VoLTE의 SIP 프로토콜 취약점 분석 환경 및 연구 동향 분석

최현영 박철준

Kyung Hee University

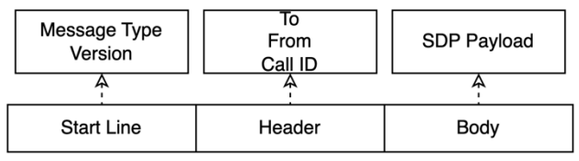
School of Computing

연구 배경

VoLTE는 **IMS 아키텍처**와 **SIP**을 통해 통화 서비스를 제공하는 LTE 네트워크의 음성 통신 기술이다. 그러나 VoLTE는 DoS (Denial of Service)와 같은 IP 기반 공격에 노출될 수 있으며, SIP 메시지에 민감한 내용이 포함되거나 악의적인 변조에 취약하다면 사용자 위치 추적과 발신자 스푸핑과 같은 공격에 취약하다. 최근, Google의 Project Zero 팀은 Samsung Exynos 모뎀을 사용하는 단말기에서 공격자는 피해자와의 상호 작용 없이 전화번호 만으로 원격으로 단말기를 제어할 수 있는 0-day 취약점을 발견하였으며, VoLTE 비활성화 조치를 권장하기까지 한 취약점이었기에 많은 주목을 받았다.
본 연구는 오픈소스 기반의 VoLTE 환경을 구축하고 다양한 공격 시나리오를 분석하고 검증하고자 한다.

SIP 프로토콜

SIP (Session Initiation Protocol)은 멀티미디어 세션의 시작과 종료를 관리하는 **애플리케이션 계층** 프로토콜이다. TCP와 UDP같은 전송 계층 프로토콜에 의존하며, 요청과 응답 메시지를 교환하며 **클라이언트-서버 방식**으로 통화 신호 전달과 연결을 관리한다.

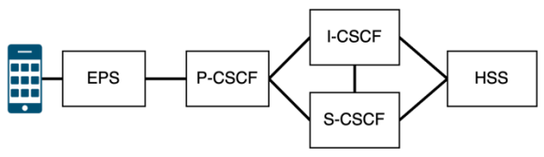


<SIP 메시지 구조>
시작 라인: 요청 유형 또는 응답 코드를 포함
헤더: 메시지의 속성을 정의
SDP: 코덱 유형 등의 정보를 포함한 미디어 세션을 정의

SIP 요청의 유형으로는 **REGISTER**, **INVITE**, **BYE** 등이 있으며, 응답은 **HTTP 상태 코드**와 유사하게 구분됨

VoLTE

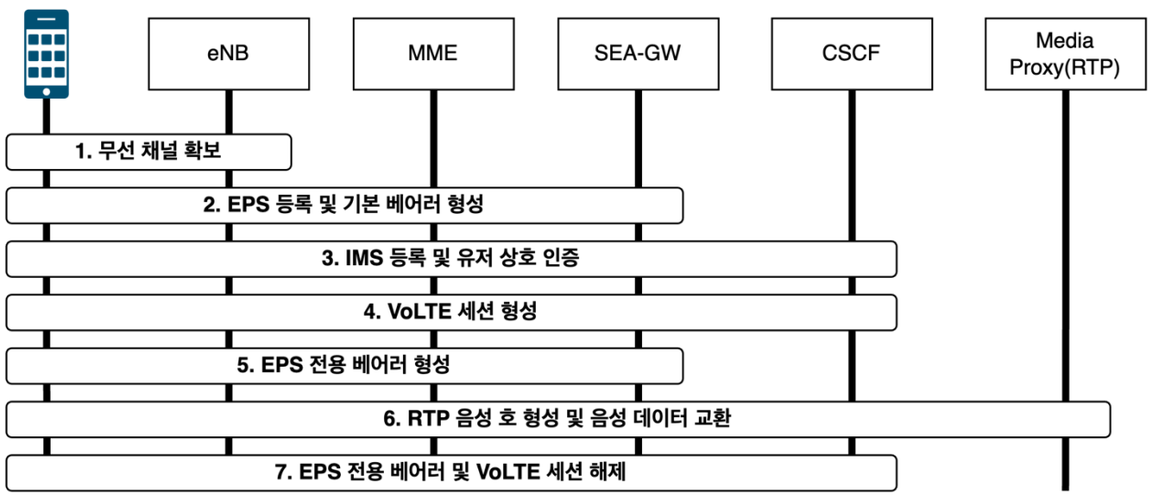
VoLTE (Voice over LTE)는 IMS (IP Multimedia Subsystem)라는 코어망에서 SIP (Session Initiation Protocol)을 통해 음성 서비스를 **IP 패킷**으로 제공한다. IMS는 사용자의 인증, 통화 신호 라우팅, 세션 제어 및 호 처리를 담당한다.



