ETRI

2019
Electronics and
Telecommunications
Trends

최신 네트워크 기술 동향 특집

Ⅰ. 서론
Ⅱ. 기존 이동통신 보안 위협
Ⅲ. 5G 네트워크 보안 위협
Ⅳ. 5G 보안 이슈
Ⅴ. 5G 보안 표준화
Ⅵ. 결론 및 시사점

초연결 지능화 인프라 보안기술 동향 –5G 시대의 이동통신 보안 중심

Mobile Network Issues regarding 5G Security

박종근 (J.G. Park, queue@etri.re.kr) 지능보안연구그룹 책임연구원
김종현 (J.H. Kim, jhk@etri.re.kr) 지능보안연구그룹 책임연구원
김익균 (I.K. Kim, ikkim21@etri.re.kr) 지능보안연구그룹 책임연구원/그룹장
진승헌 (S.H. Jin, jinsh@etri.re.kr) 정보보호연구본부 책임연구원/본부장

Recently, competition among global mobile operators has focused on the commercialization of 5G for the first time. Apart from protecting the privacy of subscribers and the confidentiality and integrity of communication, protecting the network against various cyber attacks is also important to ensure that high-quality mobile services operate safely. In this study, we examine the security vulnerabilities with respect to mobile communication environments using previous and current LTEs. We also investigate whether existing vulnerabilities can be effectively protected and identify security issues that need to be considered in the approaching 5G environment.

* DOI: 10.22648/ETRI.2019.J.340104

* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발].

© 2019 한국전자통신연구원

Ⅰ. 서론

우리나라에 이동통신 서비스가 도입된 지 지난 7월 1일을 기점으로 벌써 30년이 되었다. 물론 처음에는 아날로그 방식의 이동통신 서비스였으나 첫해 784명에 불과하던 휴대전화 가입자 수는 지난 4월을 기준으로 6,460만 명을 초과하였으며 전체 인구수를 넘어선 지도 이미 8년이 되었다[1].

이동통신 환경에서 제공되는 모바일 서비스는 오늘을 살아가는 현대인에게 최첨단을 추구하는 동시에 가장 보편적인 서비스가 된 지 오래다. 무엇보다도 2007년 발표된 애플사의 아이폰이 촉발시킨 스마트 단말의 출현과 확산, 그리고 앱스토어(Application store)를 통한 상상조차 할 수 없는 다양한 모바일 앱의 폭발적 증가는 음성전화 위주의 이동통신 서비스 패러다임을 완전히 바꾸기에 충분했다.

그러나, 현대인들이 모바일 서비스를 이용하는 시간과 모바일 서비스가 일상에서 차지하는 비중이 점차 늘어나면서, 이동통신 환경의 취약점을 이용한 보안 위협이나 공격 위험에 노출될 가능성도 더불어 증가하고 있다. 이동통신 환경에서의 대표적인 보안 공격 유형으로는 위조된 기지국을 이용하여 사용자 식별자(IMSI: international mobile subscriber identifier)를 탈취하는 행위, 사용자의 위치 정보를 탐지하거나 동선을 추적하는 행위, 사용자의 서비스 내용이나 중요 정보를 수집하는 행위, 서비스 거부 공격(denial of service)을 통해 사용자의 정상적인 서비스 이용을 방해하는 행위 등을 꼽을 수 있다.

최근 국내 이동통신 시장의 경쟁은 세계 최초 5G 상용화에 초점이 맞춰져 있다. 초고속 광대역 전송 서비스, 초저지연 서비스, IoT(Internet of Things)와의 융합, 클라우드에 대한 의존성 증가, 다양한 모바일 융합 서비스 등장 등 초연결 지능화 인프라의 근간이 되는 5G는 이동통신 서비스의 다양한 메가트렌드가 총망라될 것으로 전망하고 있다. 고품질의 이동통신 서비스가 안전하게 운용되기 위해서는 기본적으로 가입자의 개인정보와 통신의 기밀성 및 무결성을 보호하는 것 외에도 다양한 사이버 공격에 대한 네트워크 자체 보호가 무엇보다 중요하다.

본고에서는 과거부터 현재의 LTE(Long Term Evolution)까지 이동통신 환경에서 논의된 사이버 보안 취약점을 살펴보고, 초연결 지능화 인프라의 근간이 될 5G 환경에서도 기존의 취약점들이 유효할 수 있는지, 그리고 5G 시대의 변화된 환경에서 우려되는 위협은 무엇인지에 대해 관련 문헌을 통해 고찰함으로써 다가올 5G 시대의 다양한 사이버 위협에 대비하고자 한다.

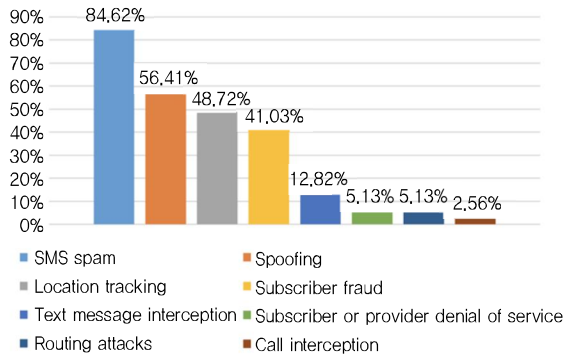
Ⅱ. 기존 이동통신 보안 위협

모바일 서비스가 보편화되면서 이동통신 네트워크는 적대국가의 정보기관이나 사이버 군 등과 같이 의도적인 적대자에게는 매우 매력적인 공격 대상이다. 이들은 VIP(very important person) 등 공격 목표의 위치를 추적하거나 음성 통화 또는 데이터의 내용을 도청하기 위해 이동통신 네트워크를 활용하기도 한다.

본 장에서는 이동통신 네트워크에서 서비스 연결 설정을 위한 시그널링 프로토콜의 취약점을 살펴보고, 현재 전세계적으로 널리 운용되고 있는 4G LTE 환경에서의 보안 위협 이슈 유형을 정리한다.

