VoLTE에서의 SIP 메시지를 이용한 스캐닝 공격 및 탐지 방법

박성민, 조준형, 김세권, 임채태
한국인터넷진흥원
e-mail:(smpark, scorch, heath82, chtim)@kisa.or.kr

Scanning Attack by using SIP message and Detection Method in VoLTE

Park Seong Min, Cho Jun Hyung, Kim Se Kwon, Im Chae Tae
Korea Internet & Security Agency

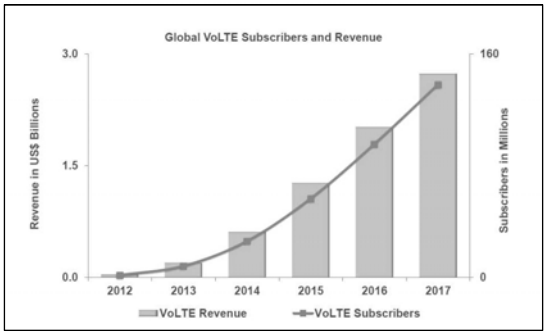
요 약

최근 이동통신 사업자들은 All-IP 기반의 서비스를 개발하고 상용화하기 위해 힘쓰고 있다. 그 이유는 All-IP 기반의 서비스가 LTE의 넓은 대역폭을 사용하여 기존 서비스와는 현저한 차별성을 가지고 있기 때문이다. 음성통화를 LTE 기반으로 제공하는 VoLTE 서비스도 그 중의 하나로서 현재 이동통신 3사 모두 상용화하여 이 새로운 고음질 및 고화질 커뮤니케이션 서비스에 대해 마케팅을 벌이고 있다. 하지만 VoLTE 서비스는 보안에 대한 충분한 고려가 이루어지지 않은 상태로 상용화되었으며, VoLTE에서 사용되는 SIP(Session Initiation Protocol) 프로토콜을 악용한 여러 유형의 공격에 매우 취약하다. 본 논문에서는 VoLTE 서비스에 대한 보안 위협 중 가장 기본이 되는 스캐닝 공격에 대해 기술하고 이를 탐지할 수 있는 방안을 제시한다.

1. 서론

최근 이동통신 망은 아이폰에서 시작된 스마트폰의 보급과 함께 4G 망으로 급격히 변화하였다. 뿐만 아니라 음성전화를 LTE 기반으로 제공하여 고품질 음성통화가 가능한 VoLTE 서비스를 출시하였다.

VoLTE 서비스는 고품질의 음성 뿐 아니라 영상, 문자 등을 패킷 단위로 동시에 주고받을 수 있어, 데이터 서비스를 이용하면서 통화가 가능한 All-IP 기반의 서비스이다. 미국의 경우 T-mobile이 작년부터 VoLTE 서비스를 시작했으며, AT&T는 올해 5월, 그리고 스프린트는 올해 9월부터 서비스를 시작하였다. 반면 국내에서는 작년부터 통신 3사 모두 상용화 되어 있으며 가입자가 점차 증가하는 추세이다. 세계적으로도 VoLTE 가입자는 2013년 8백만 명에서 2017년 138백만 명으로 증가할 것으로 예상되고 있다.[1]



(그림 1) 세계 VoLTE 가입자 예상 증가율

하지만 가입자와 트래픽이 증가함과 동시에 보안 위험성도 같이 증가하게 되었다. 특히 VoLTE 서비스는 All-IP를 기반으로 동작하기 때문에 기존 3G 음성 서비스에서는 고려되지 않았던 보안 취약점을 가질 수 있다. 특히 VoLTE 서비스는 SIP라는 텍스트 기반의 프로토콜을 사용하기 때문에 메시지 패킷의 위·변조가 쉬운 취약점이 존재한다.

본 논문에서는 VoLTE 보안 위협 중 가장 기본적인 공격인 스캐닝 공격에 대해 살펴보고 그에 대한 탐지 방안을 제시한다.

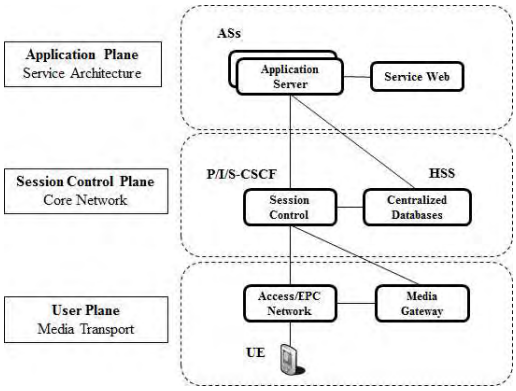
2. VoLTE 개요

VoLTE는 “Voice over LTE“의 약자로 LTE 환경을 이용한 음성 서비스를 의미한다. 3GPP 규격에 따라 SIP 프로토콜을 기반으로 하며 IMS(IP Multimedia Subsystem) 망을 이용한다. IMS 망은 크게 어플리케이션 플레인과 제어플레인, 그리고 유저 플레인으로 나눌 수 있다.