<IMS의 주요 구성 요소>

1. **P-CSCF** (Proxy-CSCF): UE (User Equipment)와 IMS 망 간의 최초 접속 지점으로, SIP 메시지의 프록시 역할을 수행
2. **I-CSCF** (Interrogating-CSCF): 외부에서 들어오는 모든 호에 대한 접점으로, 가입자의 위치를 파악하고 적절한 S-CSCF로 라우팅함
3. **S-CSCF** (Serving-CSCF): 사용자 프로파일(정보) 관리와 SIP 세션 제어를 담당하며, 호 처리를 수행함
4. **HSS** (Home Subscriber Server): 사용자 인증 정보를 관리하는 데이터베이스

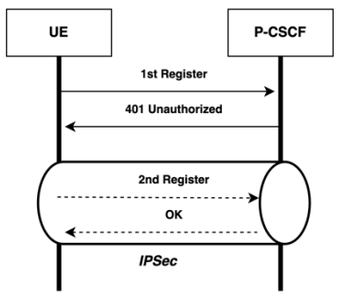
<VoLTE 절차>



연구 동향 분석

1.텍스트 형태의 REGISTER 메시지

1차 REGISTER 메시지는 **IPSec**를 통해 전송되는 2차 REGISTER 메시지와는 다르게 텍스트 형태로 보호되지 않은 채 전송된다. 헤더에 담겨있는 IMSI, 전화번호, eNB ID 등의 **민감 정보**가 노출될 수 있다. 공격자는 해당 메시지를 스니핑하여 사용자의 정보를 탈취할 수 있다. 또한, 해당 정보를 바탕으로 등록한 사용자로 위장할 수도 있다.

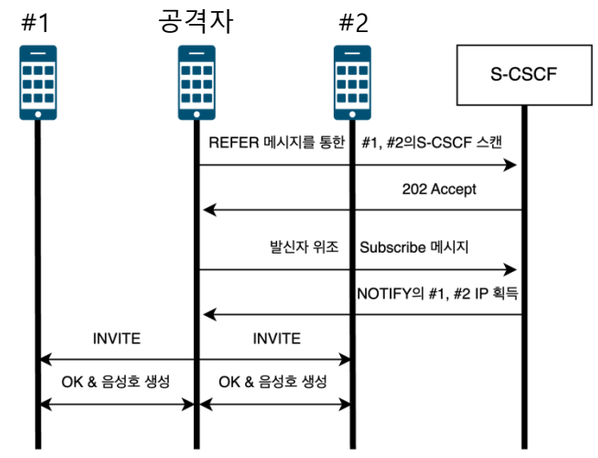


2. SIP 플러딩

초기 REGISTER 요청 시 단일 **401 Unauthorized** 응답이 반환되지만, IMS 내부에서는 여러 **CSCF**와 **HSS** 간의 메시지 교환 및 인증 정보 교환이 이루어진다. 만일 대량의 변조된 REGISTER 메시지가 **P-CSCF**로 전달되면, CSCF 서버들 간의 메시지 교환이 급증하여 IMS 망에 큰 부하가 발생하게 된다. 이러한 부하는 REGISTER 메시지가 정상 여부에 관계없이 P-CSCF가 응답하는 특성을 악용한 것으로, 결과적으로 **서비스 품질 저하**로 이어질 수 있다.

3. 비정상 세션 형성

공격자는 자신의 단말기로 S-CSCF의 IP 주소를 확인한 후, SIP REFER 메시지를 통해 희생자의 S-CSCF의 IP 주소를 스캐닝한다. 이후 SUBSCRIBE 메시지를 사용해 희생자의 IP 주소를 획득하고, 발신자 번호로 위조한 SIP INVITE 메시지를 희생자에게 요청함으로써 비정상 세션을 형성하여 통화를 도청할 수 있다.

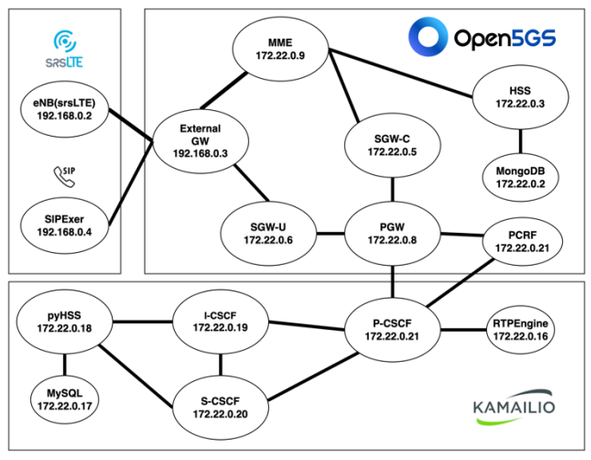


4. 사용자 위치 정보 노출

```
P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=0010100010019b01
```

SIP 헤더 부분의 필드 중 하나인 **P-Access-Network-Info** 필드는 **MCC**(국가 코드), **MNC**(네트워크 코드), **LAC**(위치 영역 코드), **Cell-ID** 등의 정보를 포함하여 단말의 **위치 정보**를 전달한다. 이 필드의 값을 통해 사용자의 위치 정보를 습득할 수 있다.