1. 시그널링 프로토콜 보안 위협

유럽네트워크정보보호원(ENISA: European Union Agency for Network and Information Security)이 최근 발간한 보고서[2]에 따르면, 이동통신 네트워크 환경에서 사업자의 망간 상호접속(interconnection) 프로토콜의 취약점을 이용한 보안 위협이 존재한다. 본 절에서는 본 보고서의 주요 내용을 바탕으로 시그널링 프로토콜의 보안 위협에 대해 살펴보기로 한다.



(그림 1) 시그널링 프로토콜 공격 유형

[출처] Reprinted from ENISA, "Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation," Mar. 2018.

2G/3G 시대의 초기 이동통신 네트워크에서는 수십 년 전에 설계된 시그널링 프로토콜인 SS7(Signalling System No. 7)과 이의 IP 버전인 SIGTRAN(Signalling Transport)을 이용하여 상호접속 시스템을 구축하였다. 이들 시그널링 프로토콜은 이동통신 망간 사용자의 호 라우팅(call routing), 로밍(roaming) 정보, 가입자의 서비스 특성 정보 등을 교환하기 위해 사용된다. 당시에는 모바일 서비스가 현재와 같이 급속도로 성장할 것을 충분히 예상하지 못했기 때문에 시그널링 프로토콜의 신뢰성이나 보안 이슈는 크게 논의되지 않았지만, 그럼에도 불구하고 여전히 기존의 시그널링 프로토콜을 사용하고 있다. 물론 4G에서는 보다 개선된 Diameter 프로토콜을 사용하고 있지만 유선망에서 이어온 동일한 상호접속 원칙을 염두에 두고 구축되었기 때문에 프로토콜의 취약점이 그대로 존재한다.

보고서에 따르면, SS7 및 Diameter 프로토콜과 관련된 보안 위험을 강조한 연구 결과가 최근까지 꾸준히 발표되고 있다. (그림 1)과 같이 실제 이동통신 환경에서 시그널링 프로토콜의 취약점을 이용한 공격의 범위도 SMS(short message service) 스팸, 전화 도청(call intercept), 서비스 거부, 가입자 계정 도용(fraud), 위치 추적 등으로 다양하게 나타난다. 또한 시그널링 프로토콜을 이용한 대표적인 공격 사례는 〈표 1〉과 같다.

결국 SS7 프로토콜 기반의 이동통신 네트워크는 안전하지 않으며, 가입자의 데이터는 항상 위험에 처해 있고, 이동통신 사업자는 보안을 완전하게 보장할 수 없다. SS7 기반 이동통신 네트워크를 대상으로 여러 유형의 공격을 시도했을 때 서비스 거부 공격의 80%, 데이터 유출 공격의 77%, 사기(fraud) 행위의 67%가 성공한 것으로 보고되기도 했다[3].

SS7 시그널링 프로토콜과 관련된 보안인식 수준은 4G LTE 환경에서 채택된 Diameter 프로토콜에 비해 상대적으로 높은 편이다. Diameter는 RADIUS (Remote

〈표 1〉 시그널링 프로토콜을 이용한 공격 사례

발표주체	주요 내용	시기
Corelan Team	벨기에 이동통신사업자인 Belgacom 네트워크의 GTP(GPRS tunneling protocol) 프로토콜 공격을 통한 데이터 세션 하이재킹	2013년
CBS	CBS 60 minutes TV 쇼에서 이동통신망 도청 공격 시연	2016년 4월
O2	독일 이동통신사업자인 O2는 자사의 네트워크에서 일부 가입자의 계정 정보가 SS7 프로토콜을 이용하여 유출되었음을 확인	2017년 5월
Nokia	IEEE International Conference on Communications 학술대회에서 LTE 네트워크에서의 SMS 및 OTP(one time password) 가로채기 발표	2017년 5월
Nokia	International Conference on Network and System Security 학술대회에서 Diameter 상호접속을 통한 가입자 프로파일 추출 및 수정 발표	2017년 8월
Positive Technology	SS7 취약점을 이용한 문자 메시지에서의 OTP 이중 인증토큰 가로채기 입증	2017년 9월

[출처] Reprinted from ENISA, "Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation," Mar. 2018.

Authentication Dial-In User Service)에서 진화되었으며 네트워크에 대한 인증(Authentication), 권한 부여(Authorization) 및 계정관리(Accounting) 기능을 제공한다. 프로토콜 설계 면에서 SS7의 기본 개념과 그 취약점을 이양 받았다는 평가를 받고 있고, IP 기반 프로토콜이기 때문에 해킹을 통한 접근 가능성도 있다.

SS7 및 Diameter를 보호하기 위해 MAPsec(Mobile Application Part security), TCAPsec(Transaction Capabilities Application Part user security), Diameter over IPsec(IP security), Diameter over SCTP/ DTLS (Stream Control Transmission Protocol/Data-gram Transport Layer Security) 등이 제안된 바는 있었으나 아직 실제 운용 환경에 채택되지는 않았다[2].

2. 4G LTE 이동통신 보안 위협

4G LTE 이동통신의 보안은 LTE 인증, NAS(Non Access Stratum) 보안, AS(Access Stratum) 보안으로 이루어진다. LTE 인증은 이동통신 망에 접속하려는 가입자 단말과 이동통신 망간의 상호 인증 체계로서, EPS(Evolved Packet System) AKA(Authentication And Key Agreement) 절차를 사용하여 가입자는 망을 인증하고 망은 가입자를 인증한다. NAS 보안은 단말과 MME(Mobility Management Entity) 간의 NAS 시그널링에 대한 무결성(Integrity)을 보증하고 암호화(Ciphe-ring)를 수행한다. AS 보안은 단말과 eNB(evolved node B) 간의 RRC(Radio Resource Control) 시그널링에 대한 무결성 보증과 암호화, 그리고 사용자 트래픽에 대한 암호화를 제공한다.

