국내 이동통신 3사의 M-TMSI 값 유지 기간 분석을 통한 보안 취약점 연구*

김성욱○ 박철준†
경희대학교 컴퓨터공학부
so3659@khu.ac.kr cheoljunp@khu.ac.kr

A Security Vulnerability Analysis through M-TMSI Persistence Period in Korean Mobile Network Operators

Kim SeongUk○ Park CheolJun †
School of Computing, Kyunghee University

요 약

3GPP 표준에 따르면 이동통신 사업자는 가입자의 신원을 기밀로 유지하기 위해 영구 식별자 대신 임시 식별자를 사용해야 한다. 임시 식별자에는 LTE(Long-Term Evolution) 네트워크에 사용되는 글로벌 고유 임시 식별자 GUTI(Globally Unique Temporary Identifier)가 있다. 불행히도 최근 연구에 따르면 이러한 식별자들이 정적이고 지속적인 값을 가지기 때문에 GSM/3G 및 LTE에서 가입자를 보호하지 못하고 있는 것으로 나타났다. 이들 식별자는 가입자의 위치를 추적하는 데 사용될 수 있다. 이러한 연구는 이러한 개인 정보 문제를 해결하기 위해 임시 식별자가 자주 재할당되어야 한다고 제안했다. 현재 LTE 구현에서 임시 식별자를 갱신하는 유일한 메커니즘은 GUTI 재할당이다. 우리는 현재의 GUTI 재할당 메커니즘이 가입자의 프라이버시를 보호하기에 충분한 보안을 제공할 수 있는지 조사한다. 이를 위해 국내 이동통신 3사를 대상으로 데이터를 수집하여 각 사업자의 GUTI 유지 기간과 재할당 빈도를 분석한다. 또한 페이징(Paging) 메세지의 트래픽 비교를 통해 3사의 스마트 페이징 사용 여부를 조사한다. 스마트 페이징은 네트워크 리소스 사용과 배터리 소비를 최소화할 수 있다는 장점이 있으나, 일반 페이징이 TA(Tracking Area) 전체 영역에서만 위치 추적이 가능한 것과 달리 단일 셀 수준까지 위치 추적이 가능하여 가입자의 프라이버시 침해 위험이 더 높다. 분석 결과, KR-I의 경우 평균 지속시간이 1,872.65초로 가장 길어 GUTI 재할당이 충분히 자주 이루어지지 않았으며, 이는 가입자의 위치 정보가 장기간 노출될 수 있음을 의미한다. 또한 3사 중 KR-III만이 스마트 페이징을 사용하는 것으로 확인되었다. 이러한 보안 취약점은 악의적인 공격자가 가입자의 위치를 추적하는 데 악용될 수 있음을 시사한다.

1. 서 론

모바일 네트워크는 현대 통신의 핵심 인프라로서 전 세계에 무선 인터넷 접속과 다양한 서비스를 제공하고 있다. 이러한 네트워크의 보안성은 개인정보 보호 측면에서 매우 중요하며, 특히 가입자의 위치 정보 보호는 핵심적인 요구사항이다.

네트워크를 향한 공격 수단 중 하나는 이동통신 네트워크 설계에 따라 가입자 신원이 무선 인터페이스 상에 노출될 수밖에 없다는 점을 악용하여 휴대전화와 모바일 네트워크 기지국 사이의 브로드캐스트 메시지를 도청하는 공격이다. 그중에서도 'IMSI catcher'는 무선 인터페이스 상에 평문으로 노출되는 가입자의 영구 신원인 IMSI (International Mobile Subscriber Identity)를 포착하여 가입자의 위치를 추적하는 데 사용되어 왔다. 최근 많은 연구에서는 IMSI 포착을 방지하는 방법에 대해 집중해왔다 [1], [2], [3]. 3GPP는 이 문제를 인식하고, 불가피한 상황을 제외하고는 영구 신원 대신 2G/3G에서 TMSI (Temporary Mobile Subscriber Identity)를 사용하도록 이동통신 프로토콜을 설계했다 [5]. LTE(Long Term Evolution) 네트워크에서는 GUTI(Globally Unique Temporary Identifier)가 사용된다. 그러나 3GPP 표준은 임시 식별자를 언제, 어떻게 갱신할지에 대한 가이드라인을 명시하지 않으며, 구현과 갱신 빈도는 이동통신 사업자에게 맡겨져 있다.

