정 보 보 호 학 회 지
제 30 권 제6호, 2020. 12

5G 구조에 적합한 보안 기술 설계를 위한 해외 보안요구사항 동향 분석

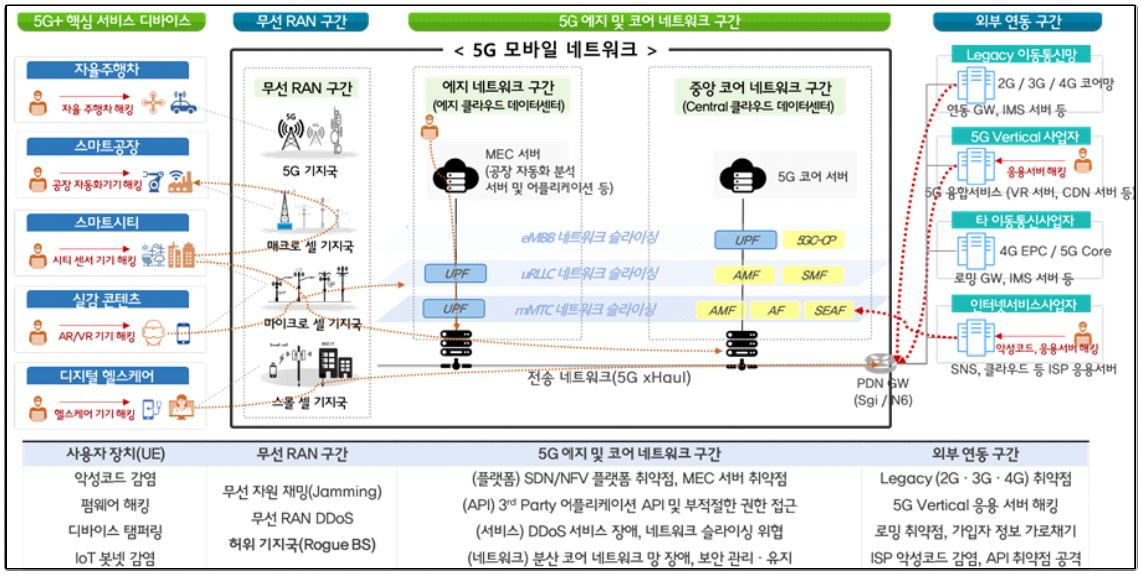
김 환 국*

요 약

2019년 NAS기반 5G 서비스가 국내에서 상용화 된지 1년 반이 지났다. 그동안 5G로의 전환에 따라 발생 될 수 있는 새로운 보안 위협에 대한 우려가 지속적으로 제기되었고, 현재 보안기술의 한계를 극복하기 위한 다양한 5G 보안 연구들이 다 각도로 시도되고 있다. 5G 보안은 이전 세대 보안과는 강한 보안 기능의 설계가 요구된다. 특히 5G 보안 위협 요소들을 식별하고 분석을 통한 5G 네트워크 및 서비스의 보안 아키텍처 설계가 중요한데, 이는 인증, 암호화, 침입탐지 등 기존 보안 메커니즘들이 새로운 5G 기술을 통합되고 수용될 수 있도록 유연하게 설계가 되어야 하기 때문이다. 본 논문에서는 해외 3GPP, NGMN, 5G Americas 분석한 5G 보안 요구사항을 살펴보고, 5G 네트워크의 구성요소별 보안 요구사항을 고찰하고자 한다.

Ⅰ. 서 론

5G 네트워크의 진일보한 기술적 진화는 반면 사이버 보안관점에서 잠재적 보안위협과 새로운 도전과제를 준다. [그림 1]는 5G 모바일 네트워크를 중심으로 연결되는 각 구간별 대표적 보안위협을 요약하여 도식화 하였다[1]. 일반적으로 모바일 트래픽 경로는 사용자 단말 UE: User Equipment)부터 무선 액세스 네트워크(RAN : Radio Access Network, 기지국)와 코어 네트워크(이동성 관리, 인증, 과금 등을 위한 모바일 네트워킹 기능)를 거쳐 IP 서비스망(인터넷 서비스 사업자, 국가 간 로밍 연동 등)의 응용 서버와 연결된다. 이때 5G 네트워



〔그림 1〕 5G 네트워크와 5G+ 융합서비스 연결에 따른 구간별 보안 위협 개요

* 상명대학교 정보보안공학과(교수, rinyfeel@smu.ac.kr)

