KISA 한국인터넷진흥원

# 5G 보안 위협 대응 3GPP 표준 동향


2021.06.04

권성문

인프라보안기술팀

*skwon@kisa.or.kr*

# Content



KISA 한국인터넷진흥원

# Content

# 1.1 사업개요

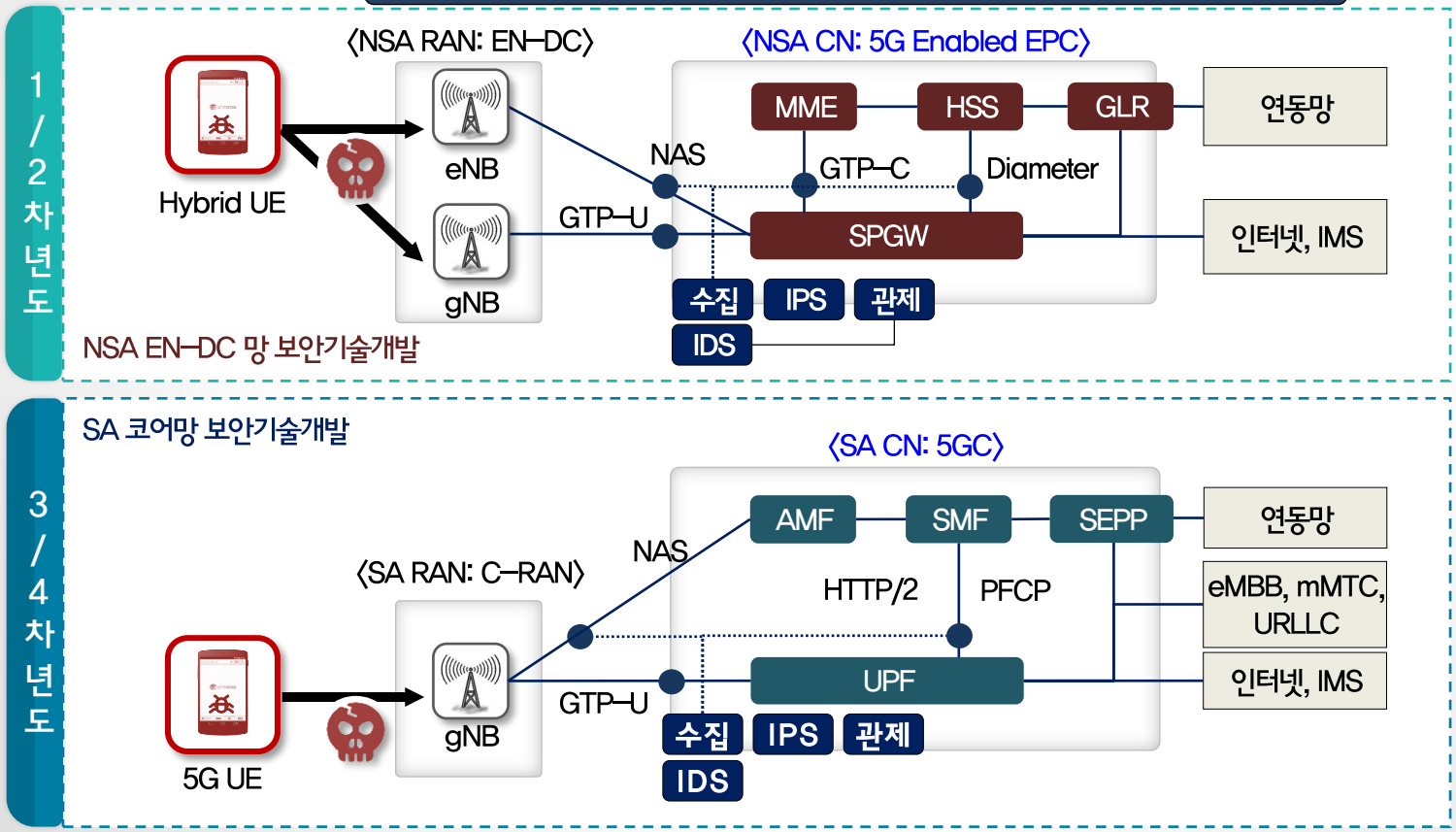
| | |
|---|---|
| 과제명 | 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술 개발 |
| 총 연구기간 | 2019. 4. 1. ~ 2022. 12. 31. (총 45개월) |
| 총 연구비 | 총 87.73억원 (정부출연금 70.1억원 + 민간부담금 17.63억원)<br>1차년도 17.41억원 (정부출연금 14억원 + 민간부담금 3.41억원)<br>**2차년도 21.81억원 (정부출연금 17.4억원 + 민간부담금 4.41억원)**<br>3차년도 23.44억원 (정부출연금 18.7억원 + 민간부담금 4.74억원)<br>4차년도 23.44억원 (정부출연금 18.7억원 + 민간부담금 4.74억원) |
| 주관 연구기관 | 한국인터넷진흥원 |
| 참여 연구기관 | SKT㈜, ㈜LG U+, ㈜KT, ㈜모비젠, ㈜윈스, ㈜루테스, 한국과학기술원, 순천향대학교 |
| 연구 책임자 | 한국인터넷진흥원 인프라기술보안팀 김도원 팀장 |

# 1.2 최종 연구 목표

## 5G망 DDoS, 구성 설정오류 및 프로토콜 취약점을 악용한 공격으로부터 5G 코어망 인프라를 보호하기 위한 보안기술 (탐지·차단·모니터링) 개발

- 최종 결과물 : ① 5G 코어망 트래픽 수집 기술, ② 5G 비정상 공격 탐지 및 차단 기술(5G IDS, 5G IPS), ③ 5G 보안 관제 및 모니터링 시스템, ④ 5G 보안 취약점 연구, ⑤ 국제 표준화 연구

