정 보 보 호 학 회 지
제 29 권 제5호, 2019. 10

3GPP 5G 보안 구조의 특징 및 주요 개선사항

박 종 근*, 김 종 현*, 문 대 성*, 김 익 균*

요 약

우리나라는 세계 최초로 초고속·초연결·초저지연의 5G 이동통신 상용화에 성공하였다. 비록 아직은 4G LTE 코어망과 연계하여 5G 서비스를 제공하고 있지만, 향후 5G 코어망이 구축된 이후에는 완전한 5G 네트워크를 통해 5G 융합서비스가 본격화될 전망이다. 그러나, 우리 실생활과 밀접한 새로운 미래 혁신 서비스에 대한 기대와 열망 때문에 5G 네트워크 환경이 갖고 있는 잠재적 보안위협이나 취약점을 간과해서는 안된다. 보다 고도화되고 지능화되는 사이버 공격에 대응하기 위해 위협 대응전략 또한 고도화되어야 한다. 본 논문에서는 5G 보안 기술을 이해하기 위해 3GPP의 5G 보안 기술규격인 TS 33.501을 바탕으로 5G 보안의 근간을 이루는 구조적 특징과 4G 대비 주요 개선사항을 중심으로 소개한다.

Ⅰ. 서 론

1984년 한국이동통신의 설립과 함께 카폰 서비스를 필두로 우리나라에서도 이동통신 서비스가 시작되었다. 이후 이동통신의 역사는 디지털 통신의 2세대와 모바일 데이터 서비스의 3세대, 그리고 All-IP 기반의 광대역 서비스를 제공하는 4세대를 거쳐, 지금은 4차 산업혁명의 핵심 인프라로서 초고속, 초연결, 초저지연의 디지털 혁신서비스를 제공하는 5세대까지 매 10년을 주기로 빠르게 발전해 오고 있다.

흔히 5G라고 부르는 이동통신기술은 2015년 국제전기통신연합(International Telecommunication Union; ITU)에서 IMT-2020(International Mobile Telecommunications-2020)으로 그 비전을 제시하면서 시작되었다. 4G 대비 20배 더 빠른 최대 전송속도 20Gbps의 초고속성, 전송지연이 10분의 1로 단축된 1ms의 초저지연성, 1㎢ 당 10배 더 많은 100만개의 기기를 연결할 수 있는 초연결성을 핵심성능으로 요구한다[1].

실감컨텐츠, 스마트제조, 자율주행차, 스마트시티, 디지털 헬스케어 등과 같은 초고속·초연결·초저지연의 미래 ICT(Information and Communication Technology) 혁신서비스는 4차 산업혁명과 함께 우리 실생활에도 많은 변화를 불러올 것으로 기대된다. 그러나, 한편으로는 5G 이동통신 환경의 취약점을 악용한 사이버 공격 위험에 노출될 가능성도 갈수록 늘어나고 있다.

지금까지의 많은 연구결과에 따르면, LTE(Long Term Evolution) 환경에서는 무선 재밍(jamming), 가입자 신원정보인 IMSI(International Mobile Subscriber Identifier)의 탈취, 허위 기지국을 이용한 중간자 공격(Man-in-the-middle attack) 그리고 상호접속 프로토콜인 Diameter의 취약점을 활용한 공격 등을 대표적인 위협으로 꼽을 수 있다. 그러나, 5G 환경에서는 4G 보안위협 뿐만 아니라 5G 네트워크의 구조적 변화, 서비스 트래픽의 변화 그리고 서비스 특성의 변화에 따른 새로운 잠재적 보안위협이 부각되고 있다[2]~[4].

우리 실생활과 밀접한 다양한 5G 융합서비스 환경에 대한 사이버 공격은 단순히 이동통신서비스의 장애 유발로 그치지 않고, 국민의 재산과 생명을 위협하는 재난으로 이어질 수 있다는 점에서 보다 고도화된 정보보호 및 위협 대응전략이 요구된다.

본 논문에서는 5G 보안 기술을 이해하기 위해 5G 기술규격을 제정하는 3GPP(The 3rd Generation Partnership Project)의 5G 보안 기술규격인 TS 33.501([5])을 바탕으로 5G 보안의 근간을 이루는 구조적 특징과 4G LTE 대비 주요 개선사항을 중심으로 소개하기로 한다.

본 연구는 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)
* 한국전자통신연구원 지능화융합연구소 정보보호연구본부 (queue@etri.re.kr, jhk@etri.re.kr, daesung@etri.re.kr, ikkim21@etri.re.kr)

Ⅱ. 3GPP 5G 보안 구조

본 장에서는 Release 15으로 발간된 TS 33.501 규격에 제시된 5G 보안 구조와 보안 기능에 대해 살펴본다.

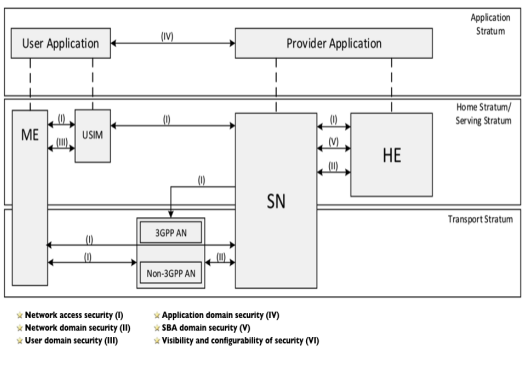
2.1. 보안 구조

3GPP 표준에서는 (그림 1)과 같이 보안 구조를 총 6개의 도메인으로 구분하여 정의한다.