크에 기존 Legacy 이동통신망(2G·3G·4G)과 인터넷 서비스망(SNS, 클라우드 서버 등)과의 연결뿐만 아니라 타 수직 산업 군(제조, 의료 등)의 네트워크 및 IoT 기기들이 연결되어 5G 네트워크를 중심으로 복잡한 네트워크 구조를 만들게 될 것이다. 이러한 망의 복잡성은 서로 다른 보안요구사항과 보안 기술 수준이 상이함으로써 취약한 연결 고리가 발생 시 5G 네트워크 및 서비스의 보안성을 저하시킬 수 있다는 점이 가장 큰 도전과제가 될 수 있다. 다음 [표 1]는 5G 기술특성과 관련하여 7개 보안 도전과제(Security Challenges)를 용약 정리하였다[1,4].

(표 1) 5G 기술적 특성 대비 7가지 보안 과제

단계	5G 네트워크 장점	보안도전과제
사용자 장치	IoT 장치 수용	보안 취약한 IoT 장치
무선 RAN	이기종 무선 접속,과 커버리지 확대	무선 RAN 장애, 초소형 스몰셀 보안관리
분산 코어 네트워크	분산화로 모바일 트래피 부하 분산	보호대상 증가/분산과 보안 가시성, Legacy 네트워크·장비와 연동
가상화 및 슬라이싱	물리적 자원의 효율성, 확장성, 가용성	공유 자원 부하와 접근제어 등
MEC 도입	수직산업의 초저지연 서비스의 실시간 제공	3rd APP 신뢰성 및 내부통신망 연결경로
서비스기반 아키텍처	인터넷프로토콜 확대 및 API 개방성	알려진 웹 취약성 상속, 오픈 API 신뢰성
5G 사설망	5G 공중망 공유 및 임대하여 사설 5G 망과 응용서비스 구축	5G 통신사업자와 5G 사설망 구축기관과 보안역할과 책임 이슈

Ⅱ. 해외 5G 보안위협, 표준화 및 권고사항

2.1. ENISA 5G 보안 공통위협

유럽 ENISA는 5G 기술의 보안위협 연구가 활발하게 진행중이며 다음 [표 2]는 ENISA의 5G 네트워크 및 서비스에서 발생 가능한 10대 공통 보안위협이다[2].

(표 2) ENISA 5G 공통 보안위협

위협	주요내용
서비스 거부 공격 (DoS)	·DDoS 공격은 5G 네트워크 서비스를 일시적 또는 무한정 방해하거나 방해함으로써 네트워크 자원을 의도한 사용자가 이용할 수 없게 만들기 위한 공격 ·DDoS 공격은 과도한 이상 트래픽으로 인한 피해이며, 대표적으로 플러딩(flooding), 증폭(Reflection), 시그널링 스톰(signaling storm), 포화 공격으로 5G 기지국, 네트워크 장비 및 서비스 장애를 초래함
데이터 침해, 누출, 도난 및 정보 조작	·이동통신 시스템 및 네트워크에 대한 무단 액세스, 개인 식별 가능 정보/biometric/의료(개인정보 침해), 회사 기밀 정보(지적 재산, 상업 및 재무 데이터) 또는 정부 관리를 통한 개인 정보 도난 위협임 ·예를 들어 국가 관련 정보(상호 정보). 사용자 자격 증명, 암호화 키, 네트워크 보안 로그, 소프트웨어 구성 등과 같은 다른 유형의 데이터를 도난, 침해 또는 유출 등을 포함함
도청	·도청은 다양한 5G 망 구성요소(SDN 컨트롤러, 네트워크 기능, 에지 노드, 가상화 오케스트레이션), 애플리케이션 및 통신 계층 통과하는 트래픽 정보를 수집하고 변조하려고 하는 위협임 ·가입자(subscriber) 데이터 도청, 기밀 정보, 시스템 시간, 위치, 전자 메시지, 네트워크를 통해 중계되는 데이터의 신호 등을 포함 ·공격자는 사용자 위치를 추적하거나 중요한 정보에 액세스하기 위해 국가 시민 및/또는 조직을 감시하고, 스파이를 감시하거나 도청
SW 및 HW 취약성 공격	·SW 및 HW 취약성 공격은 악의적인 행위자가 장비 제조사 및 운영자에게 알려지지 않거나 패치되지 않은 소프트웨어 또는 하드웨어 결함을 이용한 위협 ·예를 들어 멜트다운, 스펙트라 및 버퍼 오버플로와 같은 하드웨어 및 소프트웨어 결함의 공격을 말함 ·SS7, Diameter와 같은 이전 세대의 이동통신 및 이전 신호 프로토콜과 관련된 알려진 다른 취약성의 이용도 포함
악성 코드	·악성코드 위협은 악성 소프트웨어 설치 및 배포 또는 제품 또는 업데이트 내부에 특정 코드 또는 소프트웨어를 삽입하는 위협임 ·예로는 악성 소프트웨어, 랜섬웨어, 바이러스, 웜, 트로이 목마, SQL 인젝션, 가짜 보안 소프트웨어, 가짜 소프트웨어 등이 있음 ·5G 악성코드 감염되는 예시로 악성 API를 노출하기 위해 코어 네트워크에 강제적으로 악성코드를 설치하고 등록할 수 있는 허가되지 않은 VNF의 사용할 때 발생 가능함