### 지능형 5G 코어망 비정상 공격 탐지 및 대응 기술




SKT, LGU+, KT
**통신사 실증**

DDoS 스캐닝
무선자원고갈
외부 무단 접근
프로토콜 취약점
**보안취약점 연구**

3GPP, ITU-T
**국제표준화**

# 1.3 5G 보안 취약점 대응 및 완화 전략

# Content

# 2.1 5G 보안 취약점 발굴 및 대응

- 코어망 대상 보안 위협 : 표준 또는 구현 상의 취약점을 사용하여 DoS 유발
- 가입자 대상 보안 위협 : 표준 상의 취약점 또는 중간자 공격을 통해 가입자 정보 탈취 및 메시지 위변조

- **정책적 대응** 5G 보안 핵심기술 확보를 위한 ITU-T·3GPP 국제 표준화 (제안 10건, 채택 7건)
- **기술적 대응** 신규 보안 취약점 연구/실증 추진(13건), 기술 개발 및 적용을 통한 사전 위협 대응

| 구간 | 주요 보안위협 | 개발도구 | 테스트 시나리오 | 대응방법 |
|---|---|---|---|---|
| 제어 | RRC DoS | LTE Fuzz | 피해자와 기지국 간에 MitM 설정 후 RRC 메시지 변조 | 국제 표준화 (ITU-T, 3GPP) |
| | NAS 비암호화 채널 | | 피해자와 기지국 간에 MitM 설정 후 NAS 메시지 변조 | 기술 개발 (비암호화 채널 탐지) |
| 사용자 | 장비 스캐닝 | Exploit App. | 패킷을 변조하여 망 장비 스캔 | 기술 개발 (Scanning 탐지) |
| | GTP 자원고갈 | | GTP 메시지를 변조하여 코어망 자원(IP) 고갈 | 기술 개발 (GTP-in-GTP 탐지) |
| | SIP 스푸핑 | | SIP 메시지의 전화번호를 조작하여 피싱 | 기술 개발 (SIP Spoofing 탐지) |
| 연동망 | SS7/Diameter IMSI 탈취 | 오픈 소스 (jss7) | SendIMSI 메시지를 조작하여 IMSI 탈취 | 기술 개발 (비정상 Diameter 탐지) |
| | SS7/Diameter 위치변경/문자탈취 | | Update Location 메시지를 조작하여 피해자 위치변경 후 문자 탈취 | |

표준화 ← 국제 표준화 (ITU-T, 3GPP)

IDS ← 기술 개발 (비암호화 채널 탐지), 기술 개발 (Scanning 탐지)

IPS ← 기술 개발 (GTP-in-GTP 탐지), 기술 개발 (SIP Spoofing 탐지), 기술 개발 (비정상 Diameter 탐지)

# 2.2 5G 코어망 보안 위협 – 허위 기지국과 중간자 공격

- 허위 기지국(FBS – False Base Station)을 이용한 중간자 공격

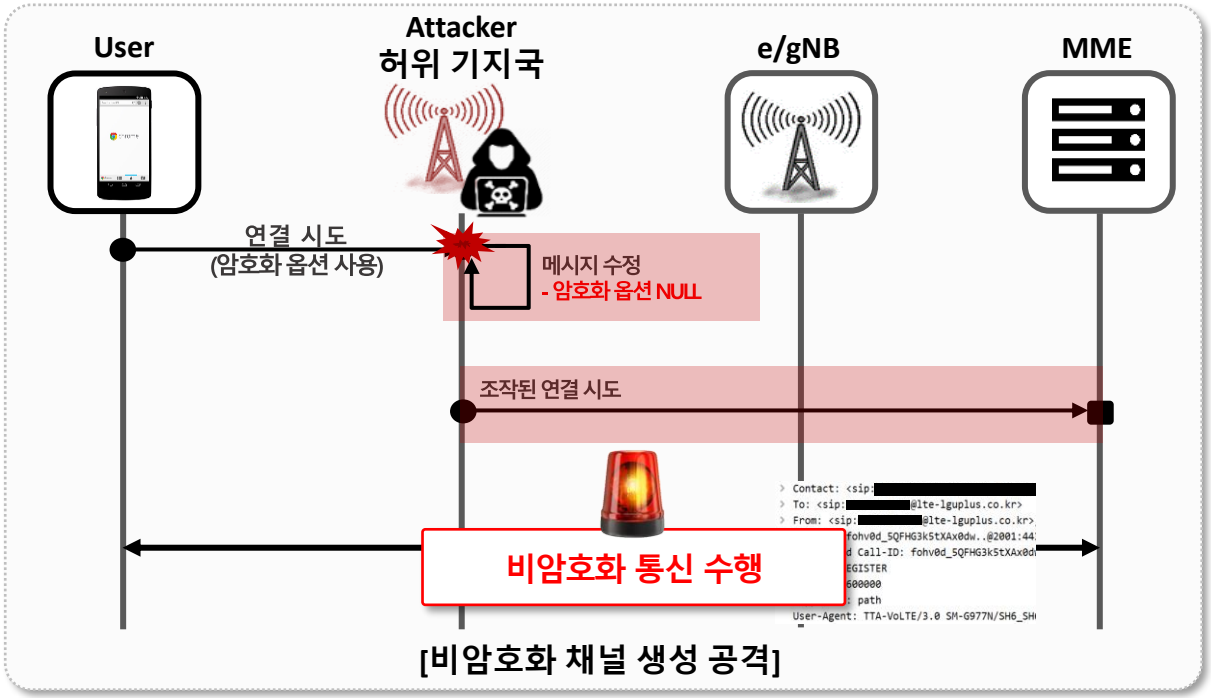
  1) 중간자 공격을 위해 공격자는 피해자 주변에 신호 세기가 강한 허위 기지국 설치

