 octet 값이다.

● Sending PLNM-ID

송신 PLNM의 ID number로서, PLNM-Id에 대한 값은 송신 네트워크의 MCC와 MNC의 결합으로 이루어진다.

● Security Parameter Index (SPI)

MAP-SA을 유일하게 식별하기 위해서 송신측의 PLNM과 결합하여 사용되는 임의의 32비트 값이다.

● Original Component identifier

안전하게 전송되어질 MAP operation(Error Code에 의해 정의된 Error, 사용자 정보 등) 내의 성분의 형태(invoke, result, error)를 나타낸다.

2) Protected Payload

● 보호모드 0

보호모드 0에서는, 어떤 보호 서비스도 제공되지 않고 Protected Payload는 원래 MAP operation의 payload와 동일하다. 따라서 Security Header 없이 전송하는 것이 가능하다.

● 보호모드 1

보호모드 1에서의 Protected payload는 다음과 같이 구성된다.

Cleartext || f7(security Header || Cleartext)

||

Cleartext || $H_{KSXY(int)}$(Security Header || Cleartext)

여기서 cleartext는 original MAP 메시지의 payload이고, 데이터 출처 인증과 무결성을 위한 32 비트 MAC 값은 SA에서 협상된 무결성 키 $KS_{XY}(int)$를 사용한 f7(Security Header || Cleartext) = $H_{KSXY(int)}$(Security Header || Cleartext) 이다. 무결성 알고리즘으로는 ISO/IEC 9797 Part 1의 padding method 2를 이용한 CBC MAC 모드 AES를 사용한다.

● 보호모드 2

보호모드 2에서의 Protected Payload는 다음과 같이 구성된다.

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

||

$E_{KSXY(con)}$(Cleartext) || $H_{KSXY(int)}$(Security Header || $E_{KSXY(con)}$(Cleartext))

여기서 cleartext는 original MAP 메시지의 payload이고, SA에서 협상된 기밀성 키 $KS_{XY}(int)$와 초기화 벡터 IV 및 암호화 함수 f6을 사용해서 기밀성이 보장된다. 이때 사용되는 기밀성 암호 알고리즘은 ISO/IEC 10116 counter mode를 이용한 stream cipher mode의 AES이다. 또한, 인증과 무결성은 무결성 키 $KS_{XY}(int)$와 메시지 인증 코

드(MAC-M) f7을 이용해서 보장된다.

V. 결론

본 논문에서는 3GPP Network Domain Security에 관한 최근 표준 내용을 분석하였다. 무선 구간에 비해서 아직까지는 구체적인 내용까지 표준으로 제정되지는 않았다. 하지만, 3GPP NDS에 관한 TS 문서를 살펴보면, 최근 1년 동안에 상당히 많은 부분들에 관한 개념이 명확해지고 요구사항이나 기본 정책들이 안정화되어가고 있는 추세이다. Release 4 시스템에서는 MAP 보안과 IP에 기반한 보안 메커니즘이 공존하다가 Realease 5에서는 점점더 IP에 기반한 보안쪽으로 많이 기술하고 있다. 따라서. 3GPP의 표준을 계속 follow-up 하는 동시에 IETF 표준안에 대한 분석이 병행해서 이루어져야 할 것으로 판단된다.

참고문헌

[1] 3GPP TS 33.200 v0.3.2 Network Domain Security (Release 5)
[2] 3GPP TS 33.200 v0.4.0 Network Domain Security (Release 4)
[3] 3GPP TS 33.210 v0.5.5 IP network layer security (Release 5)
[4] 3GPP TS 33.800 v0.4.0 MAP application layer security (Release 5)
[5] 3GPP TS 33.800 v4.0.0 MAP application layer security (Release 4)
[6] 3GPP TS 33.203 v0.4.0 Access security for IP-based services (Release 5)
[7] 3GPP TSG SA WG3 Security - S3#19
[8] 3GPP TS 43.020 v4.0.0 Security related network function (Release 4)
[9] 3GPP TS 33.800 v0.3.5 Principle for network domain security (Release 4+5)