그러나 좀비화되거나 위조된 가입자 단말 또는 eNB를 이용한 보안 위협 가능성과 공격 사례에 대한 연구가 최근 활발히 이루어지고 있다. LTE 이동통신 환경에서의 대표적인 보안 위협 유형은 다음과 같다.

가. 중간자 공격(Man-in-the-Middle Attack)

3G UMTS(universal Mobile Telecommunication Standard)에서는 단말과 이동통신 망간 상호인증 체계가 도입되었지만, 위조된 GSM(Global System for Mobile Communication) 기지국을 이용하여 GSM/UMTS 무선 인터페이스를 동시에 갖고 있는 단말에 대한 중간자 공격이 가능함을 보인 바 있다[4]. 공격자는 사전에 확보한 피해(Victim) 단말의 IMSI를 이용하여 정상적인 이동통신 망으로부터 인증 정보를 획득하고 피해 단말을 속인 채 모든 서비스 데이터를 탈취할 수 있다.

4G LTE에서도 이와 유사하게 피해 단말의 IMSI를 사전 확보한 상태에서 중간자 공격이 가능하다. 공격자는 위조된 단말과 eNB를 이용하여 피해 단말의 망 재접속을 유도한 다음, 피해 단말의 서비스를 전체 또는 선별적으로 차단하거나, 또는 서비스의 이용 패턴이나 특성 정보를 수집하는 인증 릴레이(Authentication Relay) 공격이 가능하다[5]. 이 공격은 통상의 중간자 공격과 달리, 공격자가 LTE 보안 기능을 무효화하지 않고 EPC(Evolved Packet Core)에 연결할 수 있게 한다. 그러나 운영자가 약한 보안 컨텍스트를 사용하지 않는 한 공격자는 정상적으로 암호화된 메시지를 해독하거나 삽입할 수 없다.

또한, 특정 LTE 동글(Huawei E3276 USB Dongle)의 구현 결함을 이용하여 LTE에 대한 중간자 공격을 시연한 사례도 있다[6].

나. IMSI 획득 공격

IMSI 획득 공격은 2G/3G 네트워크에서와 마찬가지로 4G LTE 네트워크에도 여전히 유효하다. IMSI는 가입자 단말의 USIM(Universal Subscriber Identity Module) 칩과 HSS(Home Subscriber Server)에 각각 저장되어 있으나, 망 접속 단계에서 암호화되지 않은 채 전송되기 때문에 악의적인 공격자에 의해 쉽게 탈취당

할 수 있는 취약점을 갖고 있다. 탈취된 IMSI는 다른 유형의 보안 공격을 위한 단초로서 활용될 수 있기 때문에 더욱 위험하다.

3G 환경에서 IMSI를 보호하기 위해 공개 키 암호화 메커니즘을 적용하는 방안이 제안되기도 하였으나[7], 공개 키 암호화는 오버헤드를 유발할 수 있고 일부 프로토콜을 수정해야 한다.

IMSI 획득 공격을 무력화하기 위해 IMSI 대신에 무작위로 변경되는 가상의 식별자인 PMSI(Pseudo Mobile Subscriber Identifier)를 사용하는 방안이 제안되기도 했다[8]. PMSI는 LTE 인증 단계에서 인증 서버가 무작위로 생성하여 단말에 제공하며, 단말은 추후 인증 단계를 거칠 때 이전에 제공받은 PMSI를 이용한다. 이 방식은 표준 규격의 수정 없이 SIM과 인증서버를 변경하는 것만으로 적용할 수 있다.

다. 위치 추적(Traceability) 공격

이동통신 환경에서는 사용자의 신원 정보를 보호하고 위치 추적을 방지하기 위해 IMSI 대신 주기적으로 변경되는 TMSI(Temporary Mobile Subscriber Identity)를 사용하며 단말과 EPC 사이에 암호화되어 전송된다. 그러나, TMSI 재부여 절차에 대한 3GPP(3rd Generation Partnership Project) 표준의 일부 결함을 이용한 위치 추적 공격이 소개되기도 하였다[9].

또한, LTE 페이징 메시지의 전송 반경과 GUTI(Globally Unique Temporary Identifier) 갱신에 대한 표준 규격의 취약점을 이용하여 단말의 위치를 추적하기도 하였으며[10], 피해 단말의 접속과정에서 전송되는 LTE NAS 보안 정보를 확보한 다음, 위조된 eNB를 이용하여 셀 내 피해 단말의 존재 여부를 확인하거나, 페이징 메시지를 통해 피해 단말의 재접속을 유도한 다음 접속 요청(Attach Request) 메시지가 수신되면 셀 내 단말의 존재 여부를 확인하는 공격도 가능하다[5].

라. 서비스 거부 공격

서비스 거부 공격은 대표적인 네트워크 보안 공격으로서 이동통신 네트워크 환경에서도 다양하게 이루어질 수 있다.

단말이 위치 갱신 요청(Tacking Area Update) 메시지나 접속 요청 메시지를 전송할 때 악의적으로 위조된 eNB를 이용하여 단말의 서비스를 2G/3G로 강등시키거나 전체 또는 일부 서비스를 차단하는 공격이 가능하다[5], [10].

공격자가 피해 단말의 IMSI를 확보한 경우, 위조된 단말을 이용하여 피해 단말의 망 접속을 무산시킬 수도 있다. 위조된 단말에서 피해자의 IMSI를 이용하여 지속적으로 접속 요청 메시지를 EPC에 전송하여 HSS의 SQN 값을 증가시키면, 피해 단말이 LTE 인증 과정에서 SQN 유효성 검증에 실패하여 망 접속 절차를 중단하도록 유도하는 공격이다[5].

좀비화된 단말과 eNB를 이용하여 EPC에 엄청난 수의 접속 요청 메시지를 보내어 EPC의 장애를 유도할 수도 있다[11]. 마찬가지로 유사한 서비스 거부 공격 상황에서 피해 단말의 트래픽 용량을 소모시키는 좀비화된 단말을 시뮬레이션한 사례도 있다[12].