  2) 피해자는 통신사 기지국보다 신호 세기가 강한 공격자의 허위 기지국으로 망 접속 시도

  3) 공격자는 허위 기지국으로 전송된 메시지를 가로채어 위변조 후 통신사 기지국에 전송

- 비암호화 채널 생성 공격

  – 중간자 공격으로 피해자 단말이 망 접속 시 암호화 옵션을 NULL으로 전송하여 비암호화 채널 생성을 유도하여 도청 수행

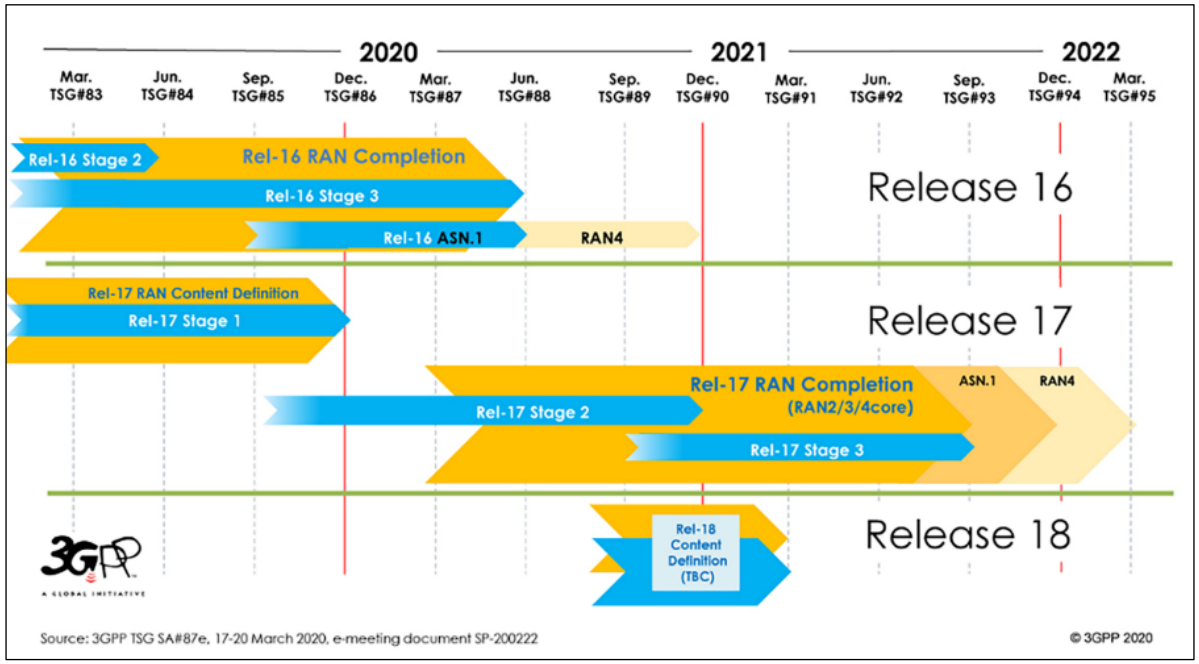



[비암호화 채널 생성 공격]

# Content

# 3.1 3GPP 5G 표준 현황

- 3GPP 표준화 : R15 – ’19.3월 Freezing / R16 – ’20.7월 Freezing / R17 – ’22.3월 Freezing 예정
- 5G 주요 표준
  - 5G 시스템 : 3GPP TS 23.501, System architecture for the 5G system
  - 5G 절차 : 3GPP TS 23.502, Procedures for the 5G system
  - 5G 보안 : 3GPP TS 33.501, Security architecture and procedures for 5G system
  - 5G NF 별 보안 : 3GPP TS 33.511 ~ TS 33.519, Security Assurance Specification for NF



# 3.2 3GPP TR – Technical Report

- 3GPP TR(Technical Report) XX.8XX, XX.9XX
  - 표준 적용 이전 단계로 특정 기술의 적용 가능성을 검토한 결과를 정리한 보고서 등

- 3GPP TR 33.8XX, 5G 보안 기술 보고서 – 36종
  - 5G 특화/신규 서비스의 보안 강화를 위한 기술 보고서
    - 3GPP TR 33.813, Study on security aspects of network slicing enhancement
    - 3GPP TR 33.825, Study on the security of Ultra-Reliable Low-Latency Communication for the 5G System
    - 3GPP TR 33.851, Study on security for enhanced support of Industrial Internet of Things
    - 3GPP TR 33.861, Study on evolution of Cellular Internet of Things security for the 5G System
  - 신규 보고되는 취약점을 보완하기 위한 기술 보고서
    - 3GPP TR 33.809, Study on 5G security enhancements against False Base Stations
    - 3GPP TR 33.814, Study on the security of the enhancement to the 5G Core location services
    - 3GPP TR 33.853, Key issues and potential solutions for integrity protection of the User Plane

# Content

# 4.1 3GPP TR 33.809 개요

- 3GPP TR 33.809, Study on 5G Security Enhancement against False Base Stations
  - 허위 기지국에 대한 보안 이슈와 이에 대한 대응 기법을 기술하고 있는 기술 보고서
  - Apple 주도하에 Samsung, Ericsson, Qualcomm, Huawei, ZTE, Lenovo 등 5G 관련 다수의 기업이 참여
  - 2018.11 작성을 시작하여 가장 최신 버전은 “Detection of Man-in-the-Middle false base station”, “PKC를 이용한 보안 기법” 이 추가된 2021.03, V0.14.0
  - 아직 일부 공란이나 업데이트가 필요한 부분이 있으며 꾸준히 작업이 수행되고 있음

