정 보 보 호 학 회 지
제 31 권 제6호, 2021. 12

5G 단독모드 기기 보안 인증 현황

권 성 문*, 박 성 민**, 김 도 원***

요 약

미국, 중국 등에 이어 국내에서도 KT에서 2021년 7월 5G 단독모드(StandAlone)를 상용화 하였다. 5G 비단독모드(Non-StandAlone)에서는 다년간 사용되었던 기존 LTE(Long Term Evolution) 망의 장비를 재활용하기 때문에 신규 장비의 도입은 5G 기지국으로 제한된다. 그러나 5G 단독모드에서는 새롭게 정의된 5G 장비들을 사용하기 때문에 이에 대한 위협 분석과 보안 기능의 정의에 따라 각 장비에 보안의 구현이 제대로 되어 있는지 검증하는 절차가 요구된다. 이러한 환경에서 본 논문은 5G 단독모드 기기의 보안 인증 현황을 제공하고자 한다.

Ⅰ. 서 론

5G 이동 통신 시스템은 크게 5G 비단독모드(Non-StandAlone)와 5G 단독모드(StandAlone)로 나뉜다. 5G 비단독모드는 5G 전용 기지국과 4G때 사용하던 LTE(Long Term Evolution) 코어 망을 사용하며 2019년 4월 한국의 최초 상용화를 시작으로 전 세계적으로 사용되고 있다. 반면 5G 단독모드는 5G 신규 코어 망을 사용하며 2020년 8월 미국의 T-mobile을 시작으로 2021년 6월 기준 9개국, 12개의 통신사에서 서비스 되고 있다[1]. 한국에서는 이동 통신사 3사 중 KT만이 2021년 7월 상용화하여 서비스가 제공되고 있다.

기존 LTE 통신에서는 사용자 고유 식별 값인 IMSI (International Mobile Subscriber Identity)가 망 최초 접속 시 평문으로 전송된다. 공격자가 이를 스니핑 할 시 이를 이용한 사용자 도용, 추적 등 다양한 보안 이슈가 보고되었다. 이러한 보안 이슈에 대응하기 위해 5G 통신에서는 IMSI를 암호화한 SUCI (Subscription Concealed Identifier) 체계를 만드는 등 기존 LTE 통신에서 알려진 보안 취약점에 대응할 수 있는 보다 강력한 보안 기능을 설계하였다. 그러나 강화된 보안 기능들이 설계되어 있더라도 이를 구현한 통신 기기에서 특정 암호 인자를 초기화하지 않아 보안에 취약해 지는 ReVoLTE 취약점[2]이 보고된 바 있어 5G 기기의 5G 보안 기능 인증 또한 중요한 보안 요소이다.

따라서 본 논문은 5G 기기에 대한 보안 인증 현황을 제공하고자 하며, 2장에서는 IT 기기의 보안 인증에 널리 활용되는 공통평가기준(Common Criteria) 인증과 5G에 대해, 3장에서는 5G 표준화 그룹들이 진행하고 있는 NESAS 인증에 대해 설명하며 4장에서 논문을 맺는다.

Ⅱ. 5G 인증 – 공통평가기준 인증

공통평가기준 인증은 IT 제품의 보안 인증 제도로 제품의 유형에 따라 요구사항이 다르다. 2021년 12월 기준 인증이 유효한 기기는 총 14유형의 1,630 종의 기기가 있다[3]. 공통평가기준 인증을 주제로 5G 기기 제조사의 인증 현황과 5G 전용 공통평가기준, 보호 프로파일(Protection Profile) 개발 연구 현황을 설명한다.

공통평가기준 인증을 취득한 5G 기기로는 삼성, 화웨이, ZTE의 5G 기지국(gNodeB)이 있으며 모두 네트워크 관련 기기 및 시스템 유형이다. 화웨이 기지국은 2020년 6월[4], 삼성의 5G 기지국은 2020년 11월[5], ZTE의 5G 기지국은 2021년 8월[6]에 인증을 받았다. 인증 세부 내용을 살펴보자면 각 제품마다 보안 인증

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 (선임 연구원, skwon@kisa.or.kr)
** 한국인터넷진흥원 (책임 연구원, smpark@kisa.or.kr)
*** 한국인터넷진흥원 (팀장, kimdw@kisa.or.kr)

