정 보 보 호 학 회 지
제 32 권 제4호, 2022. 8

ITU-T SG17 5G(IMT-2020) 보안 국제표준화 동향

오 흥 룡*, 염 흥 열**

요 약

한국은 평창 동계올림픽을 통해 세계 최초 5G 상용화 서비스를 시연하였으며, 대부분의 사람들이 5G 스마트폰을 사용하고 있다. 전 세계적으로도 5G 스마트폰의 사용자수와 5G 네트워크를 이용한 헬스케어, 자율주행, 스마트제조, 가상융합, 대용량 데이터처리 등 산업체 중심의 활용 및 서비스가 계속해서 증가되고 있다. 5G 네트워크는 속도, 대기 시간, 대역폭 측면에서 4G 보다 개선되었지만, 5G 코어 네트워크 자체에 존재하고 있는 보안위협과 5G 네트워크를 구축 및 운영하는 관점에서 다양한 보안 문제들이 존재할 수 있다. 이러한 보안 문제들을 해결하기 위해 UN 산하 정보보호 국제표준을 개발하고 있는 ITU-T SG17에서는 통신사업자 및 부가서비스 제공자들이 5G 네트워크를 구축하고 운영할때에 요구되는 보안 지침에 대한 국제표준을 개발하고 있다. 본 논문은 ITU-T SG17에서 추진되고 있는 5G 보안 국제표준화 동향에 대해 살펴하고자 한다.

(* 참고: ITU 내에 '5G' 용어는 'IMT-2020' 용어로 표기함)

Ⅰ. 서 론

이동통신 국제표준을 선도하고 있는 3GPP는 1998년 12월에 신설되었으며, TTA(한국), ETSI(유럽), ATIS(미국), ARIB/TTC(일본), CCSA(중국), TSDSI(인도)에 소속한 이동통신 사업자, 제조사, 서비스사 등 약 770여개 기관 및 산업체들이 이동통신 기술규격을 개발하고 있다. 5G 기술규격은 Release 15(NR, 5GC) 무선접속 규격, Release 16(5G 부가서비스), Release 17(이전 규격의 개선 및 기술 안정화, 멀티캐스트/브로드캐스트 등 추가)로 구성되어 있다. ITU-T SG17에서는 3GPP에서 정의하고 있는 네트워크 구조를 기반으로 통신사업자 및 부가서비스 제공자들이 5G 네트워크를 구축하고 운영할때에 요구되는 보안 지침에 대한 국제표준을 개발하고 있다.

Ⅱ. ITU-T SG17 5G 보안 국제표준화 현황

ITU-T SG17에서 5G 보안은 2018년 3월, 중국에서 제안을 시작으로 표준 개발 작업이 착수되었다. 현재는 총 12건의 표준화 아이템 중에 3건이 국제표준(Recommendation)으로 제정되었고, 1건이 기술문서(Technical Paper)로 채택되었으며, 8건이 개발 중에 있다(SDN, NFV 등 제외). ITU-T SG17에서 개발되고 있는 5G 보안 국제표준화 현황은 [표 1]과 같다.

2.1. X.1811 (X.5Gsec-q)

본 국제표준(X.1811)은 2021년 4월에 제정되었으며, 5G 시스템 환경에서 양자컴퓨터에 내성이 있는 알고리즘을 활용하기 위한 가이드라인을 정의하는데 목적이 있다. 주요 내용은 5G 시스템의 보안구조를 정의하고, 양자컴퓨터가 도입되었을 때, 현재 암호 알고리즘들의 보안위협을 평가 및 이에 적합한 양자 내성 알고리즘을 정의하고 있다. 알고리즘은 비대칭형 및 대칭형 알고리즘, 해시 알고리즘, 이산대수 기반 알고리즘 등 폭넓게 암호알고리즘의 활용성을 검토하였고, 이에 대한 가이드라인을 정의하였다. 아직까지 양자컴퓨터가 정확하게 언제 상용화될지는 아무도 예측하기 어렵지만, 대칭형 알고리즘과 해쉬 알고리즘은 키 사이즈를 크게 함으로써 사용이 가능할 것으로 예측하고 있으며, 공개키 기반