- 3GPP TR 33.809 Key Issues – 7항목,
  - Key issue details, Security Threats, Potential Requirements로 구성
    - Key issue details : 보안 이슈 사항 설명
    - Security Threats : 해당 보안 이슈로 인해 발생 할 수 있는 보안 문제
    - Potential Requirements : 보안 이슈를 해결하기 위한 요구사항 기술
- 3GPP TR 33.809 Candidate Solutions – 26항목
    - Solution details, Evaluation으로 구성
    - Solution details : 보안 기술 설명
    - Evaluation : 해당 보안 기술의 유효성 평가

# 4.2 3GPP TR 33.809 Key Issues (1/2)

- KI #1 : Security of unprotected unicast message
  - RRC UE Capability Enquiry, NAS Reject 등 암호화 기능이 사용되지 않는 메시지에 대한 위변조 위험성
  - 사용자 단말에 대한 DoS나 서비스 속도 저하 유발 가능
- KI #2 : Security protection of system information
  - System Information(SI) 메시지란 기지국이 주기적으로 Broadcasting 하는 셀 정보로 사용자 단말이 셀 재선택 등을 통해 효율적인 서비스를 이용할 수 있도록 하는 메시지
  - System Information 메시지에 보안이 적용되지 않아 허위 기지국이 가짜 System Information 전송 가능
  - 사용자 단말에 대한 DoS
- KI #3 : Network detection of false base stations
- KI #7 : Protection against Man-in-the-Middle false gNB attacks
  - 허위 기지국을 통한 MITM 등 일반적인 보안 문제 설명
  - 사용자 단말과 네트워크에 대한 DoS, 위변조, 사용자 단말 정보 노출 등

# 4.2 3GPP TR 33.809 Key Issues (2/2)

- KI #4 : Protection against SON poisoning attempts
  - Self-Organizing Networks(SON) 기술이란 2008년 3GPP LTE 표준에 포함되어 현재 RAN 단에서 사용되고 있는 기술로 Self-Configuration, Self-Optimization, Self-healing을 수행
  - SON 기술에 있어 기지국이 사용자 단말에 전송하는 Synchronization Signal Block 시그널에 대해서는 보안이 적용되지 않아 허위 기지국이 위변조 가능
  - 사용자 단말과 네트워크에 대한 DoS 유발 가능
- KI #5 : Mitigation against the authentication relay attack
  - 허위 기지국과 다른 장소에 위치한 공격자의 단말이 사용됨
  - 피해자의 단말이 허위 기지국으로 접속 시 망 접속 메시지를 가로채어 공격자의 단말로 전송, 공격자의 단말이 망에 접속
  - 거짓 알리바이 생성, 과금 유도 등 유발 가능
- KI #6 : Resistance to radio jamming
  - Multiple-input and Multiple-output(MIMO) Beamforming, Dedicated network slice, Self-healing 등의 5G 기능으로 Radio jamming에 대한 내성을 어느정도 가지고 있어 본 표준에서는 상세히 다루지 않음

# 4.3 3GPP TR 33.809 Solutions (1/2)

- 중간자 공격 내성을 가지도록 보안 기능 강화
  - Solution #1: Protection for the UE Capability Transfer
  - Solution #2: Protection of RRCReject message in RRC_INACTIVE state
  - Solution #3: Protection of uplink UECapabilityInformation RRC message
  - Solution #7: Verification of authenticity of the cell
  - Solution #9: Using symmetric algorithm with assistance of USIM and home network
  - Solution #10: Protection on the unicast message based on EC오
  - Solution #11: Certificate based solution against false base station
  - Solution #12: ID based solution against false base station
  - Solution #13: Protecting RRCResumeRequest against MiTM
  - Solution #14: Shared key based MIB/SIBs protection
  - Solution #16: Protection of RRC Reject Message
  - Solution #17: Integrity protection of the whole RRCResumeRequest message
  - Solution #19: AS security based MIB/SIBs integrity information provided by gNB
  - Solution #20: Digital Signing Network Function (DSnF)
  - Solution #21: Certificate based solution against false base station for Non-Public Networks
  - Solution #23: Cryptographic CRC to avoid MitM relay nodes
  - Solution #26: KI#2 with PKC-based and without tight time synchronization

# 4.3 3GPP TR 33.809 Solutions (2/2)

- 허위 기지국 탐지
  - Solution #4: Enriched measurement reports
  - Solution #5: Mitigation against the authentication relay attack
  - Solution #6: Avoiding UE connecting to false base station during HO
  - Solution #8: Network detection of nearby false base stations from call statistics and measurements
  - Solution #15: Mitigation against the authentication relay attack with different PLMNs
  - Solution #18: Avoiding UE connecting to False Base Station during Conditional Handover
  - Solution #22: Detecting false base stations based on UE positioning measurements
  - Solution #24: UE&Network-assisted UE avoidance and Network detection of FBS
  - Solution #25: Detection of Man-in-the-Middle false base station

