VoLTE의 SIP 프로토콜 취약점 분석 환경 및 연구 동향 분석*

최현영*, 박철준**

경희대학교 (*학부생, **조교수)

Analysis of VoLTE's SIP Protocol Vulnerability Environment and Research Trends

HyunYeong Choi*, CheolJun Park**

Kyung Hee University(*Undergraduate Student, **Assistant Professor)

요 약

LTE 네트워크에서의 음성 통신 기술인 VoLTE는 IMS 아키텍처를 기반으로 하며, 이는 SIP 프로토콜을 통해 통화 서비스를 제공한다. SIP 프로토콜은 음성 통화의 세션 설정, 종료를 관리하는 프로토콜로 통화 연결을 위해 LTE 코어망을 통해 사용자 간의 신호를 교환하며, IMS와 인증 절차를 통해 사용자가 올바른 사용자인지 검증하여 허가된 사용자만 서비스를 이용할 수 있도록 한다. 이러한 이유로 SIP 메시지에 민감한 내용이 포함되거나, 악의적인 변조에 취약하다면 발신자 스푸핑, DoS 공격과 같은 취약점에 노출될 수 있다. 따라서 본 논문에서는 기존 SIP 프로토콜에 관한 보안 연구 동향을 분석하고, 단말에서 보안 취약점을 검증하기 위한 테스트 환경을 바탕으로 상용 단말의 베이스 밴드 제조사와 관계없이 무선 인터페이스를 기반으로 SIP 프로토콜에 대한 공격 시나리오를 제시한다.

I. 서론

LTE는 고속 데이터 전송과 낮은 지연시간을 제공하는 이점 덕분에 현재 사회에서 필수적인 통신 인프라로 자리잡았다. 특히 LTE 네트워크는 All-IP 통신을 기반으로 데이터를 주고받으며, 기존의 회선 교환 방식 대신 패킷 교환 방식만을 사용한다. 이에 따라 패킷 기반의 고음질 음성 통화 서비스를 제공할 수 있는 VoLTE가 도입되었다.

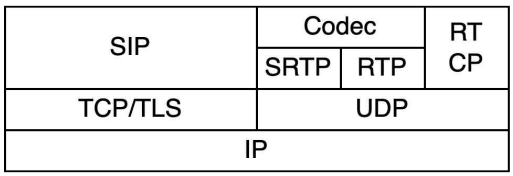
VoLTE는 LTE 환경에서 음성 서비스를 제공하기에 스푸핑, DoS와 같은 IP 기반의 공격에 노출될 수 있으며, 애플리케이션 계층에서 동작하는 SIP 메시지를 악의적으로 변조한다면 비정상 통화로 이어질 수 있다. 최근, Google의 Project Zero 팀은 Samsung Exynos 모뎀을 사용하는 단말기에서 공격자는 피해자와의 상호 작용 없이 전화번호만으로 원격으로 단말기를 제어할 수 있는 0-day 취약점을 발견하였으며, VoLTE 비활성화 조치를 권장하기까지 한 공격이었기에 많은 주목을 받았다.

본 논문에서는 VoLTE의 보안성을 검증하기 위해 오픈소스 기반의 VoLTE 환경을 구축하고 SIP 프로토콜의 취약성에 관한 연구 동향을 분석하며, 다양한 공격 시나리오를 제시한다.

* "본 연구는 과학기술정보통신부 및 정보통신기획평가원의 융합보안핵심인재양성사업의 연구 결과로 수행되었음" (IITP-2024-RS-2023-00266615*)

II. SIP 프로토콜 동작 개요

2.1 SIP 프로토콜 개요

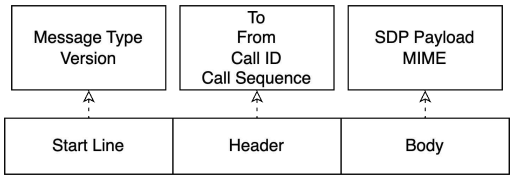


[그림 1] SIP 프로토콜 스택

[그림 1]에서 보는 바와 같이 SIP (Session Initiation Protocol)는 멀티미디어 세션의 시작, 종료를 관리하는 프로토콜로 TCP와 UDP 같은 전송 계층의 프로토콜에 의존하며 애플리케이션 계층에서 동

작한다. SIP는 클라이언트-서버 방식으로 작동하며, 통화 신호 전달과 연결 관리를 담당한다.