위협	주요내용
공급망 위협	・공급망 위협은 통신장비 및 어플리케이션 벤더가 은폐된 하드웨어, 악성 소프트웨어 및 소프트웨어 결함의 제품에 의도적으로 삽입하거나 통제되지 않은 소프트웨어 업데이트의 이행, 기능 조작, 백도어, 생산 버전에 남아 있는 미등록 시험 기능 등을 우회기능임 ・제품 시험, 유지보수, 구성 및 운용 중에 신뢰할 수 없는 제3자 직원이 수행한 활동과도 관련이 있으며, 유지보수 활동을 수행하고 기술 지원을 제공하기 위해 (로컬 인터페이스와 원격 인터페이스를 통해) 네트워크 관리 시설에 접근할 수 있음 ・네트워크의 운영 및 관리에 대한 이러한 접근은 신뢰할 수 없는 제3자의 직원이 가입자정보, 시스템 및 네트워크 구성, 원격 측정 데이터와 같은 다양한 유형의 데이터에 접근함으로 써 발생 가능
지능형 타겟 공격 (APT)	・지능형 지속성 위협(APT)은 민감한 정보(예: 국가 기밀, 산업 기밀 또는 지적 재산)를 대상으로 하거나 민감하고 중요한 서비스의 기밀성과 가용성 침해를 목적으로 함
보안 관리 및 운영 절차 결함	・네트워크의 운영과 보안 관리, 소프트웨어의 구성, 업데이트 및 패치 관리의 결함뿐만 아니라 운영 및 보안 절차의 부족 또는 부실한 설계로 인한 오류는 네트워크의 무결성과 가용성에 영향을 줌
인증 남용	・인증 남용은 사용자 장비(모바일 기기 및 IoT), 운영 및 관리 인터페이스, 로밍 및 vertical 서비스 등 복수의 네트워크 진입점에 영향을 줌 ・공격자가 5G 인증 시스템을 악용하기 위해 사용하는 기법으로 사용자 자격 증명 도용, 사용자 계정의 brute force(무차별 대입), 암호 크래킹, 사용자 ID 마스킹, IoT 그룹 인증의 손상 등이 해당
ID 도용 또는 스푸핑	・악의적인 행위자가 합법적인 ID를 도용하여 공격을 개시하기 위해 위장할 때 실현될 수 있다. ・ID 도용 또는 스푸핑은 SW 구성요소나 휴먼 에이전트에 영향을 미칠 수 있는 위협 ・공격자는 합법적인 컨트롤러의 ID를 스푸핑하고 합법적인 컨트롤러에 의해 제어되는 네트워크 기능(즉, 데이터 평면(data plane)의 요소)과 상호 작용하여 몇 가지 다른 유형의 공격(즉, 네트워크 흐름, 트래픽 우회 등)을 확장 가능함 ・소셜 엔지니어링, 사용자 계정/암호를 무차별 대입하여 크래킹 공격은 사용자 자격 증명을 스푸핑하거나 도용하는 기법으로도 사용됨

2.2. 3GPP 5G 보안 표준화 동향

5G 통신장비를 위한 기술표준은 3GPP SA3 워킹그룹 담당하고 있으며, 보안표준문서는 TS33.xxx 시리즈 이름으로 명명하여 다양한 5G 보안 표준을 다루고 있다[3]. 대표적으로 5G 보안의 TS33.501에서 5G 시스템의 보안구조와 절차를 다루고 있는 5G 보안 아키텍처와 요구사항 기본 문서이다. TS33.511-522 시리즈 표준은 5G SCAS(SeCurity Assurance Specification)로 5G 통신장비들의 보안 기능 요구사항(명세서) 정의하고 있다. 또한, TS 33. 535, 536은 5G 시스템의 인증 및 키관리(AKMA)와 5G기반 V2 서비스를 위한 보안 요구사항 관련된 표준이 개발되어 있다.