본 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.
[No.2022-0-00013, ICT 국제표준화 전문가 양성 및 역량 강화, No.2021-0-00112, 차세대보안 표준전문연구실]
* 한국정보통신기술협회 표준화본부 (수석연구원, hroh@tta.or.kr)
** 순천향대학교 정보보호학과 (교수, hyyoum@sch.ac.kr)

〔표 1〕 ITU-T SG17 5G 보안 국제표준 현황

No.	제안 국가	권고안 번호	권고안 제목	완료 시기
1	중국	X.1811 (X.5Gsec-q)	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems	2021.4.
2	중국	X.1047 (X.nsom-sec)	Security requirements and architecture for network slice management and orchestration	2021.10.
3	중국 한국	X.1812 (X.5Gsec-t)	Security framework based on trust relationship for IMT-2020 ecosystems	2022.5.
4	일본 한국	XSTP-5Gsec-RM	5G Security Standardization Roadmap	2022.5.
5	한국	X.1813 (X.5Gsec-vs)	Security requirements for the operation of vertical services supporting ultra reliable and low latency communication (URLLC) in the IMT-2020 private networks	2022.9.
6	한국	X.1814 (X.5Gsec-guide)	Security guidelines for IMT-2020 communication system	2022.9.
7	중국 한국	X.5Gsec-ecs	Security guideline for IMT-2020 edge computing services	2023.3.
8	중국	X.5Gsec-ssl	Guidelines for classifying security capabilities in IMT-2020 network slice	2023.3.
9	중국	X.5Gsec-netec	Security capabilities of network layer for 5G edge computing	2023.9.
10	중국	X.5Gsec-message	Security Requirements for 5G message service	2023.3.
11	중국	X.5Gsec-srocvs	Security Requirements for the Operation of 5G Core Network to Support Vertical Services	2024.3.
12	중국	TR.5Gsec-bsf	Guidelines of built-in security framework for telecommunications network	2024.3.

〔표 2〕 5G 시스템에서 활용 가능한 암호 알고리즘

구분	암호명	기능	응용 시나리오
대칭형 암호 알고리즘	128-NEA1	Encryption	사용자 단말(UE)과 액세스/이동성 관리 기능(AMF) 구간, 사용자 단말과 무선기지국(gNB) 구간에 기밀성 확보를 위해 응용 가능
	128-NEA2		
	128-NEA3		
	128-NIA1	MAC	사용자 단말(UE)과 액세스/이동성 관리 기능(AMF) 구간, 사용자 단말과 무선기지국(gNB) 구간에 무결성 보호를 위해 응용 가능
	128-NIA2		
	128-NIA3		
	AES-128	Encryption	IPsec, TLS, DTLS, JWE, ECIES, NFVI
	AES-256	Encryption	IPsec, TLS, DTLS, JWE, NFVI
	Blowfish	Encryption	SDN
	3DES	Encryption	SDN
	SHA-256	Hashing	IPsec, TLS, DTLS, JWS, NFVI
	SHA-384	Hashing	IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-256	Key derivation/ MAC /Pseudo Random Function	Key hierarchy IPsec, TLS, DTLS, JWS, NFVI
	HMAC-SHA-384	Key derivation/ MAC /Pseudo Random Function	IPsec, TLS, DTLS, JWS, NFVI
비대칭형 암호 알고리즘	RSA	Signature	IPsec, TLS, DTLS, JWS, NFVI
	ECDSA	Signature	IPsec, TLS, DTLS, JWS, NFVI
	DH	Key agreement	IPsec, TLS, DTLS, NFVI
	ECDH	Key agreement	IPsec, TLS, DTLS, NFVI

비고 1) - SHA-1 알고리즘은 보안 강도가 취약하여 활용 불가
비고 2) - 현재 사용되고 있는 비대칭형 암호 알고리즘의 키 사이즈는 계산량이 높은 양자 컴퓨터가 활용될 경우 키 사이즈에 관계없이 무력화될 수 있어, 표기하지 않음
비고 3) - TLS 보안 프로토콜은 보안상의 문제로 버전 1.2 이상을 사용해야 함

