정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

5G 보안 표준 현황과 미래

권 성 문*, 박 성 민*, 김 도 원*

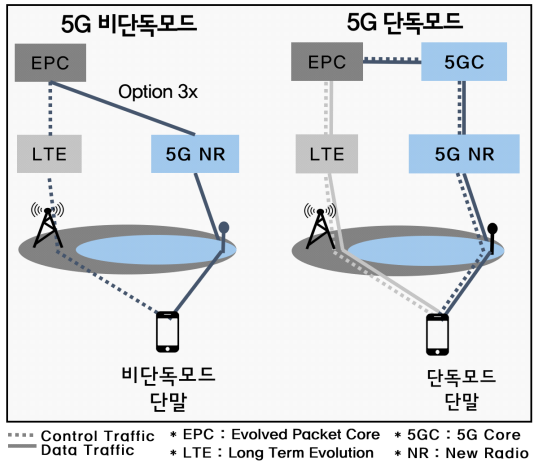
요 약

5G 단독모드(StandAlone)가 미국, 중국 등에 상용화됨에 따라 고속 서비스 eMBB(enhanced Mobile BroadBand), 저 지연 서비스 URLLC(Ultra Reliable Low Latency Communication), 다 연결 서비스 mMTC(massive Machine-Type Communications) 기술 또한 곧 상용 기술화 될 것으로 예상된다. 이러한 5G 서비스의 기술 개발에는 다양한 기업과 기관들이 참여하여 매년 신규 표준이 생성되고 있다. 따라서 본 논문에서는 5G 보안 표준화에 대한 현황을 파악하여 전반적인 5G 보안 동향에 대한 정보를 제공하고자 한다.

Ⅰ. 서 론

5G 기술은 ITU-R(International Telecommunication Union Radiocommunication sector)에서 2015년 IMT-2020(International Mobile Telecommunications-2020)으로 정의한 기술이다.

[그림 1]과 같이 5G는 비단독모드(Non StandAlone)와 단독모드(StandAlone)으로 구분될 수 있다. 5G 비단독모드는 제어 트래픽은 기존 LTE(Long Term Evolution)를, 데이터 트래픽은 5G 기지국을 사용하며 코어 망은 기존 LTE의 EPC(Evolved Packet Core) 망을 사용하는 구조로, 2019년 4월 3일 대한민국에서 최초 상용화를 시작한 기술이다. 5G 단독모드는 제어 및 데이터 트래픽을 모두 5G 기지국과 5G 코어 망을 사용하는 신규 구조로 2020년 8월 4일 미국에서 최초 상용화를 시작한 기술이다. 5G 단독모드에서는 5G 핵심 기술인 고속 서비스 eMBB(enhanced Mobile BroadBand), 저 지연 서비스 URLLC(Ultra Reliable Low Latency Communication), 다 연결 서비스 mMTC(massive Machine-Type Communications) 기술이 접목된 신규 서비스가 적용 가능하다. 신규 서비스에는 각 서비스에 맞는 새로운 보안이 필요하며, 이러한 현 시점에서 5G 보안 표준화 현황이 어떻게 진행되고 있는지 분석한다.



〔그림 1〕 5G 비단독모드와 단독모드 구조

5G 기술에 대한 보안은 ITU-T(ITU-Telecommunication standardization sector) SG17 (Study Groups 17) Q6/17, 통신 서비스 및 네트워크와 IoT(Internet of Things) 보안 부서에서 2018년부터 전담하고 있다. ITU-T SG17 Q6/17은 5G 네트워크를 활용한 응용 기술에 대한 보안 표준 개발[1] 외에도 타 기관과 협업 중에 기관 간의 중복된 업무가 없도록 5G 보안에 대한 중심 기관으로서의 역할을 수행하고 있다.[2]