네트워크 접속 보안(Network Access Security)은 단말이 3GPP 접속망(access network)과 3GPP가 아닌 접속망을 통해 안전하게 서비스를 인증하고 접속할 수 있도록 하며, 특히 무선 인터페이스 등에 대한 공격으로부터 망을 보호하는 일련의 보안 기능이다. 또한 접속 보안을 위해 서비스를 제공하는 망(Serving Network; SN)에서 접속망으로 보안 컨텍스트를 전달하는 것도 포함된다. 특정 보안 메커니즘으로는 양방향 인증, 전송 암호화 및 무결성 보호가 있다.

네트워크 도메인 보안(Network Domain Security)은 네트워크 노드가 시그널링 및 사용자 데이터를 안전하게 교환할 수 있도록 하는 일련의 보안 기능으로서, 서비스를 제공하는 망(SN)과 사용자가 가입한 홈망(Home Network; HN) 사이 또는 접속망과 코어망(core network) 사이의 인터페이스에 대한 보안 기능을 정의한다.

사용자 도메인 보안(User Domain Security)은 모바일 기기에 대한 사용자의 접근을 보호하는 일련의 보안 기능이다. 모바일 기기는 PIN(Personal Identification Number) 코드와 같은 내부 보안 메커니즘을 이용하여 모바일 기기와 USIM (Universal Subscriber Identity Module) 간의 보안을 보장한다.



〔그림 1〕 5G 보안 구조

응용 도메인 보안(Application Domain Security)은 사용자 도메인과 서비스 제공자 도메인에 있는 응용들이 메시지를 안전하게 교환할 수 있도록 하는 일련의 보안 기능이다. 응용 도메인 보안 메커니즘은 전체 이동통신망과는 독립적(transparent)이며 응용 공급자가 제공한다.

서비스 기반 구조(Service based Architecture; SBA) 도메인 보안(SBA Domain Security)은 서비스 기반 구조에 의한 네트워크 기능들이 안전하게 통신할 수 있도록 하는 일련의 보안 기능이다.

보안의 가시성과 설정가능성은 (그림 1)에는 나타나 있지 않지만, 보안 기능의 동작여부를 사용자에게 알려줄 수 있도록 하는 일련의 기능이다.

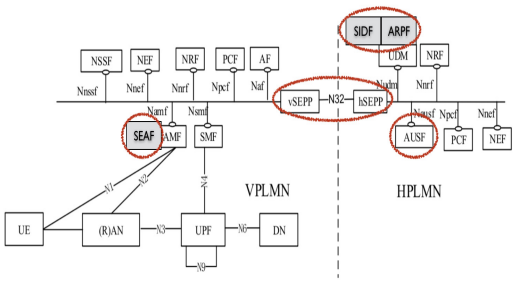
이상과 같이 6개의 도메인으로 정의된 5G 보안 구조에서 4G 보안 구조([6])에 대비하여 눈에 띄는 차이점은 네트워크 접속 보안 도메인의 변화와 서비스 기반 구조 도메인 보안이 추가된 것이다. 네트워크 접속 보안 도메인의 경우 5G 요구사항에 따라 3GPP 접속망 뿐만 아니라 3GPP가 아닌 접속망을 통해서도 동일한 하나의 인증 체계를 통해 접속할 수 있도록 개선되었다. 또한 서비스 기반 구조 도메인 보안은 5G에 새롭게 도입된 서비스 기반 구조로 인해 추가된 보안 기능으로서 4G 보안 구조에서는 정의되지 않았던 기능이다.

2.2. 보안 기능

5G 시스템 구조에서는 서비스 기반 구조(Service based Architecture)에 따라 다양한 제어 기능이 정의되어 있다. 본 절에서는 5G 제어 기능 중 보안과 관련된 기능에 대해 살펴본다.

4G LTE의 HSS(Home Subscriber Server)에서 담당하는 기능은 AUSF(Authentication Server Function)과 ARPF(Authentication Credential Repository and Processing Function)에서 각각 처리한다.

AUSF는 단말로부터의 인증 요청을 처리하고, 인증 완료단계에서 단말이 접속하고 있는 망(SN)에 암호화되지 않은 가입자의 신원정보인 SUPI(Subscription Permanent Identifier)를 전달하며, 가입자의 인증 결과를 UDM(Unified Data Management)에 보고하고,



〔그림 2〕 5G 구조와 보안 기능

S_{EAF}(Security Anchor Function)에 전달할 키인 K_{SEAF}를 생성하는 기능 등을 수행한다.

ARPF는 UDM에 속한 부분 기능으로서 가입자의 고유 신원정보인 SUPI와 키 생성에 사용되는 최상위 키(long-term key)를 보관하며, 하위 키 생성과정에서 CK, IK, K_{AUSF} 등을 생성한다.

AUSF와 ARPF 외에 5G에서 보안 기능 강화를 위해 새롭게 도입된 기능으로는 SIDF(Subscription Identifier De-concealing Function), SEAF(Security Anchor Function), SEPP(Security Edge Protection Proxy)가 있다.

SIDF는 ARPF와 함께 UDM에 속한 부분 기능으로서, 초기 인증 단계에서 단말에서 전송한 SUCI (Subscription Concealed Identifier)를 다시 복호화하여 SUPI를 얻는 기능을 수행한다.

SEAF는 단말이 서비스를 제공받는 망(SN)에서 단말에서 전송한 SUCI를 이용한 인증을 수행하는 기능을 담당한다. 현재 Release 15에서는 SEAF는 AMF(Access and Mobility Management Function)에 속한 부분 기능으로 정의되어 있다.

마지막으로 SEPP는 로밍시 이동통신망 사업자간 주고 받는 시그널링 메시지에 대한 응용계층의 메시지 암호화 및 무결성 보호 기능을 수행한다.