〔표 3〕 비대칭형 암호 알고리즘을 무력화시키기 위해 요구되는 양자컴퓨터의 연산량

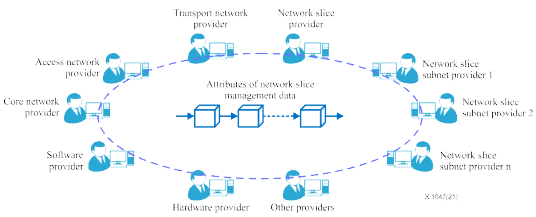
암호 알고리즘	공개키 사이즈 (bits)	대칭형 알고리즘에 준하는 보안 수준 (bits)	논리적 큐비트 (Logical qubits)	물리적 큐비트 (Physical qubits) (비고 1)	토폴리 게이트 (Toffoli gates) (비고 1)	알고리즘이 무력화되기 위해 소요되는 시간 (비고 2)
RSA 〔b-Häner〕	1,024	80	2,050	7.38×10^6	5.81×10^{11}	9.68 h
	2,048	112	4,098	1.48×10^7	5.2×10^{12}	3 days 14 h
	4,096	128	8,194	2.95×10^7	5.59×10^{13}	31 days 21 h
ECC based 〔Roetteler〕	256	128	2,330	8.39×10^6	1.26×10^{11}	2.1 h
	384	192	3,484	1.25×10^7	4.52×10^{11}	7.5 h
	521	256	4,719	1.69×10^7	1.14×10^{12}	19 h

비고 1 - 양자 컴퓨터는 오류 정정을 위해 여분의 물리적 양자비트가 요구된다. 논리적 큐비트당 예상되는 물리적 큐비트 수는 10에서 10,000까지 다양하다. 본 국제표준은 3,600 물리적 큐비트당 하나의 논리적 큐비트로 가정하였다〔14〕.
비고 2 - 본 국제표준에서 토폴리 게이트의 운영 시간은 60ns로 가정하였다〔15〕.

알고리즘들을 더 이상 사용하지 못할 것으로 예측하고 있다. 본 국제표준에서 정의하고 있는 5G 시스템에서 사용 가능한 알고리즘은 [표 2]와 같으며, 비대칭형 암호 알고리즘을 무력화시키기 위해 요구되는 양자컴퓨터의 연산량은 [표 3]과 같다[2].

2.2. X.1047 (X.nsom-sec)

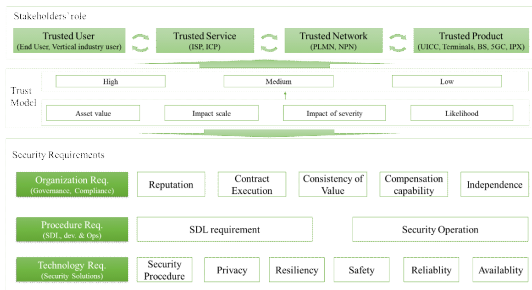
본 국제표준(X.1047)은 2021년 10월에 제정되었으며, 네트워크 슬라이싱 관리 및 오케스트레이션을 위한 보안 요구사항 및 구조를 정의한다. 특히, 네트워크 슬라이싱을 위한 하부 구조와 NFV 구조에서 요구되는 보안 요구사항을 정의한다. 네트워크 운영자와 고객 간에 네트워크 슬라이싱 서비스가 자동으로 운영될 수 있는 구조와 절차를 정의하였고, [그림 1]과 같이 블록체인 메커니즘을 응용하여 네트워크 슬라이싱 서비스 참가자 간에 데이터 관리와 추적 기능을 정의하고 있다[3].