여러 연구들은 표준 가이드라인의 부재로 인해 GUTI의 재사용 문제가 발생함을 지적하고 있다 [6], [7], [8]. Hong 등은 많은 이동 통신사에서 예측 가능한 패턴을 통해 GUTI를 재할당하기에 가입자가 여전히 개인정보 유출로부터 안전하지 않다고 밝혔다 [6]. Kune 등은 기존의 IMSI 캐처 공격과 마찬가지로 TMSI를 재사용하면 피해자의 위치가 노출될 수 있는 보안 위협이 발생한다고 밝혔다 [7]. 그들은 공격자가 피해자에게 여러 번 전화를 걸면 무선 인터페이스의 방송 채널에서 피해자의 TMSI가 노출될 수 있음을 지적했다. 공격자는 피해자가 전화를 받기 전에 전화를 끊어 피해자가 알지 못하게 하는 무음

†Corresponding author

호출을 사용한다. 피해자가 공격자와 동일한 LA(Location Area)에 있을 경우 피해자에게 반복적으로 전화를 걸 때마다 동일한 TMSI가 채널에 나타난다. Shaik 등은 동일한 공격이 VoLTE(Voice over LTE)에서도 가능하다고 밝혔다 [8]. 세 연구 모두 GUTI를 자주 재할당하면 가입자의 위치 추적이 어렵기 때문에 이 문제를 해결하기 위해 GUTI의 빈번한 재할당과 예측 불가능한 패턴을 제안했다.

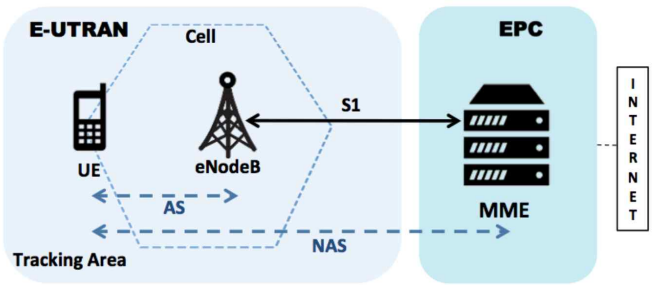
하지만 여전히 많은 이동통신 사업자들이 네트워크 성능 최적화를 위해 GUTI를 자주 재할당하지 않는다. 이러한 실태를 파악하기 위해 우리는 경기도 용인시에 위치한 한국의 이동통신 3사의 기지국을 대상으로 네트워크 패킷 탐지기인 LTE-Sniffer [3]를 이용하여 페이징 메시지를 수집했으며 이 데이터셋을 각 사업자별로 신중하게 분석하였다. 먼저 몇몇 사업자 내에서 GUTI 재할당이 자주 일어나지 않는다는 점을 확인할 수 있었다. 즉, 특정 GUTI값이 상당히 긴 시간 동안 꾸준하게 관측되는 것을 확인할 수 있었다. 또한 3사 중 1개의 사업자만이 스마트 페이징(Smart Paging)을 사용하는 것을 발견할 수 있었다. GUTI 재할당이 자주 일어나지 않는다는 점은 심각한 보안 취약점을 보여주며 악의적인 공격자가 가입자의 위치를 추적하는 데 악용될 수 있음을 보여준다.

이 논문은 다음과 같이 구성된다. 먼저, 2장에서는 이동통신 네트워크와 관련된 배경 정보를 제공한다. 3장에서는 관련 연구를 설명한다. 4장에서는 수집된 데이터와 분석 방법에 대해 상세히 설명한다. 5장에서는 분석에서 얻은 정보를 바탕으로 각 사업자별 GUTI 재할당 문제에 대해 논의하며, 마지막으로 6장에서 결론을 맺는다.

2. 연구 배경

LTE 인프라 및 보안과 페이징 메커니즘을 간략히 설명하여 본 논문에서 설명하는 취약점을 이해하는 데 도움을 주고자 한다.

