5G 코어네트워크의 보안이슈와 대응

2020.07.16.

김 환 국

상명대학교 정보보안공학과

rinyfeel@smu.ac.kr

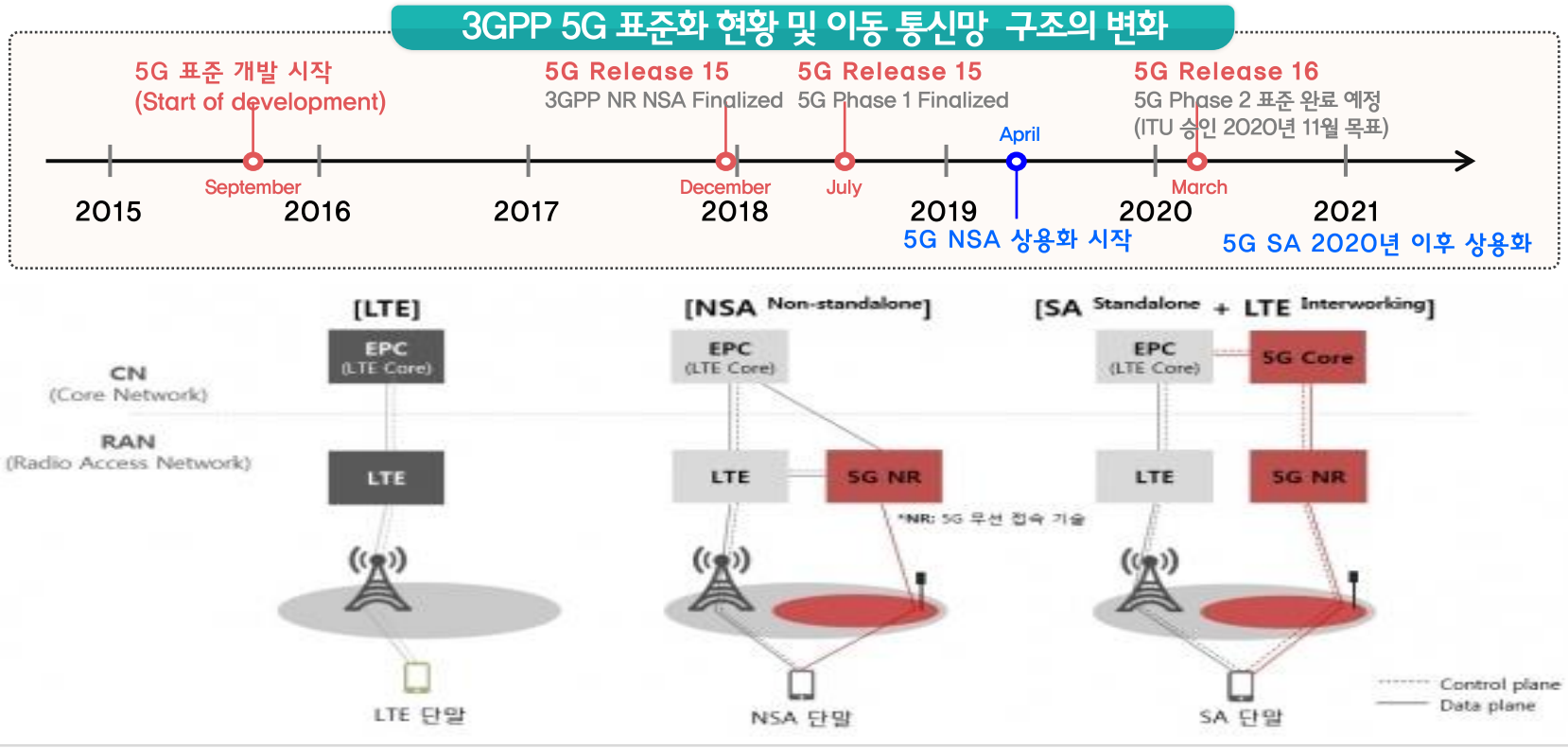
5G 네트워크 기술특성과 보안 이슈

1.1 현재 5G 네트워크

2019년 세계 최초 5G 상용 서비스가 시작 ('19.4월 NSA 서비스, '20년 하반기 SA 서비스)
"사이버공격으로 5G 통신망 장애 시 모든 것이 연결된 국민의 실생활에 막대한 영향을 미침"

≫ 초기 5G망은 LTE와 연동하는 비 단독(NSA) 구조로 구축, 2020년 단독(SA) 구조로 서비스가 시작될 예정

※ 5G 망은 NSA와 SA, 2가지 방식이 있으며, 현재 이동통신사들은 기존 망과 연동하는 NSA 방식의 5G 표준을 기반으로 상용화 시작



1.2 네트워크 보안 취약점 이슈

ENISA, KAIST, KISA 결과 **기존 2G~4G망 알려진 취약점 이 5G 망에서 발생 우려 지속 제기**

≫ 'RAN, 코어망, 연동망' 구간에서 장비·프로토콜 ·설정오류 등 다양한 보안 취약점 존재

≫ 최근 5년간 국내 이통망 장애 1,753 만명 발생 (보상금 668.7억원 지급) ('18.9, 국회 자료)

* 기존 시그널링 프로토콜 알려진 취약점→2차 인증용 SMS 메시지 유출, DDoS 공격

구분	RAN 프로토콜	코어망 구간 취약점	연동 구간 프로토콜 취약점
발견 취약점	▪ 카이스트) RAN 구간 취약점 51건 발견 ※ NAS, RRC 취약점	▪ (KISA) VoLTE 서비스 취약점 11건 발견	▪ (ENISA) 프로토콜 취약점 17건 발견
관련 연구	▪ 모바일 NW 퍼징 툴(LTE Fuzz) 개발('18) : 무선망(RAN) 취약점 ✓ 단말이 LTE망에 최초 접속하는 과정에서 발생 ✓ 상용망 테스트 결과 51개 취약점 발견	▪ 4G망 보안기술 R&D 과제('13~'16) : 4G 코어망 위협 분석 및 대응 ✓ 국내 이동통신망 대상4G 데이터 서비스 ✓ VoLTE 서비스에 대해 11개 취약점 발견 → 이동통신 3社 조치 완료	▪ 기존 Diameter 취약점 활용 가능성('18) ✓ 2차 인증으로 사용하는 SMS 메시지 유출 ✓ DDoS 공격 등이 5G 망에서 가능 ▪ AKA 인증 프로토콜 결점 분석 ✓ 공격자 근처 5G 단말 정보 악용 가능 → 3GPP 표준 수정 중

1.3 3GPP 보안 표준 : 보안 기능의 지속적인 강화

5세대 이동통신까지 (시그널링 보호 위한 암호 · 인증, 접근통제 중심) 보안 기능이 지속적으로 강화

≫ 3GPP, SA3 워킹 그룹, 2018년 (Release 15) 5G 보안 기술 표준 : TS 33.501 발표

※ 2G 보안 (Air 구간 암호화, 사용자 인증 SIM 카드 도입) → 3G 보안 (상호인증 AKA, 시그널링 무결성 보호 및 암호화 강화) → 4G 보안 (NAS/AS 보안, 시그널링 암호화 등 강화) → 5G Release 15 (IMSI 암호화, SEPP, SEAF 등)

3GPP 표준 보안기능 강화

- 사용자 인증 강화 (SIM 카드 도입)
- 무선 인터페이스 암호화
- 상호인증(AKA)
- 시그널링 메시지 무결성 보호(RRC) 및 암호화(IPSec 등)
- NAS/AS 보안기능 (시그널링 메시지 보호 강화)
- IMSI 정보 암호화
- SEPP (Security Edge Protection Proxy)
- 3GPP & non 3GPP 통합인증 (SEAF)