〔그림 1〕 블록체인 기반 참가사 간에 신뢰성 구축 예시

2.3. X.1812 (X.5Gsec-t)

본 국제표준은 2022년 5월에 제정되었으며, 5G 생태계를 구성하고 있는 각 엔티티들 간에 신뢰성 관계를 기반으로 보안 프레임워크를 정의하는데 목적이 있다. 주요 내용은 5G 생태계의 핵심 엔티티들을 식별 및 정의하고, 그들 간에 운영 관계를 분석한다. 각 엔티티들의 고유 취약점 및 관계성에서의 취약점을 규정하고, 이를 해결하기 위해 [그림 2]과 같은 신뢰성 관계 기반 보안 프레임워크를 정의한다. [그림 2]는 3개의 콤포넌트 형태로 구성되어 있다. 첫 번째 컴포넌트의 엔티티들(stakeholers) 간에 역할 관련성은 사용자 단말에서 서비스 제공자까지의 5가지 시나리오(가상 네트워크 구축, 망연계 및 로밍, 자동차 원격 임대, 산업용 네트워크 활용, 공급망(supply chain))를 근거로 관계성을 정의하였다. 두 번째 컴포넌트의 신뢰모델 기준은 4가지 신뢰 기준(자산 가치, 영향력 규모, 심각성 규모, 위험 발생 가능성)을 3단계 척도(상, 중, 하)로 구분하였다. 마지막 세 번째 컴포넌트는 조직 운영관점에서의 보안 요구사항, 보안 절차 및 프로세스관점에서의 보안 요구사항, 기술적 구현관점에서의 보안 요구사항을 정의하고 있다[4].



〔그림 2〕 신뢰성 관계 기반 보안 프레임워크

2.4. XSTP-5Gsec-RM

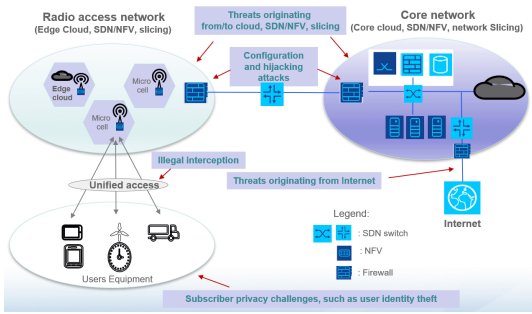
본 기술문서(Technical Paper)는 전 세계 표준개발기구에서 개발되고 있는 5G 보안에 대한 표준화 로드맵을 작성하는 기술문서로 2022년 9월에 승인되었다. 5G 보안관점에서 총 16가지 카테고리로 각 표준개발기구에서 발행된 문서들을 정의하였다. 즉, 5G 코어 네트워크, 무선접근네트워크(RAN), 무선접근, 네트워크 기반 구조, 네트워크 슬라이싱, SDN, NFV, 멀티접근에지컴퓨팅(MEC), 3G와 4G 간에 상호운용성, 로밍, 사용자 단말, 5G 네트워크 기능을 이용한 서비스, 보안 통제, 사기/침해(Fraud), 사설네트워크(NPN), 기타 항목이다. [표 4]는 각 항목별로 개발되었거나 개발중에 있는 국제표준 현황을 도식화한 5G 국제표준화 로드맵이다[5].

2.5. X.1813 (X.5Gsec-vs)

본 권고안은 5G 네트워크를 이용해서 산업용이나 IIoT 서비스 등 특화된 5G 사설망을 위한 초저지연 고신뢰 서비스를 위한 URLLC(Ultra-Reliable Low Latency Communication) 보안 요구사항을 정의하는데 목적이 있다. 특히, URLLC 지원하는 버티컬 서비스를 위한 5G 사설망에서의 보안위협과 이를 해결하기 위한 방법, 안전한 운영을 위한 보안 구축 시나리오 3가지를 정의한다. 첫 번째 구축 시나리오는 5G 사설망 내에 다중 엑세스 에지 컴퓨팅(MEC)에 네트워크 모니터링 서버 기능을 구축하는 방법이다. 두 번째 구축 시나리오는 5G 사설망 내에 독립된 스위치 형태로 네트워크 모니터링 서버 기능을 구축하는 방법이다. 세 번째 구축 시나리오는 앞에 두 가지를 하이브리드 형태로 각각 구축해서 통합 운영하는 방법이다[6]. 본 권고안은 2022년 5월에 사전채택되어 9월에 최종 국제표준으로 제정될 예정이다.