# 4.4 3GPP TR 33.809 Key Issues and Solutions

- KI #1 : Security of unprotected unicast message
  - Solution #1, 2, 3, 9, 10, 11, 12, 13, 16, 17, 21
  - 해당 이슈에 대한 논의 완료
- KI #2 : Security protection of system information
  - Solution #7, 9, 11, 12, 14, 19, 20, 21, 26
- KI #3 : Network detection of false base stations
  - Solution #4, 6, 8, 18, 22, 23, 24, 25
- KI #4 : Protection against SON poisoning attempts
  - TBD
- KI #5 : Mitigation against the authentication relay attack
  - Solution #5, 15, 23
- KI #6 : Resistance to radio jamming
  - None, 해당 이슈에 대한 논의 완료
- KI #7 : Protection against Man-in-the-Middle false gNB attacks
  - Solution #23

# Content

# 5.1 향후 5G 보안 표준의 방향

현재 5G 핵심 구조에 대한 기능적 정의는 모두 된 상태

5G 핵심 구조에 대해서는
Security Assurance Specification과 같은 각 NF에 대한 보안 표준이 논의되고 있음

기존 정의된 핵심 기능에 대한 심층적인 보안 분석에 따라
가용성과 보안성을 고려한 기능 개선이 예상됨

이외 Network Slice와 신규 5G 서비스에 대해서는
기술 적용을 통해 주요 기능 및 보안에 대해 논의될 예정

# 5.2 참고문헌


- Draft new Report ITU-R M.[IMT-2020.TECH PERF REQ] - Minimum requirements related to technical performance for IMT-2020
- Cisco Systems, Innovation Towards SP Transformation, Cisco Connect 2018
- HP Enterprise, 5G A new Ocean of Opportunities, Leti Innovation Days 2018
- Netmanias, 5G Network Architecture
- Cisco, 5G Security Innovation with Cisco (WP)
- NDSS 2019, Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information
- IEEE S&P 2019, Touching the Untouchables Dynamic Security Analysis of the LTE Control Plane
- USENIX 2020, Call Me Maybe: Eavesdropping Encrypted LTE Calls With REVOLTE
- IJWGS 2017, Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment
- Shmoocon 2020, 5G protocol vulnerabilities and exploits
- ACM WiSec 2019, LTE Security Disabled – Misconfiguration in Commercial Networks
- ACM CCS 2019, 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol
- Positive Technologies 2020, 5G Standalone core security research

KISA 한국인터넷진흥원

# Internet On, Security In!

## 감사합니다

# A.1 IMSI Cracking : Side Channel Attack

## 단말의 Paging 알고리즘을 악용하여 IMSI Cracking이 가능한 보안 위협

- ① PFI 확인 : 공격자는 브로드캐스팅되는 Paging 메시지를 스니핑
- ② IMSI Cracking : PFI를 통해 피해자 IMSI를 후보군을 추출하고 IMSI Paging

※ 참고 표준 : 3GPP TS. 36.211

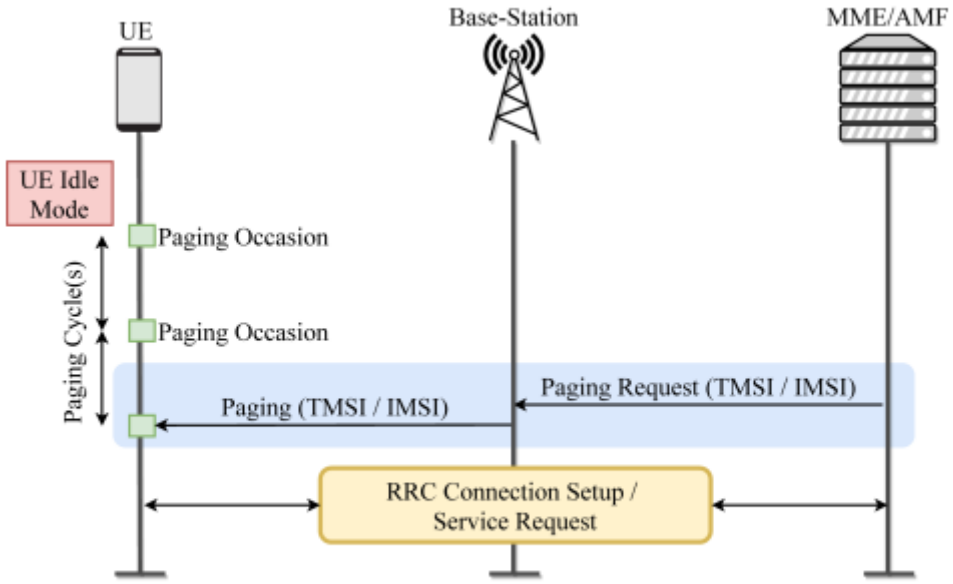



Fig. 2. Paging Procedure.

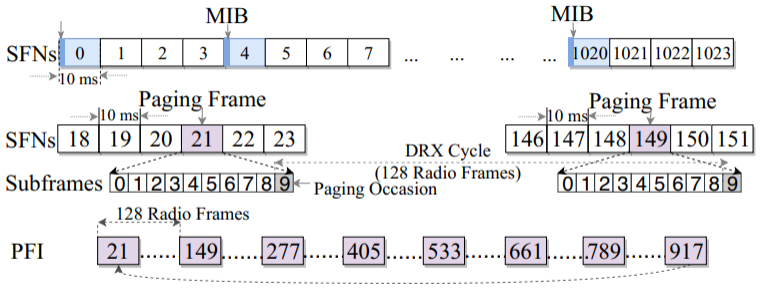



**Fig. 2:** Network time/frame synchronization, and paging frame and paging occasion calculation.

$$\text{PFI} = \frac{\text{T}}{N} \times (\text{UE\_ID mod } N) \text{ where } N = \min(\text{T}, \text{nB}).$$

Equivalently,

$$\text{PFI} = \begin{cases} \text{UE\_ID mod T} & \text{when T} \leq nB \\ \frac{\text{T}}{\text{nB}} \times (\text{UE\_ID mod nB}) & \text{when T} > \text{nB} \end{cases}$$

