오픈소스 기반 LTE 한국 재난문자 스푸핑

정제원, 이수기, 신재민, 김유성*

*성균관대학교

doubele112@skku.edu, sglee0323@gmail.com, alex93950@gmail.com *yskim525@skku.edu

Spoofing Korean LTE Alert Message using Open-source

Jewon Jung, Sugi Lee, Jaemin Shin, Yusung Kim*

*Sungkyunkwan Univ.

요 약

LTE 무선 이동통신 서비스는 재난 상황 혹은 공공안전과 관련된 정보를 서비스 지역 내 모든 단말들에게 전달하는 표준 재난문자 시스템 CMAS(Commercial Mobile Alert System)을 정의하고 있다. 재난문자는 일반 문자메시지와는 달리 정부가 공식적으로 전송하는 만큼 위조 및 악용될 경우 경제적 및 사회적으로 큰 혼란을 불러올 수 있다. 본 논문은 LTE 오픈소스를 기반으로 허위 기지국을 만들어 국내 이동통신 3사에 대해 안전, 긴급 및 위급 문자 메시지를 모두 스푸핑 할 수 있음을 보인다.

Ⅰ. 서 론

LTE는 재난 상황 혹은 공공안전을 위해 정부가 시민들에게 긴급히 알려야 할 정보가 있을 때 특별한 문자메시지를 브로드캐스팅(Broadcasting) 할 수 있도록 CMAS(Commercial Mobile Alert System)라는 체계를 갖추고 있다.[2] 재난문자는 일반 문자메시지 와는 달리 정부가 공식적으로 전송하는 특별한 메시지로 취급된다. 때문에 만약 재난문자가 위조 당할 경우 피싱 공격, 허위 정보 전파 등에 악용될 수 있어 자칫하면 사회에 큰 혼란을 불러올 수 있다. 그러나 현 LTE 시스템은 재난문자 메시지를 암호화나 무결성 보장 없이 브로드캐스팅하고 있으며 최근 연구결과에 따르면 이를 이용해 해외 통신사의 특정 재난문자 스푸핑(Spoofing)에 성공한 바 있다.[1][7]

본 논문은 오픈소스와 SDR장비를 통해 국내 통신 3사가 서비스 하는 재난문자 메시지가 스푸핑 가능함을 확인했다. 또한 국내에서 서비스하는 모든 종류의 재난문자 메시지에 대해 공격이 가능함을 보인다.

Ⅱ. LTE 재난문자 송수신 절차

국내에서는 3GPP의 LTE 표준을 기반으로 한국정보통신기술협회에서 KPAS(Korean Public Alert System) 라는 표준을 통해 코어 망과 단말 간의 메시지 형식, 전송 시간 등을 정의하고 있다.[3] KPAS는 CMAS 메시지를 통해서 모든 재난문자 서비스를 운용하며 메시지의 CMAS 식별자를 통해 안전 안내 문자, 긴급 재난 문자, 위급 재난 문자로 구분한다.[3]

그림 1.은 eNB가 단말에게 CMAS 메시지를 전송하기 위해 보내는 RRC(Radio Resource Control) 과정을 도식화한 것이다. eNB가 재난문자를 전송하기 위해서는 몇 가지 단계를 거쳐야 한다. 우선 단말은 CMAS 수신절차를 수행하기 전 사전에 eNB가 주기적으로 브로드캐스팅 하는 MIB(Master Information Block)을 통해 eNB에 연결한다. 그 후 eNB는 코어 망에게 CMAS 메시지를 브로드캐스팅 하라는 명령을 받으면 CMAS indication항목의 값이 참으로 설정된 페이징(Paging) 메시지를 송신한다. 이를 수신한 단말은 그 즉시 SIB1(System Information Block 1) 수신을 준비하고 eNB는 SIB1에 SIB12의 스케쥴링 정보를 담아서 보내게 되고 단말은 이를 통해 SIB12를 수신할 수 있다. 단말은 SIB12에 담긴 CMAS 메시지를 디코딩하여 재난문자를 사용자에게 보여준다.[2][9]