3GPP(3rd Generation Partnership Project)는 다양한 기관이 참여하여 2017년 3월부터 작업이 시작된

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00793, 국가기간망 사이버공격 사전 예방을 위한 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술 개발)
* 한국인터넷진흥원 (skwon@kisa.or.kr, 주임 연구원, smpark@kisa.or.kr, 책임 연구원, kimdw@kisa.or.kr 팀장)

Release 15부터 5G 코어 기술 및 보안에 대한 표준을 개발 및 배포하고 있다. 5G 보안에 대한 내용은 3GPP TSG(Technical Specification Group) SA (Service & system Aspects) WG3(Working Group 3)에서 전담하고 있다. 3GPP는 표준 및 기술문서 작업 외에도 GSM 협회와 취약점 공개 조정 절차(Coordinated Vulnerability Disclosure)를 담당하고 있다. 각 취약점에 대한 내용은 공개되지 않으나 유럽전기통신표준협회(European Telecommunications Standards Institute) 정기 보안 모임에서 밝혀진 내용[3]에 의하면 14건의 5G관련 보안 취약점이 보고되었으며 주요 보안 이슈는 가짜 기지국(false base station), 보안기능이 제공되지 않은 연결 및 페이징 메시지이다.

이외 5G 보안 표준 움직임으로 유럽의 사이버보안을 위한 NIS 협력 그룹(Network and Information System Corporation Group)에서는 5G 유럽 Toolbox 표준을 만들고 이를 구현하는 절차를 수행 중에 있다.

따라서 본 논문은 5G 보안 표준 현황을 설명하기 위해 2장에서는 ITU 기관의 5G 보안 표준 현황을, 3장에서는 3GPP 기관의 5G 보안 표준 현황을, 4장에서는 NIS 협력 그룹의 5G 보안 표준 현황에 대해 설명한다. 그리고 마지막 5장 결론으로 논문을 끝맺는다.

Ⅱ. 5G 보안 표준 현황 - ITU

ITU-T SG17 Q6/17이 2018년 4월부터 현재까지 작업한 표준은 총 7건으로 이 중 1건이 완료되었다. [표 1]은 ITU-T SG17 Q6/17의 5G 보안 표준을 정리한 것이다. ITU-T SG17 Q6/17은 5G 네트워크를 활용한 응용 기술에 대한 보안 표준 개발을 목표로 하고 있다. X.5Gsec-t 표준은 5G 에코시스템에 참여하는 이해당사자를 정의하고 이들 간의 위협과 보안에 대한 책임을 정의하고 있다. X.5Gsec-ecs 표준은 엣지 컴퓨팅 서비스 도입과 사용 시나리오를 분석하고 보안 위협과 보안 요구사항을 정의하고 있으며, X.5Gsec-guide 표준은 5G 통신 네트워크에 연결된 기기들의 개인 정보 보호를 위한 상위 수준의 보안 요구사항을 정의하고 있다. 이를 위해 5G 네트워크의 특성인 엣지 컴퓨팅, 동적 네트워크 가상화, 네트워크 슬라이싱을 고려한 사용자 단말, 접근 네트워크, 코어 네트워크, 서비스 및 설비의 취약성 분석 및 보안 요구 능력을 도출하는 것을 목표로

〔표 1〕 5G 보안 표준 현황 - ITU 5G 보안 표준

표준 번호	표준 명	완료 예정/ 최근 작업 일시
X.5Gsec-t	Security framework based on trust relationship in 5G ecosystem	2021.09 2020.10
X.5Gsec-ecs	Security framework for 5G edge computing services	2021.09 2020.10
X.5Gsec-guide	Security guideline for 5G communication system	2021.09 2020.09
X.5Gsec-netec	Security capabilities of network layer for 5G edge computing	2021.09 2020.09
X.5Gsec-vs	Security requirements for vertical services supporting URLLC in the 5G non-public networks	2022.09 2020.09
X.5Gsec-ssl	Guidelines for classifying security capabilities in 5G network slice	2022.09 2020.09
X.1811	Security guidelines for applying quantum-safe algorithms in 5G systems	2020.09 2020.09