* 출처 : IT 동아(5G 통신의 현재와 미래, 이상엽), 그림과 에릭슨 자료를 인용하여 재구성

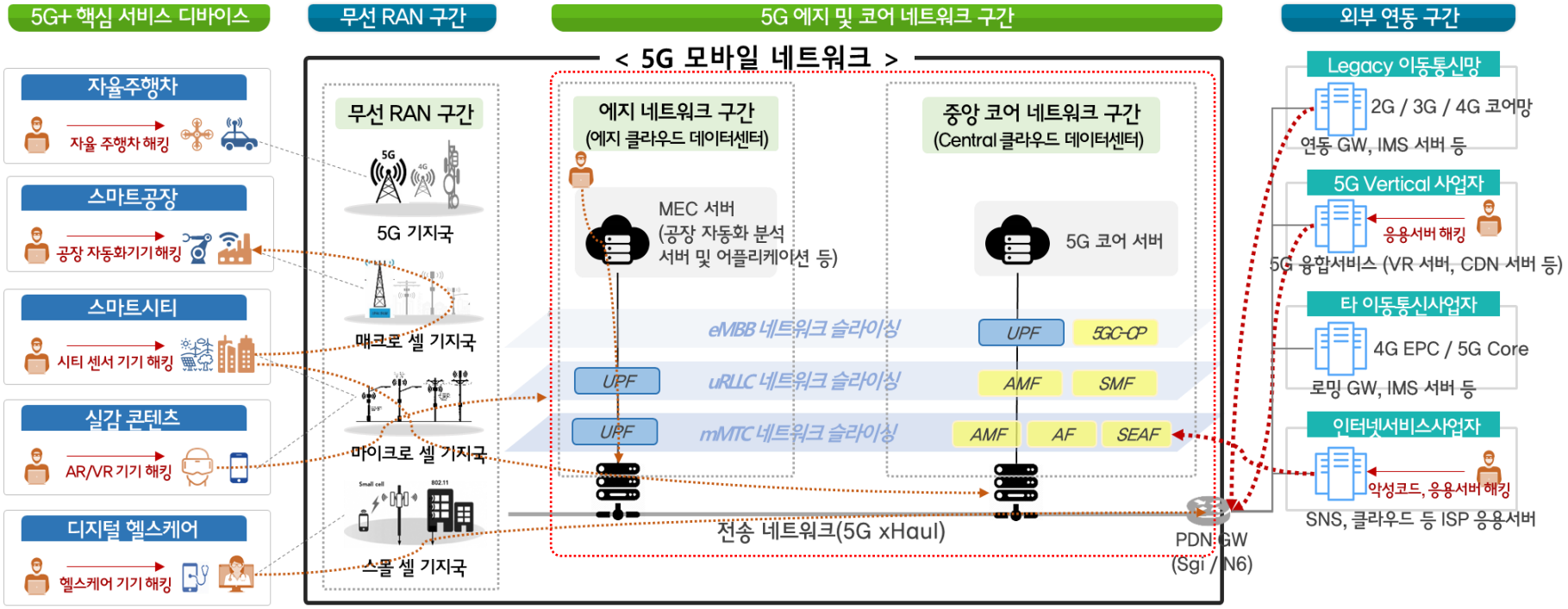
1.4 5G 기술 변화 : 중앙 집중 코어망 → 소프트웨어기반 분산 아키텍처

구성요소		현재 4G 기술	5G SA 구조 (Release 16)	특성
UE (사용자 장치)		스마트폰, 테블릿 등 개인용 기기 (음성, 문자, 영상, 인터넷 등)	**B2B 비즈니스용 IoT 기기 수용** (스마트폰, AR·VR, 드론, 의료기기, 센서 등)	스마트폰 → → IoT → 위성
무선 엑세스 네트워크 (RAN)	접속방식	단일 무선 RAT Access (2G, 3G, 4G 3GPP access 허용)	**다중 엑세스 (Multi-RAT access)** (Wifi 등 Non-3GPP access 수용)	3GPP 및 Non-3GPP access
	기지국	매크로셀, 펨토셀 등	**초고밀도 소형 셀 구축 증가**	
	구현기술	Centralized RAN (RU-DU-CU)	**Cloud RAN 구조** (기능 분할, 가상화 기술 기지국 슬라이싱)	
코어 네트워크 (Core Network)	물리적 배치	중앙 집중형 단일 코어망	**에지 및 코어 네트워크** (코어 기능의 지역적 분산화 및 클라우드화)	물리적 장비 중심의 Fixed 네트워크 구축 Software 기반 Flexible 네트워크 아키텍처 (초저지연 특성 반영)
	전송망	물리적 공유, 단일 네트워크 제공 (IP 패킷 데이터 통신)	**종단간 네트워크 슬라이싱 (논리적 망 분리)**	
	장비형태	물리적장비 (PNF) 중심 (Physical Network Function)	**가상화 NF (SDN/NFV 기술 적용)** (Visualization Network Function)	
	인터페이스	Peer-to-Peer I/F Architecture (multiple 인터페이스)	**SOA(Service-based I/F Arch.)** (HTTP2/RESTful)	
	제어신호	CUPS (Control Plane 과 User Plane 분리)	**물리적 CP / UP 경로 분리** (UPF 기능 분산 및 에지 재배치)	
	데이터 저장	네트워크 컴퓨팅 기능과 데이터 저장 기능이 한군데 처리	**무상태 네트워크 기능(Stateless NFs)** (네트워크 기능과 데이터 저장소 분리)	
외부 연동 및 어플리케이션		통신사의 코어망과 외부 GW(SGi 등)를 거쳐 연결	**MEC (내부 에지 네트워크 전진 배치)**	코어 내부망 Open 개방화

* 출처 : 넷마니아즈(http://www.netmaniaz.com/kr), ETRI(신명기), NIA(신동형), 삼성 리서치 자료 인용하여 재구성

1.5 5G 네트워크 구간 별 보안 위협

이종 망들의 초연결성으로 인해 상이한 보안요구사항과 기술로 인한 취약 연결고리 발생



사용자 장치(UE)	무선 RAN 구간	5G 에지 및 코어 네트워크 구간	외부 연동 구간
악성코드 감염	무선 자원 재밍(Jamming)	(플랫폼) SDN/NFV 플랫폼 취약점, MEC 서버 취약점	Legacy (2G · 3G · 4G) 취약점
펌웨어 해킹	무선 RAN DDoS	(API) 3rd Party 어플리케이션 API 및 부적절한 권한 접근	5G Vertical 응용 서버 해킹
디바이스 탬퍼링	허위 기지국(Rogue BS)	(서비스) DDoS 서비스 장애, 네트워크 슬라이싱 위협	로밍 취약점, 가입자 정보 가로채기
IoT 봇넷 감염		(네트워크) 분산 코어 네트워크 망 장애, 보안 관리 · 유지	ISP 악성코드 감염, API 취약점 공격

* 출처 : Cisco Systems, "Innovation Towards SP Transformation, Cisco Connect 2018 " 자료 재구성

1.6 5G 특성과 보안이슈 : ① 분산 코어망 아키텍처

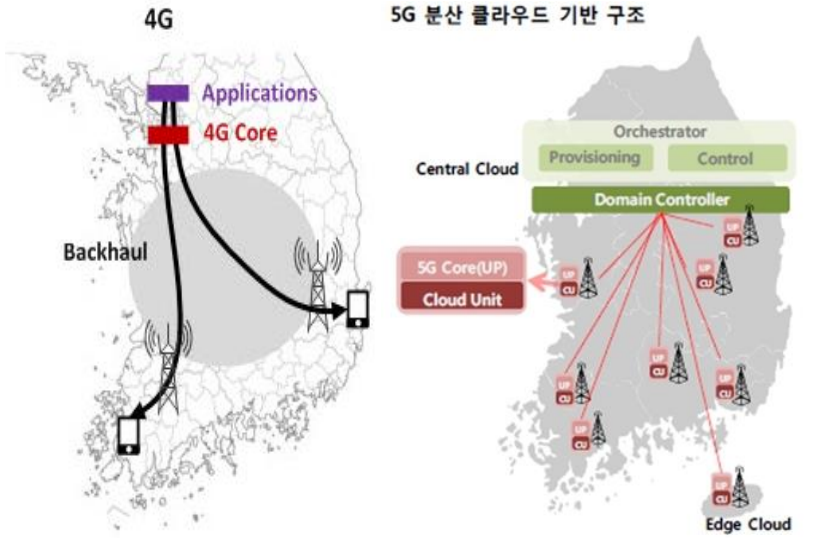
중앙국사로 트래픽 집중된 중앙 집중형 단일코어망 → 지역 분산화 및 기능 재배치, 클라우드 센터

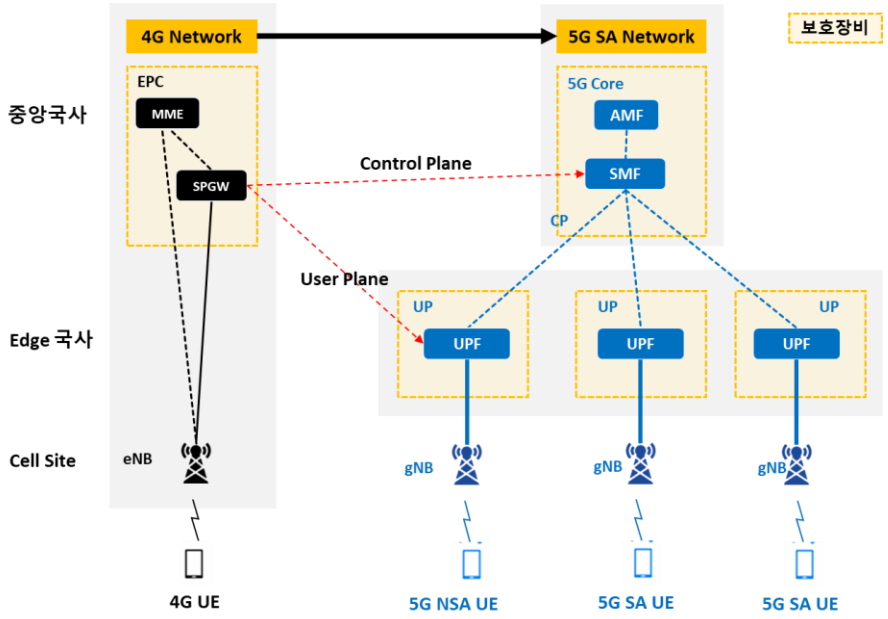
Security Challenges 통신 장비 분산으로 보호대상 (attack surface) 증가에 따른 보안 가시성