범위가 크게 차이가 나는데, 삼성의 5G 기지국 보안 인증은 5G 기능을 제외한 일반적인 네트워크 기기에 대해서만 보안 인증을 받았다. 따라서 삼성의 5G 기지국의 경우 5G 보안 기능에 대해서는 검증되지 않았다. 반면, 화웨이의 5G 기지국 보안 인증은 화웨이에서 5G 통신망에 대한 위협을 정의 및 보안 요구사항을 도출하고 이에 대한 내용을 포함한 보안 인증을 받아 5G 보안 기능에 대한 자체적인 검증이 수행되었다고 볼 수 있다. 이러한 인증 범위의 차이는 실제 취약점 테스트 결과에서 보안 유효성이 드러났는데, 현재는 보안 패치가 완료된 ReVoLTE[2] 취약점의 경우 5G 보안 기능 검증이 수행된 화웨이의 5G 기지국에서는 취약점에 대해 보안이 안전한 것으로 분석되었으나 삼성의 5G 기지국의 경우 취약한 것으로 분석된바 있다. 2021년에 인증을 받은 ZTE의 5G 기지국의 경우 3GPP(3rd Generation Partnership Project)의 5G 기지국 보안 보증 요구사항 표준(Security Assurance Specification)에 기반한 보안 요구사항을 포함하여 보안 인증을 받아 보다 객관적으로 5G 보안 기능이 검증되었다고 볼 수 있다. 그러나 3GPP의 보안 보증 요구사항 표준이 미완성 된 부분을 포함하고 있으며 이외 작성된 부분에서도 꾸준히 수정작업이 수행되고 있기 때문에 인증을 취득한 것으로만 판단 할 수 없으며 지속적인 보안 검토가 필요하다.

5G 전용 공통평가기준 개발 연구는 5G 전용 보호 프로파일 도출에 초점이 잡혀져 있다[7-8]. 공통적인 무선통신 보안 요구사항과 LTE 및 5G의 알려진 취약점을 분석하여 보안 요구사항을 도출한 연구로 화웨이의 5G 기지국의 공통평가기준 인증과 맥락이 유사한 면이 있다.

Ⅲ. 5G 인증 – NESAS

NESAS(Network Equipment Security Assurance Scheme) 인증은 이동통신 네트워크에 특화된 인증제도이다. NESAS 인증 제도는 세계 이동통신 사업자협회(Global System for Mobile Communications Association)와 3GPP가 2019년 10월에 공동 제정하였으며 세계 이동통신 사업자협회에서는 전체적인 테스트 프레임워크를, 3GPP에서는 각 이동통신 기기마다 공통평가기준 인증의 보호 프로파일의 수준과 유사한 구체적인 보안 보증 요구사항을 담당한다. 테스트 프레임워크는 크게 2단계로 제품 개발 및 제품 수명주기 프로세스 검사와 제품 보안 보증 테스트로 나뉘어져 있다.

이동통신 사업자협회와 3GPP의 본사가 모두 유럽에 위치하여 유럽의 통신 보안 강화를 위해 유럽 이동통신 보안 표준의 하나로 채택하려는 움직임이 진행중이다[9]. 그러나 이러한 움직임이 진행되고 있을 뿐 아직 표준이나 주요 인증으로 채택된 제도가 아니기 때문에 공통평가기준 인증과 달리 실질적으로 효력을 행사하기 힘든 한계점이 있다. 현재 총 40 종류의 5G

〔표 1〕 3GPP 보안 보증 표준 현황

구분	대상	표준 작성 현황
TS 33.511	gNodeB	2021.12 테스트 케이스 업데이트 테스트 케이스 1건 미작성 전반적인 작업 완료
TS 33.512	AMF	2021.12 테스트 케이스 업데이트 테스트 케이스 1건 미작성 전반적인 작업 완료
TS 33.513	UPF	2021.9 테스트 케이스 업데이트 전반적인 작업 완료
TS 33.514	UDM	2021.6 신규 항목 추가 전반적인 작업 완료
TS 33.515	SMF	2021.9 오탈자 수정 전반적인 작업 완료
TS 33.516	AUSF	2020.12 레퍼런스 추가 작업 중
TS 33.517	SEPP	2021.6 신규 항목 추가 전반적인 작업 완료
TS 33.518	NRF	2020.7 테스트 케이스 업데이트 전반적인 작업 완료
TS 33.519	NEF	2020.12 레퍼런스 추가 전반적인 작업 완료
TS 33.520	N3IWF	2021.2 세부 내용 작성 작업 중
TS 33.521	NWDAF	2021.9 내용 명료화 작업 중
TS 33.522	SCP	2021.11 세부 내용 작성 작업 중
TS 33.526	MnF	미작성
TS 33.527	가상 네트워크 장비	미작성