악의적인 단말이 피해 단말을 대신하여 페이징 응답 메시지를 전송하여 단말의 정상적인 전화 착신이나 SMS 수신을 방해할 수도 있다[13]. 반대로 위조된 eNB를 이용하여 정상 eNB의 페이징 신호와 같은 주기, 더 강한 신호 세기로 무의미한(empty) 페이징 메시지를 피해 단말로 보내어 단말이 유휴(idle) 상태를 벗어나지 못하도록 페이징 채널을 장악(hijacking)함으로써 단말의 정상적인 서비스 수신을 방해하기도 한다. 페이징 채널을 장악한 경우 다양한 후속 공격이 가능한데, 악의적인 eNB가 피해 단말의 IMSI를 포함하여 페이징 메시지를 전달하면 피해 단말은 표준 규격에 따라 네트워크 장애(failure) 상황으로 오인하여 스스로 EPC와의 접속을 종

료하고, 재접속을 시도하기도 한다[5].

또 다른 유형으로는 단말이 위조된 eNB에 연결될 때마다 접속 해제 요청(detach request) 메시지를 단말에 전송하여 서비스를 거부하거나 2G/3G로의 서비스 강등을 유도할 수도 있다.

마. 패닉 공격

악의적인 eNB가 조작된 응급 페이징 신호를 셀 내 모든 단말에 전송하여 사용자의 패닉을 유도하는 공격이다.

바. 에너지 고갈 공격

단말의 과도한 암호화 작업을 유도하여 배터리를 소모시키는 공격으로서, 피해 단말의 IMSI를 포함한 페이징 메시지를 반복적으로 발송하여 단말의 재접속 절차를 계속 유도하거나, GUTI를 포함한 페이징 메시지를 발송하여 피해 단말이 서비스 요청(service request) 절차를 수행하도록 유도한다[5].

Ⅲ. 5G 네트워크 보안 위협

서비스 측면에서 5G의 특징은 모바일 광대역 서비스(Enhanced Mobile Broadband), 고신뢰 초저지연 서비스(Ultra Reliable and Low Latency Communication), 대규모 머신 타입 통신(Massive Machine Type Communications)을 꼽을 수 있다[14]. 이러한 서비스 특성을 반영하기 위해 네트워크 구조적 관점에서 모바일 에지 클라우드(Mobile Edge Cloud), 클라우드 무선 액세스 네트워크(cloud RAN(Radio Access Network)/vRAN), 그리고 네트워크 슬라이싱(slicing) 개념이 새롭게 도입된다. 본 절에서는 A. Dutta[15]의 발표 내용을 바탕으로 5G 네트워크 특징별 보안 이슈를 살펴본다.

1. 모바일 에지 클라우드 보안

5G 코어 네트워크에서는 가상화 기술을 기반으로 한 SDN(Software-Defined Networking), NFV(Network Function Virtualization) 및 클라우드의 활용도가 크게 증가한다. 모바일 에지 클라우드 도입과 관련된 특징과 보안측면에서의 고려사항은 〈표 2〉와 같다.

- 저지연, 고속 인증을 위해 민감한 보안정보의 에지 클라우드 저장에 따른 보안 위협 증가
- 에지 컴퓨팅 응용들이 동일한 물리적 플랫폼에 동시 운용됨에 따라 가상 네트워크 장비(Virtual Network Functions)의 자원 고갈 위험
- 에지 클라우드와 코어 사이의 민감한 보안정보 교환에 따라 공격자에 의한 악의적 재사용(스푸핑(spoofing), 도청, 데이터 조작 등) 위험
- 방문 네트워크에 가입자 인증정보를 저장 및 캐싱함으로써 공격자에 의한 인증정보 유출 및 남용 위험

이와 같은 보안 위협에 대응하기 위해 에지 클라우드

〈표 2〉 모바일 에지 클라우드에 따른 특징과 보안 고려사항

5G 특징	보안측면 고려사항
• 저지연 응용을 위한 인증 지연 최소화 • 보안 콘텍스트를 네트워크 에지에 배치 • 핸드오버 및 데이터 오프로딩 시간 감소 • 서버 기능을 네트워크 에지에서 수행 • 에지 네트워크에서 탐지 및 피해감소	• 단말과 방문 네트워크에 과거 보안 콘텍스트의 캐싱 유지에 따른 보안성 약화 • 가상화 환경에서 민감 보안 정보 손상 가능성 • 다중 액세스 기술 사용시 인증을 위한 복수의 네트워크 자격 증명 필요 • 공격자는 컨텍스트 전송 중에 연결을 획득하거나 스푸핑, 도청 또는 데이터 조작 공격을 수행 가능 • 모바일 에지 서버에서 중간자 공격 가능

[출처] Reprinted with permission from A. Dutta, "Security Challaenges and Opportunities in SDN/NFV and 5G Network," ETSI Security Day, 2017.

〈표 3〉 클라우드 무선 액세스 네트워크에 따른 특징과 보안 고려사항

5G 특징	보안측면 고려사항
• 공유 무선 액세스로 더 많은 단말(IoT) 수용 • RAN의 가상화 및 프로그램화는 동적 트래픽 처리 및 다중 사업자 망 접속에 적합 • 대규모 MIMO 및 고밀도화로 대용량 광대역 트래픽 전송 가능 • SoftRAN은 DoS 탐지 및 완화 기능을 포함 • 동적 무선자원 스케쥴링을 통해 전파방해(jamming) 공격의 위험 경감 가능 • 기지국에서 트래픽 보안 모니터링 가능	• 분산 서비스 거부 공격을 통한 RAN 자원 과부하 위험 • 프로그램화 및 소프트웨어 RAN은 기지국에서의 중간자 공격 가능성 증가 • 제어 신호 또는 사용자 데이터 메시지에 대한 재밍 가능성 • 손상된 IoT 장치가 패킷 주입 공격에 동원될 수 있음 • 다수의 봇(bot)으로 구성된 봇넷에 의해 외부 플러딩 공격 가능 • 공유 리소스 손상 위험 증가

[출처] Reprinted with permission from A. Dutta, "Security Challaenges and Opportunities in SDN/NFV and 5G Network," ETSI Security Day, 2017.