(표 3) 3GPP 5G 보안 표준 문서 시리즈

문서번호	주요내용
TS 33.501	5G 시스템을 위한 보안 구조와 절차
TS 33.511	5G SCAS(보안 보증 명세); 5G 기지국(gNb)
TS 33.512	5G SCAS(보안 보증 명세); 접근과 이동관리 기능(AMF)
TS 33.513	5G SCAS(보안 보증 명세); 사용자평면기능(UPF)
TS 33.514	5G SCAS(보안 보증 명세); 통합 데이터 관리
TS 33.515	5G SCAS(보안 보증 명세); 세션 관리 기능(SMF)
TS 33.516	5G SCAS(보안 보증 명세); 인증 서버 기능(AUSF)
TS 33.517	5G SCAS(보안 보증 명세); Security Edge Protection Proxy (SEPP) 기능
TS 33.518	5G SCAS(보안 보증 명세); 5G 통신 네트워크 기능(NF)의 관리를 위한(NRF) 기능
TS 33.519	5G SCAS(보안 보증 명세); 5G 통신 네트워크 기능의 외부 연동을 위한 NEF 기능
TS 33.520	5G SCAS(보안 보증 명세); Non-3GPP InterWorking Function (N3IWF) 기능
TS 33.521	5G SCAS(보안 보증 명세); Network Data Analytics Function (NWDAF) 기능
TS 33.522	5G SCAS(보안 보증 명세); Service Communication Proxy (SECOP) 기능
TS 33.535	3GPP 5G 시스템의 인증 및 키관리(AKMA) 기능
TS 33.536	V2X 서비스를 위한 3GPP 보안 요구사항

2.3. 유럽 NGMN 5G 보안 권고사항

유럽 차세대 모바일 네트워크(NGMN)에서는 현재 네트워크 아키텍처, 그리고 구현되지 않았거나 사용할 수 없어서 현재 부족한 보안 수단을 기반으로 5G에 대해 권고하며, 특히 주의할 사항에 중점을 두고 있다. 여기에는 5G가 초창기여서 존재하는 수많은 불확실성, 정의된 설계 개념의 부재, 알려지지 않은 엔드-투-엔드(E2E) 및 서브시스템 아키텍처 등이 포함된다. 이 권고는 액세스 네트워크의 제한사항과 네트워크 인프라에 대한 사이버 공격에 초점을 두고 있다. 다음은 권고사항 중 핵심적인 내용이다[5].

2.3.1. 비정상 네트워크 트래픽 대응

5G에서는 최종 사용자 장치 수가 폭발적으로 증가할 것으로 알려져 있다. 따라서 실수로, 또는 악의적으로 대규모 이벤트가 발생하는 경우 네트워크 트래픽 패턴이 크게 변경될 수 있다. 따라서 5G 시스템은 트래픽 사용이 크게 변동하는 것을 최소화해야 하며, 그러한 트래픽 급증이 발생할 때마다 복원력을 제공하고 허용될 만한 성능 수준을 유지해야 한다.

2.3.2. 무선 인터페이스 키 보안

4G를 비롯한 이전 세대에서는 무선 인터페이스 암호화 키가 홈 네트워크에서 생성되어 비보안 링크를 통해 방문 네트워크에 전송됨으로써 키가 공개되는 지점이 있었다. 비보안 링크를 통해 키를 전송하지 않거나(예: SS7/다이어미터), 키를 적절하게 보호할 것을 권장한다.

2.3.3. 사용자 플레인(User Plane) 무결성

3G와 4G는 일부 신호 메시지에 대한 보호는 제공하지만, 사용자 데이터 플레인을 위한 암호화 무결성 보호를 제공하지는 않음. 모바일 네트워크 범위를 지나서 종료되는 전송 또는 애플리케이션 계층에서 보호를 제공할 것을 권장 한다. 리소스가 제한된 사물 인터넷이나, 대기 시간에 민감한 5G 장치 및 서비스에 대한 네트워크 수준 보안은 예외일 수 있으며. 애플리케이션 수준에서 E2E 보안을 제공하는 경우 패킷 헤더와 핸드셰이크에서 데이터 전송 시 오버헤드 시간이 너무 오래 걸릴 수 있다.