기기가 인증을 받았으며, 인증 업체로는 화웨이, ZTE, 에릭슨, 노키아가 인증을 받았다[10]. 올해 6월부터 삼성 또한 인증 절차를 진행 중에 있어 주요 이동통신 업체가 모두 NESAS 인증에 참여하게 되어 앞으로 주요 제도로 정착될 가능성이 있다. 특히 공통평가기준 인증의 경우 시간과 비용 적인 측면에서 비효율적이기 때문에 이동통신 장비 및 모바일 기기에 최적화되어 비교적 간단한 프로세스를 가진 NESAS 인증이 업체에서도 선호될 수 있다. 다만, 아직 제도 자체가 다듬어져 가고 있을 뿐만 아니라 구체적인 테스트 항목인 3GPP TS 33.5XX 넘버링되어 있는 5G 기기별 보안 보증 요구사항이 기기 종류에 따라 작성이 거의 되지 않은 표준도 있는 한계점이 있다. 특히 표준 작업의 완성도가 부족한 기기 유형에 대해서도 NESAS 인증을 취득한 기기가 공개된 인증 기기 목록에 존재하기 때문에 아직까지는 인증 제도의 정립이 완벽히 되지 않은 것으로 분석된다. [표 1]은 2021년 12월 기준 14종의 3GPP 보안 보증 표준 현황을 정리한 것이다.

Ⅳ. 결 론

현재 5G 보안 기기의 인증은 크게 일반 네트워크 기기 수준의 보안 인증, 자체적으로 작성한 5G 보안 요구사항을 포함한 보안 인증, NESAS 보안 인증으로 나누어 볼 수 있다. 일반 네트워크 기기의 보안 인증은 5G 보안 기능을 검증하지 못하기 때문에 ReVoLTE 취약점과 같은 5G 보안 기능 구현에서 그 한계가 드러났다고 볼 수 있다. 자체적으로 작성한 5G 보안 요구사항은 5G 기기 제조사의 주관적인 항목으로 3GPP 5G 보안 표준의 보안 항목들이 모두 테스트 항목으로 포함되어 있는지 확인해야 한다. NESAS 보안 인증의 경우 3GPP 5G 보안 표준에 기반하여 도출된 표준이기 때문에 현재 방향성으로는 가장 적합해 보이나 아직 보안 보증 요구사항 표준이 아직 미흡한 한계가 있다. 또한 NESAS 인증 절차에서 보안 보증 요구사항이 업데이트됨에 따른 재감사 규정이 없기 때문에 NESAS 인증 제품 도입 시 해당 기기의 보안 보증 요구사항 표준의 항목을 체크하고 새로운 버전의 출시와 재감사를 제조사에 요구해야 한다.

참 고 문 헌

[1] Global mobile Suppliers Association. 5G Stand Alone Global Market Status: Executive Summary, June 2021.

[2] Rupprecht, David, et al. "Call Me Maybe: Eavesdropping Encrypted {LTE} Calls With ReVoLTE." 29th {USENIX} Security Symposium ({USENIX} Security 20). 2020.

[3] Common Criteria Certified Products, Available: https://www.commoncriteriaportal.org/products/

[4] Organismo de Certificación de la Seguridad de las Tecnologías de la Información, “Certification Report: Huawei 5900 Series 5G gNodeB Software V100R015C00SPC108”, 2020.04

[5] Canadian Common Criteria Scheme, “Common Criteria Certification Report: Samsung 5G gNB AU, DU v19.A”, 2020.12

[6] TÜV Rheinland Nederland B.V., “Certification Report: ZTE 5G-RAN Solution V3.00.30.20P10”, 2021.04

[7] 홍바울, 김예준, 조광주, 김승주, 5G 기지국에 대한 보안성평가기준 연구, 정보보호학회논문지 31.5 (2021): 919-939

[8] Hyungjin Cho, Sungmoon Kwon, Daeun Kim, Dowon Kim, and Ieckchae Euom, Development Protection Profile for 5G Mobile Core Network Equipment, The 5th International Symposium on Mobile Internet Security, 2021.10.

[9] Joonho Lee, Introduction to Network Equipment Security Assurance Scheme (NESAS), The 5th International Symposium on Mobile Internet Security, 2021.10.

[10] NESAS Evaluated Network Equipment Products, Available: https://www.gsma .com/security/nesas-evaluated-network-equipment-products/

〈저 자 소 개〉

권 성 문 (Sungmoon Kwon)

2013년 2월 : 아주대학교 정보컴퓨터공학과 공학사
2020년 8월 : 아주대학교 컴퓨터공학과 공학박사
2020년 7월~현재 : 한국인터넷진흥원 선임연구원
<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