하고 있으며 주요 내용은 3GPP의 관련 표준 내용을 참고 및 정리하여 작성될 예정이다. X.5Gsec-netec 표준은 엣지 컴퓨팅을 구현함에 있어 통신사 네트워크와 사설 네트워크의 구분이 모호해지는 특성에 대응하기 위한 네트워크 계층의 보안 요구사항 및 조치를 정의하고 있다. X.5Gsec-vs 표준은 사설 네트워크에서 매우 안정적이며 초 저 지연 통신 기술인 URLLC(Ultra Reliable and Low Latency Communication)을 지원하기 위한 보안 요구사항과 예상되는 보안 위협을 정의하고 있다. X.5Gsec-ssl 표준은 다양한 5G 네트워크 슬라이스 적용 경우를 조사하여 다양한 네트워크 슬라이스 유형에 따른 보안 수준을 분류함으로써 네트워크 슬라이스에 대한 보안 지침을 제공하기 위한 표준이다. X.5Gsec-q의 완료 표준인 X.1811은 양자 컴퓨팅의 도입에 앞서 현재 5G 시스템에서 사용되는 암호 알고리즘을 분석하여 발생 가능한 위협을 도출하였다. 또한 양자 컴퓨팅에 안전한 대칭, 비대칭 암호 기술을 분석하고 이를 안전하게 적용하기 위한 지침을 정리하고 있다.

Ⅲ. 5G 보안 표준 현황 - 3GPP

3GPP TSG SA3는 5G 보안을 위해 2019년 3월 Release 15 표준 세트를 완료하고 2020년 7월 Release 16 표준 세트를 완료하였으며 Release 17표준 세트의 작업이 2021년 9월을 목표로 진행되고 있다.

전반적인 5G 보안 내용은 TS(Technical Specification) 33.501, “Security architecture and procedures for 5G System”에 정의되어 있으며, 2017년 6월 논의가 시작되어 2018년 3월 최초의 V15.0.0 버전이, 수정 및 보완된 2019년 3월 Release 15의 V15.10.0 버전이 공개되었다. 가장 최신 버전은 2020년 9월에 완료된 Release 16의 V16.4.0이며 Release 17에서는 추가적인 작업이 아직 예정되어 있지 않다.

3GPP TSG SA3에서는 TS 33.501 외에도 다양한 주제로 5G 보안 표준 작업을 수행하고 있으며 3GPP TSG SA3의 보안 표준 중 5G와 관련 있는 보안 표준은 TS 33.5XX로 번호가 매겨져 있다. 이외 5G 보안 문서로 TR(Technical Report) 33.8XX~TR 33.9XX는 5G 보안 연구에 대한 기술문서이다. 현재 공개된 5G 보안 문서는 철회된 문서를 제외하고 [표 2]의 15개의 TS 33.5XX 표준과 72개의 TR 33.8XX~TR 33.9XX 보안 기술 문서가 있다.