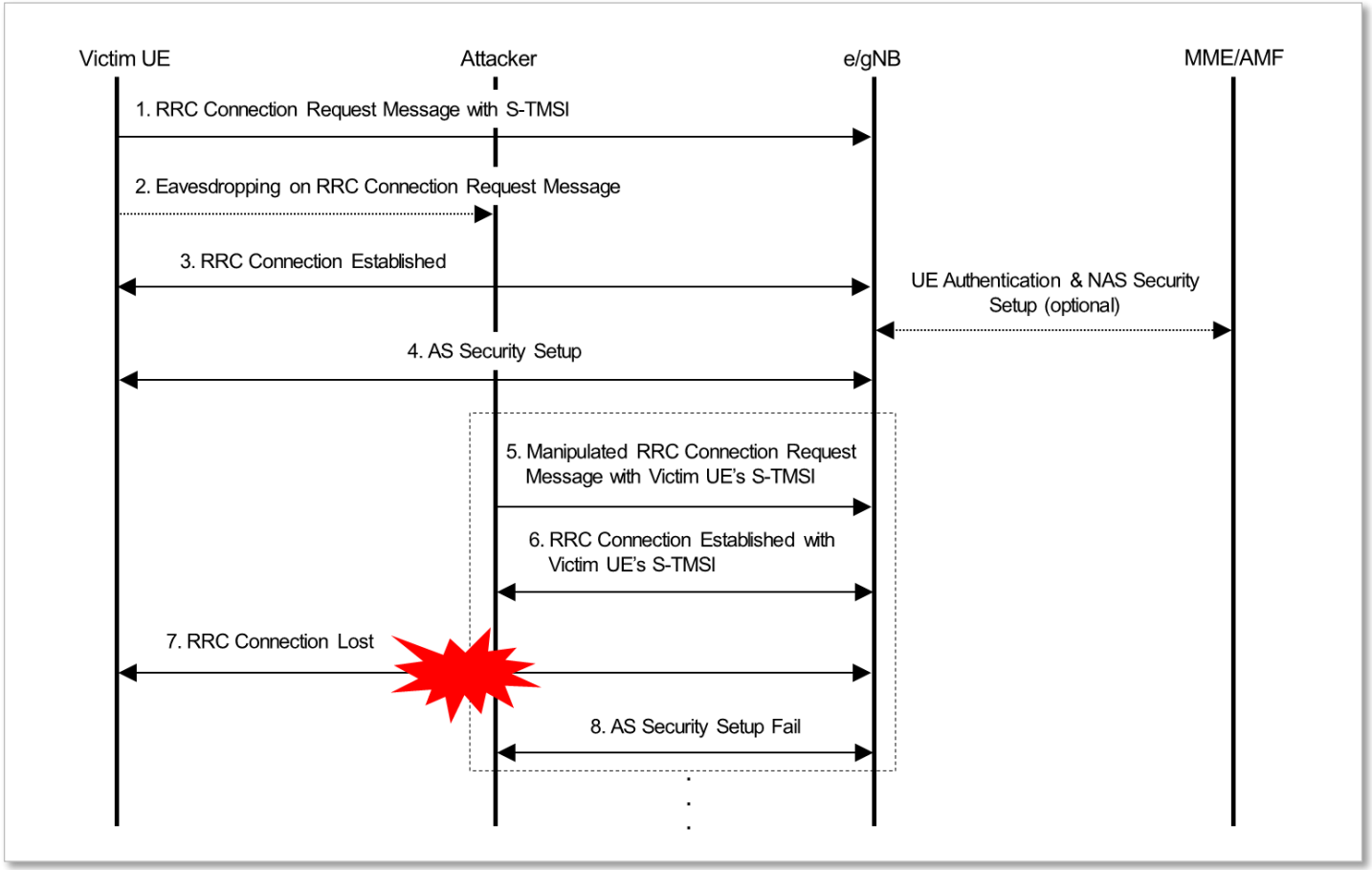
※ PFI (Paging Frame Index), UE ID = IMSI, T = 1024
※ Another public parameter (nB)는 기지국에서 선정
= {4T, 2T, T, T/2, T/4, T/8, T/16, T/32}

* 출처 : NDSS 2019, Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information

# A.2 RRC DoS : LTE Fuzz

UE 주위에 False Base-station 설치하고 피해자 ID를 탈취하여 RRC DoS 유발

- RRC 메시지 내 피해자의 TMSI를 삽입하고 피해자가 접속된 기지국으로 전송하여 기존 무선 연결 해제

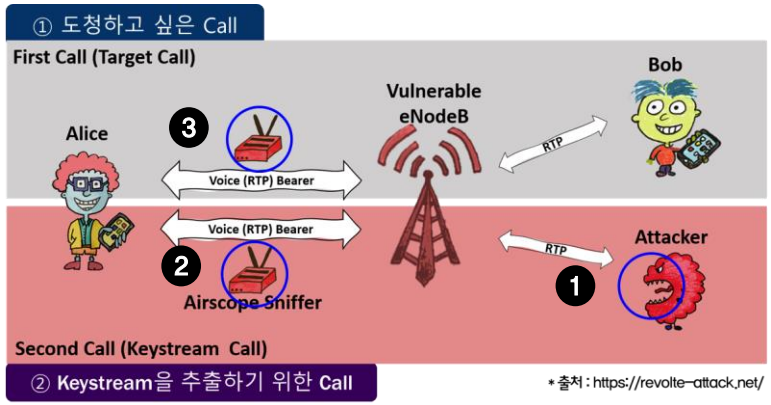



* 출처 : IEEE S&P 2019, Touching the Untouchables Dynamic Security Analysis of the LTE Control Plane