Ⅲ. 주요 보안 개선사항

이동통신기술이 새로운 세대로 발전할 때마다 보안 위협과 취약점도 더욱 증가하기 마련이다. 일반적으로 기존 세대에서 발견되었던 보안 취약점들이 그대로 다음 세대에서도 유효하기도 하지만, 새로운 통신기술과 구조를 채택함에 따라 불가피하게 수반되는 새로운 보안위협과 취약점들이 부각되기도 한다. 물론 표준 기술 규격을 제·개정함으로써 알려진 보안 취약점을 해소하기도 한다. 본 절에서는 TS 33.501 표준에서 기능이 강화되거나 새롭게 추가된 주요 5G 보안 기능들을 소개한다.

3.1. 가입자 신원정보 보호 강화

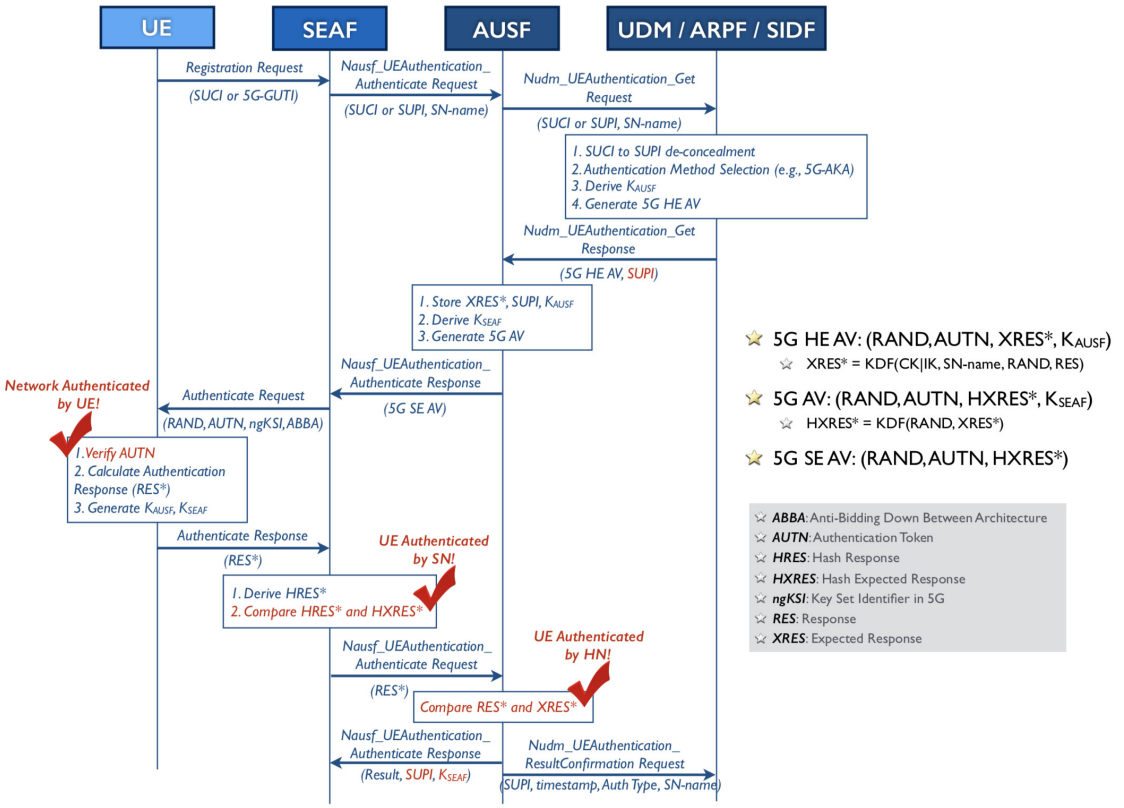
2G부터 4G까지 이동통신 환경에서 가장 부각되어 온 보안 이슈는 단말과 기지국 사이의 무선 구간에서 암호화되지 않은 채 전달되는 가입자 신원정보인 IMSI가 악의적인 공격자에 의해 탈취되는 것이다. 무엇보다도 IMSI 탈취 공격은 정상적인 사용자의 신원정보를 획득하는 것으로서 그 자체로 끝나지 않고 다른 유형의 공격을 위한 단초로 사용될 수 있다는 측면에서 그 위험성이 더욱 크다. 대표적인 예로는 피해 단말의 서비스를 차단하거나 서비스 정보를 탈취할 수도 있으며, 상대적으로 보안이 더욱 취약한 2G 또는 3G로의 접속을 유도하여 공격을 이어나가기도 한다.

이와 같은 문제의 심각성으로 인해 가입자 신원정보가 전달되는 초기 접속과정(5G의 Registration Request 메시지 전달 과정이며, 4G에서는 Attach Request 메시지에 해당함)에서 가입자 신원정보를 암호화해서 전달하도록 보안 기능이 강화되었으며, 5G에서 가장 눈에 띄는 보안 기능 개선사항 중 하나로 꼽을 수 있다.

IMSI 또는 NAI(Network Access Identifier) 등의 가입자의 신원정보는 SUPI로 불리우며, SUPI는 초기 접속과정에서 단말이 이동통신사업자의 Home Network Public Key로 암호화한 SUCI로 변형된 다음 기지국으로 전달된다. 전달된 SUCI는 앞서 소개한 UDM의 SIDF에서 SUPI로 복호화되어 가입자의 신원을 확인하는데 사용된다.

3.2. 인증 및 키 공유 체계 개선

인증은 이동통신 망에 접속하려는 가입자 단말과 이동통신 망간의 상호 인증 체계로서 4G LTE 환경에서는 EPS(Evolved Packet System) AKA(Authentication and Key Agreement) 절차를 사용하여 가입자는 망을 인증하고 망은 가입자를 인증하는 상호인증 절차를 진행한다. 그러나, EPS AKA 절차는 앞서 언급된 바와 같이 가입자의 신원정보인 IMSI가 보호되지 않은 채



〔그림 3〕 5G-AKA 인증 절차

Attach Request 메시지를 통해 기지국으로 전달되며 이 과정에서 악의적인 공격자에 의해 탈취되는 위험이 존재한다. 또한 망이 단말을 인증하는 과정에서 단말이 접속한 망(SN)은 단말을 인증하지만 단말이 가입되어 있는 망(HN)은 인증과정에 참여하지 못하는 한계가 있다.