2.2 SIP 메시지



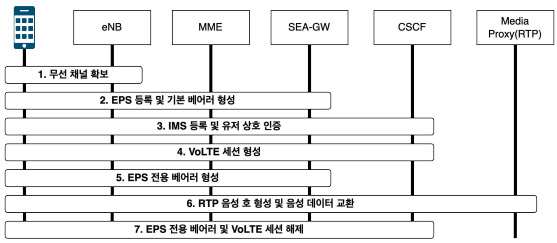
[그림 2] SIP 메시지 구조

[그림 2]는 메시지 구조를 나타낸 것으로 시작라인, 헤더, SDP 부분으로 구성된다. 시작라인에는 요청의 유형이나, 응답 코드 등을 포함하고, 헤더에는 메시지의 속성을 정의한다. SDP 부분은 코덱 유형을 포함하여 미디어 세션을 정의한다. 요청의 유형으로는 REGISTER, INVITE, BYE 등이 있으며, 응답은 HTTP Status Code처럼 구분된다.

2.3 VoLTE

VoLTE는 교환망 역할을 수행하는 IMS (IP Multimedia Subsystem)라는 코어망에서 SIP 프로토콜을 통해 음성 서비스를 IP 패킷으로 제공한다. IMS는 사용자의 인증, 통화 시그널 라우팅, 세션 제어와 호 처리를 담당하는 여러 CSCF (Call Session Control Function)로 구성되어 있다.

2.4 VoLTE 절차



[그림 3] VoLTE 음성 세션 수립 절차

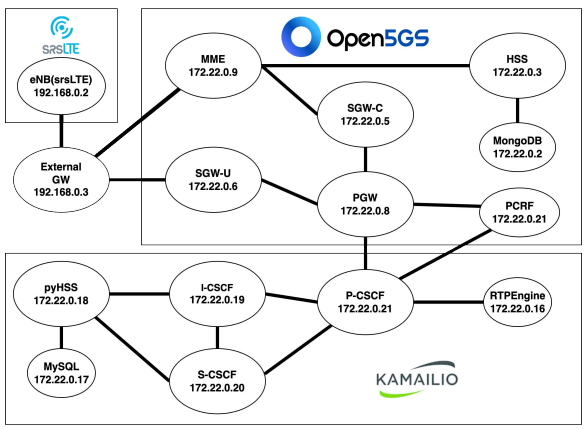
우선, UE와 eNB과 연결하여 무선 채널을 확보하고, EPC와 인증 절차를 통해 IP 주소를 획득하고 EPS 베어러를 형성한다. UE는 SIP REGISTER 메시지를 Proxy-CSCF에 요청함으로써, IMS 코어에 접근한다. 이후 Serving-CSCF와 상호 인증 절차를 통해 사용자를 인증한다. SIP INVITE 메시지를 사용하여 종단 간의 통화 세션을 형성한다. 이후 음성 호를 위한 전용 베어러가 설정되고, 미디어 세션을 통해 RTP 기반 음성 패킷이 전송된다. 통화 종료 시 한쪽이 SIP BYE 메시지를 전송함으로써 세션이 해제된다 [1].

III. SIP 프로토콜 취약점 분석

3.1 오픈소스 기반 테스트 환경

[그림 4] 테스트 환경 개요

SIP 프로토콜 취약점을 검증하기 위해서 VoLTE 및 인터넷 서비스를 지원하는 테스트 이동통신망을 Software-Define Radio (USRP B205) 장치와 오픈소스 기반 이동통신 스택으로 구현하였다. 특히 srs RAN을 사용하여 eNB(기지국)을, Open5GS 오픈소스로 코어망(EPC)을, Kamailio 오픈소스로 IMS 서버를 구성하였다. EPC 코어망과 IMS 코어망은 동일한 호스트에서 구성하였으나, 기지국 호스트와는 다른 호스트에서 구현하여 E-UTRAN과 EPC를 구분하였다. 또한, 각 호스트는 Ubuntu 22.04 LTS OS를 사용하였으며, 같은 사설 네트워크 환경에서 운영체제에 의존하지 않는 Docker 기반으로 각 오픈 소스 스택을 구축하였다. 실험에서 상용 LTE 모바일 단말기를 사용하여 다양한 LTE 밴드 대역에서 VoLTE를 통한 음성 통화를 테스트하였다. [그림 5]는 실습 환경의 구성도이다.