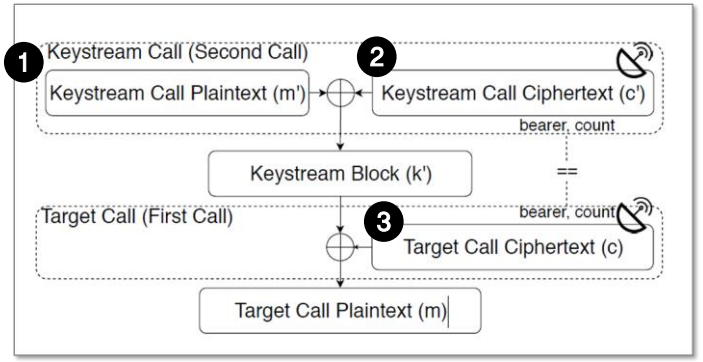
# A.3 ReVolte(1/2) : Eavesdropping in AS Security

## 5G NSA 망에서 단말과 기지국간 무선 구간 보안(AS Security) 채널 설정

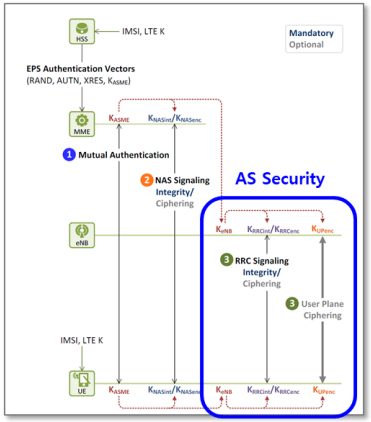
- 단말과 기지국사이의 무선 구간에서 사용자 트래픽(음성통화 등) 암호화를 위한 Keystream 생성
- Call Keystream이 동일한 경우 → 도청하고 싶은 Call 과 동일한 Keystream을 사용해 복호화 가능



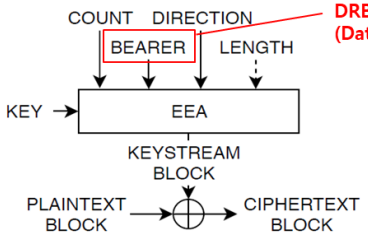

* 출처 : https://revolte-attack.net/




* 출처 : USENIX 2020, Call Me Maybe: Eavesdropping Encrypted LTE Calls With REVOLTE




* 출처 : Netmanias




※ 출처: 3GPP TS. 33.401

For each radio bearer an independent counter (COUNT, as specified in TS 36.323 [8]) is maintained for each direction. For each DRB, the COUNT is used as input for ciphering. For each SRB, the COUNT is used as input for both ciphering and integrity protection. It is not allowed to use the same COUNT value more than once for a given security key. In order to limit the signalling overhead, individual messages/ packets include a short sequence number (PDCP SN, as specified in TS 36.323 [8]). In addition, an overflow counter mechanism is used: the hyper frame number (TX_HFN and RX_HFN, as specified in TS 36.323 [8]). The HFN needs to be synchronized between the UE and the eNB. The eNB is responsible for avoiding reuse of the COUNT with the same RB identity and with the same $K_{eNB}$, e.g. due to the transfer of large volumes of data, release and establishment of new RBs. In order to avoid such re-use, the eNB may e.g. use different RB identities for successive RB establishments, trigger an intra cell handover or an RRC_CONNECTED to RRC_IDLE to RRC_CONNECTED transition.

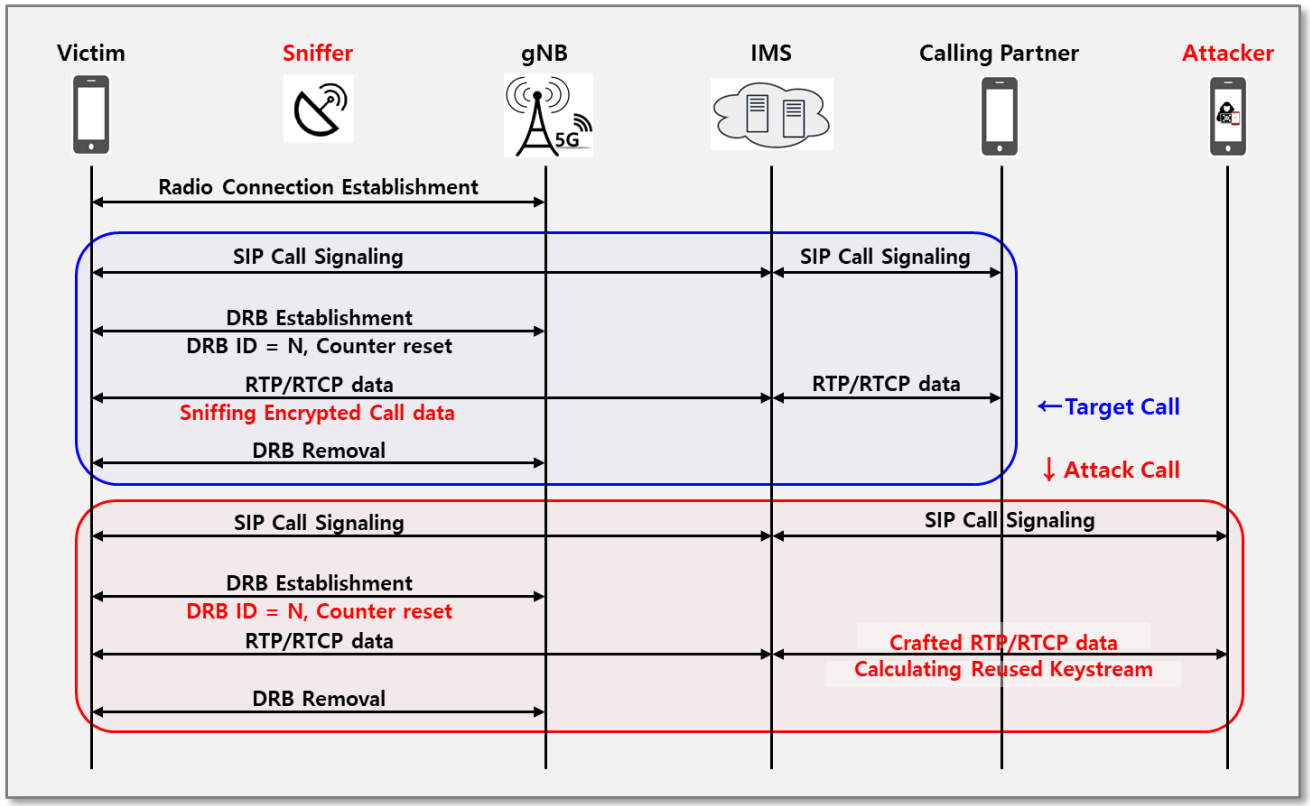
due to the transfer of large volumes of data, release and establishment of new RBs. In order to avoid such re-use, the eNB may e.g. use different RB identities for successive RB establishments, trigger an intra cell handover or an RRC_CONNECTED to RRC_IDLE to RRC_CONNECTED transition.