5G에서의 인증은 5G AKA와 EAP(Extensible Authentication Protocol)-AKA' 절차가 기본 인증(Primary Authentication) 규격으로 정의되어 있다.

5G-AKA의 대략적인 절차는 (그림 3)과 같다. 단말에서 가입자 신원정보인 SUCI 또는 임시 신원정보인 5G-GUTI(Globally Unique Temporary UE Identifier)를 포함한 Registration Request 메시지를 SEAF/AMF로 전송한다. 이때 5G-GUTI가 사용되는 경우는 단말이 이전 등록과정에서 인증에 성공한 이후 AMF로부터 5G-GUTI를 부여받았을 때이며, 5G-GUTI는 AMF에서 매핑되는 SUPI로 변환된다. 만일 단말이 5G-GUTI를 갖고 있지 않거나 또는 보유한 5G-GUTI로 인증을 요청했으나 AMF로부터 5G-GUTI의 매핑정보가 없어 Identity Request 메시지를 전달받게 되면 단말은 즉시 SUCI를 이용하여 인증을 요청해야 한다.

등록요청을 수신한 SEAF는 SUCI 또는 SUPI를 바탕으로 단말이 가입한 이동통신사업자 정보를 얻고, 해당 이동통신 망(HN)의 AUSF로 현재 접속되어 있는 망(SN)의 정보와 함께 인증요청 메시지를 전달하면 AUSF는 다시 UDM으로 전달한다. UDM에서는 우선 SIDF를 이용하여 SUCI를 SUPI로 복호화하여 사용자를 확인하고 인증방법(5G-AKA 또는 EAP-AKA')을 선정한 다음, ARPF에 저장된 최상위 키 값을 이용하여 AUSF Key와 5G HE AV (Home Environment Authentication Vector)를 생성한다. AUSF에서는 UDM으로부터 전달받은 5G HE AV로부터 5G AV를 생성하고, 이 중에서 SEAF Key를 제외한 5G SE AV(Serving Environment Authentication Vector)를 SEAF에 전달한다. SEAF는 5G SE AV의 HXRES* 값을 제외한 값

을 포함한 Authenticate Request 메시지를 단말에 전달한다. 단말에서는 수신한 RAND 값과 단말의 USIM에 저장된 최상위 키 등을 이용하여 AUTN을 생성하고, 이 값이 SEAF로부터 전달받은 AUTN과 같은지를 검증함으로써 망을 인증한다. 그 다음으로 단말 인증에 사용될 RES* 값과 단말에서 사용될 AUSF Key와 SEAF Key를 순차적으로 생성한 다음, RES*를 Authenticate Response 메시지를 통해 SEAF로 전달한다. SEAF는 단말이 전송한 RES*를 이용하여 HRES*를 얻은 다음, AUSF로부터 전달받았던 5G SE AV의 HXRES* 값과 비교하여 단말을 인증한다. 즉, 단말에 서비스를 제공하는 망(SN) 입장에서 단말을 인증한다. 단말 인증을 완료한 SEAF는 단말에서 받은 RES*를 다시 AUSF에 전달하며, AUSF는 UDM으로부터 전달받았던 5G HE AV의 XRES* 값과 비교함으로써 홈망(HN) 입장에서 단말을 재차 인증한다. 인증이 성공적으로 완료된 후, AUSF는 단말이 접속한 망(SN)의 SEAF로 가입자의 신원정보인 SUPI와 SEAF Key를 전달하고 UDM에는 인증결과를 보고한다.

5G-AKA 절차의 특징은 4G EPS-AKA 절차의 약점을 보완한 것이다. 먼저 SUCI를 이용하여 초기 무선구간에서의 가입자 신원정보 탈취를 방지하였으며, 단말 인증과정에 있어 단말이 접속하여 서비스를 제공받고 있는 망(SN) 뿐만 아니라 단말이 가입하고 있는 홈망(HN)으로부터 동시에 인증을 받음으로써 인증을 한층 강화한 점이다. 또한 홈망에 의한 인증까지 완료되어야 가입자의 신원정보인 SUPI가 단말이 접속하고 있는 망(SN)으로 전달되도록 하고 이 SUPI가 있어야만 AMF Key를 생성할 수 있도록 함으로써, 홈망의 인증없이 단말이 접속한 망이 독자적으로 인증절차를 완료하고 후속 키 공유 및 보안 컨텍스트 설정 절차를 진행하는 일련의 비정상 절차가 진행될 수 있는 여지를 차단한다.

EAP는 IETF(Internet Engineering Task Force) 표준(RFC(Request for Comments) 3748)으로서 다양한 인증 매커니즘 및 프로토콜과의 결합을 통해 약 40여종의 다양한 인증방식을 제공하는 범용의 인증 프레임워크이다[7]. 5G에서는 5G-AKA 외에 EAP-AKA’ 방식을 표준으로 채택하고 있다. EAP-AKA’이 5G-AKA와의 차이점을 간단히 살펴보면, 첫째, SEAF는 EAP 인증 프레임워크 특성상 단순히 EAP 메시지를 전달하는 EAP 인증자(authenticator) 역할만 수행하며 별도의 인증 기능을 수행하지 않는다. 둘째, SEAF가 별도 인증기능을 수행하지 않기 때문에 단말이 접속한 망(SN)에 의한 단말 인증단계가 없다. 셋째, 키 생성과정에 있어서 CK, IK로부터 CK’, IK’을 생성하는 단계가 추가되며, AUSF Key와 SEAF Key를 생성하는 시점이 상호인증이 완료된 이후에 이루어지는 점을 차이로 꼽을 수 있다.