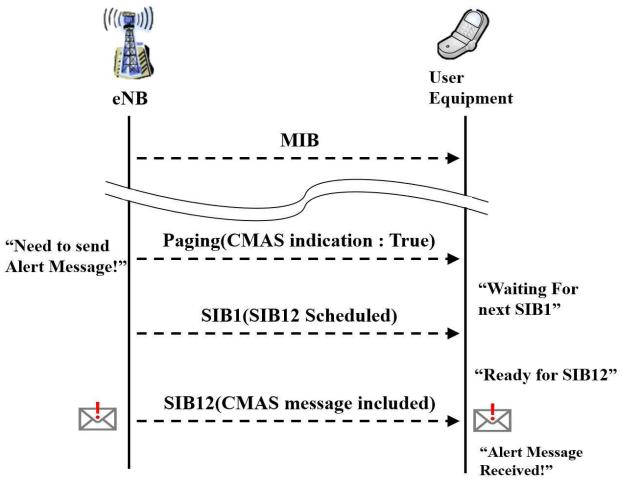


그림 1. CMAS 메시지 전송 과정

Ⅲ. 공격 방법 및 결과

Ⅲ-1. 공격 과정

그림 2.는 재난문자 스푸핑 공격 과정을 도식화한 것이다. LTE 표준에 의하면 단말은 현재 위치를 기준으로 가장 신호 세기가 강한 MIB의 eNB와 연결을 시도한다. 이를 이용해 단말 주변에 허위 eNB를 위치시키고 MIB를 브로드캐스팅해 단말의 핸드오버(handover)를 유도한다. 허위 eNB는 단말에 대한 정보가 없기 때문에 RRC 연결 이후 NAS(Non Access Stratum) 연결 과정을 수행할 수 없으나, 허위 eNB가 이를 무시 혹은 거부 메시지를 보내더라도 단말은 일시적으로 eNB와 RRC 연결을 유지한다. 이 짧은 시간 동안 eNB가 위조된 페이징, SIB1, SIB12를 브로드캐스팅하면 현 LTE 시스템은 이와 관련한 암호화 및 무결성 보장을 수행하지 않기 때문에 단말은 해당 메시지를 별다른 검증 없이 사용자에게 보여준다.[1]

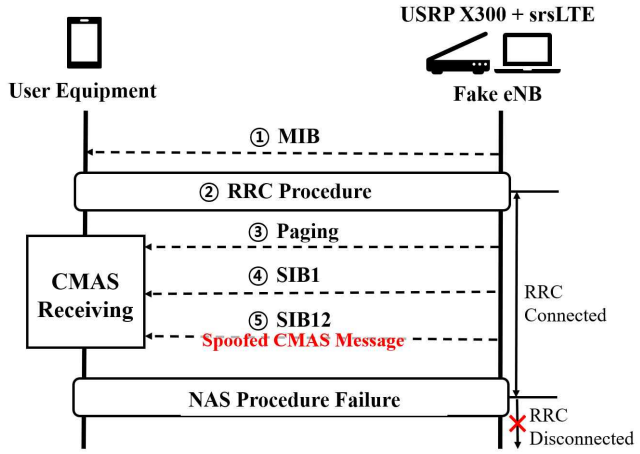


그림 2. 재난문자 스푸핑 공격 과정

Ⅲ-2. 실험 환경

본 실험의 허위 기지국은 SDR(Software Defined Radio) 장비로 USRP X300[4]을 사용했고 LTE를 구현한 오픈소스인 srsLTE[5]를 소프트웨어로 사용했다. 본 연구진은 Ⅲ-1에서 언급한 방법으로 공격하기 위해 srsLTE 소스 코드의 페이징, SIB1, SIB12 등을 수정했다.

실험은 국내 주요 이동통신 3사를 이용하는 6대의 서로 다른 단말을 대상으로 진행했다. 오픈소스 SCAT[6]과 Wireshark를 통해 단말이 기지국과 주고받는 제어 평면 메시지를 캡쳐해 단말의 SIB12 수신 및 공격자의 위조 재난문자를 화면에 표시하는 지 여부를 확인했다.

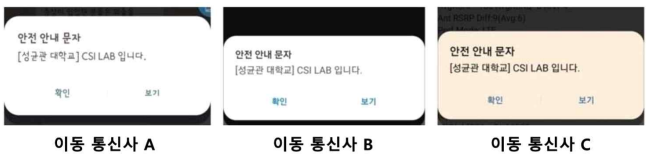
또한 본 실험과 관계없는 단말들이 영향을 받지 않도록 실험 단말을 SDR 장비에 최대한 가까이 위치시키고 송신 세기를 최대한 낮게 설정하였음을 밝힌다.