2.1 이동통신 네트워크 구조



[그림 1] 이동통신 네트워크 구조[1)]

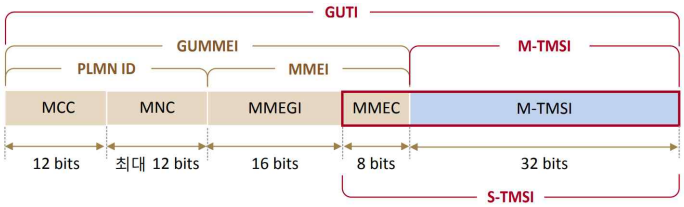
그림 1은 간소화된 LTE 네트워크의 전체 구조를 보여준다. UE(User Equipment), E-UTRAN(Evolved Universal Terrestrial Radio Access Network), EPC(Evolved Packet Core)라는 세 가지 주요 구성 요소를 포함하는 간소화된 아키텍처를 나타낸다. 이 세 가지 구성 요소를 통칭하여 EPS(Evolved Packet System)이라 부른다. 본 논문에서는 전체 시스템을 LTE로 지칭한다.

UE는 네트워크에 가입하고 통신하는 가입자의 장치를 의미한다. UE에는 IMSI와 여러 인증 정보를 저장하는 USIM(Universal Subscriber Identity Module)이 포함되어 있으며, 이는 가입자를 고유하게 식별하는 데 사용된다.

E-UTRAN은 기지국으로 구성되어 있으며, UE와의 무선 통신을 관리하고 UE와 EPC 간의 통신을 지원한다. LTE에서 기지국은 eNodeB(evolved NodeB)로 명명된다. eNodeB는 UE와 신호 메시지를 교환하기 위해 AS(Access Stratum)을 사용하며, 이 AS 메시지에는 RRC 프로토콜 메시지가 포함된다. eNodeB의 다른 기능에는 UE의 페이징, 무선 보안 등이 포함된다. 각 eNodeB는 S1 인터페이스를 통해 EPC에 연결된다.

EPC는 LTE 시스템을 위한 코어 네트워크로, 여러 새로운 요소로 구성된다. 그러나 본 연구에서는 MME(Mobility Management Entity)만을 설명한다. MME는 UE가 네트워크에 연결할 때 인증 및 자원 할당을 담당한다. MME의 다른 중요한 기능으로는 무결성 및 암호화 설정과 UE의 위치를 추적하는 기능이 포함된다. UE와 MME 간에는 NAS(Non-Access Stratum)을 통해 신호를 교환한다.

2.2 이동통신 네트워크 식별자



[그림 2] GUTI의 구조[2)]

IMSI는 이동통신 네트워크에서 가입자의 영구적이고 고유한 식별자이다 [5]. 이는 SIM에 저장되며, 이를 노출하면 위치 추적 및 도청과 같은 보안 문제로 이어질 수 있다. 따라서 IMSI를 무선 인터페이스를 통해 전달하는 대신, 사업자는 가입자의 신원을 숨기기 위해 임시 식별자를 사용한다. LTE 이전의 시스템은 식별을 위해 TMSI를 사용한 반면, LTE는 GUTI를 사용한다. GUTI는 GUMMEI(Globally Unique Mobility Management Entity Identifier)와 M-TMSI(MME-Temporary Mobile Subscriber Identity)의 두 부분으로 구성된다 (그림 2). GUMMEI는

1) Shaik et al

2) 넷매니아즈 기술문서, “LTE Identification I”, January 2011, http://www.netmanias.com/ko/?m=view&id=techdocs&no=5156

[표 1] M-TMSI Count 결과

TIME / M-TMSI	2024-11-21 23:19:33 PM	2024-11-21 23:19:34 PM	2024-11-21 23:19:35 PM	2024-11-21 23:19:36 PM	2024-11-21 23:19:37 PM
c0:00:02:99	0	0	1	1	1
c0:00:06:f0	0	0	0	0	1
c0:02:0f:72	0	0	0	0	0
c0:08:04:b5	0	1	1	1	2