어플리케이션 플레인의 구성요소로는 다양한 서비스들을 제공하는 AS(Application Server)들이 존재한다. 예를 들어 발신번호표시, 착신전환과 같은 음성 부가서비스는

TAS(Telephony AS)에서 제공하고, 웹 발신표시와 같은 SMS(Short Message Service)에 대한 부가 서비스는 MSG-AS(Message AS)에서 제공한다. 제어 플레인은 SIP에 의한 세션제어 계층으로서 CSCF(Call Session Control Function)와 HSS(Home Subscriber Server)로 구분된다. CSCF는 다시 P/I/S-CSCF로 구분할 수 있는데, P(Proxy)-CSCF는 유저 플레인에서 수신한 SIP 메시지를 종류에 따라 다른 CSCF로 전달해주는 역할을 한다. I(Interrogating)-CSCF는 다른 IMS 또는 외부 망과의 관문 역할을 한다. 그리고 마지막으로 S(Serving)-CSCF는 IMS 망에 등록된 가입자의 DB인 Registrar와 연동하여 가입자의 Registration을 처리하고, AS로 호를 전달하여 메시지 종류에 따른 각각의 서비스를 제공받도록 한다. HSS는 IMS 가입자 정보에 대한 DB로서, Registration시에는 가입자 인증, 호에 대한 착신시에는 착신자의 등록정보를 알려주는 역할을 한다. 유저 플레인은 단말에 어플 형태로 삽입되어 있는 SIP 클라이언트를 말한다. SIP 클라이언트는 SIP서버에 해당하는 AS, CSCF와 함께 User-Agent로 분류된다.[2][3]

VoLTE는 LTE 환경의 넓은 대역폭을 사용하기 때문에 고품질의 음성코덱을 사용한 통화가 가능하다. 현재 국내에서는 AMR-WB 코덱을 사용하여 16kHz 의 Sampling rate를 가지는 HD(High Definition) Voice 통화 서비스를 제공하며, 화면공유와 같은 다양한 멀티미디어 서비스와의 융합도 가능하다. 또한 H.264 영상코덱을 사용한 고화질의 HD 영상통화 및 영상회의통화도 제공 중에 있다.[4]



(그림 2) IMS 네트워크 구조

3. SIP 프로토콜

SIP 프로토콜은 RFC3261에 근거하여 User-Agent간 멀티미디어 세션의 설정, 수정, 종료하여 주는 텍스트 기반의 프로토콜이다. 과거부터 인터넷전화를 이용한 VoIP 서비스에서 사용되어 왔으며 최근 VoLTE, RCS(Rich Communication Suite) 등의 서비스에서 기본적인 프로토콜로 사용되고 있다. SIP 프로토콜은 Request와 Response로 구분되며, Request에는 Registration을 위한 Register와 호 셋업을 위한 Invite가 대표적인 Method로 사용된다. Response에는 1xx~6xx 범위의 상태코드로 정의되며, 각 상태코드에 따라 용도가 정의되어 있다.[5]

SIP 메시지는 텍스트 기반으로서 헤더부분과 바디부분으로 나뉜다. 헤더부분에는 Method를 비롯하여 세션의 고유한 ID인 Call-ID 및 발, 착신 정보가 포함된 SIP헤더가 정의되고, 바디부분에는 세션의 미디어 정보가 정의되는데 음성, 영상통화의 경우 SDP(Session Description Protocol) 프로토콜을 사용하여 미디어 코덱을 표시한다. 특히 SIP 프로토콜은 텍스트 기반이기 때문에 헤더 정의 및 인식이 용이하나, 그만큼 위·변조 또한 쉽다는 단점을 가진다.

<표 1> SIP 프로토콜의 Method 종류 및 기능

Method	Function
REGISTER	Used by a UA to indicate its current IP address and the URLs for which it would like to receive calls
INVITE	Used to establish a media session between user agents
ACK	Confirms reliable message exchanges
BYE	Terminates a session between two users in a session
CANCEL	Terminates a pending request
OPTIONS	Requests information about the capabilities of a caller, without setting up a call

<표 2> SIP 프로토콜의 상태코드 종류 및 기능

Status-code	Function
1xx (Informational)	Request received and being processed
2xx (Success)	The action was successfully received, understood, and accepted
3xx (Redirection)	Further action needs to be taken (typically by sender) to complete the request
4xx (Client Error)	The request contains bad syntax or cannot be fulfilled at the server
5xx (Server Error)	The server failed to fulfill an apparently valid request
6xx (Global Errer)	The request cannot be fulfilled at any server

4. SIP메시지를 이용한 스캐닝 공격

본 논문에서는 VoLTE 서비스에서 SIP 메시지를 이용한 스캐닝 공격을 살펴보고자 한다.