〈표 4〉 네트워크 슬라이싱에 따른 특징과 보안 고려사항

5G 특징	보안측면 고려사항
• 제어 평면과 데이터 평면의 분리를 통한 확장성 • 서로 다른 유형의 응용을 위한 유연한 QoS 보장 • 가상 네트워크 장비와 기타 응용 공존 가능 • 수요에 기반한 맞춤형 자원 활용 • 복수 모바일 사업자 및 다기능 네트워크 협업 가능	• 다른 슬라이스에 대한 서비스 거부 • 다른 슬라이스의 보안 리소스 고갈 • 슬라이스를 가로 지르는 사이드 채널 공격 • 운영자 네트워크 내의 네트워크 슬라이스 인스턴스에 대한 가장 공격 • 운영자 네트워크 내의 다른 네트워크 슬라이스 관리자에 대한 명의도용(impersonation) 공격 • 단말이 복수의 슬라이스에 연결되었을 때 슬라이스 간 격리

[출처] Reprinted with permission from A. Dutta, "Security Challaenges and Opportunities in SDN/NFV and 5G Network," ETSI Security Day, 2017.

에 가상 방화벽/침입탐지 기능을 배치하거나, 보안정보 암호화, 클라우드 자원 분산 배치, 임시 가입자 인증정보에 대한 유효기간 설정 등의 방안을 고려할 수 있다.

2. 무선 액세스 네트워크 보안

5G 무선 액세스 네트워크(RAN) 또한 부분적으로 가상화되고 클라우드 기반으로 설계된다. 무선 액세스 기술 및 무선 액세스 네트워크 특징으로 인한 추가적인 영향을 살펴보면 〈표 3〉과 같다.

- 대규모 감염된 IoT 단말의 과도한 접속 요청으로 인한 5G RAN DDoS(Distributed Denial of Service) 공격
- 대규모 IoT 단말에서 발생된 과도한 악의적 트래픽 증가에 따른 가상 방화벽 자원 소요 증대 및 타 가상 네트워크 장비의 자원 고갈 초래
- 다양한 사업자의 가상 네트워크 장비 간 협업 및 연동에 따른 공유 자원 고갈, 가상 머신 조작, 데이터 유출 및 파괴 문제 발생 가능

마찬가지로 상기의 보안 위협에 대응하기 위해 DDoS 탐지 대응을 위한 가상 네트워크 장비 개발, 클라우드 RAN 스케일 제어 기능 개발, 가상 네트워크 장비 속성에 따른 지능적 배치 및 자원할당 기술 개발 등을 고려할 수 있다.

3. 네트워크 슬라이싱 보안

네트워크 슬라이싱은 서비스 응용별로 독립된 가상의 클라우드 인프라를 제공하기 위한 기술이며, 특성상 다양한 무선 액세스 기술이 특정 슬라이스에 연결될 수도 있다. 네트워크 슬라이싱으로 인한 추가적인 보안 영향을 살펴보면 〈표 4〉와 같다.

- 서로 다른 네트워크 슬라이스가 같은 하드웨어에 공존하는 경우, 부채널 정보를 이용하여 다른 슬라이스의 실행 정보(예, 암호화 키 또는 기타

보안정보)를 취득하거나 공격 가능

네트워크 슬라이싱과 관련된 보안 위협에 대응하기 위해 서로 다른 민감도 또는 취약성을 갖는 슬라이스를 서로 분산하여 배치하거나 또는 부채널 정보를 차단하는 강화된 격리 매커니즘 개발을 고려할 수 있다.

Ⅳ. 5G 보안 이슈

최근 LTE 환경에 대한 공개 소프트웨어 프로젝트가 생겨나면서 보안 연구자뿐만 아니라 해커들에 의해 이동통신 환경의 취약점을 검증하거나 또는 악의적으로 공격을 시도할 가능성이 점점 더 증가하고 있다. 이동통신 네트워크에 대한 사이버 공격으로부터 가입자의 개인 정보 보호, 통신의 기밀성과 무결성 보호뿐만 아니라 네트워크 자체를 보호하고 네트워크의 가용성을 보장하기 위해서는 5G 네트워크 구조를 설계하는 단계부터 보안 고려사항을 함께 검토하고 반영하여야 한다.

5G 보안의 주요 요구사항에 대한 이슈를 정리하면 다음과 같다[16].

1. 사용자 식별자의 기밀성

앞서 Ⅱ장에서 논의된 바와 같이 LTE 환경에서는 IMSI 획득 공격이 가능하며 악의적인 공격자에 의해 탈취된 IMSI는 다른 유형의 공격을 위해 활용될 수 있다. 이러한 문제를 해결하기 위해 LTE 표준에서는 다양한 방안을 논의했음에도 불구하고 채택되지 않았지만, 5G에서는 충분히 재논의될 수 있다.

2. 단말과 네트워크간 상호 인증 및 키 공유

LTE의 상호 인증 및 키 공유를 위해 EPS-AKA 알고리즘이 사용되고 있으며 매우 효율적인 장점을 갖고 있다. 다만 공개 키 기반 방식의 경우 인증을 위해 홈 네트워크에 접근할 필요가 없으며 서비스 요청에 대한 거부 방지가 가능한 특성 등으로 인해 5G 보안에서 다시 검토될 가능성이 있다.

또한, LTE에서는 사용자의 자격 증명(credentials)은 네트워크 사업자에 의해 제공되는 USIM에 저장되며, 사업자를 변경할 때에는 USIM을 변경해야 한다. 그러나 사람이 개입하지 않는 머신 타입 통신 환경에서는 USIM 변경이 매우 번거럽거나 불가능할 수도 있다. 따라서 이러한 자격 증명을 원격에서 프로비저닝하는 방법을 포함한 다양한 방안이 논의될 수 있다.