네트워크 식별을 위한 다수의 식별자를 포함하며, MCC(Mobile Country Code), MNC(Mobile Network Code), MMEGI(MME Group Identifier), MMEC(MME Code)로 구성된다. LTE 사업자는 여러 MME로 구성되는 MME 그룹을 여러 개 가질 수 있으므로 한 사업자 안에서 MME ID는 MME 그룹을 나타내는 MMEGI와 MME 그룹 안에서 하나의 MME를 나타내는 MMEC로 표시된다. 여기에 PLMN ID가 붙으면 전세계적으로 고유한 MME ID인 GUMMEI를 나타낸다. M-TMSI는 MME 내에서 UE를 식별하기 위해 사용되는 임시의 고유한 32비트 값으로 구성된다. MME는 UE가 네트워크에 접속하거나 추적 영역을 갱신할 때 UE에 GUTI를 할당한다. 이후 UE와 MME는 IMSI 대신 할당된 GUTI를 사용하여 UE와 MME 간의 식별 및 통신을 수행한다. 가입자와 GUTI 간의 매핑 정보를 숨기기 위해 MME는 종종 GUTI를 재할당한다. 3GPP 표준은 이 재할당의 빈도나 규칙을 명시하지 않으므로 이는 사업자별 설정에 따라 수행된다 [5].

2.3 페이징

페이징은 데이터 서비스, 수신 통화 또는 SMS(Short Message Service)를 설정하기 위해 네트워크가 UE를 깨우는 절차이다. 이는 MME가 특정 지역에서 UE의 위치를 파악하고 네트워크 서비스를 제공해야 할 때 사용되는 RRC 계층의 AS 메시지이다. 대부분의 경우 UE와 네트워크는 계속 연결되지 않는다. Connection 상태에서 UE와 eNodeB 사이에 별다른 활동이 없다면 UE는 IDLE 상태로 넘어간다. 이때 네트워크는 페이징 메시지를 통해 특정 UE를 깨워서 통신을 시작하거나 서비스를 제공한다. MME는 UE가 IDLE 상태일 때 이를 커버하는 정확한 eNodeB를 알 수 없으므로, TA(Tracking Area) 내의 모든 eNodeB로 페이징 메시지를 전송한다. 이때 MME는 페이징 타이머를 시작하고 타이머가 만료되기 전에 UE로부터 응답을 기대한다.

MME로부터 페이징 메시지를 수신한 eNodeB는 페이징 제어 채널(PCCH)을 통해 페이징 메시지를 방송한다. 페이징 메시지에는 ue-Identity 필드에 UE를 지정하는 식별자가 포함되며, UE 식별에는 S-TMSI와 IMSI라는 두 가지 옵션이 있다 [10]. S-TMSI는 GUTI의 일부이다.

IDLE 상태에 있는 UE는 주기적으로 페이징 채널을 수신하고 페이징 메시지 내의 PagingRecords를 디코딩한다. 페이징 메시지는 암호화되지 않으므로, 동일한 페이징 채널을 청취하고 동일한 TA에 있는 다른 사람들도 페이징 메시지의 식별자를 볼 수 있다. UE가 IMSI를 감지하면 새로운 연결 절차를 시작하여 GUTI를 수신하며, 자신의 GUTI를 감지하면 “Random Access Procedure”를 통해 무선 채널을 획득하여 eNodeB에 RRC 연결을 요청한다. “RRC Connection Setup”은 신호 메시지를 교환하기 위한 무선 자원 구성을 포함하며, UE는 “RRC Connection Setup Complete“ 메시지와 함께 “Service Request“ 메시지를 보내는 방식으로 연결 설정을 완료한다. 이 시점에서 UE는 IDLE 상태를 벗어나 CONNECTED 상태로 진입하며, eNodeB는 서비스 요청 메시지를 MME에 전달하고 보안 컨텍스트를 설정하여 UE에 네트워크 서비스를 제공하기 시작한다.

LTE에서는 페이징 절차가 스마트 페이징(Smart Paging)이라는 기술을 통해 개선되었다. 이는 페이징 메시지를 UE가 마지막으로 관찰된 eNodeB를 통해 선택적으로 전송하여 신호 부하를 줄이고 UE의 위치를 더 빠르게 찾을 수 있도록 한다. 응답이 없는 경우에는 TA 전체에서 페이징이 반복된다. 몇몇주요 도시에서는 LTE 페이징 절차 실험을 통해 여러 네트워크 사업자와 벤더들이 스마트 페이징을 구현한 것을 확인할 수 있었다 [8].