이상의 두가지 인증방식 외에 추가적으로 3GPP에서는 TS 33.501의 부록에 EAP-TLS(Transport Layer Security) 방식을 참고용으로 정의하고 있다. EAP-TLS는 EAP-AKA’ 이외의 다른 EAP 메커니즘을 상호인증 목적으로 어떻게 적용할 수 있는지 그 예를 들기 위한 것으로서, 타 이동통신사업자 망과의 로밍 등을 고려하지 않는 독립된 사설망이나 IoT(Internet of Things) 환경 등에서 적용할 수 있는 AKA 방식이 아닌 인증 메커니즘이다. 예를 들어, 유무선 융합 환경에서 노트북을 이용하여 5G 망에 접속하려는 경우 노트북에 가입자 신원정보와 최상위 키(long-term key)를 담고 있는 USIM 등이 없다면 AKA 방식의 인증 절차를 진행할 수 없다. 따라서, 5G에서의 다양한 단말 및 기기가 사용되는 서비스 환경을 고려했을 때 AKA 방식 이외의 다양한 인증 방식도 수용할 수 있는 유연성을 가져야 하며, 이 점이 기존 4G까지와는 다른 5G 인증체계의 큰 특징 중 하나이다.

3.3. 무선 구간 사용자 데이터 보호 강화

망과 단말 사이의 상호인증 절차가 성공적으로 마무리되면, 단말과 망 사이에 주고받는 시그널링 메시지와 사용자의 서비스 데이터를 보호하기 위한 암호화 및 무결성 보호 절차가 진행된다. NAS(Non Access Stratum) 보안 설정과 AS(Access Stratum) 보안 설정 절차가 이에 해당한다. NAS 보안 설정은 단말과 코어망의 AMF 사이에 주고받는 NAS 시그널링 메시지에 대한 무결성 보호 및 암호화를 위한 설정과정이며, AS 보안 설정은 단말과 기지국 사이에 주고받는 RRC(Radio Resource Control) 시그널링 메시지와 사용자의 서비스 데이터 각각에 대한 무결성 보호와 암호화를 위한 설정과정이다.

4G LTE에서는 NAS와 RRC 시그널링 메시지에 대한 무결성 보호만을 강제사항으로 정의하고 있으나 (그

	5G (TS 33.501)	4G (TS 33.401)
NAS Integrity	Mandatory	Mandatory
NAS Confidentiality	Optional+	Optional
RRC Integrity	Mandatory	Mandatory
RRC Confidentiality	Optional+	Optional
UP Integrity	Optional	Forbidden
UP Confidentiality	Optional+	Optional

☆ Optional+: Optional to use, but should be used whenever regulations permit

〔그림 4〕 4G 및 5G에서의 암호화 및 무결성 요구사항

림 4)와 같이 사용자 데이터에 대한 무결성은 요구사항에서 제외되었다. 사실상 무결성 보호는 패킷 크기와 함께 무엇보다도 단말과 기지국에서 무결성 검증을 위한 부하가 증가하는 부담이 매우 크다. 그러나, 5G에서는 사용자 데이터 전송에 대한 무결성 보호 기능을 강제사항은 아니지만 선택사항으로 명시함으로써 무선 접속 환경에서의 데이터 위·변조가 우려되는 민감한 서비스 환경에서는 가급적 사용자 데이터에 대한 무결성도 보호하도록 권고하여 데이터 보호 체계를 강화하였다.

또한 (그림 4)에 나타난 바와 같이, 암호화를 통한 시그널링 데이터 및 사용자 데이터의 기밀성 보호 체계에 있어서도 4G에서와 같이 단순 선택사항으로 권고하기보다는 특별한 제약사항이 없는 한 암호화를 사용하도록 한층 강화된 데이터 보호 체계를 정의하고 있다.

3.4. 서비스 기반 구조 보호 체계

앞서 언급한 바와 같이, 5G 시스템 구조에서 눈에 띄는 변화 중 하나는 바로 코어망의 제어 기능에 대한 서비스 기반 구조이다. 모든 네트워크 기능은 HTTP (Hypertext Transfer Protocol) 기반의 서비스 기반 인터페이스(Service based Interfaces)를 따르고, IPSec(IP Security)과 같은 네트워크 계층에서의 통신 보호 수단 외에 전송 계층에서의 메시지 보호를 위한 TLS 프로토콜을 반드시 지원해야 한다.

또한 5G 제어 평면의 모든 네트워크 기능은 각 기능이 갖고 있는 기능적 특성과 이벤트에 대한 정보를 NEF(Network Exposure Function)을 통해 제3자의 응용 기능(Application Function; AF)에게 제공할 수 있다. 이때 NEF와 AF 사이의 인터페이스는 TLS를 통해 보호되며, AF가 적절한 권한을 가졌는지는 OAuth 기반의 권한검증 메커니즘을 이용하여 NEF가 검증한다.

3.5. 이동통신 망간 시그널링 보호 체계 강화

5G에서는 로밍 환경에서 이동통신 망간의 네트워크 기능들 사이의 시그널링 메시지 보호를 위해 SEPP 기능을 새롭게 정의하고 있다. SEPP는 메시지에 대한 무결성 보호 및 기밀성을 제공하기 위해 응용 계층의 보호 체계를 제공한다.