2.3.4. 네트워크의 보안 위임

보안 수단 사용을 최적화하기 위해 일부 서비스 중심의 제약조건이 보안 아키텍처에 적용된다. 하지만 이러한 제약조건은 시스템 수준의 보안 가정을 손상 시키며, 완전히 제거할 수 없다. 다른 사업자의 수단이 부적절한 경우 특정 사업자에게 손해를 입히는 다중 사업자 시나리오에서는 이러한 문제가 증폭됩니다. 따라서 적절한 조사를 통해 가장 중요한 보안 문제를 파악한 후에, 모두는 아니더라도 어느 정도 5G에 위임할 것을 강력하게 권장한다.

2.3.5. 가입자 수준 보안 정책의 일관성

특정 사업자 네트워크에서 다른 사업자 네트워크로 로밍하는 경우 사용자 보안 매개 변수가 변경되지 않아야 한다. 매우 자주 이동하는 사용자의 경우 로밍 시 여러 위치 또는 여러 네트워크 간에 이동하기 때문에 모든 보안 서비스가 자주, 사용자당 기준으로 자주 업데이트되지 않을 가능성이 매우 높다. 사용자가 특정 사업자에서 다른 사업자로 이동하고 대기 시간에 민감한 서비스를 사용하는 경우 모바일 에지 컴퓨팅(MEC)과 같은 방문 사업자 네트워크의 에지를 통해 서비스가 제공될 수 있다. 이때 보안, 또는 사용 중인 서비스의 보안은 새로운 위치에서 자동으로 제공되거나 구성되여 되기 때문에 로밍 시 사용자 트래픽을 보호하려면 훨씬 더 빠른 속도로 네트워크 사업자 간에 보안 정책을 공유해야 한다. 이 권고에는 사용자가 이동할 때마다 어디서나 보안 정책과 서비스가 그대로 유지되도록 사용자별 슬라이스 구성을 사용할 수 있는 상황에서 가상화 기법을 사용할 수 있는 가능성에 대한 논의가 포함되어 있다.

2.3.6. 인프라에서의 DoS 공격 대응

DoS와 분산형 DoS(DDoS) 공격은 에너지, 의료, 교통, 통신과 같은 중요 인프라를 제어하는 장치의 작업을 우회함으로써 인명을 위협하는 결과를 초래하고 사람과 재산에 손해를 끼칠 수 있다. DoS 공격은 목표로 삼은

장치의 물리적, 논리적 자원을 고갈시키도록 설계되어 있다. 압도적인 수의 기계가 여러 위치에 지리적으로 분산된 상태에서 공격할 가능성 때문에 문제는 더욱 심각하다. 네트워크는 작동 기능과 제한사항이 서로 다른 커넥티드 장치(예: 사물 인터넷)가 급증함에 따라서 증가하는 연결을 처리할 수 있어야 한다. 모든 것에 대한 이상 징후 모니터링을 수행하는 새로운 접근이 필요하다.

Ⅲ. 5G 네트워크의 보안 요구사항 동향

3장에서는 5G 보안을 위한 구성요소별로 보안 요구사항을 분석하기 위해 5G Americas의 보안요구사항을 분석하여 핵심적인 내용만을 요약 정리하였다.

3.1. 클라우드 기반 시스템 보안 요구사항

5G 네트워크는 기존 HW 장비로 구성된 네트워크 구축에서 SW 중심으로 구축될 수 있도록 SDN/NFV (Software Defined Networking / Network Function Virtualization)과 클라우드 컴퓨팅 기술을 적용한 cloud native 5G 코어 구조를 적용하고 있다.

3.1.1. 클라우드 기반 MEC 보안 요구사항

5G 코어에서 클라우드 컴퓨팅 기술은 MEC, RAN 장비 등에 적용될 수 있으며 클라우드기반 MEC 시스템의 기본적인 보안 기능을 다음과 같이 제공하고 있다.

(1) 이상행위 탐지 : 각 컨테이너는 전용 기능을 수행하여, 동작 프로파일링 및 이상 탐지를 강화
(2) 컨테이너 격리 기능 : 컨테이너 간 맬웨어 및 바이러스의 확산을 방지
(3) 보안 업데이트/패치 : 분리된 소프트웨어는 효율적인 소프트웨어 버전 업데이트 및 보안 패치를 제공
(4) 리소스 격리 : 네트워크 슬라이싱을 사용한 세그멘테이션은 트래픽을 분리하고 컴퓨팅 리소스를 격리

3.1.2. 오픈소스 및 API 보안 요구사항

클라우드 시스템은 오픈소스 및 API 사용과 의존도가 심화될 것을 전망된다. 오픈소스 사용이 장점은 개발 비용 및 소요시간에 많은 장점을 가지고 있으나, 어플리케이션 보안에서 제3자 개발한 오픈소스 보안 취약점을 내재하는 위험성을 내포하고 있다. 클라우드 시스템의 오픈소스 및 API 보안 요구사항은 다음과 같다.