2.6. X.1814 (X.5Gsec-guide)

본 권고안은 3GPP 규격에서 정의하고 있는 5G 시스템 구조를 기반으로 개발하였으며, [그림 3]과 같이 5G 시스템을 구성하고 있는 사용자 단말, 액세스 네트워크, 에지 컴퓨팅, 코어 네트워크, 네트워크 슬라이싱 등 각각의 엔티티 및 컴포넌트들을 규정하고, 보안관점에서

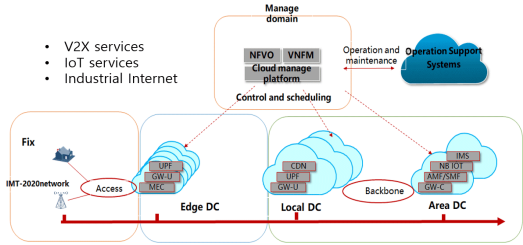


〔그림 3〕 5G 통신 네트워크 내에 보안위협 예시

의 취약점과 이를 대응하기 위한 보안 능력들을 정의한다. 특히 한국은 전파자원제어(RRC: Radio Resource Control)에 대한 보안취약점 및 대응책을 제시하였으며, 부록에 RRC 취약점에 대한 공격시나리오를 정의하였다[7]. 본 권고안은 2022년 5월에 사전 채택되어 9월에 최종 국제표준으로 제정될 예정이다.

2.7. X.5Gsec-ecs

본 권고안은 [그림 4]와 같이 에지 컴퓨팅 서비스의 구축 방법 및 응용 시나리오를 분석하고, 5G 환경에서 에지 컴퓨팅 서비스를 적용하기 위한 보안 가이드라인을 정의하는데 목적이 있다. 5G 시스템에서는 데이터 용량이 방대해지면서 중앙집중형 클라우드 환경에서 점차 사업자 중심의 에지 컴퓨팅 환경으로 변화되고 있는 추세이며, 이에 대한 보안 표준이 필요하다. 본 권고안은 3계층(인프라구조, 네트워크, 응용) 관점에서의 보안 요구사항과 이를 충족하기 위한 보안 능력을 정의하였다. 특히, 5G 네트워크 환경에서 에지 컴퓨팅 구축을 통한 서비스는 자율주행서비스, IoT 서비스, 산업제어 서비스를 목표로 하고 있다[8]. 본 권고안은 2022년 9월에 표준초안 개발 작업을 마무리하고, 국가별 의견수렴 단계로 진행될 예정이다.



