VoLTE 서비스의 DoS 공격 보안 위협과 대응 방안

윤성호, 안현민, 조준형*, 임채태*, 김명섭
고려대학교 컴퓨터정보학과, *한국인터넷진흥원

{sungho_yoon, queen26, tmskim}@korea.ac.kr, *{scorch, chtim}@kisa.or.kr

Vulnerability of DoS Attack on VoLTE Service and Countermeasure

Sung-Ho Yoon, Hyun-Min An, JunHyung Cho*, ChaeTae Lim* and Myung-Sup Kim
Dept. of Computer and Information Science, Korea Univ., * Korea Internet & Security Agency

요 약

VoLTE 서비스의 상용화로 인해 고품질의 음성 및 멀티미디어 서비스가 가능해졌다. All-IP 기반의 LTE 망 특성상, 기존 인터넷 망이 가지는 보안 위협에 대한 노출이 불가피하다. 특히, VoLTE 서비스의 DoS 공격은 정상적인 음성 통화를 방해하기 때문에 공격 파급력이 매우 크다. 본 논문에서는 VoLTE 에서 발생 가능한 SIP REGISTER, SIP INVITE, RTP DoS 공격 보안 위협에 대해 살펴보고, 각 보안 위협에 대한 대응 방안을 제안한다.

Ⅰ. 서 론

스마트폰의 보급과 LTE 망의 상용화로 인해 모바일 트래픽이 급격히 증가하고 있다. 국내의 경우 모바일 트래픽은 2012 년 기준으로 전년도에 비해 약 80% 증가하였고, 전세계적으로도 2012 년 대비 2017 년까지 약 13 배 증가할 것으로 예상된다. 특히, 4G(LTE) 트래픽은 2017 년 non-4G 트래픽의 8 배 이상 발생할 것으로 예상된다[1].

VoLTE 서비스는 " Voice over LTE"의 약자로 LTE 환경에서 제공하는 음성 서비스를 의미한다. 따라서, 고품질의 음성뿐만 아니라 영상, 문자 등을 패킷 단위로 동시에 주고받을 수 있어, All-IP 기반의 서비스가 가능하다. 최근 국내에서도 VoLTE 서비스가 통신 3 사에서 상용화되었고 점점 시장규모가 확대될 것으로 예상된다.

VoLTE 는 All-IP 를 기반으로 동작되기 때문에 고품질의 음성 서비스를 제공할 수 있지만, 기존 3G 음성 서비스에서 고려되지 않는 보안 위협에 취약점을 가진다. 특히, 음성 서비스를 제공하는 서버나 수신 단말에 과도한 서비스를 요청하여 자원을 고갈 시키는 DoS 공격은 매우 치명적이다. 기존 3G 망 환경에서 DoS 공격에 대한 연구[2, 3]가 진행되었지만, 3G 망의 경우 DoS 공격의 대상이 한정적이었고, 공격도구 제작이 어려웠기 때문에 큰 파급력을 가지지 못하였다. 하지만, All-IP 기반의 LTE 망에서는 IP 를 통해 망 내 모든 서버 및 단말에 공격이 가능하고, 스마트폰에서 쉽게 공격도구를 제작할 수 있어 DoS 공격의 파급력이 점점 증가하고 있다. 본 논문에서는 VoLTE 에서 발생 가능한 다양한 DoS 공격 보안 위협에 대해 살펴보고 각 위협에 대한 대응 방안을 제안한다.

본 논문은 다음과 같은 순서로 기술된다. 2 장에서는 VoLTE 서비스에서 발생 가능한 3 가지 DoS 공격 유형을 살펴보고, 3 장에서는 이를 보안하기 위한 방안에 대해 제안한다. 마지막으로 4 장에서 결론 및 향후 연구를 제시한다.