(1) 5G MEC 탑재된 애플리케이션 개발자는 보안 내재화(Security by Design)를 이행
(2) 클라우드-기반 시스템은 제어 평면에서 보안 인증 및 인가를 통해 제로 트러스트를 구현
(3) 3GPP TS 33.501 표준에서 정의된 것과 같이 IPSec 및 DTLS는 제어 평면 및 데이터 평면 보호에 사용
(4) 경계 보호는 DDoS 보호, 동작 프로파일링 및 이상 탐지 기능 사용
(5) 오픈-소스 소프트웨어 설치 또는 실행 중일 때 소프트웨어 구성 및 버전의 변조 방지 기록을 유지
(6) 오픈-소스 요소에 공개적으로 알려진 취약성이 포함되지 않았는지 확인하고, 다른 공개 리소스에 설명된 취약성과 함께 보고해야 함
(7) 악성 공격의 실시간 탐지 및 완화에 활용하기 위한 위협 인텔리전스 기능 사용
(8) 정적 분석 수행(정적 분석 도구를 사용해서 오픈-소스 요소에 보고되지 않은 보안 취약성이 포함되어 있지 않은지 확인

3.2. 가상화 네트워크 인프라 보안 요구사항

3.2.1. NFV 인프라 보안 요구사항

5G 네트워크 구성하는 통신 시스템들은 전용 하드웨어를 활용하였으나, 5G 코어 네트워크는 ETSI의 NFV 아키텍처를 이용하여 가상화 인프라를 구축하여 통신사업자에게 5G 코어 네트워크를 확장 가능하고 탄력적으로 운영할 수 있도록 하였다. 가상화 인프라에 대한 보안 고려사항은 가상화 계층과 하위 지원 계층에 있다. 가상화 인프라 (가상 컴퓨팅, 네트워킹 및 스토리지 리소스를 유지하는 NFVI)와 하이퍼바이저, 호스트 운영

체제 및 컨테이너 런타임 시스템과 같은 컴퓨팅 노드의 소프트웨어가 포함된다. 상기 요소의 관리 및 제어에는 네트워크 기능을 수행하는 VNF 및 CNF의 전체 수명 주기 관리를 지원하는 가상 인프라 관리자(오픈스택 등) 및 컨테이너 오케스트레이션 엔진이 포함된다. 가상화 인프라 보안 요구사항은 다음과 같다.

(1) 가상화 인프라 원격 접속 보안

운용자는 인터넷에서 접속할 수 없는 관리 네트워크를 사용하여 관리 인터페이스를 원격 접속으로부터 보호해야 한다. 만약 운용자에게 원격 접속을 허용하는 경우, 운용자는 모든 유형의 VPN 접속에 대해 다중 인증(MFA)을 사용하는지 확인해야 한다. Zero-Trust와 결합된 MFA VPN은 5GC 네트워크를 보호하기 위해 보안 원격 접속을 크게 향상시킬 수 있다.

(2) NFV 리소스 격리

NFV 인프라는 다중 테넌트 및 서비스들 간에 리소스를 공유하기 때문에 테넌트 소프트웨어 워크로드 간의 격리와 테넌트 및 서비스 수준 모두에서 트래픽 분리가 필요하다. 이때 인프라에서 소프트웨어 워크로드 인스턴스 배치에 대한 규칙은 필요한 격리 수준을 다르게 해야 한다.

(3) 네트워크 슬라이싱 보안

가상화된 네트워크를 통해 라우팅되는 네트워크 슬라이싱 트래픽은 기존 물리적 네트워크에 적용된 물리적 방화벽과 같은 기존 보안 기술로 대응하기가 어렵다. 따라서, 가상 방화벽 또는 가상 IDS/IPS와 같은 가상 보안 어플라이언스가 필요하다.

(4) NFV 플랫폼 보안

운용자는 NFV 플랫폼에 대한 DoS 공격, 알려진 NFV 플랫폼의 보안 취약성 공격을 효과적으로 모니터링해야 한다. 방화벽, ACL, IP 테이블, 레이트 리미팅, 모든 불필요한 포트 닫기, 모든 불필요한 서비스 비활성화, 강력한 기밀 무결성 알고리즘 사용 등, NFV 플랫폼을 보호하기 위해 모든 보안 계층 (심층 방어)을 사용해야 한다.