분석 환경



본 실험은 Software-Defined Radio (USRP B205) 장치와 오픈소스 기반 이동통신 스택을 활용하여 VoLTE 환경을 구성하였으며. 상용 LTE 단말기를 사용하였다.

- **기지국 (eNB)**: **srsRAN** 오픈소스를 사용하여 기지국(eNB)을 구현함
- **코어망 (EPC)**: **Open5GS** 오픈소스를 사용하여 LTE 코어망(EPC)을 구성함
- **IMS 서버**: **Kamailio** 오픈소스를 이용해 IMS 서버를 구축함
- **SIP 툴** : **SIPExer**를 사용하여 변조된 SIP 메시지 생성함

검증 방법

1. SIP 플러딩

Expire=0으로 변조한 SIP REGISTER 메시지를 P-CSCF로 보냈을 때, 모든 CSCF 서버와 HSS가 관여한 모습을 살펴볼 수 있었다. Expire값이 0이고, Contact값은 단말기의 네트워크 대역 내 임의의 IP값으로 랜덤하게 할당된 SIP REGISTER 메시지를 3대의 호스트에서 1초에 500개 가량의 메시지를 P-CSCF 쪽으로 요청하여 플러딩 공격을 수행함. 각 CSCF와 HSS 서버의 리소스 사용량 추이를 살펴보았으며, 공격 중 정상 단말기의 Register 절차를 스니핑하여 서비스 거부(DoS)가 이루어 졌는지 살펴봄.

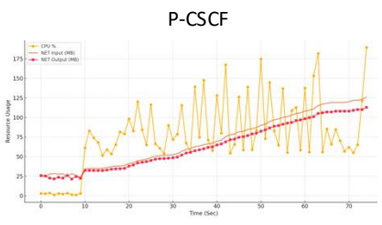
2. P-Access-Network-Info 필드 노출

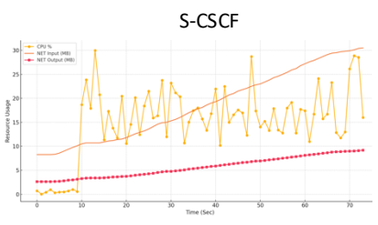
1차 등록 시 P-Access-Network-Info 필드가 포함되는 모습을 확인하여 3통사의 필드 포함 여부를 조사함. Xcode의 rvi를 통해 iOS 단말기의 패킷을 캡처하여 REGISTER 등록 과정을 살펴보았고, 해당 CELL-ID 값을 Google GeoLocation API를 통해 GPS 값을 추출함.

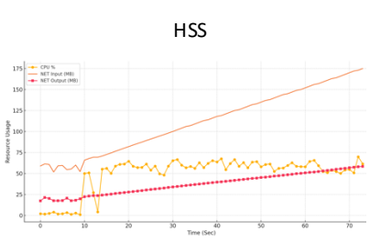
검증 결과

1. SIP 플러딩

10초 지경에 Flooding 공격을 수행한 결과 **각 서버 간의 CPU 사용량이 매우 급격하게 증가**했음을 볼 수 있었으며, 특히 **P-CSCF 서버의 성능 부하가 많이 발생**함. 30초 경에 정상 사용자가 IMS 등록을 요청하였지만 **504**(서버 응답 없음)으로 반환되어 **VoLTE 서비스를 이용할 수 없었음.**







DoS

```
Request: REGISTER sip:ims.mnc001.mcc001.3gppnetwork.org
Status: 100 Trying |
Status: 504 Server Time-Out |
Request: REGISTER sip:ims.mnc001.mcc001.3gppnetwork.org
Status: 100 Trying |
Status: 504 Server Time-Out |
Request: REGISTER sip:ims.mnc001.mcc001.3gppnetwork.org
Status: 100 Trying |
Status: 401 Unauthorized - Challenging the UE |
Request: REGISTER sip:ims.mnc001.mcc001.3gppnetwork.org
Status: 100 Trying |
Status: 504 Server Time-Out |
```

2. 3통사 노출 여부

SKT는 2차 ESP 내부(IPSec)에 담겨서 보내지고, LGU+와 KT는 1차 Register 메시지에 담겨서 보내지는 모습을 확인할 수 있었다.
GPS 값 추출 역시 Google의 **GeoLocation API**에서 쉽게 조회할 수 있었다.

결론

본 연구를 통해 SIP 메시지 변조와 평문 정보 노출을 이용한 다양한 공격 시나리오를 확인할 수 있었으며, SIP 플러딩 공격을 통해 서버 성능 저하 및 서비스 마비로 이어지는 것을 검증할 수 있었다. 추후 비정상 세션 형성 시나리오를 추가로 검증하고, 1차 REGISTER 메시지의 P-Access-Network-Info 노출 여부에 따른 취약점을 집중적으로 분석할 것이다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 융합보안핵심인재양성사업 (IITP-2024-RS-2023-00266615) 과 이동통신 및 AirGap 환경에서 스니핑 방지 기술 개발 (IITP-2024-RS-2024-00437252) 연구 결과로 수행되었음