Ⅱ. VoLTE DoS 공격

전통적인 인터넷 망의 DoS(Denial of Service) 공격은 정상적인 사용자가 특정 서버에서 제공하는 서비스를 제공 받지 못하도록 서버의 자원(메모리, 프로세서, 대역폭 등)을 고갈시키는 것이다. 이로 인해 사용자들은 서버와의 정상적인 통신이 어려워지고 기대하는 수준의 서비스를 제공받지 못하게 된다.

VoLTE 환경에서의 DoS 공격은 호 연결을 담당하는 IMS(IP Multimedia Subsystem) 서버들과 개별 단말을 대상으로 수행된다. VoLTE 서비스에서 발생 가능한 3 가지 DoS 공격 유형은 다음과 같다.

첫째, SIP REGISTER 메시지를 이용한 공격이다. VoLTE 사용 단말은 자신의 위치 및 상태 정보를 등록하기 위해 SIP REGISTER 메시지를 전송한다. 등록 요청 메시지를 지속적으로 등록 서버에게 요청함으로써 등록 서버의 오버헤드를 유발한다. 등록 과정은 사용자 인증 및 권환 확인 등 내부적으로 복잡한 수행 과정을 요구한다. 따라서, 지속적인 등록 요청은 서버에 큰 오버헤드를 줄 뿐만 아니라, 특정 사용자의 등록 키가 유출될 가능성도 있다.

본 연구는 미래부가 지원한 2013 년 정보통신 · 방송(ICT) 연구 개발사업의 연구결과로 수행되었음

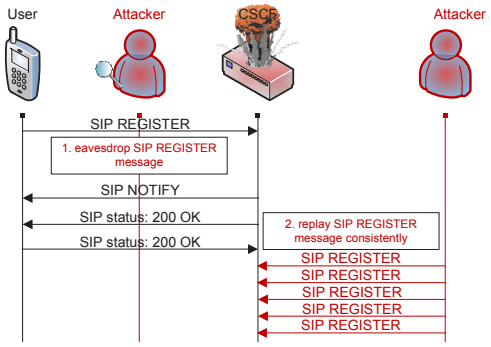

그림 1. SIP REGISTER DoS 공격

둘째, SIP INVITE 메시지를 이용한 공격이다. INVITE 메시지는 VoLTE 에서 호 연결을 시작하기 위해 사용한다. 공격 대상은 호 연결을 중계하는 서버 또는 수신 단말이다. 정상적인 호 연결 요청 메시지를 복제하여 서버와 단말에게 지속적으로 전송 시킴으로써 호 연결 요청 버퍼를 고갈시킨다. 호 연결은 모든 사용자에게 열려있기 때문에 지속석인 호 연결 요청 메시지는 서버와 단말에 정산적인 호 연결을 불가능하게 한다.

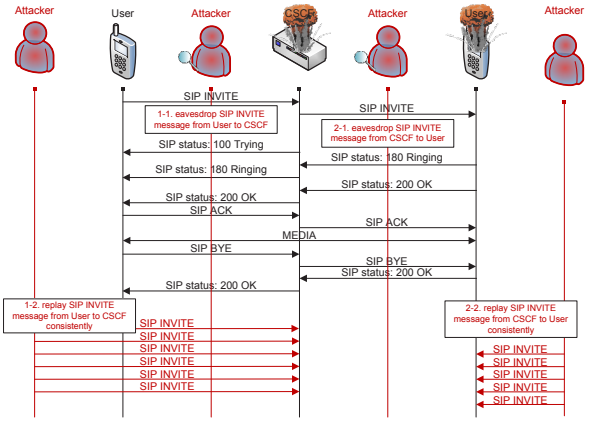

그림 2. SIP INVITE DoS 공격

셋째, RTP 를 이용한 공격이다. SIP 를 통한 호 연결이 성공하면, 음성 및 멀티미디어 데이터는 RTP(Real-time Transport Protocol)을 통해 전송된다. 보통 RTP 는 실시간성을 위해 UDP 로 전송된다. 따라서, 연결이 맺어진 단말의 RTP 포트를 대상으로 과도한 RTP 트래픽을 전송 시킴으로써, 호 연결 지연 및 통화 품질 저하를 유발 할 수 있다.