» Control Plane/User Plane 경로(CUPS) 물리적 분리: 중앙 통신 센터 (신호 처리), 지역 에지 통신센터(User 데이터 처리)

» **코어기능의 재배치 :** 네트워크 통신 기능을 에지네트워크와 코어네트워크로 분리하여 기능을 분산 재배치

» 코어 통신 기능(이동성, 인증, 과금 등) : 제어평면(중앙 센터)과 사용자 평면 및 응용서버(에지 센터) 으로 분리





* 그림 출처: (좌) 통신사업자 관점의 5G 네트워크 기술, KT 융합기술원, (우) Netmania 그림 재수정

1.6 5G 특성과 보안이슈 : ② IoT 디바이스 및 DDoS

20배 빠른 고속 · 대용량 및 10배 많은 IoT 기기 연결 (more devices, more threats)

Security Challenges DDoS 공격 빨라지고(faster), 강해지고(stronger), 대형화(bigger)

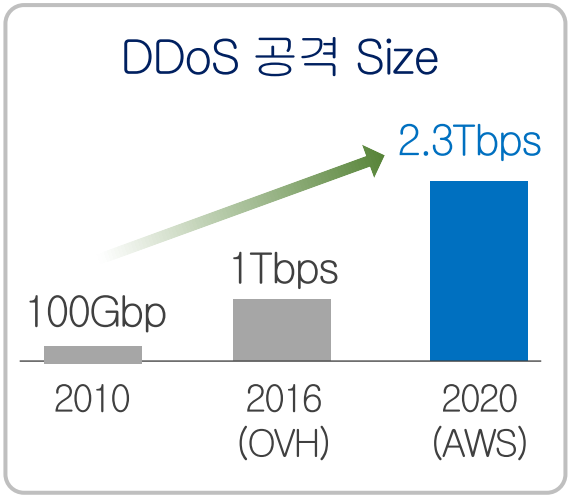
≫ (테라급 시대) 최대 DDoS 공격 규모는 급격히 증가 중 : '16년 1Tbps공격 → '20년 2.3Tbps

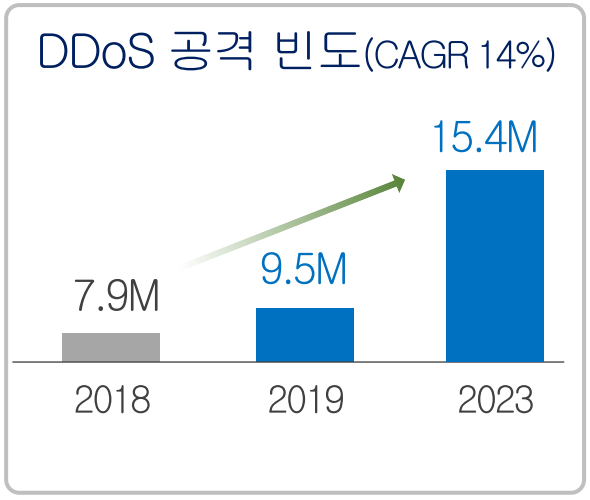
* 트래픽 증가는 DDoS 공격 Peak Size 및 빈도 비례하여 증가(DDoS 공격

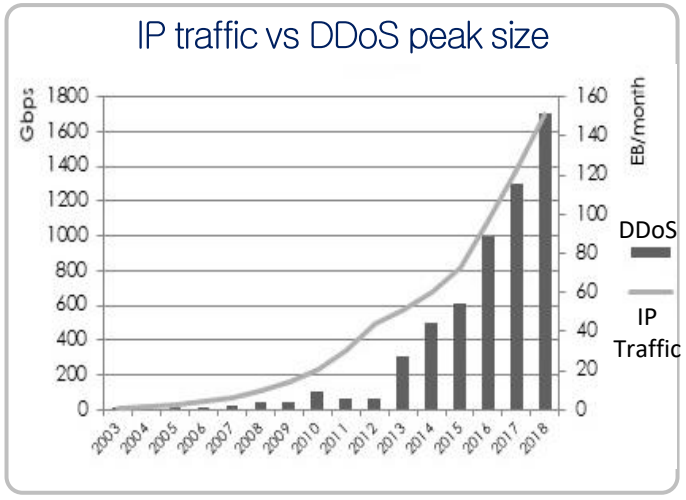
≫ (IoT 봇넷) 산업군별 기기 유형, 탑재 SW, 공급망 다양: 공통된 보안 표준과 아키텍처 설계 어려움

* 불안전한 IoT 기기 : 취약한 패스워드, 오래된 보안 취약점 내포 방치 → 해커들 IoT 무기화를 위해 준비

≫ ***DDoS 공격 트렌드*** *(*그림 출처: 2019, Cisco, Arbor Network 등 글로벌보안기업 분석)*

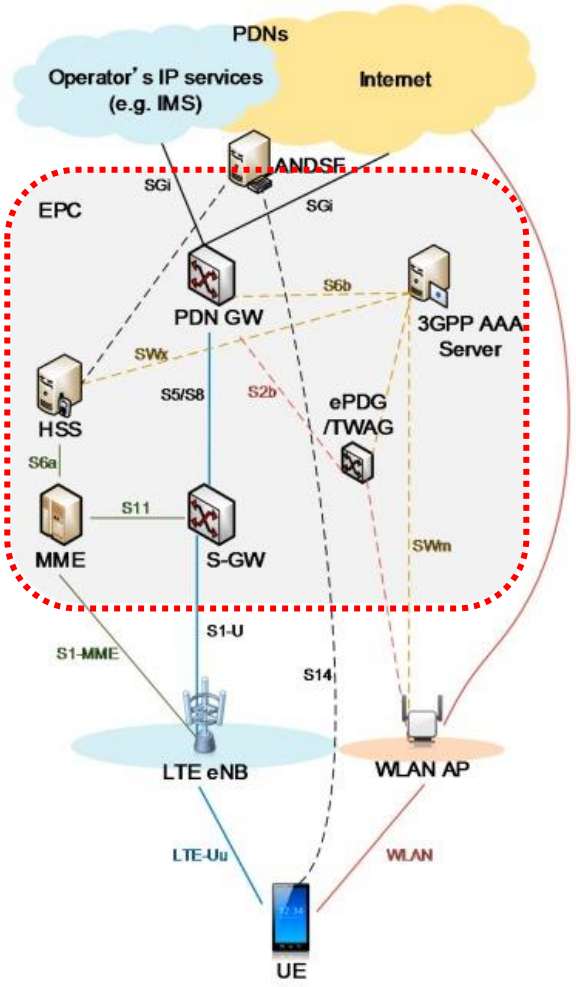






1.7 [참고] IoT 기기 Mobile Network 접속 방식

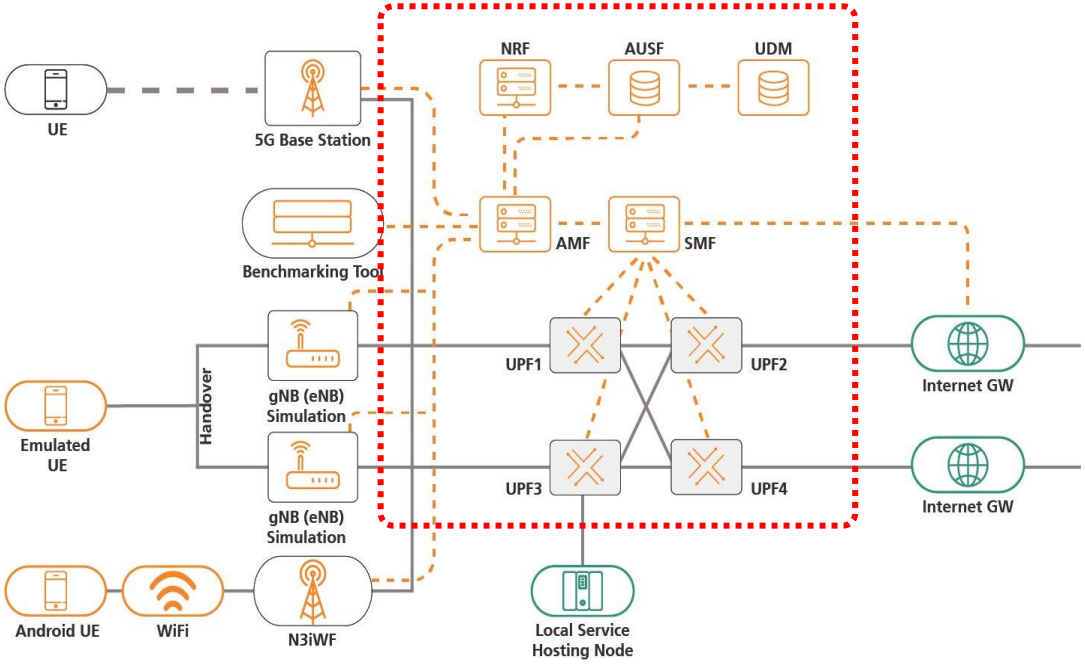
LTE : Non 3GPP Access



IoT 기기 5G 네트워크 접속 방식

1) 5G 모뎀 칩 장착, 2) 5G 허브 (브리지) 연결

3) Non-3GPP Access (N3IWF – UPF 연결)