3. 시그널링 무결성 및 기밀성

일반적으로 사용자 데이터에 비해 시그널링 데이터의 양이 적기 때문에 무결성과 기밀성을 제공하기 위한 용량 부담이 문제가 되지 않는다. 단, 머신 타입 통신에서는 극소량의 데이터가 간헐적으로 전송되는 특성을 고려할 수 있다.

지연에 민감한 초저지연 서비스의 경우에는 NAS 보안 설정 및 AS 보안 설정에 소요되는 시간도 이슈로 부각될 수 있다.

또한, LTE의 시그널링 무결성과 기밀성은 NAS 보안 설정과 AS 보안 설정으로 나뉘는데, 단말이 유휴모드 상태일 때에는 AS 보안 설정이 해제되어 있으므로 시그널링이 완전히 보호되지 않는 문제가 있다.

4. 네트워크 인터페이스 보안

현재 3GPP 규격에서는 특정 조건하에서 코어망과 백홀 인터페이스를 보호하기 위해 IPsec 사용을 강제하고 있으나, 코어망 인터페이스에서는 시그널링만 보호되는 반면, 백홀 링크에서는 사용자 평면에 대해 규정하고 있다. 이러한 구분이 유효한지에 대해서도 새롭게 논의될 수 있다.

5. 보안 가시성 및 설정가능성

보안 가시성과 설정가능성을 통해 이동통신 환경에서

적용될 보안 특성과 알고리즘을 결정하지만, 네트워크 사업자가 국가의 규제 등을 이유로 암호화를 활성화시키지 않거나 특정 알고리즘만을 허용하는 경우가 있을 수 있다. 표준에서는 사용자가 암호화 적용 여부를 확인할 수 있도록 요구하고 있지만, 실제는 그렇지 못하다.

보안 설정가능성은 사용자가 보안 특성의 제공 여부에 따라 서비스 이용 여부를 설정할 수 있는 것을 말한다. 그러나 현재 유스케이스는 사용자-USIM 인증의 활성화 여부만이 유일하다. 따라서, 5G에서는 보안 설정 가능성의 범위를 좀 더 확대할 수 있다.

6. 플랫폼 보안

LTE 규격에 따르면 각각 eNB와 Home eNB에서 안전한 실행 환경과 신뢰할 수 있는 플랫폼에 대한 필요성을 언급하고 있으나, 어떤 유형의 플랫폼 요구사항이 5G에 적합한지를 논의할 필요가 있다.

7. 서비스 거부 공격 방어

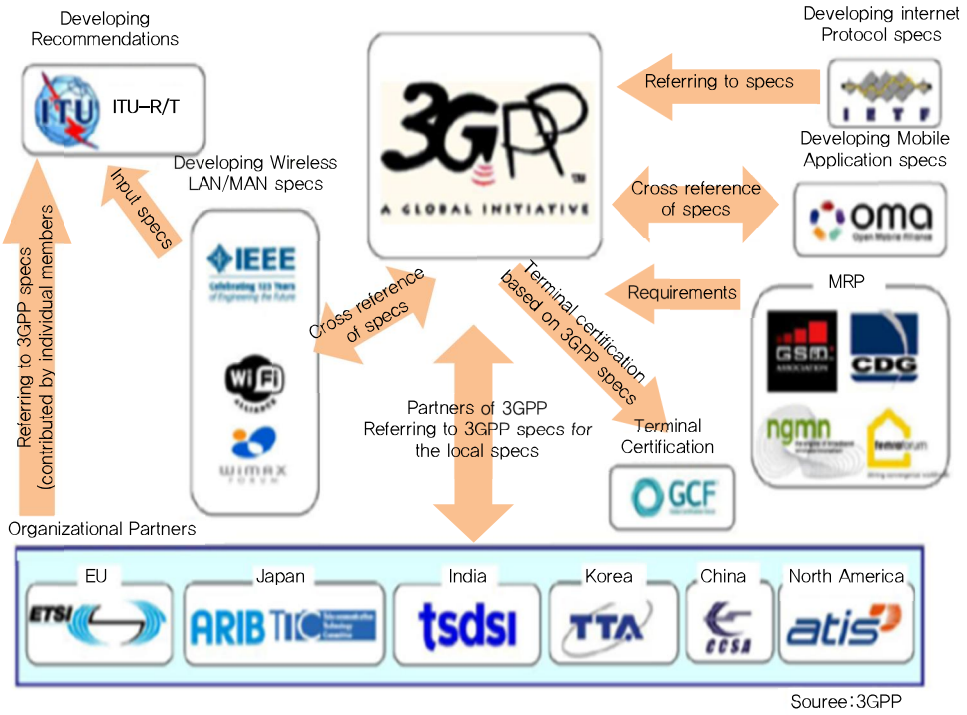
Ⅱ장에서 살펴본 바와 같이, 서비스 거부 공격은 다양한 방식으로 이루어질 수 있어 향후 5G 네트워크의 주요 위협으로 부상할 가능성이 높다. 따라서 서비스 거부 공격을 완화시킬 수 있는 방법에 대한 심도있는 논의가 필요하다.

8. SDN/NFV 도입

LTE 환경에서는 고려하지 않았던 가상화 기술이 전면적으로 도입됨에 따라 SDN/NFV와 같은 새로운 네트워킹 패러다임으로 인한 새로운 보안 요구사항이 추가로 논의되어야 한다.

V. 5G 보안 표준화

5G는 사회에 대한 광범위한 영향과 네트워크 간 유기



(그림 2) 5G 표준화 기구 및 단체

[출처] Reprinted from 5G PPP Security WG, "5G PPP Phase 1 Security Landscape," 5G PPP White Paper, 2017.

적인 상호 작용을 위해 과거보다 표준 의존도가 높을 것으로 전망된다. 따라서 보안 위험 노출을 최소화하려면 보안을 추가 기능으로 고려하는 것이 아니라, 네트워크 구조설계 단계부터 보안을 고려해야 한다. 즉, 'Security by Design' 개념에 따라 일련의 보안, 프라이버시 및 책임 문제를 표준화 및 규제 프로세스에서부터 기본적으로 다루어지도록 고려하는 것이 중요하다.