그러나 이러한 스마트 페이징 기술은 보안 측면에서 새로운 취약점을 야기할 수 있다. GSM에서는 페이징 메시지가 전체 위치 영역에 전송되어 공격자가 큰 지역(예: 100 km^2) 내에서만 가입자의 위치를 확인할 수 있었다 [9]. 반면 LTE 페이징은 큰 TA가 아닌 작은 셀로 전송되며, 이를 통해 공격자는 LTE 가입자를 훨씬 더 작은 영역(예: 2 km^2) 내에서 위치시킬 수 있다. 이는 대도시에서 수행한 실험에서 관찰된 일반적인 LTE 셀 크기이다 [8].

3. 기존연구

Hong 등은 이동통신 사업자들이 GUTI를 자주 변경하더라도, GUTI 할당 규칙이 예측 가능하거나 스트레스 상황에서 취약점이 발생할 수 있음을 보여주었다 [6]. 이는 단순히 GUTI를 자주 변경하는 것만으로는 가입자의 정보를 보호하기에 충분하지 않다는 것을 의미한다. 저자들은 이러한 문제를 해결하기 위해 예측 불가능하고 가벼운 GUTI 재할당 메커니즘을 제안하였다.

[표 2] 각 통신사 별 지속시간 및 패킷 수

통신사	평균 지속 시간(초)	최대 지속 시간(초)	최소 지속 시간(초)	패킷 수
KR-I	1,872.65	3,295.0	5.0	217,214
KR-II	1,477.13	4,086.0	2.0	77,368
KR-III	1,044.67	2,860.0	2.0	9,542

본 연구에서는 국내 이동통신 3사를 대상으로 GUTI 재할당 주기를 분석하였다. GUTI의 주요 요구사항은 공격자가 GUTI를 통해 가입자의 위치 정보를 파악하기 전에 새로운 값을 생성하는 것이다. 실험 결과를 통해 현재의 사업자들이 이러한 보호를 제공하는 데 실패하고 있음을 확인하였다. 특히 기존 연구들이 제안한 빈번한 GUTI 재할당이 실제 구현에서는 이루어지지 않고 있음을 발견하였다.

4. 실험 설정

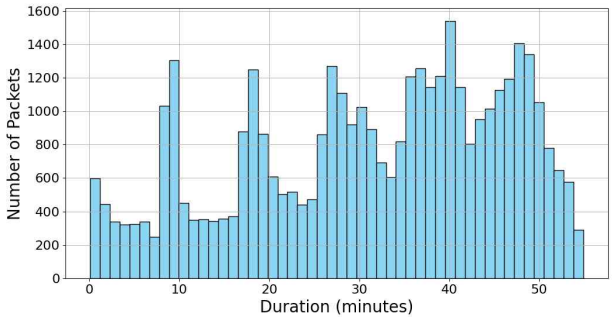
본 연구는 경기도 용인시에 위치한 경희대학교 국제캠퍼스에서 데스크탑(Ubuntu 22.04 LTS OS)에 연결된 USRP B210 장치 [11]를 사용하여 LTE-Sniffer [4]를 작동시켜 페이징 메시지를 수집하였다. 측정은 국내 이동통신 3사를 대상으로 평일 23시부터 24시까지 수집하였으며, 각 통신사는 보안상의 이유로 국가 약어와 로마 숫자로 표기하였다.

수집된 페이징 메시지는 네트워크 패킷 분석 프로그램인 Wireshark [12]와 Python 기반 파싱 프로그램인 Pyshark [13]를 통해 분석을 진행하였다. 분석 과정에서 각 페이징 메시지의 도착 시간과 M-TMSI 값을 추출하고, 고유한 M-TMSI 값들을 식별한 후 동일 값 발생 시 카운트를 증가시켰다. 측정 주기는 1초로 설정하였으며, 분석 결과는 표 1에 제시하였다..