* 그림(좌) : http://europepmc.org/

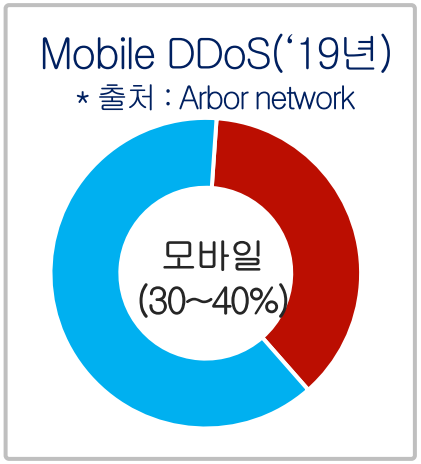
* 그림(우) : https://www.open5gcore.org/

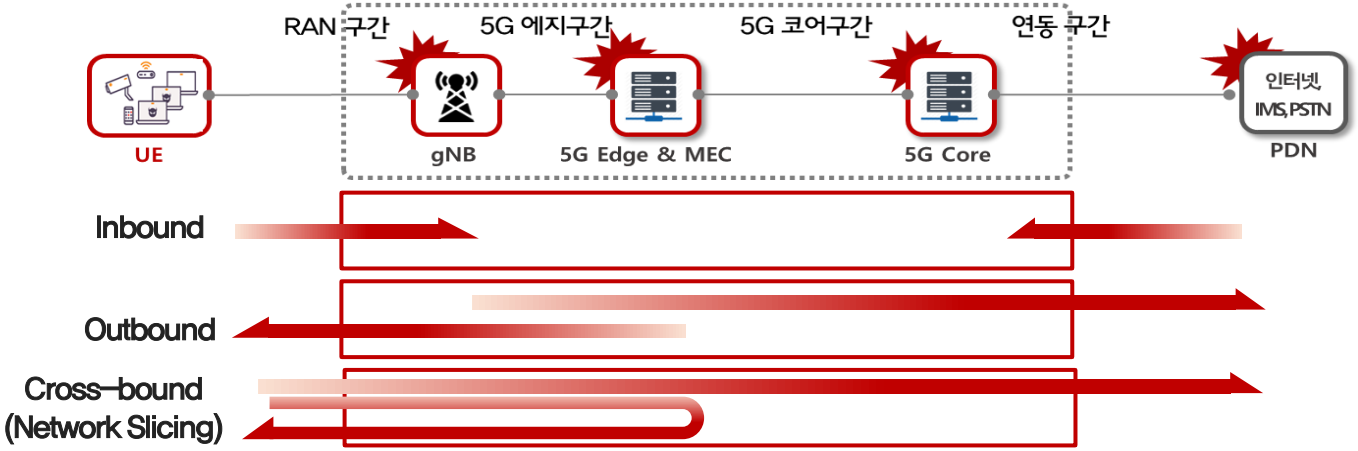
1.8 5G 특성과 보안이슈 : Mobile DDoS 공격 트렌드

DDoS 공격 타겟 : 유선 ISP → IoT, 클라우드 및 모바일 네트워크 DDoS 공격 꾸준히 증가 추세

>> Mobile DDoS 빈도(64% 증가) , 공격 크기(33% 증가) : 유선 대비 약 31% 수준

*** 공격대상 : 1) (Inbound) 5G 코어 인프라 2) (Outbound) 5G 연동 망/서비스 3) (Cross) 5G IoT (Network Slicing)**





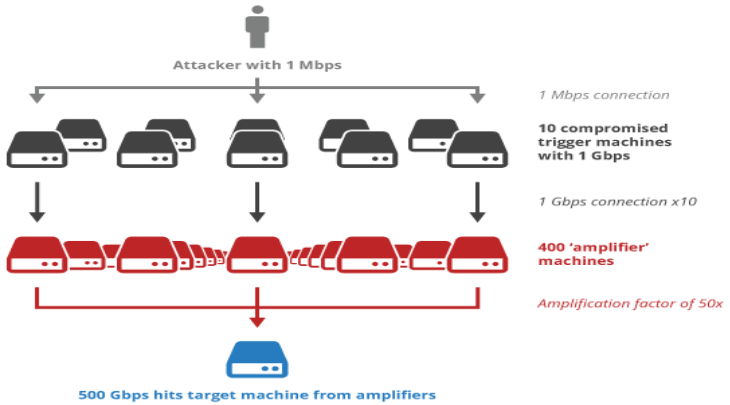
Vector1 + **vector2** + vector3 = Amplification/Reflection

>> 보안장비 우회를 위한 Complex DDoS

- **Multi-Vector DDoS (증폭 DNS, SSDP 등)**
- **Mobile DDoS 특성 (소스 IP 분석)**

  기지국(Base Station) IP 상당히 많이 발생

  (정상, DDoS 공격 구분)



1.9 5G 특성과 보안이슈 : ③ 가상화 기술 (네트워크 슬라이싱, SDN,/NFV)

(장비 · 서비스) 물리적 코어 네트워크를 다수의 가상 네트워크로 분리하여 독립 서비스 제공

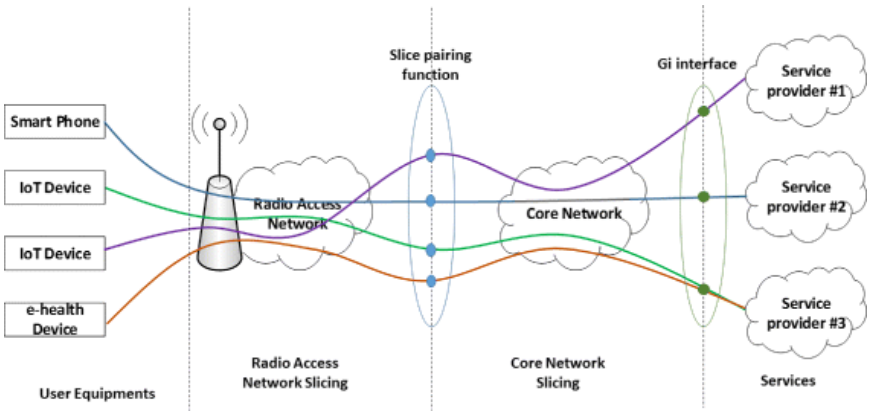
Security Challenges 가상화 기술은 물리적 IT 자원 통합관리, **효율성, 유연성, 가용성 측면 장점**

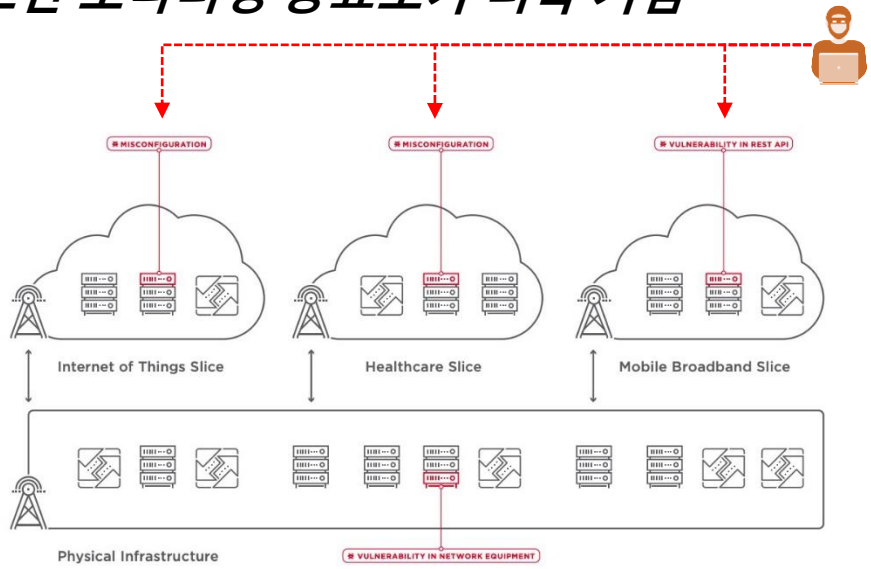
공유 HW 자원 부하 공격, 악성 공격 전파, 접근제어, Configuration 결함 · 오류 등 상대적 취약