# A.3 ReVolte(2/2) : Attack Call Flow

## 동일한 무선 연결(RRC Connection) 내 재통화하는 경우 동일한 Seed 생성

- 무선 연결은 6~8초간 지속되는데 이 시간 내 재통화시 동일 DRB ID가 할당되고 동일한 Keystream 생성

동일한
RRC Connection
↓
DRB ID동일

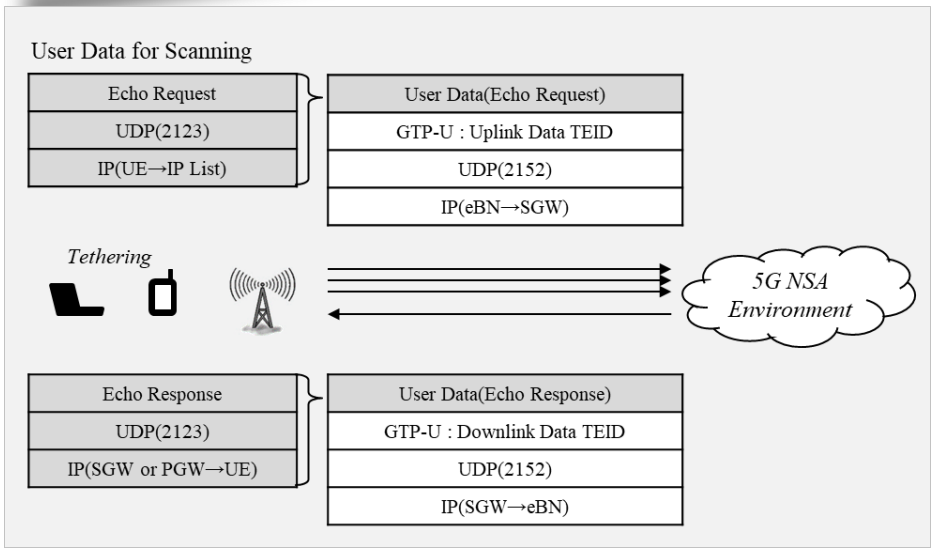


# A.4 메시지 Injection : GTP-in-GTP

## 시그널링 메시지를 데이터 페이로드에 Injection

- ① GTP-C(Echo Request)를 Payload 로 가지는 패킷 생성(packit), IP 대역 스캐닝(tracert)
- ② 스캐닝된 대역대로 생성한 패킷을 전송하면 응답(Echo Response)을 보내는 IP가 존재 (MME or SPGW)

### 5G NSA 망 메시지 Injection 공격




*출처 : IJWGS 2017 , Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment

### ①-1 패킷 생성

```
packit -t UDP -s [redacted]55 -S 2123 -d
[redacted].23 -D 2123 -p '0x48 0x22 0x00 0x24
0x29 0x6a 0xe0 0x20 0x01 0x4c 0xc8 0x00 0x4d
0x00 0x02 0x00 0x00 0x10 0x5d 0x00 0x12 0x00
0x49 0x00 0x01 0x00 0x06 0x57 0x00 0x09 0x00
0x80 0x02 0x80 0x55 0x59 0x26 0x08 0xdb 0x73';
```

### ①-2 IP 대역 스캐닝

```
C:₩Users₩Karashin>tracert www.google.com

최대 30홉 이상의
www.google.com [223.62.225.178](으)로 가는 경로 추적:

  1    <1 ms    <1 ms    <1 ms  192.168.42.129
  2     *        *        *     요청 시간이 만료되었습니다.
  3    35 ms    39 ms    39 ms  10.113.[redacted]
```

### ② GTP-in-GTP 메시지 전송

*Echo Response Messages*

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 0.00000000 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |
| 2 | 0.00011500 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |
| 3 | 0.00806400 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |
| 4 | 0.00812000 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |
| 5 | 1.68172600 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |
| 6 | 1.95599000 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |
| 7 | 1.96985900 | 10.113.[redacted] | 192.168.42.59 | GTPv2 | 55 | Echo Response |