[그림 5] 실습 환경 구성도

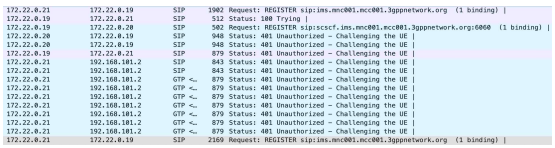
3.2 보안 위협 사례 분석

3.2.1 REGISTER 메시지 변조

[그림 6] REGISTER 메시지 패킷

[그림 6]에서 보는 바와 같이 REGISTER 메시지는 텍스트 형태로 되어있으며, FQDN의 구성요소로 IMSI값과 CALL-ID, eNB ID 식별자 등 민감 정보가 노출되어 있다. 텍스트 기반으로 구성되어 있어 네트워크 트래픽을 모니터링 할 수 있는 공격자가 REGISTER 메시지를 스니핑하여 사용자의 정보를 탈취 후, 등록한 사용자로 위장하여 Expire값을 0으로 설정한 REGISTER 메시지를 CSCF에 재송신함으로써 특정 사용자를 강제로 VoLTE 서비스를 제한할 수 있다 [2].

3.2.2 SIP 인증 실패



[그림 7] 401 Unauthorized 응답

초기 IMS 등록 시, 사용자는 CSCF에 1차 REGISTER 요청을 보내지만, 인증이 되지 않은 상태에서 401 Unauthorized 응답을 수신한다. 이후 IMS-AKA 프로토콜의 인증 벡터 기반으로 생성된 인증 데이터를 2차 REGISTER 요청에 포함하여 다시 전송하나, 만약 이 과정이 무시되면 [그림 7]에서 볼 수 있듯이 CSCF는 계속해서 인증 실패로 간주하여 지속해서 401 메시지를 송신한다. 이는 트래픽 증폭과 서버 부하를 초래하며 서비스 품질의 심각한 저하로 이어질 수 있다. 1차 REGISTER 메시지를 공격자가 보내고, 이에 대한 401 응답을 피해자에게 보냄으로써 은밀하게 세션 연결이 수행되도록 공격할 수 있다 [3].

3.2.3 비정상 세션 형성

사용자는 IMS 등록 시 세션 관리를 위한 고유한 S-CSCF를 할당받게 된다. 공격자는 자신의 단말기 역시 SIP 200 OK 응답 메시지를 통해 S-CSCF의 IP 주소를 확인할 수 있으며, 네트워크 주소를 유추해 볼 수 있다. 공격자는 호 전환에 사용되는 SIP REFER 메시지를 통해 희생자가 등록된 S-CSCF의 IP 주소 대역을 스캐닝하고, 응답을 통해 특정 IP 주소를 확인한다. 이후 MSISDN(전화번호)로 발신자 번호를 위조한 뒤 SIP SUBSCRIBE 메시지를 앞에서 확인한 S-CSCF로 보내고 응답 받은 NOTIFY에서 희생자 단말기의 IP 주소를 획득한다. 최종적으로 INVITE에 필요한 정보를 취득한 공격자는 각 희생자에게 발신자 번호인 MSISDN 헤더를 포함한 INVITE 메시지를 송신함으로써 희생자들 간에는 서로에게 전화가 온 것처럼 표시되게 한다. 그러나 실제 음성 호는 공격자를 경유하기 때문에 통화를 도청할 수 있다 [4].

IV.결론

앞선 SIP 메시지 변조와 평문의 정보를 바탕으로 다양한 공격 수법을 확인할 수 있었다. IMS에서 세션 관리와 SIP 메시지 검증을 제대로 수행하지 않는다면 네트워크 과부하로 인한 서비스 마비와 도청과 같은 사이버 범죄로 이어질 수 있다. 실습 환경을 기반으로 기존의 취약점을 분석하며, 신규 논리적 취약점 및 단말기의 메모리 취약점을 찾는 분석 기술을 개발 및 검증해 갈 것이다.

[참고문헌]

[1] Kim, H., Kim, D., Kwon, M., Han, H., Jang, Y., Han, D., Kim, T., & Kim, Y., Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015

[2] E. Belmekki, B. Raouyane, A. Belmekki and M. Bellafkih, "Secure SIP signalling service in IMS network, "2014 9th International Conference on Intelligent Systems: Theories and Applications (SITA-14), 2014

[3] 고은혜, 박성민, 김세권, 김환국. SIP 메시지 증폭을 통한 VoLTE 위협 및 공격 탐지 방법. 한국통신학회 학술대회논문집, January 21, 2015

[4] 고은혜, 김세권, 김환국, VoLTE 사용자간 비정상 전화 연결. 한국통신학회 학술대회논문집, June 24, 2015