≫ 네트워크 슬라이싱 : 물리적 단일 네트워크를 통해 엔드 투 엔드 전 구간(Device, Access, Transport, Core)을 논리적으로 분리된 네트워크를 만들어 서비스 별 전용 네트워크를 제공

≫ SDN 및 NFV 기술 채택 : 범용 서버 상에 가상화 SW 형태 구현 ☞ **동적 변화되는 환경설정은 보안관리 어려움**

Network Slicing 보안 : ***Slicing Isolation, 동적 보안 모니터링 중요도가 더욱 커짐***





* 그림 출처: 5G Core Vision, 삼성전자(2019), Positive Technologies

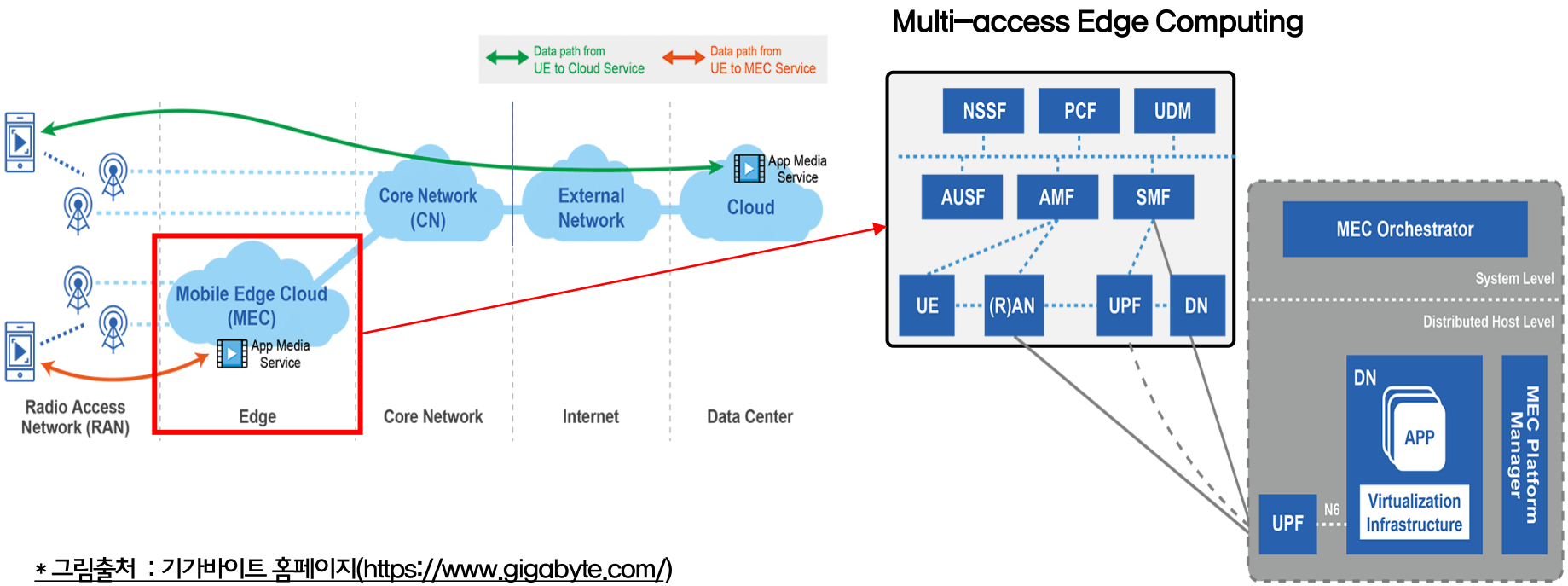
1.10 5G 특성과 보안이슈 : ④ MEC (Multi-access Edge Computing) Cloud

(어플리케이션) 대용량 정보처리를 지연 없이 실시간 제공을 위해 **단말 가까이 에지 컴퓨팅 서버를 전진배치**

Security Challenges MEC 탑재 악의적인 3rd App 신뢰성과 코어 내부 장비(UPF) 연결 경로

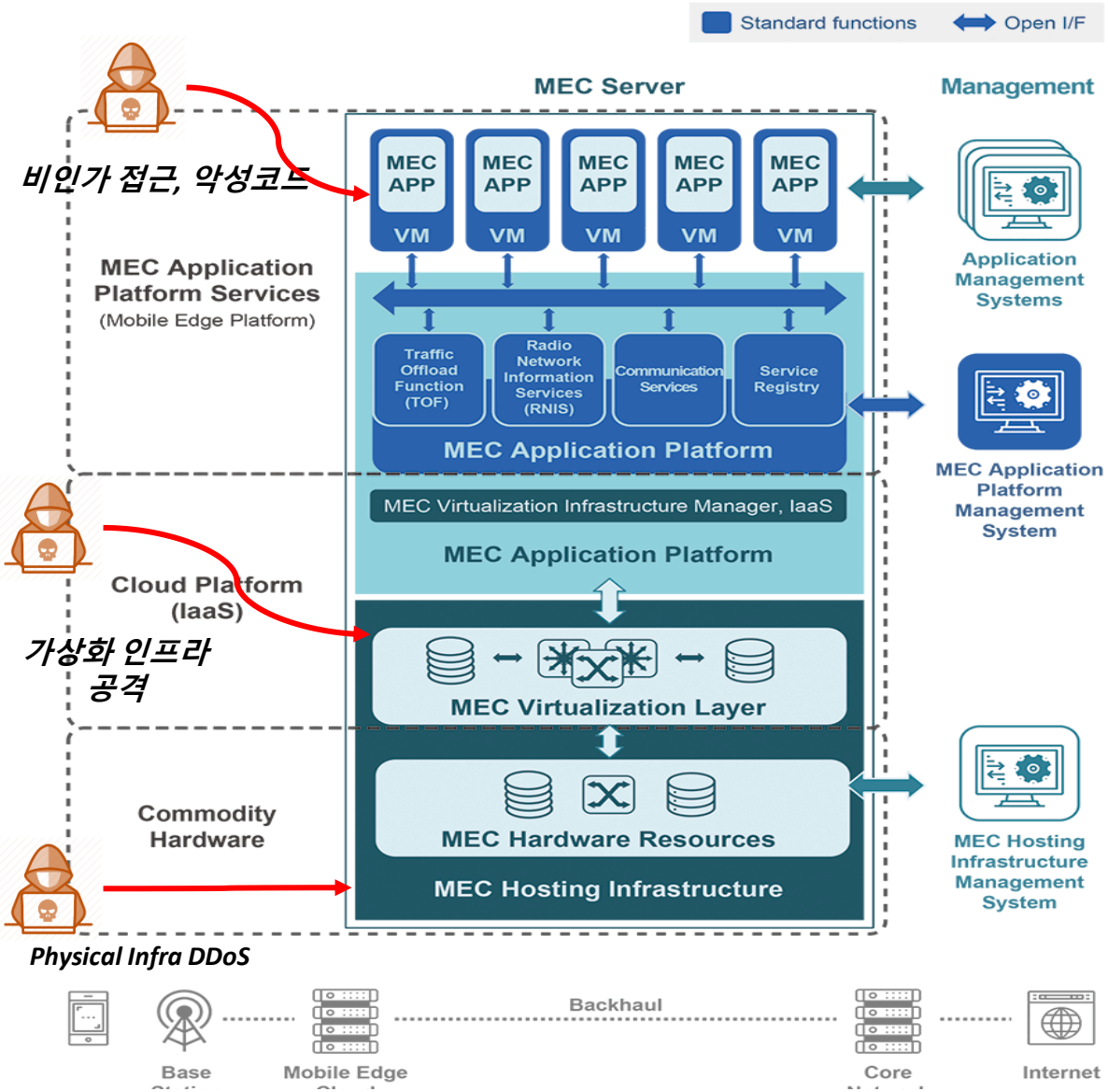
MEC Application : 스마트 공장 자동화, 자율 주행차, CDN, IoT 센서 데이터 처리 등

≫ 이동통신 코어망의 트래픽 부담을 줄이고, **응답시간(단말과 서버간 물리적인 거리로 인해 발생하는 지연시간)**을 줄이기 위해, 사용자와 가까운 위치에서 컴퓨팅 서비스를 제공하여 정보 전달 및 처리 속도를 높이는 '엣지 컴퓨팅' 기술을 이용



* 그림출처 : 기가바이트 홈페이지(https://www.gigabyte.com/)

1.11 5G 특성과 보안이슈 : ④ Cloud based MEC Security



Vertical Security
(Cross-layer Security)

Tenant Security,
3rd Open API
SECURITY
(Vertical Provider)

Virtualization
Platform Security
(Cloud Provider)

UPF 연동 Security
(Telco Provider)

* (좌) 그림출처 : 기가바이트 홈페이지(https://www.gigabyte.com/)