Ⅲ-3. 공격 테스트 및 결과

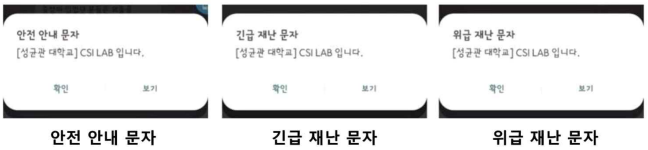
실험 결과 실험 단말 6대 모두 허위 기지국과 RRC 연결을 시도하며 허위 기지국이 브로드캐스팅하는 MIB와 페이징, SIB1, SIB12 메시지를 정상적으로 수신하는 것을 확인할 수 있었다.

그림 3. (a)는 이동통신 3사의 실험 단말이 안전 안내 문자를 수신하는 모습이며 (b)는 모든 단계의 재난문자를 수신하는 모습이다. 실험 결과 이동통신 3사의 실험 단말 모두 SIB12 메시지를 수신하는 즉시 화면에 스푸핑 된 재난문자를 표시했으며 허위 기지국에 입력한 임의의 위조된 재난문자가 정상적으로 디코딩되어 표시되는 것을 확인할 수 있었다. 또한 메시지 식별자만 수정하여 KPAS에서 정의된 안전 문자, 긴급 재난 문자, 위급 재난 문자 모두 스푸핑에 성공했다.

표 1.은 허위 기지국을 구동시킨 시점부터 A이동통신사의 단말이 연결을



(a) 통신사 3사별 재난문자 스푸핑 결과



(b) 재난문자 종류별 스푸핑 결과

그림 3. 재난문자 스푸핑 결과

표 1. A사 단말 재난문자 스푸핑 단계별 소요 시간

단위 : ms

	허위 기지국 구동 ~ 대상 단말 연결	대상 단말 연결~ 페이징 수신	페이징 수신 ~ SIB12 수신	전체 소요 시간
평균	299.9	120.4	120.1	540.4
표준편차	46.2	87.2	107.2	165.7

시도하고 SIB12 메시지를 수신해 화면에 내용이 표시되기까지의 각 단계별 소요 시간을 도표화한 것이다. 총 20회의 반복 실험 이후 도출한 평균 시간으로, 모든 단계의 시간을 합해도 1초 미만의 짧은 시간 내에 단말이 영향 받는 것을 확인할 수 있었다.

Ⅳ. 결론

본 논문에서는 LTE CMAS 재난 문자 표준의 보안 취약점을 확인하고 오픈소스와 SDR 장비를 이용해 현재 국내에서 서비스 중인 모든 종류의 재난 문자가 스푸핑 될 수 있음을 증명했다. 이를 통해 CMAS 표준의 취약점이 해외뿐만 아니라 국내에서도 동일하게 존재함을 알 수 있다.

이러한 취약점을 보완하기 위해 3GPP에서 제안한 digitally signing SIB12 메시지를 도입해 상용 기지국과 단말간의 signature를 발급하고 이를 통해 스푸핑된 SIB12를 검출하는 방법을 고려할 수 있다.[8] 다른 방법으로는 새로운 eNB를 식별하였을 때 해당 eNB에 연결을 시도하기 전 기존에 연결된 망을 통해 유효한 eNB인지 사전에 확인하는 방법도 생각해 볼 수 있다.

ACKNOWLEDGMENT

이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2020-0-00952, 5G+ 서비스 안정성 보장을 위한 엣지 시큐리티 기술 개발)

참 고 문 헌

[1] M. Hollingsworth et al., “This is your president speaking: Spoofing alerts in 4G LTE networks,” MobiSys 2019 - Proc. 17th Annu. Int. Conf. Mob. Syst. Appl. Serv., pp. 663 - 664, 2019.

[2] 3GPP TR 22.268, “Technical Specification Group Services and System Aspects; Public Warning System (PWS) requirements (Release 14),” 2017.

[3] 한국정보통신기술협회, “재난문자 서비스 제공을 위한 요구사항 및 메시지 형식,” 2019.

[4] “USRP X300.” [Online]. Available: https://www.ettus.com/all-products/x300-kit/

[5] “srsLTE.” [Online]. Available: https://github.com/srsLTE/srsLTE.

[6] “Signaling Collection and Analysis Tool (SCAT).” [Online]. Available: https://github.com/fgsect/scat.

[7] W. Li, “Hacking Public Warning System in LTE Mobile Network,” in HITBSecConf2019, 2019.

[8] 3GPP TR 33.969, “Technical Specification Group Services and System Aspects; Study on Security aspects of Public Warning System (PWS) (Release 14)”, 2017.

[9] 3GPP TR 33.331, “Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access(E-UTRA); Radio Resource Control(RRC); Protocol specification (Release 14)”, 2020.