일반적으로 두 이동통신 망 사이에 별도의 IPX (Interconnect Provider)가 없이 각 이동통신 망의 SEPP가 직접적으로 연결된 경우에는 SEPP 사이의 메시지는 TLS 프로토콜을 이용하여 보호된다. 그러나, 두 이동통신 망이 IPX를 통해 연결된 경우에는 두 이동통신 망의 SEPP 사이에서 IPX를 거치는 동안 데이터가 유출되거나 위·변조되는 것을 방지하기 위해 N32 인터페이스에 대한 응용 계층의 무결성 보호 및 암호화 체계가 적용된다. SEPP는 N32 인터페이스 상의 메시지 보호를 위해 JSON Web Encryption (RFC 7516)을 사용하며, IPX는 데이터 전송 과정에서의 무결성 검증을 위해 JSON Web Signatures (RFC 7515)를 사용한다.

〔그림 5〕 이동통신 망간 시그널링 보호 체계

3.6. 접속망에 비종속적인 통합 인증 체계

ITU-T의 IMT-2020 네트워크 요구사항에 따르면, 새로운 IMT-2020 무선기술, IMT-Advanced에서 진화된 무선기술, 무선 LAN, 유선망, 위성망 등 다양한 접속망 기술에 독립적인 공통의 코어망 및 제어 체계를 요구하고 있다[8]. 이에 따라 단말의 인증도 어떤 접속망을 통해서 망에 접속하더라도 동일한 인터페이스와 동일한 절차에 따라 인증이 제공되어야 한다.

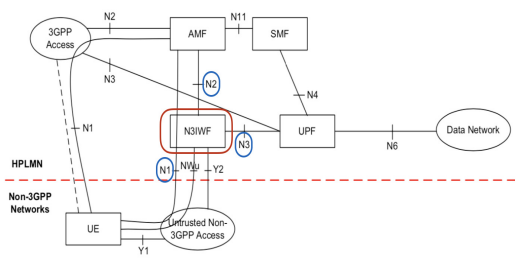
4G까지는 3GPP 무선기술을 이용한 접속, 3GPP 무선기술은 아니지만 신뢰할 수 있는 접속망을 통한 접속 그리고 3GPP 무선기술도 아닌 비신뢰 접속망을 통한 접속 규격을 정의하고 있으나, 이들 각각 서로 다른 인터페이

스와 절차에 따라 망에 접속하도록 정의하고 있다.

그러나, 5G에서는 ITU의 네트워크 요구사항에 따라 3GPP 무선기술이든 아니든, 신뢰할 수 있는 접속 기술이든 아니든 상관없이 공통된 인증체계를 제공해야 한다. 현재 Release 15에서는 3GPP 무선기술을 통한 접속 뿐만 아니라, 3GPP 무선기술이 아닌 동시에 비신뢰 접속망을 통한 접속 절차가 규격으로 정의되어 있다. 참고로 신뢰할 수 있는 3GPP 이외의 접속망을 통한 접속은 Release 16에서 규격을 개발하고 있다.

5G에서 신뢰할 수 없는 3GPP 이외의 접속망을 이용한 접속에서는 N3IWF(Non-3GPP Interworking Function)을 통해 5G 망에 접속한다. 이때 (그림 6)과 같이 단말과 AMF 사이의 NAS 인터페이스가 N1으로, N3IWF과 AMF 사이의 제어 인터페이스가 N2로, 그리고 N3IWF와 UPF 사이의 데이터 전송 인터페이스가 N3로 정의되어 있으며, 이러한 인터페이스는 3GPP 무선기술을 이용한 단말, 5G 기지국, AMF, UPF 사이의 인터페이스와 N1, N2, N3 인터페이스와 동일하게 정의된다[9].

따라서, 신뢰할 수 없는 3GPP 이외의 접속망을 통한 접속이라 할지라도 단말이 NAS 시그널링 메시지를 망과 주고 받을 수 있으며, 3GPP 무선기술을 이용한 보통의 망 접속 절차와 동일한 절차를 이용할 수 있다. 더욱이 단말이 두 가지 유형의 인터페이스를 모두 갖고 있는 경우, 하나의 단말로 3GPP 무선기술을 이용한 망 접속과 함께 신뢰할 수 없는 3GPP 이외의 접속망을 통한 접속이 동시에 가능하다. 또한, 3GPP 무선기술을 이용하여 이미 망에 접속한 단말이 동일한 AMF에 대해 신뢰할 수 없는 3GPP 이외의 접속망을 통해 접속하는 경우, 인증 과정에서 3GPP 무선기술 접속 인증 성공으로 획득한 5G-GUTI를 사용한다면 추가적인 상호 인증 절차나 NAS 보안 설정 과정을 생략할 수 있는 장점을 갖는다.



〔그림 6〕 신뢰할 수 없는 3GPP 이외의 접속망을 통한 접속 인터페이스

3.7. 외부 응용서버와의 인증 체계 도입

5G에서는 단말이 망에 접속할 때 상호인증을 위한 기본 인증(Primary Authentication) 이외에 추가로 데이터 네트워크의 응용 서버와 단말 사이에 이루어지는 2차 인증(Secondary Authentication) 절차를 정의하고 있다.