1.12 5G 특성과 보안이슈 : ⑤ Service Based Architecture

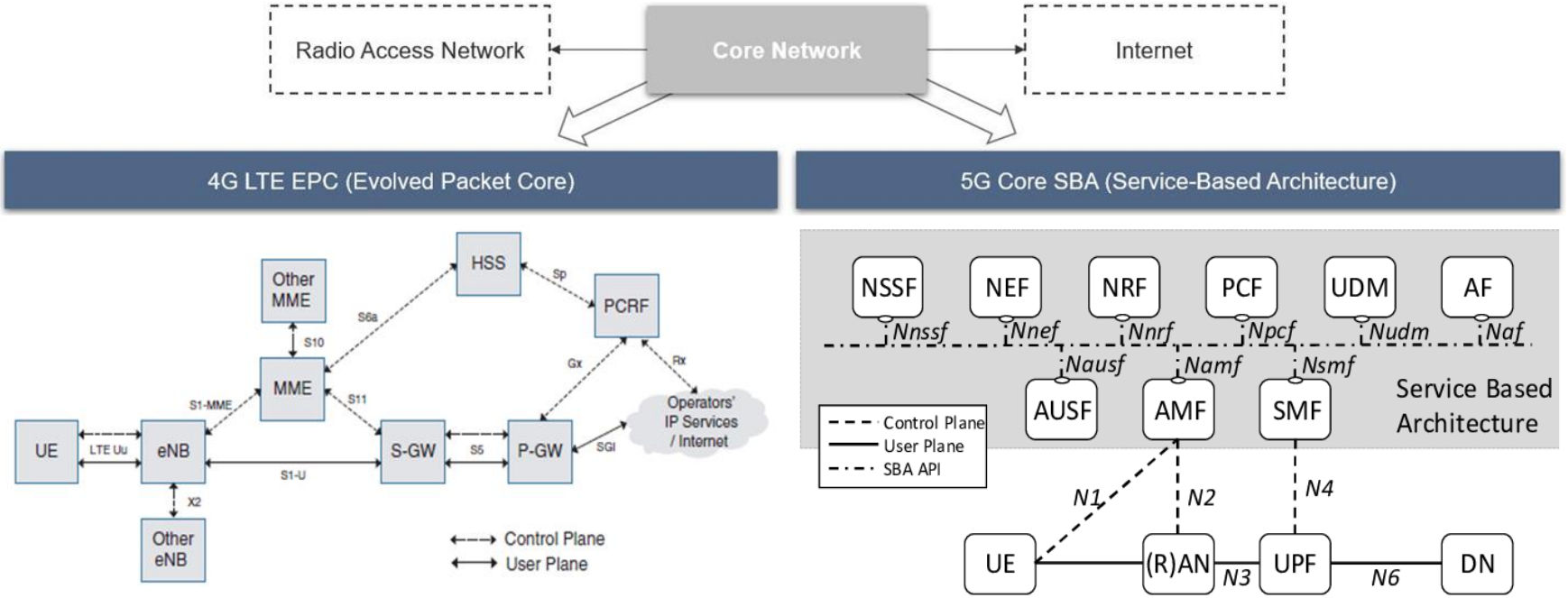
(오픈 API) 다양한 서비스들의 상이한 요구사항 수용을 위해 Service Based Architecture 구조

Security Challenges HTTP/2 · REST API 프로토콜(잘 알려진 웹 취약점 상속) 보안관리

≫ Service based Interface : 물리적 네트워크 기능 및 장비 종속 탈피하기 위한 유연한 구조

≫ 코어 통신장비 간 버스구조의 네트워크 메시지 및 API Call (Service Consumer/Provider 방식) 변화

* 오픈 API : SCEF(Service Capability Exposure Function), NEF(Network Exposure Functions) 등



Dedicated Protocol, Peer to Peer Communication

Common Message Bus & API Communication

* 그림출처: http://telcoaaminto.blogspot.com/

* 그림출처 : Andreas Kunz, IEEE, "5G Evolution of Cellular IoT for V2X"

1.13 5G 특성과 보안이슈 : ⑤ Service Based Architecture

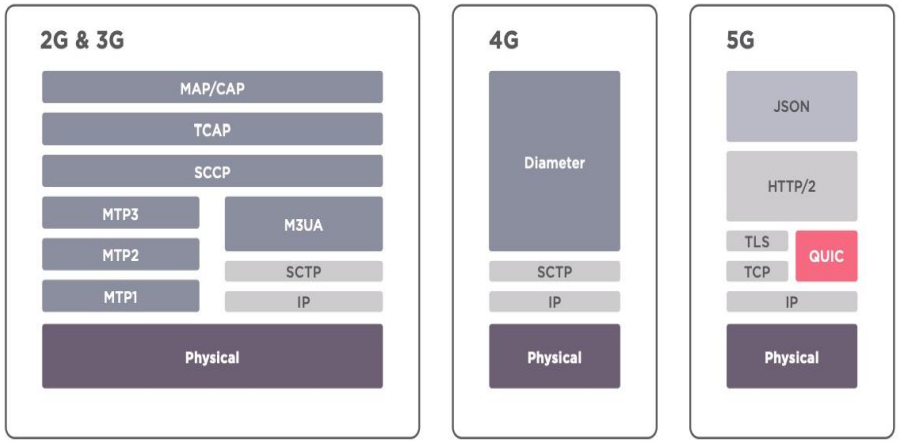
(오픈 API) 다양한 서비스들의 상이한 요구사항 수용을 위해 Service Based 구조 및 API 개방화 채택

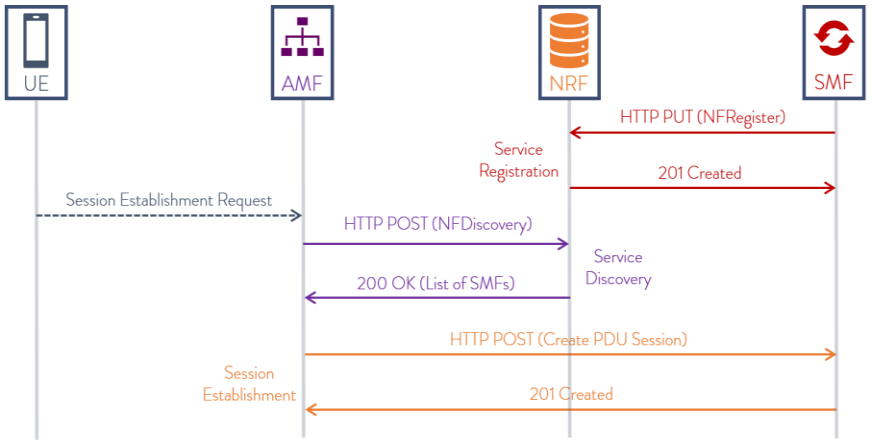
Security Challenges HTTP/2 · REST API 프로토콜(잘 알려진 웹 취약점 상속) 및 API 보안관리

≫ HTTP/2 프로토콜 취약점(DDoS 유발) : 2019년 한해 8건 CVE (high – Severity) 등록

≫ 빠른 웹 응답속도를 위한 HTTP2 over QUIC 채택(Release 16) : 응답속도 효율성 vs 보안 이슈

* UDP 프로토콜 자체에 대한 보안성은 확보된 것으로 보여지나, QUIC reflection DDoS (비정상적 Request 대응)