5G 표준화에 기여하고 있는 표준화 단체 또는 기구를 도식화하면 (그림 2)와 같다. 3GPP는 5G 표준화를 위한 핵심 표준화 기구이지만 ETSI(European Telecommunications Standards Institute), IETF(Internet Engineering Task Force) 및 ITU(International Telecommunication Union) 등에서도 5G와 관련된 표준을 개발하고 있다. 공식 표준화 기구는 아니지만 GSMA (GSM Association) 및 NGMN(Next Generation Mobile Networks)도 5G 표준 규격 수립에 중요한 역할을 수행하고 있다[17].

1. 3GPP

5G 보안에 대한 표준화 작업은 2016 년 1 월 SA3에서 차세대 시스템 보안을 연구하기 위한 특별(ad-hoc) 작업 항목(work item)을 생성하면서 시작되었다. 당시 작업 항목은 다음의 사항을 포함한다.

- 차세대 모바일 네트워크를 위한 서비스, 구조 및 무선 관련 요구사항을 바탕으로 차세대 시스템에 대한 잠재적 보안 위협 및 요구사항의 수집, 분석
- 보안 아키텍처 및 액세스 보안에 대한 분석

보안 분야에는 보안 아키텍처, 인증, RAN 보안, 가입자 개인정보, 네트워크 슬라이싱 보안 및 네트워크 도메인 보안 등과 같은 관련 내용이 포함되며, 이들 각 보안 분야별로 핵심 이슈, 위협요소 및 잠재적 보안 요구사항을 도출한다. 이러한 맥락에서 SA3 그룹은 5G 요구사항을 다루는 SA1과 5G 구조에 중점을 두고 있는 SA2와 협력관계를 유지하고 있다.

2. ETSI

ETSI CYBER 기술위원회는 사이버 보안 표준화를 위해 2014년에 설립되었다. ETSI 내부 및 외부의 이해관계자들과의 긴밀한 협력을 통해 요구사항을 수집/도출하여 정의하고 있다. 아직 5G 보안을 위한 작업 항목을 시작하지 않았지만 개인정보 보증 및 검증을 위한 지침과 메커니즘에 관한 연구를 진행하고 있다.

ETSI ISG(Industry Specification Group) NFV는 네트워크 기능 가상화에 대한 요구사항과 표준 규격 개발을 담당하고 있으며, 특히 SEC 작업반은 다음과 같은 목표를 달성하기 위해 문제정의, 잠재적 취약점 도출 및 요구사항 정의에 이르기까지 NFV 플랫폼 전반의 보안 이슈를 고려하고 있다.

- NFV 고유의 보안 문제 도출 및 네트워크 서비스의 보안을 개선할 수 있는 NFV 환경의 기술적 이점 도출
- 하드웨어부터 소프트웨어까지 신뢰를 확보할 수 있도록 체계적이며 포괄적으로 NFV 보안의 다양한 측면에 대한 지침 제공
- OpenStack과 같은 공개 소프트웨어 기반 플랫폼의 보안 이슈 해결
- NFV 환경에서 합법적 감청(lawful interception)을 제공하는 것과 관련된 문제 해결
- 다른 ETSI NFV 작업반이나 외부 단체/기구와의 긴밀한 협력 유지

3. IETF

2010년 이후 생성된 많은 IoT 작업반이 보안 이슈를 다루어 왔으며 IoT 단말에 적합한 TLS(Transport Layer Security)/DTLS 프로파일을 정의하거나, 제한된

서버 자원에 접근하기 위한 인증된 권한부여 메카니즘을 개발하기도 하였다.

특히 I2NSF(Interface to Network Security Functions)는 물리적인 또는 가상의 네트워크 보안 기능을 제어하고 모니터링하기 위한 소프트웨어 인터페이스와 데이터 모델 정의를 목표로 연구를 진행하고 있다.

4. NGMN

NGMN은 5G 요구사항, 설계 원칙, 잠재적 5G 솔루션 분석 및 미래 유스케이스와 비즈니스 모델 평가를 수행하고 있다. 특히 P1 Requirements and Architecture 프로젝트의 5G 보안 작업반은 무선 구조, 가상화, 개인정보보호, 가용성 및 IoT 분야에서의 5G 보안 이슈 표준화 및 구현을 위한 지침 제공을 목표로 한다.

5. GSMA

GSMA Network 2020 프로그램은 5G 네트워크 요구사항을 고려하여 안전하고 똑똑하며 끊김없는 서비스를 제공하는 네트워크 개발을 목표로 하며, 그 일환으로 4G 시스템의 지속적인 진화와 함께 NFV와 같은 수많은 기술적 동인(drivers)을 제안하고 있다.

6. ITU-T

5G 보안에 대한 ITU-T 표준화 작업은 SG17에서 다루고 있으며, 주요 내용으로는 5G 시스템과 보안 구조 분석, 5G 시스템에 적용할 양자 알고리즘의 요구사항 및 양자 알고리즘을 사용한 5G 네트워크 보안 방법 등이다. 또한 최근에는 5G 생태계의 보안 프레임워크 정의, 5G 시스템의 이해관계자 분석, 이해관계자 간의 보안 경계 및 보안 요구사항 정의 등을 위해 새로운 표준 항목이 채택되기도 하였다.

Ⅵ. 결론 및 시사점

지난 2월 막을 내린 평창동계올림픽은 세계 최초 5G 시범 서비스를 통해 대한민국이 ICT 강국임을 과시한 행사였다. 이후 전세계 ICT 공룡 기업들은 앞다투어 차기 도쿄올림픽 협력의사를 표명하며 자사의 5G 기술을 전세계에 알리고 새롭게 창출될 5G 시장 주도권을 확보하기 위한 경쟁에 돌입했다.