〔그림 4〕 5G 에지 컴퓨팅 서비스 구축방법

〔표 4〕 5G 보안 국제표준화 로드맵

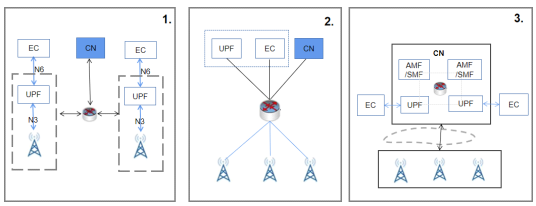
	General/ Definition	Common requirement, use cases	Architecture	Technical specification	Guideline	Certification	Others
General	3GPP TS 33.805, GSMA FS.40, 3GPP TR 33.866, 3GPP TR 33.852, ENISA Threat, ENISA Threat2	NIST SE5G			ITU-T X.5Gsec-guide, ENISA Supply, NIST SP1800-33A, NIST SP1800-33B		
5G core network	3GPP TR 33.845	3GPP TS 33.814	3GPP TS 33.501, 3GPP TS 33.535 3GPP TS 33.807	3GPP TS 33.501, 3GPP TS 33.535, 3GPP TS 33.807, 3GPP TR 33.846, 3GPP TR 33.847, 3GPP TR 33.855, 3GPP TR 33.856, 3GPP TR 33.875	3GPP TS 33.808, 3GPP TR 33.876	3GPP TS 33.512, 3GPP TS 33.513, 3GPP TS 33.514, 3GPP TS 33.515, 3GPP TS 33.516, 3GPP TS 33.517, 3GPP TS 33.518, 3GPP TS 33.519, 3GPP TS 33.520, 3GPP TS 33.521, 3GPP TS 33.522,	NGMN NCE
RAN		3GPP TS 33.840		3GPP TS 33.824	NGMN Pac1	3GPP TS 33.511	
Radio access	3GPP TR 33.865			3GPP TS 33.809, 3GPP TR 33.859, 3GPP TR 33.861, 3GPP TR 33.863			
Network infrastructure	3GPP TR 33.848	3GPP TS 33.818			3GPP TR 33.738	GSMA FS.13, GSMA FS.14, GSMA FS.15, GSMA FS.16	ENISA Virtual
Network slicing	ETSI GR ZSM 010	ITU-T X.1047, ITU-T X.5Gsec-ssl	ITU-T X.1047	3GPP TS 33.811, 3GPP TS 33.813			NGMN Pac2, GSMA NG.116
SDN	IEEE P1915.1	ITU-T X.1038, ITU-T X.1042	ITU-T X.1038, ITU-T X.1046				ENISA SDN
NFV	ETSI GS-VFV-SEC 001, ETSI GS-VFV-SEC 002, GSMA FS.33, IEEE P1915.1	ITU-T X.1044, ITU-T X.1045, ETSI GS-VFV-SEC 009, ETSI GS-VFV-SEC 014, ETSI GS-VFV-SEC 016, ETSI GS-VFV-SEC 020, ETSI GS-VFV-SEC 021, ETSI GS-VFV-SEC 022, ETSI GS-VFV-SEC 023, ETSI GS-VFV-SEC 024, ETSI GS-VFV-SEC 025	ITU-T X.1046 ETSI GS-VFV-SEC 011 ETSI GS-VFV-SEC 012 ETSI GS-VFV-SEC 026		ETSI GS-VFV-SEC 003 ETSI GS-VFV-SEC 006 ENISA NFV		ETSI GS-VFV-SEC 004 ETSI GS-VFV-SEC 010 ETSI GS-VFV-SEC 013
MEC		ITU-T X.5Gsec-ecs, ITU-T X.5Gsec-netec, ITU-T X.itssec-5	ITU-T X.5Gsec-ecs	3GPP TS 33.839	3GPP TR 33.739		NGMN Pac3, ETSI GS MEC 030, ETSI GR MEC 031
Interoperability					GSMA FS.34	3GPP TS 33.520	
Roaming	ENISA Signal				GSMA FS.21, GSMA FS.36, GSMA FS.37, GSMA IR.77, GSMA NG.113	3GPP TS 33.517	
User equipment			IEEE P1912				
Services using 5G		3GPP TS 33.536, 3GPP TS 33.819, 3GPP TS 33.835, 3GPP TS 33.836, 3GPP TR 33.850, 3GPP TR 33.851, 3GPP TR 33.854 X.5Gsec-message	NGMN E2E	3GPP TS 33.122, 3GPP TS 33.503, 3GPP TR 33.825, 3GPP TR 33.862	3GPP TR 33.740, 3GPP TR 33.881, 3GPP TR 33.889		
Security control	ETSI GR ZSM 010	ENISA 3GPP	ITU-T X.1812, NGMN Trust		ETSI GS-VFV-SEC 013. NGMN NO, ENISA EECC		
Fraud	GSMA FS.39				GSMA FS.38		NGMN Pac3
Non public network		ITU-T X.5Gsec-vs		3GPP TR 33.857			
Others	3GPP TR 33.841, GSMA FS.35	3GPP TS 33.126	3GPP TS 33.127	3GPP TR 33.842	ITU-T X.1811		

2.8. X.5Gsec-ssl

본 권고안은 5G 네트워크 슬라이싱 보안기술을 분류화해서 5G 네트워크를 구축할 때, 보안 구축비용을 서비스에 맞게 적용하는데 목적이 있다. 이를 위해, 다양한 5G 네트워크 슬라이싱 보안기술에 대한 분석과 이들을 분류할 수 있는 원칙과 방법을 정의하고 있다. 5G 네트워크 슬라이싱 보안 능력은 7가지 보안관점(네트워크 슬라이스에 특화된 인증 및 권한부여, 리소스에 대한 슬라이스 격리, 사용자 영역의 데이터 보호, 경계영역의 보호, 응용서비스 보호, 인증 및 권한부여하는 과정에서의 프라이버시 보호, 선택된 네트워크 슬라이스에 대한 프라이버시 보호)을 기반으로 분류하였다[9]. 본 권고안은 2022년 9월에 표준초안 개발 작업을 마무리하고, 국가별 의견수렴 단계로 진행될 예정이다.