(5) NFV 보안 모니터링

가상 인프라를 기반으로 하는 NFV 기술은 가상화된 모니터링 기능에 대한 다양한 보안 인터페이스 특성과 요건을 갖는다. 기존의 모니터링 기술은 물리적 노드, 액티브/패시브 하드웨어 프로브, 심층 패킷 검사, 제어 평면 및 관리 평면 정보와의 상관관계에 대한 표준화된 모니터링 인터페이스를 사용한다. 그러나, 전반적인 가시성이 훨씬 낮아 NFV 환경에서는 부족하다. NFV 보안 모니터링은 공유 메모리 및 가상 소켓 내의 모니터링 인터페이스 숨기기, 단일 VNF 내의 숨겨진 데이터 흐름, 동일한 물리적 호스트의 VNF들 사이, 가상 스위치 및 라우터 내의 흐름이 포함된다.

3.2.2. SDN 보안 요구사항

SDN 기술은 중앙집중형 논리적 구조를 가진다. 따라서, SDN 보안은 SDN 제어 프로토콜과 API 보안요구사항으로 구분한다.

(1) SDN 제어 프로토콜 보안

SDN 아키텍처의 각 영역들 간의 통신은 다양한 가상 인터페이스를 사용해서 API 및 SDN 제어 프로토콜을 통해 이루어진다. 이들 인터페이스는 내부 또는 외부일 수 있으며, 통신이 스푸핑, 중단 또는 서비스를 거부하는 데 사용될 수 있으므로 새로운 공격 접점이 될 수 있다. 따라서, 모든 통신 인터페이스에 적절한 수준의 인증 및 인가를 적용하는 것이 중요하다. 또한, 패킷 자체는 무결성, 기밀성 및 레이트 제어를 보장해야 한다.

(2) API 보안

API 보안에는 a) 전송 중인 데이터 보안(제어 평면, 사용자 평면 및 서비스들 간에 이동 중인 데이터 보안) 및 b) DoS 공격에 대한 접속 제어 및 보안이 포함될 수 있다. 예를 들어, 5G 네트워크 요소는 일부 유형의 암호화 알고리즘에서 생성한 값인 공유 키를 활용할 수 있다. 이 키들은 중앙 보안 시스템에 유지될 수 있다. 통신 프로세스 중에, 중앙 시스템은 그 레코드의 공유 키가 통신을 인증하는지 여부를 확인한다. 또한, API의 정책 집행(ratelimit, 폐기, 허용)은 인증된 5G 네트워크 요소들만 통신을 교환할 수 있도록 한다.

3.3. 유연한 보안 관리 요구사항

5G가 클라우드 및 소프트웨어 제어 평면을 활용하기 때문에, 서비스 운영은 동적으로 변화하는 네트워크 환경에 대응하는 방법을 지시하는 원격 측정, 임계값, 트리거 및 프로세스 워크플로의 각 단계를 완전히 이해해야 한다. 모든 프로세스는 완전히 기록되어 각 단계가 올바르게 작동하는 소프트웨어 코드로 전환될 수 있어야 한다. 모든 루틴과 API에는 강력한 인증이 필요하다. 각 라우팅 및 API에 대해 별도의 역할 및 권한이 필요하다. 손상된 소프트웨어 중심 작업에서 내부 확산은 치명적일 수 있으므로, 시스템 또는 개인 수준에서 권한을 부여하는 것만으로는 충분하지 않다. 루틴 및 코드 레벨에 대한 통제는 필수이다. 소프트웨어 인프라 보안 관리 및 관제를 위해 자동화 기능, 보안 오케스트레이션, AI/ML 적용한 분석이 필요하다.

(1) 자동화 기능

자동화는 운영자의 역량에 의해 운영되는 프로세스를 머신에 의해 자동화하는 프로세스로 변경하는 것이다. 5G 네트워크에서 자동화 시스템 올바르게 구현하기 위해서는 신뢰할 수 있는

(2) 보안 오케스트레이션 기능

오케스트레이션은 서로 다른 프로세스 간의 상호작용을 관리하는 개념이다. 5G에서, RAN 및 5GC 네트워크는 모두 SDN, NFV 및 클라우드-기반 인프라를 기반으로 한다. 특정 네트워크 내에서, 오케스트레이션은 네트워크 슬라이싱 생성 및 관리 등 다양한 5G 리소스 사용을 조정하는데 도움이 된다. 오케스트레이션은 프로세스들 간에 보안 통신을 해야 하며, 적절하게 작동하도록 리소스를 제어할 수 있는 올바른 권한이 있어야 한다.