Release 별로 표준 현황을 분석하자면 Release 15에

〔표 2〕 5G 보안 표준 현황 - 3GPP 5G 보안 표준

표준 번호	표준 명	최초 Release/ 최근 작업 Release
TS 33.501	Security architecture and procedures for 5G System	Rel. 15 Rel. 16
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class	Rel. 16 Rel. 16
TS 33.512	5G Security Assurance Specification; Access and Mobility management Function (AMF)	Rel. 16 Rel. 16
TS 33.513	5G Security Assurance Specification; User Plane Function (UPF)	Rel. 16 Rel. 16
TS 33.514	5G Security Assurance Specification for the Unified Data Management (UDM) network product class	Rel. 16 Rel. 16
TS 33.515	5G Security Assurance Specification for the Session Management Function (SMF) network product class	Rel. 16 Rel. 16
TS 33.516	5G Security Assurance Specification for the Authentication Server Function (AUSF) network product class	Rel. 16 Rel. 16
TS 33.517	5G Security Assurance Specification for the Security Edge Protection Proxy (SEPP) network product class	Rel. 16 Rel. 16
TS 33.518	5G Security Assurance Specification for the Network Repository Function (NRF) network product class	Rel. 16 Rel. 16
TS 33.519	5G Security Assurance Specification for the Network Exposure Function (NEF) network product class	Rel. 16 Rel. 16
TS 33.520	5G Security Assurance Specification; Non-3GPP InterWorking Function (N3IWF)	Rel. 17 Rel. 17
TS 33.521	5G Security Assurance Specification; Network Data Analytics Function (NWDAF)	Rel. 17 Rel. 17
TS 33.522	5G Security Assurance Specification; Service Communication Proxy (SECOP)	Rel. 17 Rel. 17
TS 33.535	Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System	Rel. 16 Rel. 17
TS 33.536	Security aspects of 3GPP support for advanced Vehicle-to-Everything services	Rel. 16 Rel. 16

서는 전반적인 5G 보안 기능인 TS 33.501의 작업과 8종의 추가적으로 분석이 필요한 보안 주제에 대한 기술 문서가 작성되었다. 기술 문서 주제로는 네트워크 슬라이싱 관리, 장기간 사용되는 암호화키의 업데이트 절차, 256 비트 암호화 알고리즘, 합법적 감청(Lawful Interception), 5G 서비스 기반 구조(Service Based Architecture) 등이 있다.

Release 16에서는 기 작성 표준의 업데이트와 작성된 TS 33.501에 기반을 둔 5G 각 요소의 보안 테스트 절차인 보안 보증 명세서(SeCurity Assurance Specification)가 다수 작성된 점이 특징이다. 이외 보안 표준으로는 V2X(Vehicle-to- Everything), 3GPP 자격정보 기반의 인증에 대한 보안 표준이 있다. Release 16의 보안 기술문서의 특징은 기존 보안 기능의 공개된 취약점을 보완하기 위한 기술 문서가 다수 발표되었으며, 가짜 기지국에 대한 대응, 취약한 인증 강화, 사용자 위치 노출에 대한 보안 강화, 사용자 데이터에 대한 무결성 방안 등이 있다.

Release 17에서는 보안 표준 문서로 추가적인 보안 보증 명세서 표준들이 있으며 보안 기술 문서로는 엣지 컴퓨팅, 산업 IoT에 대한 적용, MBS (Multicast-Broadcast Service), 모바일 IoT 등 5G의 주요 신규 서비스에 대한 기술 문서가 작성되었다.

따라서 3GPP의 5G 보안 표준화 흐름을 분석해보자면 5G 네트워크 상용화 이전인 Release 15는 5G 보안 기능에 대한 정의를 수행하였으며, 5G 네트워크 상용화 초기 단계인 Release 16은 정의된 보안 기능의 테스트와 주요 보안 이슈에 대한 보완을 수행하였으며, 5G 단독모드 상용화에 따른 Release 17은 본격적인 신규 5G 서비스에 대한 보안을 작업 중인 것으로 분석된다.

〔표 3〕 유럽 툴박스 보안 대책 - 전략 대책

구분	보안 대책 내용
SM01	Strengthening the role of national authorities
SM02	Performing audits on operators and requiring information
SM03	Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk for key assets
SM04	Controlling the use of Managed Service Providers and equipment suppliers' third line support
SM05	Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies
SM06	Strengthening the resilience at national level
SM07	Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU
SM08	Maintaining and building diversity and EU capacities in future network technologies

Ⅳ. 5G 보안 표준화 현황 - NIS 협력 그룹

NIS 협력 그룹은 2016년 설립된 유럽의 사이버보안을 위한 기관으로 유럽 회원국(EU Member States), 유럽 위원회(European Commission), 유럽 사이버보안 기관인 ENISA (European Union Agency for Cybersecurity)로 구성된 기관이다.