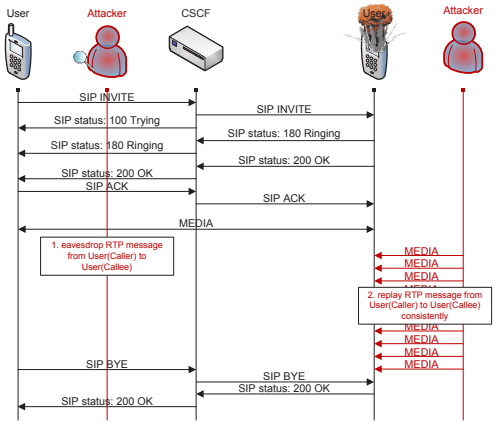

그림 3. RTP DoS 공격

Ⅲ. 대응 방안

VoLTE 서비스에서 발생 가능한 DoS 공격을 대응하기 위한 방안에 대해 기술한다. DoS 공격을 차단하기 위한 방법은 적용 위치를 기준으로 eNodeB 와 공격 대상 서버 및 단말로 구분된다.

단말이 연결되어 있는 즉, 공격 단말과 연결되어 있는 eNodeB 에서 통계 정보를 활용하여 특정 호스트가 과도한 트래픽을 요청하는 경우 차단할 수 있다. 또한, 공격 대상 서버 및 단말에서는 각 공격의 특성을 활용하여 차단할 수 있다. 앞서 살펴본 3 가지 공격 유형을 기반으로 서버 및 단말에서 DoS 공격을 차단하는 방법은 다음과 같다.

SIP REGISTER 공격을 차단하기 위해 인증된 호스트의 등록 요청만 받아 드리고, 등록 이후에는 타이머를 두어 일정 시간 이내에 발생되는 재 등록 요청을 거부한다. 또한, 매 등록 과정에서는 사용자 인증키를 요구하여 제 삼자의 악의적 등록을 원천적으로 차단한다.

SIP INVITE 공격은 호 연결 타이머를 두어 특정 사용자가 지속적인 INVITE 메시지를 보낼 경우, 해당 사용자의 요청을 차단함으로써 대응할 수 있다.

RTP 공격은 데이터의 무결성을 보장해주는 SRTP[4]를 사용함으로써 차단할 수 있다. 즉, 오직 허가된 단말에게만 데이터를 수신 받고, 그렇지 않은 단말에서 수신된 데이터를 처리하지 않는다.

Ⅳ. 결론 및 향후 연구

국내의 스마트폰 보급률은 전세계적으로 독보적이다. 이에 따라 기존 3G 망에서 고려되지 않던 새로운 보안 위협들이 고려대고 있다. 특히, VoLTE 서비스의 DoS 공격의 취약점은 All-IP 기반 LTE 망의 특성상, 더욱더 강조되고 있는 현실이다. 본 논문에서는 VoLTE 서비스에서 발생 가능한 세가지 DoS 공격 유형들에 대해 살펴보고, 이를 대응하기 위한 대응 방안을 제시하였다.

향후 연구로는 DoS 뿐만 아니라 SIP Parser 공격, SIP Message Modification 등과 같은 다양한 VoLTE 보안 위협에 대해 연구하고 이를 대응할 수 있는 방안에 대해 연구를 진행 할 예정이다.

참 고 문 헌

[1] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012- 2017," Cisco Visual Networking Index, 2013.

[2] Lee, P.P.C., Bu, T., and Woo, T. "On the Detection of Signaling DoS Attacks on 3G Wireless Networks," in IEEE INFOCOM'07, Anchorage, May 2007.

[3] Oh, J., Kang, D., Kim, S., and Im, C. "3G WCDMA Mobile Network DoS Attack and Detection Technology," in Proc of World Academy of Science, Engineering and Technology, Vol-69, 2012.

[4] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and Norrman, K "The secure real-time transport protocol (SRTP)," RFC 3711, 2004.