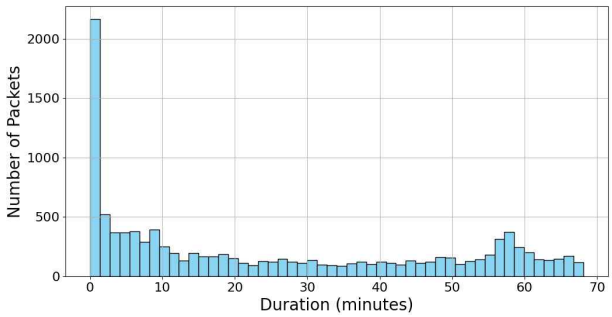
M-TMSI의 지속시간 측정은 다음과 같은 방식으로 진행하였다. M-TMSI 값이 최초로 증가하는 시점(0이 아닌 첫 값)부터 마지막으로 증가하는 시점까지의 시간 차이를 계산하여 지속시간을 산출하였다. 예를 들어, M-TMSI 값이 [0,1,1,1,1,2,3,4,4,4,5,5,5]와 같이 변화할 경우, 지속시간은 9초로 측정된다.

5. 실험 분석

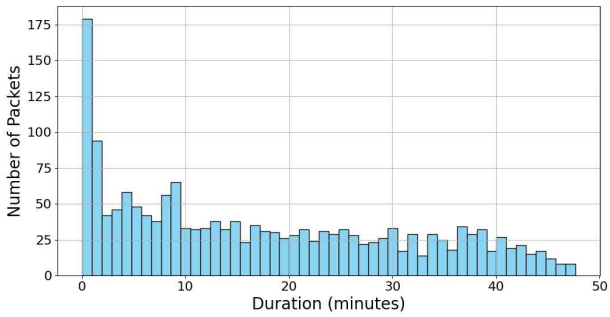
실험 결과는 표 2와 그림 3에 나타나 있다. 결과에서 볼 수 있듯이 세 통신사의 M-TMSI 지속시간 분포에서 뚜렷한 차이점이 관찰된다. KR-I의 경우 40분대에서 최대 1,500개의 패킷이 관찰되었으며, 전반적으로 20-50분 구간에서 높은 패킷 수를 보여주고 있다. 평균 지속시간 또한 1,872.65초로 가장 길며, 이는 M-TMSI 값이 비교적 오랜 시간 동안 유지되고 있음을 시사한다. 또한 전체 트래픽량도 217,214개로 가장 많은 패킷을 기록했다. 이러한 특성은 전통적인 페이징 방식을 주로 사용하고 있음을 시사한다.



(a) KR-1



(b) KR-11



(c) KR-111

[그림 3] 각 통신사 별 지속시간

KR-II는 평균 지속시간이 1,477.13초이며, 초기 5분 이내에서 약 2,000개의 높은 패킷 수를 기록한 후 급격히 감소하여 대부분 200개 이하의 낮은 수준을 유지한다. 이는 KR-II가 상대적으로 빈번한 M-TMSI 갱신 정책을 사용하고 있음을 시사한다. 전체 트래픽량은 77,368개로, 전통적인 페이징 방식을 사용하는 것으로 추정된다.

KR-III는 평균 지속시간이 1,044.67초로 가장 짧고, 전체 트래픽량도 9,542개로 현저히 적다. 초기 5분 이내에 약 175개의 최대치를 기록한 후 전반적으로 50개 미만의 패킷 수를 유지한다. 이러한 패턴은 가장 적극적인 M-TMSI 갱신 정책과 스마트 페이징 기술의 활용을 시사하며, 이는 네트워크 효율성과 보안성 측면에서 가장 진보된 접근 방식을 채택하고 있음을 보여준다.

이러한 분포 차이는 각 통신사의 보안적 수준을 확인

할 수 있다. KR-I의 경우 네트워크 효율성을 위해 상대적으로 긴 M-TMSI 지속시간을 채택했으나, M-TMSI 값이 장시간 유지되어 가입자 추적 가능성이 상대적으로 높다. KR-II는 초기에 집중된 갱신 정책으로 중간 수준의 보안을 제공한다. KR-III는 가장 낮은 패킷 수와 짧은 지속시간을 보여 가장 높은 수준의 프라이버시 보호를 제공한다. 그러나 셀 단위의 정밀한 페이징 특성으로 인해 가입자 위치 추적 가능성이 증가할 수 있다는 단점이 있다. 이러한 분석 결과는 각 통신사가 보안과 네트워크 효율성 사이에서 서로 다른 균형점을 선택했음을 보여줌과 동시에 몇몇 통신사가 더 빈번하게 재할당 규칙이 이루어야 함을 보여준다.