2.9. X.5Gsec-netec

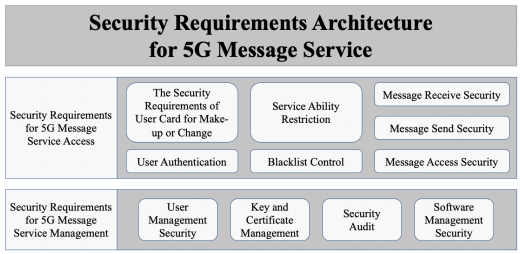
본 권고안은 5G 네트워크 환경에서 에지 컴퓨팅을 구축할 때, 네트워크 계층의 보안 위협과 이를 대응하기 위한 보안기술을 정의하는데 그 목적이 있다. 현재 5G 네트워크 환경을 구축하는 방법은 국가별, 통신 사업자별로 다양한 형태로 네트워크를 구축하고 있다. 따라서, 본 권고안은 [그림 5]에서처럼 기지국별로 에지 컴퓨팅을 구축하는 방법, 기지국을 그룹핑해서 구축하는 방법, 무선 접근 네트워크와 코어 네트워크 간에 협업하는 방법 제시하고 있으며, 이러한 다양한 구축방법을 고려한 보안 위협 및 대응방법을 정의하고 있다[10].



〔그림 5〕 5G 네트워크 환경에서 에지 컴퓨팅 구축 방법

2.10. X.5Gsec-message

본 권고안은 5G 환경에서 비즈니스용으로 많이 활용되고 있는 메시지(예: 챗봇서비스)에 대한 보안 요구사항을 정의하는데 목적이 있다. 특히, 3G, 4G 네트워크

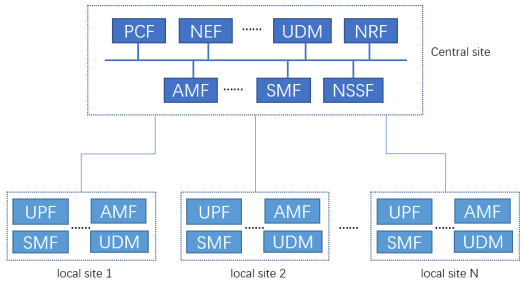


〔그림 6〕 5G 메시지 서비스를 위한 보안 요구사항 구조

환경과 5G 네트워크 환경 간에 메시지 전달하는 보안 기능 관점에서의 차이점을 정의하려고 한다. 5G 메시지 서비스를 위한 보안 요구사항은 5G 메시지 서비스의 접근을 위한 보안 요구사항과 5G 메시지 서비스의 관리를 위한 보안 요구사항으로 [그림 6]과 같은 구조이며, 이를 기반으로 세부적인 보안 요구사항들을 정의할 예정이다[11].

2.11. X.5Gsec-srocvs

본 권고안은 2022년 9월에 신설된 표준화 아이템으로 버티컬 서비스를 지원하기 위한 5G 코어 네트워크 운영방법에 대한 보안 요구사항을 정의하는데 목적이 있다. 즉, 5G 코어 네트워크가 구축된 중심 네트워크와 버티컬 서비스가 구축된 각 로컬 네트워크들 간에 안전하게 운영하기 위한 보안 요구사항을 정의하고자 하며, 기본 개념은 [그림 7]과 같다. 본 권고안은 처음 시작하는 단계에 있어, 향후 다양한 구축 시나리오 기반의 보안 위협 및 보안 요구사항들이 논의될 것으로 예상된다[12].



〔그림 7〕 X.5Gsec-srocvs 개념도

2.12. TR.5Gsec-bsf

본 기술보고서는 2022년 9월에 신설된 표준화 아이템으로 정보통신 네트워크를 위한 내장형 보안 프레임

워크를 개발하는데 목적이 있다. 본 기술보고서의 기본 취지는 5G 시스템을 안전하게 운영하기 위해 개발된 다양한 국제표준들과 현재 활용되고 있는 다양한 보안 메커니즘을 분석하여, 서로 간에 상충되는 보안 요구사항들의 이해격차를 해소하고, 이들의 보안 요구사항들을 최적화하고자 한다. 본 기술보고서는 처음 시작하는 단계에 있어, 향후 다양한 운영 사례 및 기 정의된 보안 요구사항들의 문제점들이 논의될 것으로 예상된다[13].