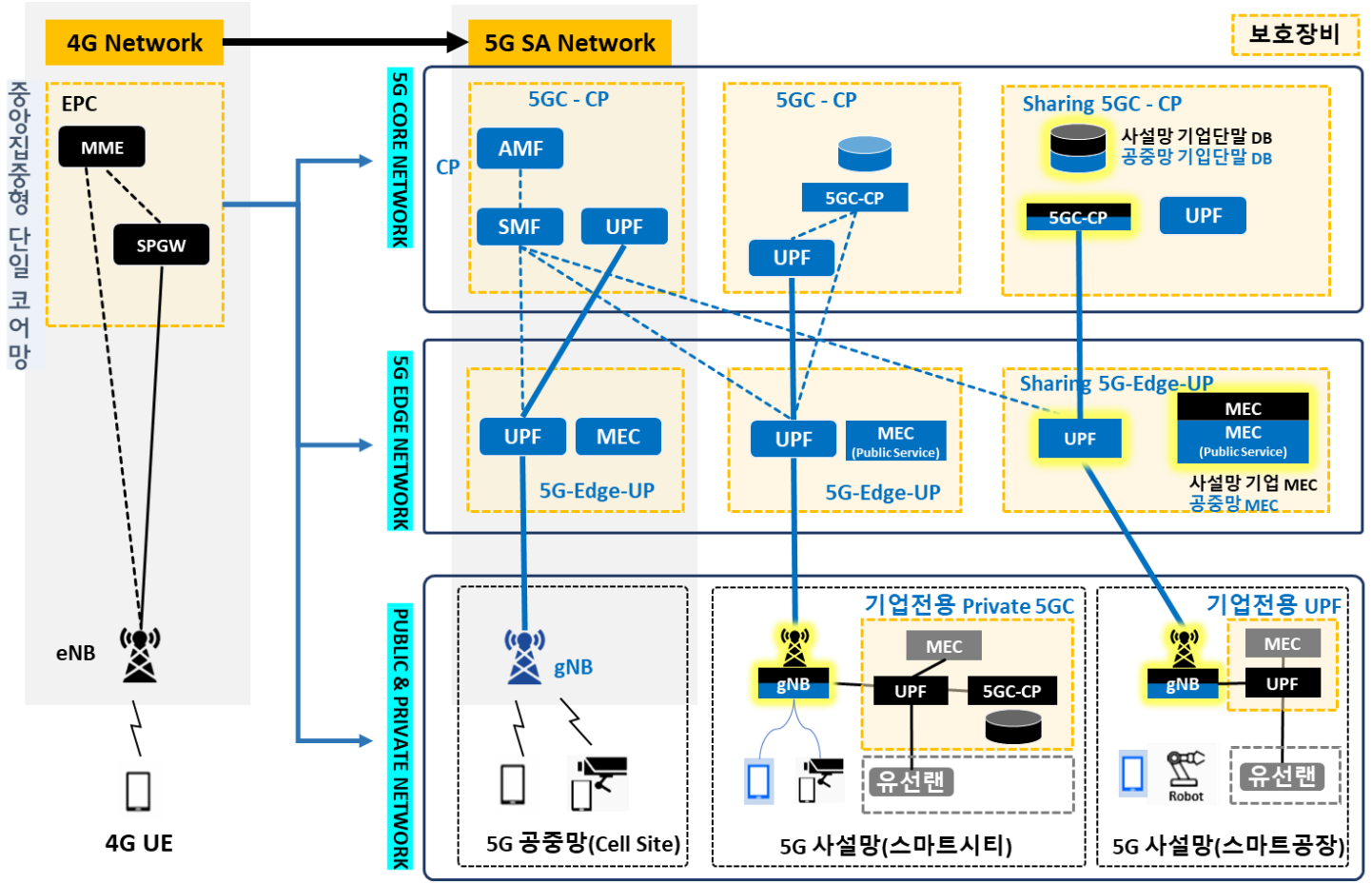
* 그림출처 : https://www.metaswitch.com/

1. CVE-2019-9511 (HTTP/2 "Data Dribble), 2. CVE-2019-9512 (HTTP/2 "Ping Flood“) 3. CVE-2019-9513 (HTTP/2 "Resource Loop“)
4. CVE-2019-9514 (HTTP/2 "Reset Flood“) 5. CVE-2019-9515 (HTTP/2 "Settings Flood“) 6. CVE-2019-9516 (HTTP/2 "0-Length Headers Leak“)
7. CVE-2017-9517 (HTTP/2 "Internal Data Buffering“), 8. CVE-2019-9518 (HTTP/2 "Request Data/Header Flood“)

1.14 5G 특성과 보안이슈 : ⑥ 5G Private Network (사설망)

스마트공장, 스마트시티 등 B2B 서비스 제공을 위해 5G Private Network 구축 예상

Security Challenges 이동통신사 Public 네트워크와 Sharing 되는 장비 보호(UPF, MEC, gNb)



* 그림출처 : 넷마니아 홈페이지(이장우) 그림을 응용하여 재구성함

5G Core Network 보안 고려사항

2.1 5G 보안 취약점 조치 관련 이슈

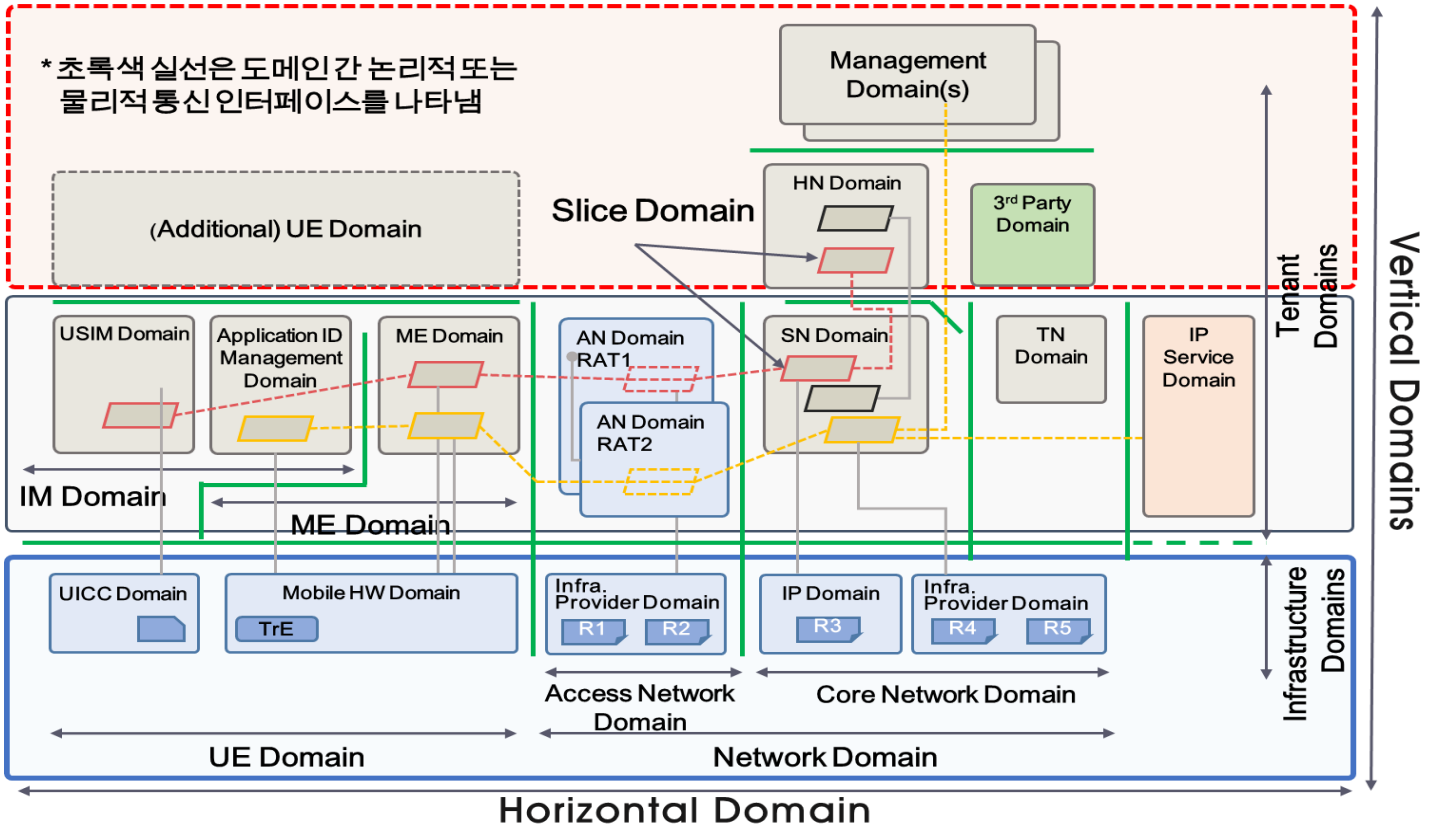
표준화 단계부터 장비 제조사 개발, 구축 및 운영까지 단계별 Security Gap 줄이는 문제

단계	보안 목표	Security Gap
표준화 단계 (Standardization)	국가 간 모바일 네트워크의 상호연동을 위해 안전한 통신 프로토콜 · 인터페이스 설계	**표준 프로토콜 취약점** 기본적 보안 요구사항과 스펙 정의 (필수 or 옵션 형태 존재)
제조사 개발 단계 (Development)	표준에서 요구하는 보안 기준 및 목표 수준에 맞는 장비 및 소프트웨어 개발	**장비 구현상 취약점** 공통기능을 다르게 구현, SW 오류 등
통신 사업자 구축 (Deployment)	안전한 네트워크 및 서비스 설계 및 구축	**구성설정 오류 및 서비스 취약점** 오픈 소스 및 3rd Party SW, 네트워크 및 서비스 구성설정 오류 등
서비스 운영 단계 (Operation)	지능형 사이버공격 탐지 및 모니터링, 침해사고 대응 관리 (권한설정, 자산관리, 취약점 관리, 침해사고 탐지 및 대응, 복구 등)	**운영상 취약점 및 사이버공격** 제로데이 SW 보안취약점 대응, 공급망 보안 검증, 사이버 침해사고 복원력