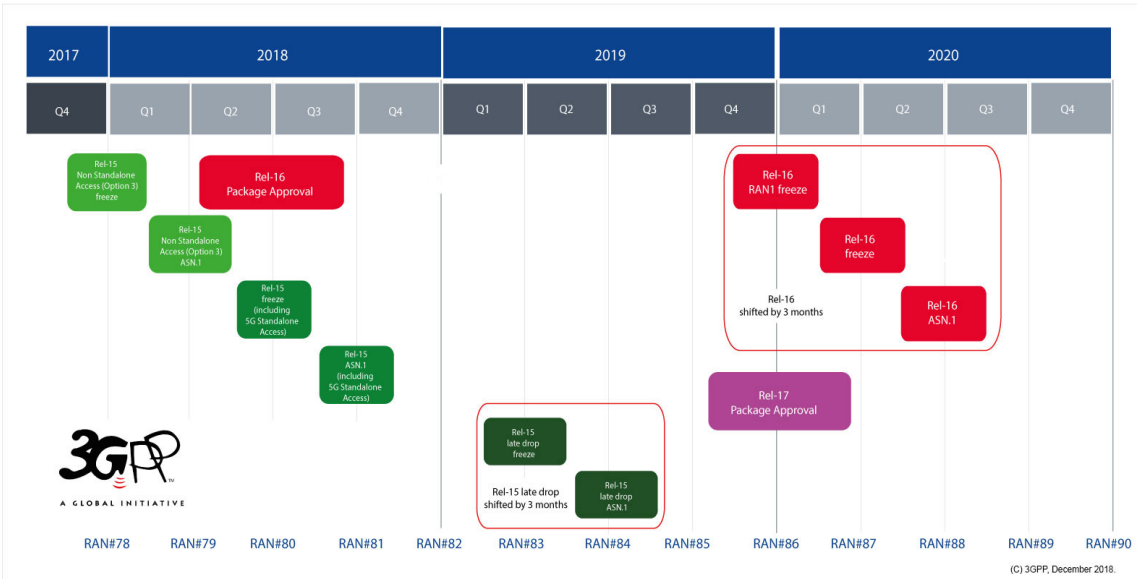
2차 인증은 응용서비스에서 필요로 하는 경우 응용서비스의 AAA(Authentication, Authorization, Accounting) 서버와 선택적으로 적용할 수 있는 기능으로서, 기본 인증을 마친 단말이 응용 서비스를 위한 PDU(Protocol Data Unit) Session을 설정하는 단계에서 필요에 따라 2차 인증을 진행할 수 있다. 이때 2차 인증을 위한 메시지는 단말에서 NAS 프로토콜을 이용하여 AMF로 전달된 다음, AMF에서 SMF(Session Management Function)로 전달되고, SMF는 UPF(User Plane Function)을 통해 외부 응용의 AAA 서버와 메시지를 교환한다.

2차 인증을 위한 인증 메커니즘으로는 EAP를 사용하며 특별히 홈망(HN)의 SMF가 EAP 인증자 역할을 수행하며, 홈망의 SMF는 UDM을 통해 단말의 요청이 사용자의 서비스 가입 프로파일에 따라 유효한 것인지 검증한다. 이와 같은 2차 인증은 사실상 인증보다는 PDU Session 생성을 위한 권한검증(authorization)의 목적이 더욱 강하다.

Ⅳ. 3GPP 5G 보안 표준화 동향

3GPP는 전세계 이동통신 사업자, 장비 제조사, 단말 제조사, 칩 제조사 및 세계 각국의 표준화 단체와 연구기관 등 약 500여개 업체가 참여하는 세계 최대 이동통신 표준화 단체이다[10].

일반적으로 이동통신기술은 UN기구인 국제전기통신연합(ITU)에서 새로운 기술에 대한 비전과 요구사항을 제정하면, 이 요구사항을 만족하는 기술을 어떤 표준화 단체라도 제정할 수 있는데 현재 IMT-2020 즉 5G 기술에 대해서는 3GPP가 거의 독점적으로 표준 규격을 개발하고 있다. 국제 표준으로서의 지위를 획득하기 위해 3GPP에서 개발한 표준 규격을 ITU에 제출하면, ITU는 요구사항 충족여부를 면밀히 심의하여 국제표준으로서 승인 여부를 결정한다. 참고로 4G라 일컫는



〔그림 7〕 3GPP의 5G 표준화 일정계획(〔11〕)

LTE 기술은 3GPP의 Release 8에서 규격이 발표되었으나 실제로 ITU의 IMT-Advanced 기술로 승인받은 것은 Release 10의 LTE-Advanced 기술이다.

3GPP의 5G 표준 규격 개발은 (그림 7)과 같이 2017년부터 시작된 Release 15을 통해 1단계 기술 규격이 개발되었으며, 현재 Release 16의 2단계 기술 규격이 내년 6월을 목표로 표준화가 진행중이다. Release 16에서는 Release 15에서 정의한 5G 시스템에 대한 전반적인 개선사항과 더불어 이동통신 기반의 IoT 서비스, V2X 서비스 그리고 고신뢰·초저지연(Ultra Reliable Low Latency Communications; URLLC) 서비스 등을 위한 기능 규격 등을 개발중이다.

특히 3GPP에서 보안 기술을 담당하는 SA(Services & System Aspects)-3 워킹그룹의 경우, Release 15에서는 본 논문에서 분석한 TS 33.501 규격을 제정한 바 있으며, 현재 Release 16에서는 다양한 5G 기반 IoT, V2X, URLLC 서비스 등에 따른 보안 이슈를 분석하고 솔루션을 개발하는 것 외에도 추가적으로 5G를 위한 보안 보증 규격(Secu- rity Assurance Specification)을 새롭게 개발하고 있어 그 결과가 주목된다.

당초 3GPP는 Release 16을 개발한 다음 ITU에 IMT-2020 국제표준으로서 승인을 받을 계획이었다. 다만 Release 16에서 초고속 서비스 이외에 초저지연·초연결 서비스의 비전 및 요구사항을 실현하기 위한 기술 규격의 완성도가 어느 정도인지 단언할 수는 없지만, 5G 기술에 대한 기술 규격의 개발 및 개선은 Release 17에서도 이어질 전망이다. 현재 Release 17에서 추진될 표준화 항목은 오는 12월 표준화 회의에서 결정될 예정이며, Release 17의 표준화 작업은 2021년 9월까지 진행될 예정이다[11].

Ⅴ. 결 론

ITU에서 IMT-2020 비전을 제시한 지 채 5년도 지나지 않아 5G 서비스가 상용화되었다. 물론 초연결 및 초저지연 서비스까지 원활히 이루어지기 위해서는 5G 코어망이 연동되는 5G 단독모드(Stand-Alone)가 구축되고 일부 5G 기술의 추가적인 개선도 이루어져야 한다. 그러나, 새로운 세대의 이동통신기술이 급속도로 우리 실생활에 파고들고 있다.