Ⅲ. 결 론

본 논문은 ITU-T SG17에서 연구하고 있는 5G 보안 국제표준화 동향에 대해 살펴보았다. 5G 보안은 전 세계적으로 주목받고 있는 이슈이고, 국가별로 많은 R&D 투자가 이루어지고 있는 분야이다. 특히 2022년 3월, 3GPP에서 5G 융합서비스 확장 규격 Release 17 표준이 승인되어, ITU-T SG17에서도 다양한 융합서비스 보안 국제표준 개발이 이루어질 것으로 예상되어, 국내 산학연 전문가들의 많은 관심과 적극적인 참여가 필요하다.

참 고 문 헌

[1] ITU-T SG17 Homepage, https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

[2] ITU-T X.1811, Security guidelines for applying quantum-safe algorithms in 5G systems, 2021.04.

[3] ITU-T X.1047, Security requirements and architecture for network slice management and orchestration, 2021.10.

[4] ITU-T X.1812, Security framework based on trust relationships for IMT-2020 ecosystem, 2022.05.

[5] SG17-TD312, Revised baseline text for XSTP-5Gsec-RM: 5G security standardization roadmap, 2022.05.

[6] SG17-TD300, 7th revised baseline text for X.1813(X.5Gsec-vs): Security requirements for the operation of vertical services supporting ultra-reliable and low latency communication (URLLC) in the IMT-2020 private networks, 2022.05.

[7] SG17-TD264R2, 8th revised baseline text for X.1814(X.5Gsec-guide): Security guidelines for 5G communication system, 2022.05.

[8] SG17-TD489, Revised baseline text for X.5Gsec-ecs: Security Guidelines for IMT-2020 Edge Computing Services, 2022.07.

[9] SG17-TD490, 4th Revised baseline text for X.5Gsec-ssl: Guidelines for classifying security capabilities in 5G network slice, 2022.07.

[10] SG17-TD317, Revised baseline text for X.5Gsec-netec: Security Capabilities of Network Layer for 5G Edge Computing, 2022.05.

[11] SG17-TD299, Revised baseline text for X.5gsec-message: Security Requirements for 5G Message Service, 2022.05.

[12] SG17-TD268, Proposal for new work item X.5Gsec-srocvs: Security Requirements for the Operation of 5G Core Network to Support Vertical Services, 2022.05.

[13] SG17-TD255R1, Proposed new work item on: Guidelines of Built-in Security Framework for the Telecommunications Network, 2022.05.

[14] Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N. (2012). Surface codes: Towards practical large-scale quantum computation. Physical Review A, 86, 032324. DOI: 10.1103/PhysRevA.86.032324.

[15] Banchi, L., Pancotti, N., Bose, S. (2016). Quantum gate learning in qubit networks: Toffoli gate without time-dependent control. npj Quantum Information 2, 16019. DOI: 10.1038/npjqi.2016.19.

〈저 자 소 개〉

오 흥 룡 (Heung-Ryong Oh)

종신회원

2002년 2월 : 순천향대학교 전자공학과 학사
2004년 2월 : 순천향대학교 정보보호학과 석사
2018년 2월 : 순천향대학교 정보보호학과 박사
2004년 2월~현재 : 한국정보통신기술협회 표준화본부 수석연구원
2005년 3월~현재 : ITU-T SG17 국내 연구반 간사(역) 및 위원
2009년~2016년 : ITU-T SG17 Q2 Associate Rapporteur
2017년~현재 : ITU-T SG17 Q2 Co-Rapporteur
2011년~현재 : 한국정보보호학회 학회지 편집위원
2012년 8월~현재 : 국방부 국방정보기술표준(DITA) 자문위원
2017년 9월~현재 : 금융결제원 바이오인증 성능위원회 자문위원
2019년 4월~현재 : 용인시 지역정보화위원회 자문위원
<관심분야> 보안프로토콜, 정보보호표준

염 흥 열 (Heung Youl Youm)

종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사
한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 8월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
2017년~현재 : ITU-T SG17 의장
2009년~2016년 : ITU-T SG17 부의장, WP3 의장
2011년 1월~12월 : 한국정보보호학회 회장
2012년 1월~현재 : 한국정보보호학회 명예회장
2016년 5월~현재 : 개인정보보호표준포럼 의장
2020년 8월~현재 : 개인정보보호위원회 위원
<관심분야> 네트워크 보안, IoT 보안, 블록체인 보안, 개인정보보호, 정보보안 국제표준