2019년 3월, 유럽 위원회의 5G 네트워크에 대한 사이버보안 권고에 따라 유럽 국가의 5G 네트워크 사이버 위협 분석이 수행되었다. NIS 협력 그룹은 2019년 7월 유럽 각 국가에서 제출된 5G 네트워크 위협 분석 보고서를 취합하여 이에 대한 보고서[4]를 2019년 8월 공개하였다. 위협 분석 방법론은 ISO/IEC 27005[5] 표준의 방법론을 따르고 있으며 이에 따라 5G 네트워크에 대한 위협 유형, 위협 행위자, 대상 자산 및 자산 중

〔표 4〕 유럽 툴박스 보안 대책 - 기술 대책

구분	보안 대책 내용
TM01	Ensuring the application of baseline security requirements (secure network design and architecture)
TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards
TM03	Ensuring strict access controls
TM04	Increasing the security of virtualised network functions
TM05	Ensuring secure 5G network management, operation and monitoring
TM06	Reinforcing physical security
TM07	Reinforcing software integrity, update and patch management
TM08	Raising the security standards in suppliers' processes through robust procurement conditions
TM09	Using EU certification for 5G network components, customer equipment and/or suppliers' processes
TM10	Using EU certification for other non 5G-specific ICT products and services

〔표 5〕 유럽 툴박스 보안 대책 - 보조 대책

구분	보안 대책 내용
SA01	Reviewing or developing guidelines and best practices on network security
SA02	Reinforcing testing and auditing capabilities at national and EU level
SA03	Supporting and shaping 5G standardization
SA04	Developing guidance on the implementation of security measures in existing 5G standards
SA05	Strengthening the role of national authorities
SA06	Exchanging best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers
SA07	Improving coordination in incident response and crisis management
SA08	Conducting audits of interdependencies between 5G networks and other critical services
SA09	Enhancing cooperation, coordination and information sharing mechanisms
SA10	Ensuring 5G deployment projects supported with public funding take into account cybersecurity risks

요도, 취약점, 위협 시나리오로 내용을 정리하고 있다.

2020년 1월에는 보고서[4]와 ENISA의 5G 위협 보고서[6]를 고려하여 5G 네트워크의 보안 위협에 대응하기 위한 5G 네트워크 사이버보안 유럽 툴박스[7]를 공개하였다. 툴박스에서 제안하는 보안 대책은 [표 3]과 같은 전략 대책(Strategic Measure) 8항목과 [표 4]와 같은 기술 대책(Technical Measure) 11항목, [표 5]와 같은 추가적인 보조 대책(Supporting Action) 10항목을 제시하였다. 그리고 각 보안대책의 수행을 위한 계획 방법론을 제시하고 있다. 툴박스는 유럽에서 국가적으로 진행 중에 있으며 실제 26개 조직의 수행 경과를 2020년 7월 정리한 툴박스 수행 현황 보고서[8]가 공개되었다. 해당 문서에는 각 보안 대책의 수행 결과에 대한 통계를 정리하고 있다.

유럽 NIS 협력 그룹의 5G 보안 결과물은 보고서에서도 기술하고 있는 바와 같이 작업이 수행된 시기가 5G 기술이 충분히 성숙된 시기가 아니기 때문에 5G 특화 보안 위협 분석에 있어 한계점이 존재한다. 따라서 보안 취약점이 5G 기술에 특화되어 분석되기보다 상위 개념의 보안 분석 내용이 주를 이루고 있는 단점이 있다. 그러나 현재 작업 중인 유럽 툴박스는 실제 유럽의 통신 관련 이해당사자들이 통신 망 보안을 위해 협업하여 도출하고 있는 결과물이다. 따라서 유럽 5G 보안 툴박스는 다양한 서비스로 인해 이해당사자가 복잡해지는 5G 통신망에 적용될 수 있는 사이버보안 가이드라인으로 활용될 수 있다.