2018년 12월에 개시된 5G의 상용서비스는 기존 3G나 LTE에 비해 단순히 속도가 더 빠르거나 대용량의 데이터를 처리하는 것을 넘어 4차 산업혁명을 앞당기고 상상 이상의 파격적인 서비스로 우리의 삶을 혁신적으로 변화시킬 것으로 전망된다. 그러나, 악의적인 해커나 공격자로부터 우리의 일상을 충분히 안전하게 보호할 수 없다면 장밋빛 전망과 달리 새로운 재난과 재앙을 초래할 우려도 병존한다.

본 고에서는 기존 이동통신 네트워크 환경에서의 보안 위협 이슈 및 공격 유형을 살펴보고, 현재 표준화 및 기술 개발이 활발히 진행되고 있는 5G 이동통신 환경의 특징과 보안 이슈 등을 간략히 소개하였다.

앞서 살펴본 바와 같이 이동통신 표준 규격의 취약점 등을 이용한 공격부터 다양한 유형의 악의적인 공격이 제시되거나 입증되었다. 따라서 앞으로 상용화될 5G에서의 보안 위험을 최소화하려면 지금과 같이 상대적으로 기술 개발 초기 단계부터 상용화 경쟁 못지 않게 네트워크 보안 취약점과 위협 요소를 연구하고 관련 기술 개발을 서둘러 추진해야 할 것이다.

약어 정리

3GPP	3rd Generation Partnership Project
5G	5th Generation
AKA	Authentication and Key Agreement
AS	Access Stratum
DDoS	Distributed Denial of Service
DTLS	Datagram Transport Layer Security
eNB	Evolved Node B
ENISA	European Union Agency for Network and Information Security

EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
GSMA	GSM Association
GTP	GPRS Tunneling Protocol
GUTI	Globally Unique Temporary Identifier
HSS	Home Subscriber Server
I2NSF	Interface to Network Security Functions
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identifier
IoT	Internet of Things
IPsec	IP Security
ISG	Industry Specification Group
ITU	International Telecommunication Union
LTE	Long Term Evolution
MAPsec	Mobile Application Part Security
MME	Mobility Management Entity
NAS	Non Access Stratum
NFV	Network Function Virtualization
NGMN	Next Generation Mobile Networks
OTP	One Time Password
PMSI	Pseudo Mobile Subscriber Identifier
RAN	Radio Access Network
RRC	Radio Resource Control
SCTP	Stream Control Transmission Protocol
SDN	Software-defined Networking
SIGTRAN	Signalling Transport
SMS	Short Message Service
SS7	Signalling System No. 7
TCAPsec	Transaction Capabilities Application Part User Security
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identifier
UMTS	Universal Mobile Telecommunication Standard
USIM	Universal Subscriber Identity Module
VIP	Very Important Person

참고문헌

[1] 최진홍, "한국 이동통신 30년, 그 격동의 역사를 넘어-통신3사의 현재와 미래," 이코노믹리뷰, 2018. 7. 2, available from http://www.econovill.com/news/articleView.html?idxno=340742.

[2] ENISA, "Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation," Mar. 2018, available from https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g.

[3] Positive Technologies, "Primary Security Threats for SS7 Cellular Networks," May 10, 2016 available from https://www.ptsecurity.com/upload/corporate/ww-.en/analytics/SS7-Vulnerabilities-2016-eng.pdf

[4] U. Meyer and S. Wetzel, "A man-in-the-Middle Attack on UMTS," *Proc. ACM Workshop Wireless Security(WiSe '04)*, Philadelphia, PA, USA, Oct. 1, 2004, pp. 90-97.

[5] S.R. Hussain et al., "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," *Netw. Distrib. Syst. Security(NDSS) Symp.*, San Diego, CA, USA, Feb. 18-21, 2018, pp. 1-15.

[6] D. Rupprecht, K. Jansen, and C. Pöpper, "Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness," *USENIX Conf. Offensive Technol. (WOOT '16)*, Austin, TX, USA, Aug. 8-9, 2016, pp. 40-51.

[7] M. Arapinis et al., "New Privacy Issues in Mobile Telephony: Fix and Verification," *ACM Conf. Comput. Commun. Security (CCS '12)*, Raleigh, NC, USA, Oct. 16-18, 2012, pp. 205-216.

[8] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating IMSI Catchers," *ACM SIGSAC Conf. Comput. Commun. Security (CCS '15)*, Denver, CO, USA, Oct. 12-16, 2015, pp. 340-351.

[9] M. Arapinis et al., "Privacy through Pseudonymity in Mobile Telephony Systems," *Netw. Distrib. Syst. Security (NDSS) Symp.*, San Diego, CA, USA, Feb. 23-26, 2014, pp. 1-14.

[10] A. Shaik et al., "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," *Netw. Distrib. Syst. Security (NDSS) Symp.*, San Diego, CA, USA, Feb. 21-24, 2016, pp. 23:1-15.

[11] R.P. Jover, "Security Attacks Against the Availability of

LTE Mobility Networks: Overview and Research Directions," *Int. Symp. Wireless Personal Multimedia Commun. (WPMC '13)*, Atlantic City, NJ, USA, June 24-27, 2013, pp. 1-9.

[12] J. Jermyn, G. Salles-Loustau, and S. Zonouz, "An Analysis of DoS Attack Strategies Against the LTE RAN," *J. Cyber Security*, vol. 3, no. 2, 2014, pp. 159-180.

[13] N. Golde, K. Redon, and J.-P. Seifert, "Let Me Answer that for you: Exploiting Broadcast Information in Cellular Networks," *SEC'13 Proc. USENIX Conf. Security*, Washington, D.C., USA, Aug. 14-16, 2013, pp. 33-48.

[14] ITU-R, "IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," ITU-R M. 2083-0, 2015.

[15] A. Dutta, "Security Challaenges and Opportunities in SDN/NFV and 5G Network," ETSI Security Day, 2017.

[16] G. Horn and P. Schneider, "Towards 5G Security," IEEE *Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 20-22, 2015, pp. 1165-1170.

[17] 5G PPP Security WG, "5G PPP Phase 1 Security Landscape," 5G PPP White Paper, 2017, available from https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf