5G 환경에서의 MEC 보안위협 및 대응 기술

Security Threat and Response Technology for Multi-access Edge Computing in 5G Environments

저자
(Authors)

김영수, 박종근, 이종훈, 장종수, 문대성, 김익균
Youngsoo Kim, Jong Geun Park, Jong-Hoon Lee, Jongsoo Jang, Dae Sung Moon, Ik Kyun Kim

출처
(Source)

정보과학회지 38(9), 2020.9, 16-24 (9 pages)
Communications of the Korean Institute of Information Scientists and Engineers 38(9), 2020.9, 16-24 (9 pages)

발행처
(Publisher)

한국정보과학회
The Korean Institute of Information Scientists and Engineers

URL

http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09910482

APA Style

김영수, 박종근, 이종훈, 장종수, 문대성, 김익균 (2020). 5G 환경에서의 MEC 보안위협 및 대응 기술. 정보과학회지, 38(9), 16-24.

특집원고

5G 환경에서의 MEC 보안위협 및 대응 기술

한국전자통신연구원 ▌김영수·박종근·이종훈·장종수·문대성·김익균

1. 서 론

2019년 4월 세계 최초로 상용화에 성공한 5G 서비스는 향후 4차 산업혁명 시대를 위한 필수적인 통신 인프라 기술로, 이전 4G LTE에 비해 다양한 서비스와 많은 분야의 변화를 가져올 것으로 전망되고 있다. 시장 선점을 위해 노력 중인 국내외 이동통신사업자들은 현재 포화상태인 B2C(Business to Consumer) 시장 공략과는 별도로 새롭게 부각되고 있는 B2B(Business to Business) 시장에 주목해 왔으며 관련 기술 발전 등을 통한 다양한 형태의 서비스 모델 발굴을 위해 무한 경쟁을 벌이고 있다 [1, 2]. 5G B2B 서비스는 초연결(mMTC[1])·초저지연(uRLLC[2])·초고속(eMBB[3])을 지향하는 5G 네트워크의 특성을 기반으로 일반 이용자(B2C)가 아닌, 제조업, 에너지, 공공안전, 헬스케어 분야 등의 기업이나 기관(B2B) 고객을 대상으로 한 서비스로, 수많은 디바이스 및 서비스 요구에 대하여 탄력적이고 안정적인 서비스를 제공하는 것이 핵심이다. 이러한 B2B 서비스를 실현하는 핵심 인프라 중 하나로서 주목해야 할 것이 바로 MEC(Multi-access Edge Computing) 기술이다 [3, 4].

MEC는 데이터의 처리와 저장 등의 컴퓨팅 서비스를 원격의 중앙 클라우드가 아닌 사용자와 가까운 네트워크 엣지에서 제공하는 기술로, 일반적으로 클라우드 RAN(Radio Access Network)이 위치한 셀 사이트, 지역 또는 광역국사, 서비스 핫스팟 지역 및 고객 사내망 내부 등에 위치할 수 있다. MEC의 대표적 특징으로는 네트워크 지연 시간을 단축하고 백홀(backhaul)의 대역폭을 감소시키는 근접성(proximity), 특정 지역 또는 기업별 MEC 플랫폼 구축을 통해 지역 맞춤형 특화 서비스를 제공하는 위치 기반 서비스(location aware services), 기지국에서 수집 가능한 RAN 상황 정보를 활용하여 실시간 송출 스트림의 품질 조절 및 컨텐츠 캐싱(caching) 등이 가능하도록 하는 맞춤형 고품질 서비스(customized QoE[4]) 등을 꼽을 수 있다.

MEC 시스템은 클라우드 및 가상화 기술을 바탕으로 제삼자(3rd Party) 애플리케이션 프로그램을 실행할 수 있는 개방형 시스템으로 상호 운영되기 때문에 보안 위협의 주요 대상이 될 수 있으며, 이에 대한 탐지 및 대응기술 개발이 요구되고 있다 [5]. 이에 본 고에서는 MEC 패러다임을 정립하고 발전시킨 ETSI[5]의 MEC 표준을 중심으로 해당 프레임워크 구조 등을 살펴보고 몇 가지 관점에서의 보안 위협에 대하여 고찰한다. 제2장에서는 MEC의 특징과 네트워크 레벨, 호스트 레벨, 그리고 시스템 레벨의 MEC 프레임워크를 소개하고 MEC 시스템 구조와 각 구성 컴포넌트들을 기술한다. 제3장에서는 MEC 보안의 개념 이해를 위해 MEC의 핵심인 가상화 기술을 소개하고 클라우드 보안 및 NFV(Network Function Virtualization) 보안과 대비하여 MEC 보안의 개념을 정의한다. 또한, 네트워크 관점, MEC 시스템 및 애플리케이션 관점, 그리고 가상화 관점 등으로 구분하여 MEC 보안 위협에 대하여 기술하고 이러한 MEC 보안 위협에 대응하기 위해 가용한 다양한 기술들을 제시하고 제4장에서 결론을 맺는다.

2. MEC(Multi-access Edge Computing)

2.1 MEC 특징

5G B2B 서비스의 핵심 기술로 손꼽히는 MEC는 데이터 처리와 저장 등의 컴퓨팅 서비스를 원격의 중앙

† 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00952, 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발)

1) Massive Machine Type Communication
2) Ultra Reliable Low Latency Communication
3) Enhanced Mobile Broadband
4) Quality of Experience
5) European Telecommunications Standards Institute

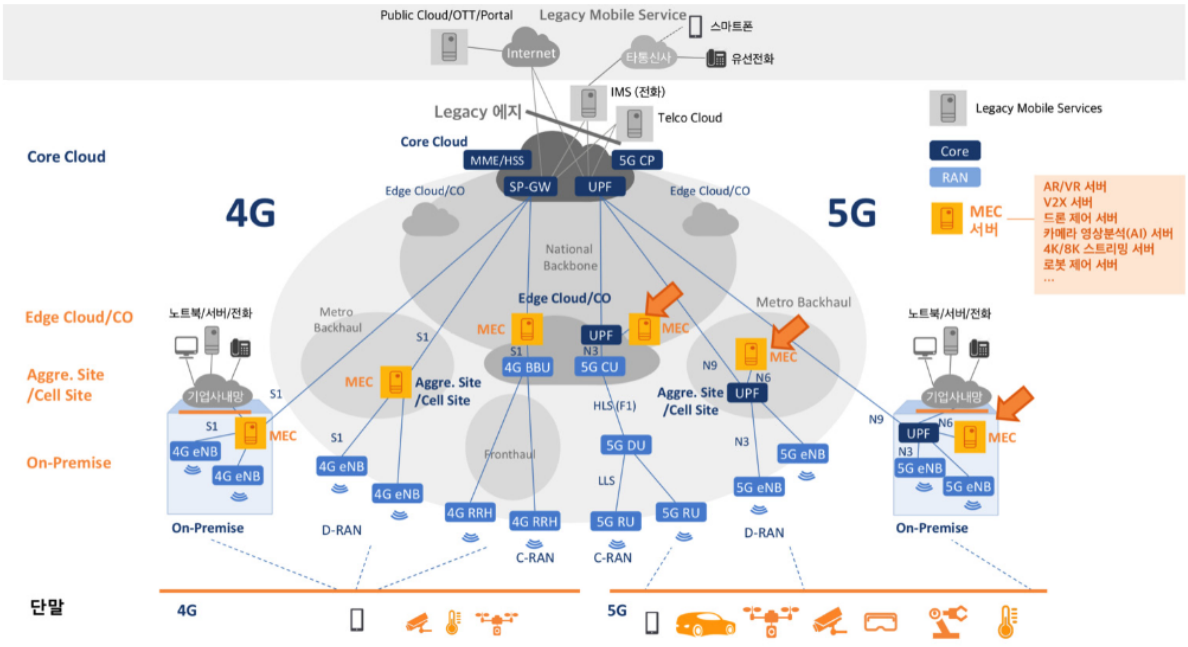

그림 1 이동통신 네트워크에서의 MEC의 위치 (출처: Netmanias[8])

클라우드가 아닌 사용자와 가까운 네트워크 엣지에서 제공하는 기술로, 그림 1과 같이 일반적으로 Cloud-RAN이 위치한 셀 사이트, 지역 또는 광역국사, 서비스 핫스팟 지역 및 고객 사내망 내부 등에 위치할 수 있다 [6, 7].

일반적인 클라우드의 경우, 중앙 집중화된 대규모 데이터센터의 우수한 컴퓨팅 파워로 인해 대용량 데이터 처리가 가능하지만, 시스템 및 데이터의 통합 관리에 대한 보안 문제가 발생할 수 있고 데이터센터의 위치에 따라 상대적으로 느린 응답 속도를 갖는다는 단점이 있다. 반면, MEC의 경우, 사용자와 근접한 엣지에 위치하므로 백홀 구간에서의 회선 증설 부담을 줄일 수 있다. 또한 빠른 응답 속도를 갖는 사용자 맞춤형 서비스를 제공할 수 있는 장점이 있다.

또한, 기지국에서 수집 가능한 무선 액세스 네트워크 상황 정보를 활용하여 실시간 송출 스트림의 품질을 조절하거나 컨텐츠를 캐싱하는 등 맞춤형 고품질 서비스를 제공할 수 있다. 5G 이동통신 환경에서 MEC를 통한 저지연·고속 서비스를 제공하기 위해서는 다음과 같은 기술적 이슈를 고려해야 한다 [9].

- 이동성(mobility): MEC 서비스에 대한 연속성 보장을 위해 사용자가 이동할 때 MEC 애플리케이션의 이동성, 즉, 새로운 MEC 서버 선택 및 애플리케이션 이동(migration)을 위한 핸드오버(handover) 처리가 필요함
- 자원제약(limited resources): 중앙 클라우드에 비해 상대적으로 제한된 자원에 대한 효율적 관리가 필요함
- 협업(collaboration): 사용자 핸드오버 및 애플리케이션 이동 등을 지원하기 위해 MEC 서버 간의 협업이 요구됨
- 정보보호(privacy and security): 사용자 및 다양한 IoT 단말의 정보가 저장되고 처리됨에 따라 정보 유출 및 사이버 공격에 대한 대응이 요구됨
- 이식성(portability): 핸드오버 등으로 인해 MEC 애플리케이션이 서로 다른 MEC 서버에서도 실행될 수 있어야 함

2.2 MEC 참조 구조

ETSI ISG[6] MEC는 2014년 새로 신설된 표준화 그룹으로 당초 LTE[7] 지원을 목적으로 만든 Mobile Edge Computing이었으나, 5G 환경에서 WiFi 등 다양한 액세스 네트워크를 함께 지원하는 Multi-access Edge Computing으로 명칭과 대상 영역을 확장하였다. MEC 표준화 그룹은 NFV[8] 표준을 참조하여 MEC 관련 표준 개발을 진행하고 있으며, 주요 표준으로는

6) Industry Specification Group
7) Long Term Evolution
8) 네트워크 기능 가상화(Network Functions Virtualization, NFV): 전용 하드웨어 기반 네트워크 장비의 하드웨어와 소프트웨어를 분리하여 네트워크 기능을 범용의 하드웨어 상에서 운용하는 기술

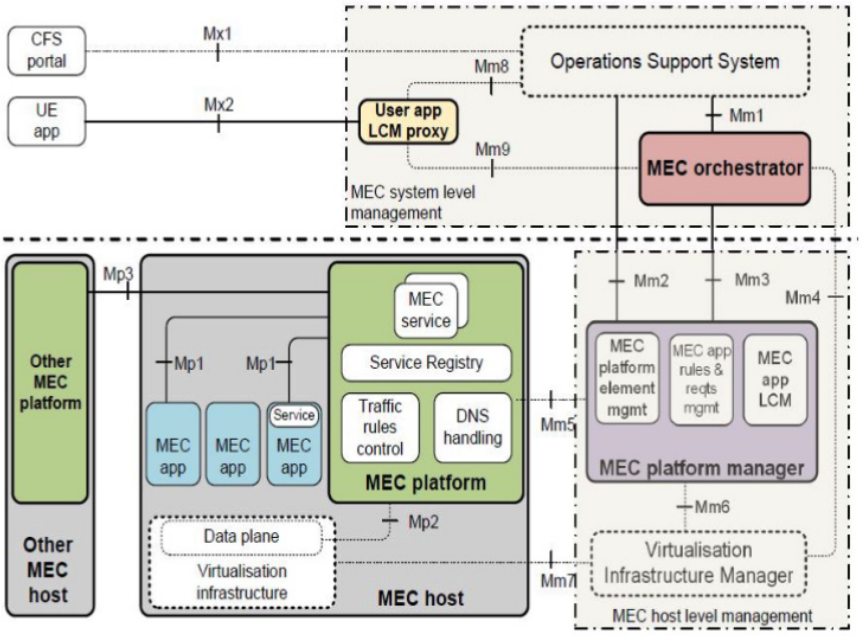

그림 2 MEC 표준 참조 구조 (출처: ETSI)

MEC 기술 요구사항(ETSI GS MEC002), MEC 프레임워크 및 참조 구조(ETSI GS MEC003), 그리고 MEC에 대한 PoC 프레임워크(ETSI GS MEC005) 등이 있다. ETSI의 MEC 표준 참조 구조는 그림 2와 같다 [10].

MEC 시스템은 크게 MEC 애플리케이션들을 실행하기 위한 MEC 호스트와 MEC 관리 및 오케스트레이터로 구성된다. MEC 호스트는 가상화 인프라에서 MEC 애플리케이션을 실행하고 서비스를 제공하는데 필요한 기능들로 구성된 MEC 플랫폼과 MEC 호스트의 가상화 인프라에서 인스턴스화되는 MEC 애플리케이션으로 구성된다. 특정 MEC 호스트 위에서 실행되는 애플리케이션을 관리하는 역할을 하는 MEC 관리는 MEC 오케스트레이터가 핵심 요소인 시스템 레벨 관리와 MEC 플랫폼 관리자와 가상화 인프라 관리자로 구성된 호스트 레벨 관리로 구분된다.

- **MEC 호스트(MEC Host):** MEC 플랫폼과 MEC 애플리케이션에 컴퓨팅, 스토리지, 네트워크 리소스를 제공하는 가상화 인프라로 구성된다. 가상화 인프라의 데이터 평면은 MEC 플랫폼이 설정한 트래픽 전달 규칙에 따라 MEC 호스트 내부 및 외부와의 트래픽 전송을 담당한다.
- **MEC 플랫폼(MEC Platform):** MEC 애플리케이션이 MEC 서비스를 찾아서 제공할 수 있도록 환경을 지원하고, MEC 플랫폼 관리자나 애플리케이션 또는 서비스로부터 트래픽 규칙을 받아 이를 데이터 평면에 전달한다. 또한, MEC 플랫폼 관리자로부터 DNS 정보를 수신하여 프록시/서버를 설정하고, MEC 서비스를 호스팅하며 스토리지와 시간 정보에 대한 접근 기능을 제공한다.
- **MEC 애플리케이션(MEC Application):** MEC 호스트가 제공하는 가상화 인프라 상에서 실행되며, MEC 서비스를 소비하고 제공하기 위해 MEC 플랫폼과 통신한다. 어떤 경우에는 MEC 플랫폼과의 상호 작용을 통해 가용성을 표시하거나 사용자 상태를 재배치하는 등 애플리케이션의 라이프사이클 지원 절차를 수행한다. 또한, 필요한 리소스, 최대 대기시간, 주요 서비스 등과 같은 일정한 규칙과 요구사항을 가질 수 있으며, 이러한 요구사항은 MEC 시스템 레벨 관리에 의해 검증되고 누락된 경우에는 기본값으로 할당될 수 있다.
- **MEC 오케스트레이터(MEC Orchestrator):** MEC 시스템 레벨 관리의 핵심 기능으로, 배포된 MEC 호스트, 사용 가능한 자원, 사용 가능한 MEC 서비스나 토폴로지 등을 기반으로 MEC 시스템의 전체 뷰를 유지한다. 패키지의 무결성과 신뢰성을 확인하고, 애플리케이션 규칙과 요구사항을 검증하며, 온보드(on-board) 패키지 기록을 보관하고, 애플리케이션을 처리하는 가상 인프라 관리자를 준비하는 등 애플리케이션 패키지를 온보

딩하는 기능을 담당한다. 또한, 대기시간, 사용 가능한 자원, 사용 가능한 서비스와 같은 조건에 기반하여 애플리케이션 인스턴스화를 위해 적합한 MEC 호스트를 선택하는 기능과 애플리케이션 인스턴스화, 재배치 및 종료 기능 등을 담당한다.

- **운영 지원 시스템(OSS, Operation Support System):** 사업자의 운영 지원 시스템을 의미하며, 이는 고객 대면 서비스(CFS, Customer Facing Service) 포털을 통해, 애플리케이션의 인스턴스화나 종료를 위한 사용자 단말(User Equipment) 애플리케이션으로부터 요청을 수신하고 승인을 결정한다. 승인된 요청은 추가적인 처리를 위해 MEC 오케스트레이터로 전달된다. 또한, 외부 클라우드와 MEC 시스템 사이에서 애플리케이션을 재배치하기 위해 사용자 단말 애플리케이션으로부터 요청을 수신한다.
- **사용자 애플리케이션 라이프사이클 관리 프록시(User Application Lifecycle Management Proxy):** 사용자 애플리케이션은 디바이스에서 실행 중인 애플리케이션을 통해 사용자 요청으로 MEC 시스템으로부터 인스턴스화된 MEC 애플리케이션이다. 사용자 애플리케이션 라이프사이클 관리 프록시는 디바이스 애플리케이션으로 하여금 사용자 애플리케이션의 온-보딩, 인스턴스화, 종료 등을 요청할 수 있도록 하는 기능과 사용자 애플리케이션의 상태를 사용자 단말 애플리케이션에 알리는 기능을 갖는다. 또한, 사용자 디바이스 내의 애플리케이션으로부터 요청을 승인하고 OSS 및 MEC 오케스트레이터와의 인터랙션을 통해 이들 요청을 추가 처리한다.
- **MEC 플랫폼 관리자(MEC Platform Manager):** 관련 애플리케이션의 연관된 이벤트를 MEC 오케스트레이터에 알리는 등 애플리케이션의 라이프사이클을 관리하고, MEC 플랫폼으로 요소 관리 기능을 제공하며, 서비스 승인, 트래픽 규칙, DNS 구성 및 충돌 해결 등 애플리케이션 규칙과 요구사항을 관리하는 역할을 한다. 또한, 추가 처

표 1 MEC 시스템 레퍼런스 포인트

종류	설명	레퍼런스 포인트
Mp1	(MEC 플랫폼 – MEC 애플리케이션) 서비스 등록, 서비스 탐색 및 서비스에 대한 통신 지원 제공뿐 아니라 애플리케이션 가용성, 세션 상태 재배치 지원 절차, 트래픽 규칙 및 DNS 규칙 활성화, 저장 장치 및 시간 정보에 대한 접근 등과 같은 기타 기능 제공	MEC 플랫폼 (Mp)
Mp2	(MEC 플랫폼 – 가상화 인프라 데이터 평면) 데이터 평면에게 애플리케이션, 네트워크, 서비스 사이에 트래픽을 보내는 방법 제공	
Mp3	(MEC 플랫폼 간) MEC 플랫폼사이에 통신 제어	
Mm1	(MEC 오케스트레이터 – OSS) MEC 시스템에서 MEC 애플리케이션의 인스턴스화와 종료 트리거링	MEC 관리 (Mm)
Mm2	(OSS – MEC 플랫폼 관리자) MEC 플랫폼 구성, 오류와 성능 관리	
Mm3	(MEC 오케스트레이터 – MEC 플랫폼 관리자) 애플리케이션 라이프사이클, 애플리케이션 규칙과 요구사항의 관리 및 이용 가능한 MEC 서비스 추적	
Mm4	(MEC 오케스트레이터 – 가상화 인프라 관리자) 이용 가능한 자원 용량을 추적하는 것을 포함한 MEC 호스트의 가상화된 자원 및 애플리케이션 이미지 관리	
Mm5	(MEC 플랫폼 관리자 – MEC 플랫폼) 플랫폼 구성, 애플리케이션 규칙과 요구사항의 구성, 애플리케이션 라이프사이클 지원 절차, 애플리케이션 재배치 관리 등을 수행	
Mm6	(MEC 플랫폼 관리자 – 가상화 인프라 관리자) 가상화된 자원을 관리	
Mm7	(가상화 인프라 관리자 – 가상화 인프라) 가상화 인프라를 관리	
Mm8	(사용자 애플리케이션 라이프사이클 관리 프록시 – OSS) MEC 시스템에서 실행 중인 애플리케이션의 사용자 단말 애플리케이션 요청 처리	
Mm9	(사용자 애플리케이션 라이프사이클 관리 프록시 – MEC 오케스트레이터) 사용자 단말 애플리케이션이 요청한 MEC 애플리케이션을 관리	
Mx1	(OSS – 사용자 서비스 포털) MEC 시스템에서 애플리케이션을 실행하도록 요청한 사용자에 의해 사용	외부 개체 (Mx)
Mx2	(사용자 애플리케이션 라이프사이클 관리 프록시 – 사용자 단말 애플리케이션) MEC 시스템에서 애플리케이션을 실행하도록 MEC 시스템에 요청하거나 MEC 시스템의 안팎으로 애플리케이션을 이동하도록 요청한 사용자 단말 애플리케이션에 의해 사용	

리를 위해 가상화 인프라 관리자로부터 가상화된 자원 오류 보고서와 성능 측정치를 수신한다.

- **가상화 인프라 관리자(Virtualization Infrastructure Manager):** 가상화 인프라의 가상화된 (연산, 저장 장치, 네트워킹) 자원 할당, 관리, 릴리즈 기능과 소프트웨어 이미지를 실행할 가상화 인프라 준비 기능, 그리고 애플리케이션의 신속한 프로비저닝 기능 등을 갖는다.
- **사용자 단말 애플리케이션(User Equipment Application):** 사용자 애플리케이션 라이프사이클 관리 프록시를 통해 MEC 시스템과 상호작용할 수 있는 기능을 가진 사용자 디바이스 내에 있는 애플리케이션을 의미한다.
- **사용자 서비스 포털(Customer Facing Service Portal):** 사업자의 고객이 특정 요구를 충족하는 일련의 MEC 애플리케이션을 선택하고 주문할 수 있도록 하고, 공급된 애플리케이션으로부터 서비스 레벨 정보를 다시 받을 수 있도록 한다.

MEC를 구성하는 각 시스템 개체 사이에는 3종류의 레퍼런스 포인트를 가지는데, 표1과 같이 Mp는 MEC 플랫폼 기능에 관한 레퍼런스 포인트를 의미하고, Mm은 관리 레퍼런스 포인트, 그리고 Mx는 외부 개체와의 연결에 관한 레퍼런스 포인트를 의미한다.

3. MEC 보안

3.1 개요

사용자와 가까운 네트워크 엣지에서 컴퓨팅 서비스를 제공하는 MEC는 NFV 기술을 바탕으로 제삼자 애플리케이션을 실행할 수 있는 개방형 시스템이기 때문에, 보안 위협의 주요 대상이 될 수 있다.

MEC 보안을 바라보는 관점은 클라우드 보안이나 NFV 보안과는 다소 차이가 있다 [11, 12]. 클라우드 보안의 경우, 클라우드 서비스(IaaS, PaaS, SaaS[9])를 위한 보안 기술과 클라우드 서비스로서의 보안(SECaaS[10]) 기술에 중점을 두고 있다. 이 중 클라우드 서비스를 위한 대표적인 보안 기술로는 네트워크 기반의 클라우드 경계 보안 기술, CASB(Cloud Access Security Broker)를 포함한 퍼블릭 클라우드 데이터 보호 기술, 서비스 사용자 인증 및 권한 관리 기술, 그리고 사용자 그룹별(Multi-tenancy) 접근 제한 기술 등이 포함된다 [13, 14].

NFV 보안의 경우, NFV 환경이 통신사업자의 망 내에 위치하며 일반 사용자의 접근 및 사용은 제한되는 특성을 갖는다. 따라서, 네트워크 기반의 경계 보안 기술, 관리자의 오류를 최소화하기 위한 인증 및 권한 관리 기술, 통신장비에 저장되는 사용자/서비스 민감 데이터 보호 기술 등이 여기에 포함된다.

이와 달리 MEC 보안의 경우, 태생적으로 NFV 보안과 속성이 동일하기는 하나, 초저지연 서비스 제공을 위한 제삼자의 애플리케이션이 이동통신사업자 망 내에서 실행될 수 있는 점이 가장 큰 차이점이라고 볼 수 있다. 따라서, MEC에 대한 잠재적인 보안 위협을 도출하고 이에 대한 대응 기술을 개발하고 적용할 수 있어야 한다.

3.2 MEC 보안 위협

MEC의 보안 위협을 도출하기 위해, 본 절에서는 네트워크 관점, MEC 시스템 및 애플리케이션 관점, 그리고 가상화 관점으로 위협 포인트(threat point)를 구분해서 정리한다.

3.2.1 네트워크 관점에서의 침해 위협

5G는 5G NR[11] 또는 E-UTRA[12]의 이동통신, 무선 LAN[13], 유선 및 위성통신 등의 다양한 액세스 기술을 통해 수많은 다양한 종류의 센서·기기가 연결되는 액세스 환경의 다변화에 따라, 액세스 망의 공격 접점(attack surface)과 잠재적 보안 위협이 크게 증가하였다. 특히, 초연결·초저지연·초고속의 서비스 품질 보장을 위해 코어망의 다양한 네트워크 기능과 서비스가 엣지 네트워크로 집중되면서, MEC 시스템에 대한 중간자(Man-in-the-middle) 공격, 도청(Eavesdropping), 스푸핑(Spoofing), 릴레이(Relay) 공격, 분산 서비스 거부(DDoS, Distributed Denial of Service) 공격 등이 발생할 수 있다 [15]. 한편, 호스트 레벨 MEC 시스템은 MEC 서비스를 위한 핵심 기능 인프라로 MEC 플랫폼 매니저, 가상 인프라 매니저(VIM, Virtualization Infrastructure Manager) 그리고 스토리지를 런칭하고 MEC 가입자들에게 서비스를 제공하는 MEC 호스트들로 구성된다. MEC 호스트들은 MEC 시스템 레벨과 인터넷, 가입된 사용자 단말 사이의 제한된 연결을 갖는 폐쇄된 환경에서 동작하므로 액세스 네트워크

9) IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)
10) Security as a Service
11) New Radio
12) Evolved UMTS Terrestrial Radio Access
13) Local Area Network

대비 상대적으로 중간자 공격이 발생할 경우가 많지는 않지만, 가상머신 조작, 가상머신 이스케이프[14], VNF 위치 쉬프트, DNS(Domain Name System) 증폭 등과 같은 가상화 기술을 타겟으로 하는 공격이 가능할 수 있다 [16]. 이런 형태의 공격들은 호스트 레벨 오케스트레이션 컴퍼넌트들의 원활한 동작에 영향을 줄 수 있는데 특히 VIM이 공격 받을 경우 MEC가 제공하는 서비스 자체가 붕괴될 수 있다. 또한, 앞서 언급한 액세스 네트워크의 위협이 통신 채널을 통해 MEC 호스트들에게 피해를 줄 수 있다. 가상머신 마이그레이션과 모바일 오프로딩을 통해 MEC 호스트에 악성 컨텐츠가 전달될 수 있다. 사용자 데이터가 MEC 엣지 레벨의 MEC 호스트에 저장되어 있기 때문에 기지국에 직접 침입한 공격자들의 물리적 공격에 취약하다.

3.2.2 MEC 시스템 및 애플리케이션 관점에서의 보안 위협

이동통신사업자의 내부망에 위치하여 일반 사용자의 접근 및 사용이 제한되는 NFV 시스템과는 달리, 제삼자 MEC 애플리케이션이 통신사업자 망내에서 실행될 수 있으므로 악성코드 등에 노출될 경우 치명적인 보안 위협을 가져올 수 있다 [9].

- 하이퍼바이저나 컨테이너 엔진 같은 가상화 소프트웨어가 공격받게 되면 MEC 애플리케이션이 장애를 일으킬 수 있고 데이터가 유출될 위험성이 큼
- MEC 관리 시스템이나 오케스트레이터에 대한 공격을 통해 MEC 애플리케이션 제어 기능에 대한 장애가 발생하거나 MEC 애플리케이션 작동 오류가 생길 수 있음
- MEC 시스템 상에서 실행 중인 가상머신이나 컨테이너 사이에 데이터 유출이 발생하거나 자원 점유 경쟁으로 인하여 자원 고갈 현상이 발생할 수 있음
- 조작되거나 악성코드에 감염된 MEC 애플리케이션을 통한 중간자 공격이나 타 MEC 애플리케이션으로의 감염 확산 및 데이터 유출이 발생할 수 있음
- 로밍이나 핸드오버시, 이전 MEC에 캐싱된 사용자 개인 정보 유출이 발생할 수 있음
- MEC 애플리케이션과 외부 애플리케이션 서버와의 상호 인증과정에서의 중간자 공격에 의한 개인 정보 유출 가능성이 있음
- 부채널(side-channel) 공격 등을 통해 다른 네트워크 슬라이스(network slice)의 민감 정보가 유출될 위험성이 있음
- 공개 소프트웨어 기반 MEC 시스템의 취약점을 악용한 공격이 발생할 수 있음
- 내부 관리자의 실수 또는 관리자 계정 유출에 따른 시스템 오작동이 발생할 수 있음

3.2.3 가상화 관점에서의 보안 위협

가상머신의 경우 완전히 격리된 컴퓨팅 환경을 제공하기 때문에 상대적으로 가상머신간 보안성이 높은 반면, 컨테이너의 경우 하나의 운영체제를 공유하는 불완전 격리 환경이기 때문에 상대적으로 보안성이 취약하다 [9, 17, 18].

표 2 시스템 가상화와 운영체제 가상화 특징 비교

시스템 가상화	구분	운영체제 가상화
독립적인 이종 다중 운영체제	운영체제	단일 운영체제 커널 공유
높음	격리	낮음
낮음	효율성	높음
제한적	확장성	무제한
완전히 격리된 독립 인스턴스	특징	빠른 빌드와 경량 인스턴스

5G에서는 클라우드 네이티브[15] 환경을 지향하고 있는 관계로 MEC 애플리케이션 실행을 위해 가상머신에 비하여 상대적으로 보안성이 취약한 컨테이너[16]의 비중이 높아지고 있는 추세이므로 이에 대한 보안 위협 또한 증가하고 있다. 가령, 컨테이너 이미지에 대한 업데이트가 지속적으로 빈번하게 발생하면서 이에 따른 악성코드 감염이나 비정상 이미지 유입의 가능성이 있다. 또한, 임의의 컨테이너 접근 권한 조작을 통해 컨테이너에 대한 제어 권한 탈취 공격이 발생할

14) VM escape: 가상머신에서 벗어나 호스트 운영체제와 인터랙션하는 것으로 2008년 VMware 워크스테이션에서 발견된 취약성 (CVE-2008-0923)

15) 클라우드 네이티브(Cloud Native): 유연성·확장성·가용성 등 클라우드 컴퓨팅 환경의 장점을 활용하기 위한 응용의 개발 및 운용 접근방법으로서, 응용을 가능한 한 작은 단위로 나누고 (Micro-service 구조), 세분화된 응용 단위는 컨테이너로 실행하며, 시장 및 서비스 요구에 따라 즉각적으로 서비스를 실행하고 빈번하게 지속적으로 업그레이드(DevOps)하기 위한 전략

16) 컨테이너는 운용체제 가상화 기술을 기반으로 서버 운영체제 공유에 따른 불완전 격리로 인해 독립적인 운영체제를 갖는 가상머신에 비해 상대적으로 보안성이 취약하나, 가상화된 객체가 가볍고 빠른 실행이 가능하여 효율성, 확장성 측면에서 활용 빈도가 증가 추세임

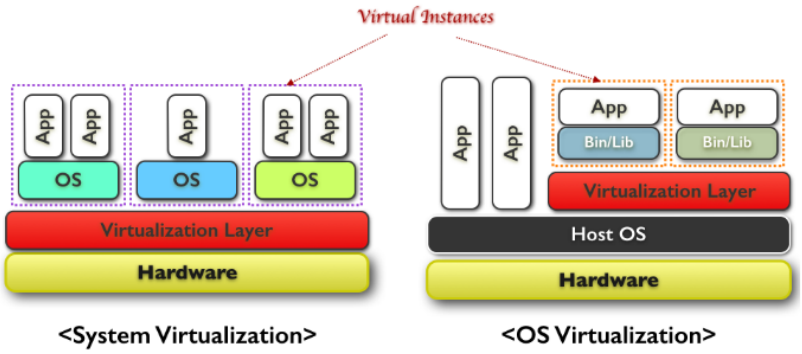

그림 3 대표적인 가상화 기술의 구조

수 있으며, MEC 애플리케이션의 개방형 API 취약점을 통해 데이터 조작이나 데이터를 유출이 발생할 가능성도 있다.

3.3 MEC 보안 위협에 대한 대응 기술

본 절에서는 위에서 기술한 MEC 보안 위협에 대응하기 위한 다양한 기술들을 네트워크, MEC 시스템, 컨테이너 런타임, 컨테이너 애플리케이션 이미지, 빅데이터 기반 분석 등 각 카테고리 별로 구분하여 제시한다.

- **네트워크 기반의 위협 대응 기술)** 5G 액세스 및 엣지 네트워크에서의 네트워크 기반 보안 위협에 유연하게 맞춤형으로 대응하기 위해 SDN[17]/NFV 기술을 이용하여 FW[18], IPS/IDS[19], DDoS 방어, DLP[20] 등의 네트워크 보안 장비를 가상머신 또는 컨테이너 형태로 가상화함으로써 다양한 보안 서비스들을 하드웨어 인프라 환경과 무관하게 맞춤형으로 제공할 수 있다.
- **MEC 시스템 보안 위협 탐지 및 대응 기술)** ETSI의 MEC 참조구조에서 MEC 시스템을 구성하고 있는 MEC 호스트, MEC 플랫폼, MEC 관리 프레임워크에 대한 보안 위협을 탐지하고 대응하는 기술이 요구된다. 대표적인 예로서, MEC 시스템의 관리자 또는 사용자가 시스템에 접근하여 허가되지 않은 시스템 자원으로의 접근을 시도하거나 시스템 또는 서비스를 제어하는 행위를 탐지하고 차단할 수 있어야 한다. 이러한 비인가된 시스템 자원에 대한 접근, 제어, 임의 변조, 권한 변경 등의 비정상행위를 탐지하고 차단하기 위하여 고수준의 세분화된(fine-grained) MEC 시스템 접근 제어 및 탐지 기술이 필요하다. 또한, 글로벌 사실 표준(de-facto standard)인 공개 소프트웨어 기반의 가상화 소프트웨어(예, KVM, QEMU, Docker 등)나 클라우드 운영체제(예, OpenStack, Kubernetes 등)의 취약성을 악용한 공격에 대응하는 기술도 요구된다.
- **컨테이너 런타임 기반 이상징후 탐지 기술)** MEC 환경에서 컨테이너의 사용 비중이 점차 증가함에 따라 가상머신 대비 상대적으로 보안성이 취약한 컨테이너에 대한 보안위협 대응 기술의 개발이 요구된다. 특히 MEC 시스템에서 실행중인 컨테이너의 이상징후를 탐지하고 데이터 유출과 같은 공격에 대응할 수 있어야 한다. 대표적인 예로는 생성된 컨테이너 내부에서 허용되지 않은 파일이나 애플리케이션에 접근하는 것을 탐지하고 컨테이너 외부와의 네트워킹 시도가 있을 경우 이를 탐지하고 차단할 수 있어야 하며, 정책에 기반하여 컨테이너 내부에서의 정보유출 여부를 모니터링하고 차단하는 기술이 필요하다. 또한, 컨테이너 실행 상태를 모니터링하여 컨테이너에 할당되어 사용되는 시스템 자원 상태의 이상 징후를 탐지할 수 있도록 하는 기능과 컨테이너가 실행중에 비정상적으로 MEC 호스트의 자원을 과다하게 점유하는지를 파악하여 이를 방지하는 기술도 요구된다.
- **컨테이너 애플리케이션 이미지의 무결성 및 취약성 검증 기술)** 클라우드 네이티브를 지향하는 MEC 운용 환경의 특성상 MEC 애플리케이션의 빠른 설치와 서비스 제공은 물론 지속적인 업데이트를 통한 서비스의 즉시성, 유연성 및 가용성을 보장할 수 있어야 한다. 따라서, MEC의 애플

17) 소프트웨어 정의 네트워킹(Software-defined Networking): 네트워크 장비의 제어부분을 트래픽 전송부분과 분리하여 트래픽 전달 동작을 개방형 인터페이스를 통해 제어하는 기술
18) Firewall
19) Intrusion Protection System/Intrusion Detection System
20) Data Loss Protection

리케이션 이미지는 지속적인 업데이트 과정에서 자칫 유입될 수 있는 비정상 이미지 또는 악성코드에 감염된 변조된 이미지가 이동통신사업자의 MEC 환경으로 유입되는 것을 차단할 수 있어야 한다. 대표적인 예로서, MEC 시스템의 애플리케이션 이미지 저장소(repository)에 저장할 컨테이너 이미지에 대한 무결성을 검증하는 기능과 비인가자가 특정 이미지를 생성하거나 유포하는 것을 차단하는 기능, 그리고 MEC 제삼자 애플리케이션에 대한 정적·동적 분석을 통해 이미지 및 API의 취약성을 탐지하고 MEC 애플리케이션 내부에 악성코드가 내포되어 있는지 여부를 탐지하는 기능도 요구된다.

- **빅데이터 기반 5G MEC 보안 위협 분석 및 탐지 기술)** 지능화되고 고도화되는 MEC 시스템 전체에 대한 보안 위협을 종합적으로 분석하고 탐지 및 대응하기 위해서는 각 컴퍼넌트에서 생성되는 데이터나 구간별 전송 데이터 등에 대한 인공지능 기반의 보안위협 분석이 요구된다. MEC 보안 상황 및 상태 모니터링 로그를 수집하고 행위에 기반한 MEC 플랫폼 이상징후를 판단하기 위한 룰셋을 도출할 필요가 있으며, 이를 통해 MEC 시스템의 이상징후를 판단하고 침해시스템을 검출하는 기능도 필요하다.

4. 결 론

본 고에서는 ETSI MEC 참조 구조를 살펴본 다음 5G 환경에서의 잠재적인 MEC 보안 위협을 다양한 포인트 별로 도출하고 카테고리별로 대응 가능한 기술들을 살펴보았다.

MEC 기술은 5G 이동통신 환경에서 특히 저지연·고속 서비스 제공을 위한 핵심 인프라 기술로 멀티미디어의 제어, 위치/지역 기반 서비스, 실시간/대용량 데이터 처리 및 초저지연 스마트 시스템 구축 등을 가능하게 한다. 특히, 스마트팩토리, 스마트시티, 자율주행차, 디지털헬스케어, 실감 컨텐츠 등 5G 융합서비스가 확대되면 MEC를 활용한 융합서비스 제공도 급속히 증가할 것으로 전망된다. 더욱이 MEC에 대한 보안 침해 공격이 발생할 경우, 단순히 서비스의 일시적 장애로 그치지 않고 실생활과 밀접한 융합서비스의 경우 재산상의 피해 등 그 파급이 매우 클 것으로 예상된다. 따라서, 점차 고도화되고 지능화되는 보안 위협에 대해 체계적으로 대응할 수 있는 지능화된 보안 위협 대응기술에 대한 지속적 연구가 진행되어야 할 것이다.

참고문헌

[1] 박종근, 김종현, 문대성, 김익균, "3GPP 5G 보안 구조의 특징 및 주요 개선사항," 정보보호학회지, 제29권, 제5호, pp.21-30, 2019.

[2] 김희천, "5G 버티컬의 성공을 위한 거버넌스 확립의 필요성," 전문가칼럼, 정보통신정책연구원, 2019.

[3] 박종근, 김종현, 김익균, 진승헌, "초연결 지능화 인프라 보안기술 동향 – 5G 시대의 이동통신 보안 중심," 전자통신동향분석, 제34권, 제1호, pp.36-48, 2019.

[4] ITU-R Recommendation, M.2083.0, "IMT-Vision: Framework and overall objectives of the future development of IMT for 2020 and beyond," 2015.

[5] 3GPP, TS 33.501, "Security Architecture and Procedures for 5G System," V15.3.1, 2018.

[6] NETMANIAS, "MEC의 개념과 5G, 4G망에서 MEC 도입 구조," https://www.netmanias.com/ko/ ?m=view&id=oneshot&no=14273

[7] Q. Pham et al, "A Survey of Multi-Access Edge Computing in 5G and beyond: Fundamentals, Technology Integration, and State-of-the-Art," IEEE Communications Surveys and Tutorials, pp.1-43, 2020

[8] NETMANIAS, "4G/5G 모바일 망에서 엣지 위치와 엣지 서비스의 진화 트렌드," https://www.net manias.com/ko/?m=view&id=oneshot&no=14019

[9] 박종근, "5G 엣지 보안 기술," KRnet 2020, 2020

[10] ETSI, "Multi-access Edge Computing (MEC); Framework and Reference Architecture," ETSI GS MEC003, V2.1.1, 2019.

[11] 박종근, "5G 엣지 보안," NetSec-KR 2020, 2020

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

[13] 박종근, "5G 환경에서의 보안 이슈와 3GPP 보안 구조 기술," NetSec-KR 2019, 2019

[14] R. Roman et al, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, Vol.78, pp.680-698, ELSEVIER, 2018.

[15] X. Lu et al, "Managing Physical Layer Security in Wireless Cellular Networks: A Cyber Insurance Approach," IEEE Journal on Selected Areas in Communications, 2018.

[16] F. Zheng et al, "A Survey on Virtual Machine Migration: Challenges, Techniques, and Open Issues," IEEE Communications Surveys and Tutorials, Vol.20, No.2, pp.1206-1243, 2018.

[17] P. Ranaweera et al, “Realizing Multi-Access Edge Computing Feasibility: Security Perspective,” Proc. of CSCN’19, IEEE Conference on Standards for Communications and Networking, 2019.

[18] R. Khan et al, “A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions,” IEEE Communications Surveys and Tutorials, pp.1-55, 2019

약 력

김 영 수

1998 성균관대학교 정보공학과 학사
2000 성균관대학교 컴퓨터공학과 석사
2009 성균관대학교 컴퓨터공학과 박사
2012~2015 충남대학교 컴퓨터공학과 겸임교수
2000~현재 한국전자통신연구원 책임연구원
관심분야: 5G보안, 네트워크보안, 디지털포렌식, 암호프로토콜
Email: blitzkrieg@etri.re.kr

박 종 근

1997 성균관대학교 산업공학과 학사
1999 성균관대학교 산업공학과 석사
2013 충남대학교 컴퓨터공학과 박사
1999~2001 국방과학연구소 연구원
2001~현재 한국전자통신연구원 책임연구원
관심분야: 이동통신보안, SDN/NFV, 클라우드 보안
Email: queue@etri.re.kr

이 종 훈

1999 경북대학교 컴퓨터공학과 학사
2002 경북대학교 컴퓨터공학과 석사
2002~현재 한국전자통신연구원 책임연구원
관심분야: 정보보호, 네트워크 보안, 5G 보안, 인공지능 기반 SIEM, 지능형 위협 탐지, 빅데이터 기반 위협 탐지
Email: mine@etri.re.kr

장 종 수

1984 경북대학교 전자공학과 학사
1986 경북대학교 전자공학과 석사
2000 충북대학교 컴퓨터공학과 박사
1989~현재 한국전자통신연구원 네트워크보안그룹장, 보안응용연구부장, 기술기획연구그룹장/책임연구원
2006~현재 대검찰청 디지털수사자문위원회 위원
관심분야: 네트워크 보안, 클라우드 보안, 개인정보보호, 5G 보안
Email: jsjang@etri.re.kr

문 대 성

2007 고려대학교 전산학과 박사
2009~현재 과학기술대학원대학교(UST) 정보보호공학 전공책임교수
2000~현재 한국전자통신연구원 네트워크·시스템보안연구실장/책임연구원
관심분야: 정보보호, 네트워크보안, 5G보안, 인공지능 보안
Email: daesung@etri.re.kr

김 익 균

1994 경북대학교 컴퓨터공학과 학사
1996 경북대학교 컴퓨터공학과 석사
2009 경북대학교 컴퓨터공학과 박사
2004~2005 Purdue University 초빙연구원
1996~현재 한국전자통신연구원 정보보호연구본부장/책임연구원
관심분야: 네트워크 보안, 컴퓨터 네트워크, 클라우드 보안, 빅데이터 분석
Email: ikkim21@etri.re.kr