Ⅴ. 결 론

현재 5G 코어 네트워크에 대한 주요 보안 기능은 정의가 마무리되어 5G 코어 네트워크에 대해서는 새로이 발견되는 보안 이슈에 대해서만 보완이 논의되는 것으로 분석된다. 특히 유럽은 NIS 협력 그룹의 주도하에 전반적인 5G 네트워크에 대한 보안을 점검 중에 있다. 따라서 현재 활발히 논의 중인 신규 5G 보안은 5G 네트워크를 활용한 신규 서비스에 대한 보안으로 네트워크 슬라이싱, 엣지 컴퓨팅, 모바일 IoT 등의 5G 신규 서비스에 대한 보안이 논의 중에 있다. 특히 5G 단독모드의 도입과 2020년 9월 23일자 삼성에서 공개한 일본 이동통신 사업자 KDDI와 5G 네트워크 슬라이싱 기술 검증 소식[9]은 3GPP Release 15의 표준 중 TS 33.811, “Study on security aspects of 5G network slicing management”와 같은 CR(Change Request) 상태로 중단되었던 표준들의 신규 업데이트를 가능하게 할 것으로 예상된다. 5G 신규 서비스는 eMBB, URLLC, mMTC 기술을 접목한 다양한 서비스일 수 있으며 이러한 서비스의 상용화를 위해서는 보안이 필수적이다. 따라서 5G 이해당사자들은 미래 5G 신규 서비스 보안에 대한 표준화 움직임에 관심을 기울일 필요가 있다.

참 고 문 헌

[1] 백종현, 5세대 이동통신(5G) 보안 기술 표준화 동향, IoT 기술 및 표준 동향, 2019(16), 2019년 11월.

[2] Heungyoul Youm, "5G security standardi- zation strategies in ITU-T", ITU-T Study Group Leadership Assembly 2019.

[3] James Skuse, “Improving 5G Security through Coordinated Vulnerability Disclosure - GSMA CVD Programme”, ETSI Security Week, 2020.06.

[4] NIS COOPERATION GROUP, “EU coordinated risk assessment of the cybersecurity of 5G networks”, 2019.10.
[5] International Organization for Standardization, “Information technology - Security techniques - Information security risk management”, ISO/IEC 27005, 2018.07.
[6] Marco Lourenco and Louis Marinos, “ENISA THREAT LANDSCAPE FOR 5G NETWORKS”, ENISA, 2019.12
[7] NIS COOPERATION GROUP, “Cyber-security of 5G networks EU Toolbox of risk mitigating measures”, 2020.01.
[8] NIS COOPERATION GROUP, “Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity”, 2020.07.
[9] Samsung Newsroom, “삼성전자, KDDI와 ‘5G 네트워크 슬라이싱’ 기술 검증 성공”, 2020년 9월 23일.

〈저 자 소 개〉

권 성 문 (Sungmoon Kwon)
2013년 2월 : 아주대학교 정보컴퓨터공학과 공학사
2020년 8월 : 아주대학교 컴퓨터공학과 공학박사
2020년 7월~현재 : 한국인터넷진흥원 주임연구원

<관심분야> 정보보호, 5G 보안, 제어시스템 보안

박 성 민 (Seongmin Park)
2009년 2월 : 서강대학교 이학·공학사
2015년 2월 : 서강대학교 기술경영대학원 공학석사
2009년 3월~2013년 7월 : LGU+ 코어망개발팀 대리
2013년 8월~현재 : 한국인터넷진흥원 책임연구원

<관심분야> 이동통신망 보안, 네트워크 보안, 융합 보안

김 도 원 (Dowon Kim)
2010년 8월 : 고려대학교 컴퓨터정보통신공학과 공학석사
2005년 3월~현재 : 한국인터넷진흥원 팀장

<관심분야> 정보보호, 5G 보안, AI 보안관제