2.2 개발 및 구축 단계 : 보안 관점에서 5G 생태계 복잡성 이슈

단말–네트워크–서비스 각 도메인 별로 보안을 담당할 다양한 Vertical Domain 존재

<5G ENSURE : Domain overview of the 5G security architecture>



* 출처: 5G PPP ENSURE 프로젝트 : EU, 제조사, 통신사, 서비스사업자, 연구기관이 참여한 5G 연구 수행 기구

* IM(Identify Management), ME(Mobile Equipment), SN (Serving Network), HN(Home Network), TN(Trust Network), IP(Internet Provider), Tenant(물리적 자원 공유하는 임대 사업자)

2.3 (개발 · 구축 단계) 보안 고려사항 : 복잡한 생태계 이슈

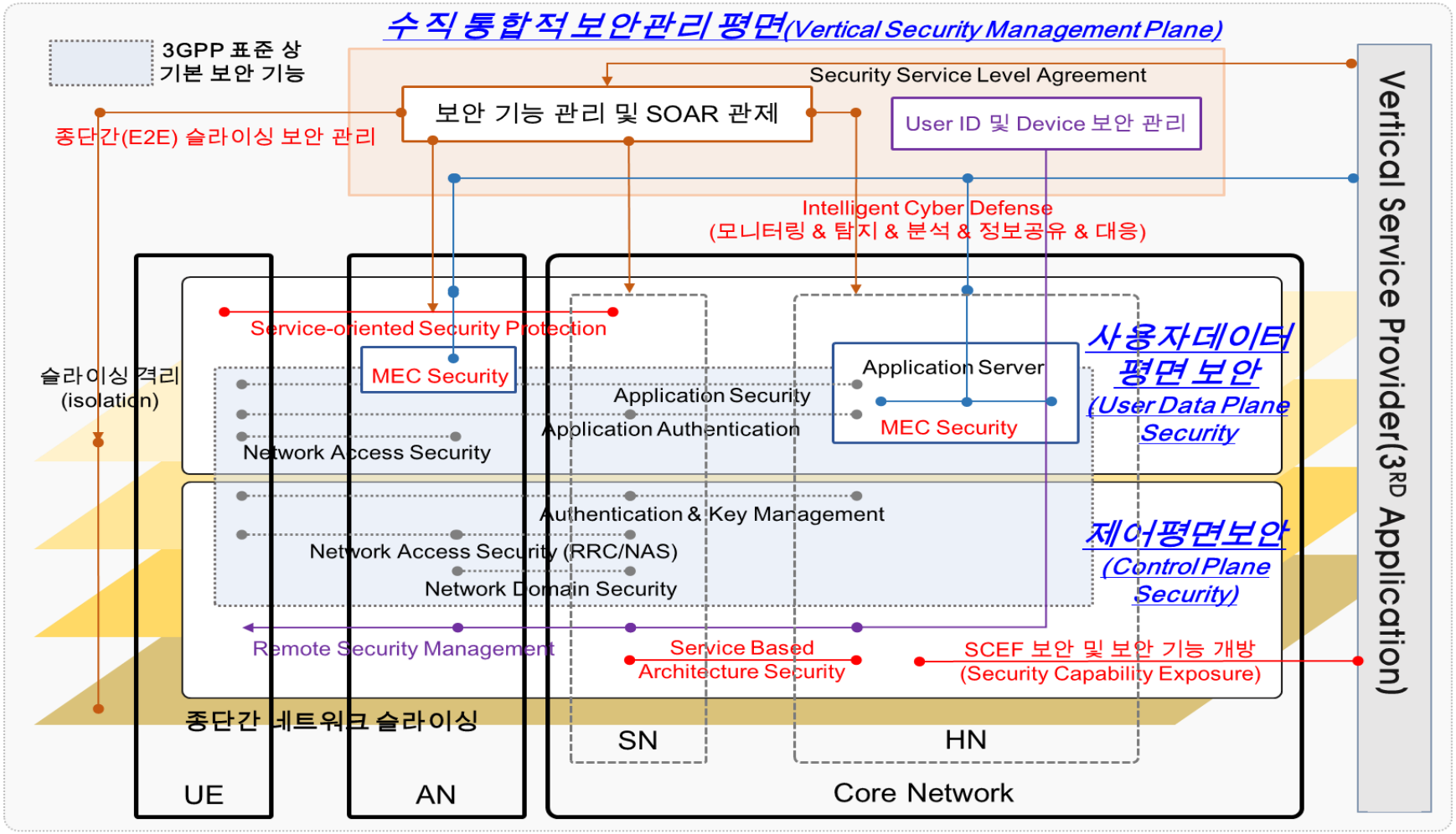
종단 간 보안 중심에서 계층 간 보안 및 멀티 도메인 간 보안 설계가 필요

보안 요구사항	주요 내용
종단 간 보안 (End to end Security)	• 사용자 장치(UE)부터 무선 액세스 및 전송 네트워크를 포함하여 코어네트워크의 종료 지점 간 **수평적 통신 경로에 대한 보안(기밀성, 무결성)을 유지**
계층 간 보안 (Cross-layer Security | Vertical Security)	• 분산되고 유연한 특성은 수평적 도메인 간 경계방어와 종단 간 보안만으로 한계가 있음 • SDN/NFV, 논리적인 네트워크 슬라이싱, MEC 구축 시 : **물리적 계층, 가상화 계층, 어플리케이션 계층 같은 수직적 계층 (Vertical Layer) 존재** • 각각의 계층에 맞는 보안 기술도 효과적이지만 **서로 다른 계층의 보안 기술 조정을 위해 수직적 관점의 보안 통합 프레임 워크가 필요 (Vertical Security)**
멀티 도메인 간 보안 (Domain Security)	• 상호 운용성은 네트워크, 서비스 및 장비 등 **다양한 공급자 도메인의 공존으로 보안 문제 야기** 예) 네트워크 사업자, 가상화 솔루션, MEC 사업자, 3rd 사업자 등 새로운 공급자 도메인간의 보안 솔루션들의 상호 연계를 통해 보안이 구현되어야 함 • 각 도메인 별 계층 간 보안 구현이 되어야 다른 도메인과 안전하게 작동 할 수 있음
보안 내재화 (Security by Design)	• 보안기술은 표준 제정/장비 개발/네트워크 설계 프로세스의 일부로 초기에 고려 및 배포 필요 • 시스템이 완전히 구축되어 운영될 때 발생되는 잠재적 **보안 갭 차이를 최소화를 위해 DevOpsSec 개발 방법론 적용이 필요**

* 출처 : 영국 정부(DCMS)의 5G Network Security Architecture 보안 요구사항을 인용하여 재정리함

2.4 (운영 단계) 지능형 사이버공격 방어 프레임워크

Top-down Security



* UE(사용자 장치), AN(Access Network), SN(Serving Network), HN(Home Network)

* 출처 : 화웨이 "5G Security Architecture Framework" 내용과 그림을 인용하여 재수정함

2.5 지능형 사이버공격 방어를 위한 고려사항

도메인 별 Physical 장비(단일 솔루션) 중심의 사이버공격 방어 메커니즘에서
분산 방어, 유연하고 확장 가능 방어, 수직 계층적,자동 보안관제 접근이 중요

단계	주요 내용
(도메인 관점) 분산 사이버공격 방어기술 (Distributed Security)	• 제어 트래픽과 사용자 데이터 트래픽 분리되어 서로 다른 경로로 여러 도메인을 걸쳐 전송 • 각 도메인별 (엑세스 네트워크, 코어 네트워크) 보안위협과 요구되는 보안 수준이 상이 • 잠재적인 공격 지점에 가까운 위치에 탐지 및 대응기능을 분산배치가 필요 • 예) Massive IoT DDoS 에 의한 RAN 공격 방지를 위해 기지국 또는 에지 네트워크 배치
(기능 관점) 유연하고 확장 가능 방어기술 (Flexible Security)	• 각 서비스 슬라이싱 별 **차등화 된 보안 기능의 구성과 호출이 유연하게 적용** (슬라이스별 인증 방법과 암호화 차등 지원, 어플리케이션 레벨 종단 간 보안을 선택 가능) • 네트워크 슬라이스 상에서 사이버공격 탐지와 완화 그리고 슬라이싱 간 격리 (isolation) 등 동적으로 모니터링이 되고 대응 정책이 통합 관리 되어야 함
(관제 관점) 수직 계층적 보안관제 자동화 기술 (Security Orchestration & Automation Response)	• 멀티 도메인 상에서 논리적 수직적 계층(Cross-layer)에 걸쳐 보안이 다루어 지므로, 도메인에 걸친 수직 계층 간 보안을 관리하고 사이버공격을 통합 모니터링/탐지하는 체계 • 수직 보안관리 : 각 도메인별 기본 보안 기능(로그분석), 3rd 수직적 서비스 사업자에게 개방되는 API 보안, 원격 IoT 보안관리, Service-oriented 보안, MEC 보안 등 포괄 • 복잡한 보안 가시성 문제 : 보안 오케스레이션 및 AI 기술을 활용한 자동화 개념 적용(SOAR)

감사합니다

rinyfeel@smu.ac.kr