새로운 세대의 기술은 더 빨리, 더 많은 기기를 연결하여, 더 좋은 서비스를 제공할 수 있지만, 기존 세대에서 존재했던 보안 취약점 뿐만 아니라 새로운 세대 기술에 의해 초래되는 잠재적인 보안 취약점까지 더하면 사이버 위협이나 공격의 위험은 더욱 증가하고 이로 인한 폐해는 가늠할 수 없을 정도로 커진다. 심지어 자율주행차, 스마트시티, 스마트제조, 디지털 헬스케어 등 5G 융합서비스에 대한 사이버 공격은 단순히 통신 장

애를 떠나 국민의 재산과 생명을 위협하는 재난으로 발전할 수도 있다. 따라서, 이동통신 환경에서 예상되는 보안 취약점을 해소하고 점차 고도화되는 보안 위협에 능동적으로 탐지하고 대응할 수 있는 기술의 개발이 무엇보다 필요하다.

본 논문에서는 3GPP의 5G 보안 기술을 정의한 TS 33.501 규격을 바탕으로 5G 보안 구조의 특징과 새롭게 도입된 보안 기능을 살펴보고, 5G에서 강화되었거나 새롭게 추가된 보안 기능과 그 특징을 살펴보았다. 물론 TS 33.501 규격은 5G의 기본적인 보안 기술을 정의하고 있으며, 본 규격에 정의된 보안 기술만으로 현재까지 알려진 이동통신 환경에서의 보안 위협을 모두 해소하지는 못한다.

더욱이 IoT, V2X, URLLC 등의 서비스를 제공하기 위해서는 Release 15에서 정의한 5G 시스템의 구조나 기능 또는 절차의 변화나 개선이 불가피하며, 이에 따른 또다른 보안 위협을 해소하기 위한 추가적인 보안 기능과 절차를 지속적으로 표준화하여 개발할 것으로 전망된다.

따라서, 현재까지 규격으로 제정된 5G의 시스템 구조와 보안 기술에 대한 이해를 바탕으로 5G 이동통신 환경에서 예상되는 보안 취약점과 위협을 해소할 수 있는 보안 기술을 개발하고 표준화에 반영하는 일련의 활동이 지속적으로 이루어져야 한다.

참 고 문 헌

[1] ITU-R Recommendation, M.2083.0, IMT-Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, 2015.

[2] S.R. Hussain, et.al., “LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE,” *NDSS Symposium 2018*, Feb. 2018.

[3] A. Dutta, “Security Challenges and Oppor- tunities in SDN/NFV and 5G Network,” *ETSI Security Day*, 2017.

[4] 박종근, 김종현, 김익균, 진승헌, “초연결 지능화 인프라 보안기술 동향 – 5G 시대의 이동통신 보안 중심,” *전자통신동향분석*, 34(1), pp. 36-48, 2019.

[5] 3GPP, TS 33.501, Security Architecture and Procedures for 5G System, V15.3.1, 2018.

[6] 3GPP, TS 33.401, 3GPP System Archi- tecture Evolution(SAE); Security Archi- tecture, V14.6.0, 2019.

[7] https://en.wikipedia.org/wiki/Extensi-ble_Authentication_Protocol

[8] ITU-T Recommendation, Y.3101, Requi-rements of the IMT-2020 network, 2018

[9] 3GPP, TS 23.501, System Architecture for the 5G System, V15.4.0, 2018

[10] 삼성전자, 5G 국제 표준의 이해, 2018

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

[12] 박종근, “5G 환경에서의 보안 이슈와 3GPP 보안 구조 기술,” NetSec-KR 2019, 2019.

[13] 박종근, “5G 보안 구조 및 주요 절차,” 한국정보보호학회 3차 단기강좌(5G+보안), 2019.

〈저 자 소 개〉

박 종 근 (Jong-Geun Park)

정회원

1997년 2월 : 성균관대학교 산업공학과 학사

1999년 2월 : 성균관대학교 산업공학과 석사

2013년 2월 : 충남대학교 컴퓨터공학과 박사

1999년 3월~2001년 4월 : 국방과학연구소 연구원

2001년 5월 ~ 현재 : 한국전자통신연구원 책임연구원

<관심분야> 이동통신보안, SDN/NFV, 클라우드보안

김 종 현 (Jong-Hyun Kim)

정회원

2000년 5월 : 오클라호마주립대 컴퓨터과학과 석사

2005년 5월 : 오클라호마주립대 컴퓨터과학과 박사

1995년~1998년 : 삼성전자 SW연구개발 연구원

2005년 ~ 현재 : 한국전자통신연구원 책임연구원

<관심분야> 네트워크 포렌식, 클라우드 보안, SDN/NFV, 이동통신보안

문 대 성 (Moon, Daesung)

정회원

2007년 2월 : 고려대학교 전산학과 박사

2009년 3월~현재 : 과학기술대학원 대학교(UST) 정보보호공학 전공책임교수

2000년 12월 ~ 현재 : 한국전자통신연구원 네트워크·시스템보안연구실 실장

<관심분야> 정보보호, 네트워크보안, 5G보안, 인공지능보안

김 익 균 (Kim, Ikkyun)

종신회원

1994년 2월 : 경북대학교 컴퓨터공학과 학사

1996년 2월 : 경북대학교 컴퓨터공학과 석사

2009년 2월 : 경북대학교 컴퓨터공학과 박사

2004년 ~ 2005년 : Purdue University 초빙 연구원.

1996년 ~ 현재 : 한국전자통신연구원 정보보호연구본부 본부장/책임연구원

<관심분야> 네트워크 보안, 컴퓨터 네트워크, 클라우드보안, 빅데이터 분석