6. 결론 및 향후 연구

이동통신 네트워크 사업자와 표준 기관은 가입자의 정보를 안전하게 보장하기 위해 네트워크에서의 정보 관리에 상당한 노력을 기울여 왔다. 그러나 관련 기관의 불완전한 표준과 통신사의 잘못된 운영으로 인해 가입자는 여전히 개인정보 유출로부터 안전하지 않다. 본 논문에서는 국내 이동통신 3사의 페이징 메시지 속 M-TMSI 값 유지 기간을 분석하였고, 이를 통해 몇몇 통신사의 보안 수준이 부족함을 보였다. 특히 GUTI가 무선 링크에서 노출될 경우 발생할 수 있는 보안 위험성을 고려할 때, 이러한 분석 결과는 향후 네트워크 설계에서 보안과 효율성의 균형을 고려할 때 중요한 참고 자료가 될 것으로 기대된다.

다만, 본 연구는 몇 가지 한계점을 가지고 있다. 우선 수집된 데이터셋의 규모가 제한적이라는 점이다. 또한 KR-I의 경우 측정 장소에서 활발하게 작동하는 기지국을 정확하게 확인하여 해당 기지국의 주파수를 통해 데이터를 수집할 수 있었으나, KR-II와 KR-III의 경우 해당 기지국의 주파수가 근방에서 활발한 주파수인지 확인할 수 없었다는 점이 아쉬움으로 남는다. 더불어 통신사별 시장점유율과 가입자 특성의 차이가 결과에 미치는 영향을 고려하지 못한 것도 본 연구의 한계로 볼 수 있다.

향후 연구에서는 더 정확한 분석을 위해 더 많고 정밀한 데이터셋을 수집할 예정이다. 또한 GUTI가 재할당 됐을 경우 그 값이 이전 값과 얼마나 랜덤하게 변하는지와 GUTI가 재할당 된 후 오랜 시간이 지났을 때 이전 GUTI가 다시 등장하는지 재등장 주기도 살펴보고자 한다. 더불어 이러한 연구 결과를 이용하여 또 다른 위험한 공격 수단인 FBS(Fake Base Station)을 탐지할 수 있는 수단도 살펴보고자 한다. 이러한 추가 연구를 통해 이동통신 네트워크의 보안성 향상을 위한 더욱 구체적인 가이드라인을 제시할 수 있을 것으로 기대된다.

참고 문헌

[1] Kareem, Karwan Mustafa. “The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks.“ arXiv preprint arXiv:2405.00793 (2024).

[2] Alrashede, Hamad and Riaz Ahmed Shaikh. “IMSI Catcher Detection Method for Cellular Networks.” 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (2019): 1-6.

[3] Park, Shinjo et al. “Anatomy of Commercial IMSI Catchers and Detectors.” Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (2019): n. pag.

[4] Hoang, Tuan Dinh, et al. “LTESniffer: An open-source LTE downlink/uplink eavesdropper.“ Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2023.

[5] 3GPP. TS 23.003, “Numbering, addressing and identification,” 2017

[6] Hong, Byeongdo, Sangwook Bae, and Yongdae Kim. “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier.“ NDSS. 2018.

[7] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, “Location leaks on the GSM Air Interface,” in Proceedings of the Network and Distributed System Security Symposium (NDSS), 2012.

[8] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems,” Proceedings of the Network and Distributed System Security Symposium (NDSS), 2016.

[9] N. H. Foo Kune, John Koelndorfer and Y. Kim, “Location leaks on the GSM air interface,” in 19th Network and Distributed System Security Symposium, 2012.

[10] 3GPP. TS 36.331, “Evolved Universal Terrestrial Radio Access (EUTRA); Radio Resource Control (RRC); Protocol specification,” 2017.

[11] Ettus. USRP B210. [Online]. Available: http://www.ettus.com/product/details/UB210-KIT

[12] Wireshark. [Online]. Available: https://www.wireshark.org/download.html

[13] Pyshark. [Online]. Available: https://github.com/KimiNewt/pyshark