3.4. 에지 데이터 보안

(1) 데이터 자산 식별

MEC 구축 및 서비스 운영 중에는 사용자 식별 및 액세스 위치를 포함하되 이에 국한되지 않는 관련 사용자 데이터 자산을 파악 등 데이터 자산 식별이 필요하다.

(2) 데이터 위변조 및 유출 방지

IPSec, TLS 등 전송되어 데이터 유출과 변조 방지 기술적 조치가 필요하다.

(3) 안전한 데이터 활용

데이터 처리, 분석 및 사용은 데이터 운영 객체 인증 및 인가와 결합하여 개인정보보호법 및 규정을 준수해야 한다.

(4) 개인정보 및 민감 데이터 비식별 조치

개인정보 데이터 프라이버시가 관련되면 개인 데이터를 마스킹 등 비식별 조치가 수행되어야 한다.

(5) 저장 데이터 보호

서비스 유형과 데이터 등급에 따라 보안 요건이 높은 데이터(개인정보, 민감정보)는 국제표준 암호 알고리즘을 통해 데이터 암호화를 수행해야 한다.

Ⅳ. 결 론

지금까지 3GPP 보안표준 NGMN 5G 보안 권고사항, 미국 5G Americas 보안요구사항 등 해외 5G 보안 연구를 살펴보았다. 5G 네트워크와 서비스 기술이 초고속, 초연결, 초시뢰의 다양한 성능 요구사항을 만족하기 위해 최신 IT 기술을 적용하여 속도, 효율성, 확장성 등의 장점과 큰 기술적 변화를 가져오게 되었다. 따라서, 5G 보안 시스템도 5G의 설계 및 아키텍처 관련 요구사항에 맞게 설계가 요구된다.

첫 번째는 5G 보안은 이전 세대와 달리 더 높은 보안 수준을 유지되어야 한다. 5G 네트워크와 서비스는 복잡한 네트워크 연결구조(5G 공중망, 사설망)와 다양한 도메인을 걸쳐 서비스가 동작(예, 네트워크 슬라이싱)되고역할과 책임이 불불명한 생태계(이동통신사업자, 클라우드 플랫폼 제공자, 응용서비스 사업자, 운용자/소유자/테넌트 등)가 더욱 복잡해질 것으로 예상되므로 5G 시스템과 구성요소 간 강력한 상호인증과 권한 부여, 역할과 책임이 명확하게 구분되어 제공되어야 한다.

두 번째는 5G는 매우 유연하고 민첩한 특성을 가지는 가상 네트워크 기능(VNF) 및 소프트웨어 기반 네트워크 제어기술을 적용함에 따라 이에 따라 보안 기능도

유연한 보안 매카니즘이 제공되어야 한다.

세 번째는 보안 시스템은 환경, 위협 또는 보안 제어에 따라 지능적으로 시스템을 자체 조정 및 적용할 수 있게 보안 자동화가 가능해야 하며 보안 오케스트레이션과 관리가 요구된다.

참 고 문 헌

[1] 김환국, 최보민, 고은혜, 박성민 “5G 네트워크 기술 진화에 따른 새로운 보안도전과제와 해외 5G 보안 아키텍처 연구도향”, 한국정보보학회, 정보보호학회지, 29(5), 2019.10.

[2] M. Lourenco, “ENISA Threat Landscape for 5G networks”, ENISA white paper, Nov. 2019.

[3] 3GPP, SA3 WG Security homepage, [online] https://3gpp.org

[4] Ahmad, Ijaz, et al. "Security for 5G and beyond." IEEE Communications Surveys & Tutorials, pp 3682-3722, 21(4), 2019

[5] Alliance, NGMN, “NGMN 5G white paper,” Next Generation Mobile Networks, White paper, 2015.

[6] 5G Americas, “Security Considerations for 5G”, July 2020 [online]

〈저 자 소 개〉

김 환 국 (Kim Hwan Kuk)

종신회원

2017년 2월 : 고려대학교 정보보호학과 공학박사

2020년~현재 : 상명대학교 정보보안공학과 조교수

2007년~2020년 : 한국인터넷진흥원 지능형사이버방어R&D 팀장

2002년~2006년 : 한국전자통신연구원 정보보호본부 연구원

2017년~현재 : TTA 표준화위원회 TC5 사이버보안PG 의장

2020년~현재 : 과학기술정보통신부 5G 보안협의회 기술분과 위원

<관심분야> 5G 보안, IoT SW 취약점 분석, AI 보안 등