(1) Registration을 이용한 CSCF 주소획득

앞서 살펴본 바와 같이 VoLTE 서비스는 SIP 프로토콜을 기반으로 한다. 따라서 VoLTE 단말의 패킷을 모니터링하면 SIP 메시지의 내용을 확인할 수 있다. SIP 메시지 내 헤더에는 여러 가지 정보들이 포함되어 있기 때문에 이를 확인하는 것만으로도 IMS 망 장비의 정보를 알아낼 수 있다. 특히, 단말이 전송한 Register 메시지에 대한 응답으로 수신되는 200 OK Response 에는 Service-Route 헤더가 포함되어 있다. Service-Route 헤더는 S-CSCF의 주소로서 단말이 Registration된 S-CSCF를 가리킨다. 단말이 Invite를 전송할 때의 첫 번째 목적지는 P-CSCF이지만, 해당

P-CSCF에 가입자의 S-CSCF 정보가 없는 경우 Registration 된 S-CSCF로 Invite를 전달할 수 없고 호 셋업은 실패하게 된다. 따라서 단말에서 통화 셋업 요청을 위한 Invite를 전송할 때, Registration시 200 OK 응답메시지를 통해 수신했던 Service-Route 헤더 내 S-CSCF 정보를 Route 헤더에 포함함으로서 P-CSCF에서 발신 단말이 등록된 S-CSCF를 찾을 수 있게 하는 것이다.[6]

S-CSCF 주소정보는 일반적으로 도메인에 기반하여 URI(Uniform Resource Identifier)로 표시되나, IP 주소로 직접 정의하기도 한다. 따라서 S-CSCF 주소가 IP 주소로 정의된 경우 단말의 패킷을 통해 S-CSCF IP 주소를 즉시 알아낼 수 있다. 뿐만 아니라 이와 같이 알아낸 S-CSCF IP 주소 대역으로 SIP Request들을 대량 전송하고 SIP Response가 오는 IP 주소에 대해 모니터링하면 IMS 망 장비들의 IP 리스트를 획득할 수 있게 된다. 일반적으로 IMS 망 장비들은 같은 대역을 사용할 확률이 크기 때문이다.

(그림 3) 단말의 SIP Registration 패킷

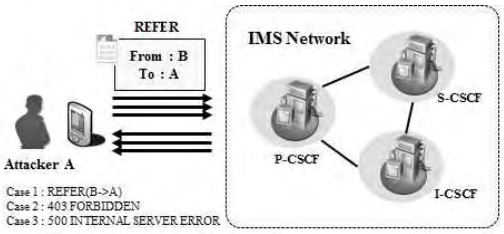
(2) Refer메시지를 이용한 단말 등록 정보 획득

두 번째는 SIP Refer 메시지를 이용한 VoLTE 단말에 대한 등록 정보를 획득하는 방법이다. Refer는 일반적으로 3자 회의통화를 시도할 때 기존 통화세션에 새로운 통화자를 초대하는 용도로 사용되는 Method이지만 아래와 같이 VoLTE 스캐닝 공격에 이용될 수 있다.[7]

스캐닝을 하려는 공격자가 Refer 메시지를 Registration 시 알아낸 S-CSCF IP주소 대역으로 전송하면 SIP 응답이 상황에 따라 다르게 수신된다. 여기서 공격자는 Refer의 발신번 및 착신번을 조작하여 Refer 메시지가 공격자에게로 돌아오게 만든다. 즉, Refer 메시지 내 From 헤더를 피해자의 번호로 위조하고, To 헤더를 Refer 메시지를 전송하는 공격자의 번호로 위조하게 되면, Refer 메시지가 전송된 목적지 IP가 피해자가 등록된 S-CSCF인 경우 Refer 메시지는 그대로 공격자에게 다시 전달된다. 만약 Refer 메시지가 돌아오지 않고 403 Forbidden 이라는 SIP 에러 응답이 수신된다면 해당 목적지 IP는 IMS 망 내에 존재하는 피해자가 등록되지 않은 또 다른 S-CSCF로 추측할 수 있다. 또다른 경우로는 500 Internal Server Error라는 SIP 에러 응답이 수신될 수 있는데, 이 경우는 목적지 IP가 S-CSCF가 아닌 IMS 장비라고 예상할 수 있다.

이와 같이 Refer 메시지를 사용하면 피해자 VoLTE 단말이 등록된 S-CSCF 주소를 알아낼 수 있다. 공격자가 피해자 VoLTE 단말이 등록된 S-CSCF 주소를 알아내게 되면, 공격자는 피해자 등록 정보를 이용하여 Invite 메시지의 위·변조할 수 있고, 보이스 피싱 또는 오과금 위협을 일으킬 수 있다.

특히 Invite 메시지와는 달리 Refer 메시지를 사용하면 실제 세션을 연결하기 위한 메시지가 아니기 때문에 망에서 과금 정보와 같은 스캐닝 공격에 대한 흔적을 남기지 않을 수 있다.



(그림 4) Refer 메시지를 이용한 스캐닝 공격

5. VoLTE 스캐닝 공격 탐지 방법

지금까지 살펴본 VoLTE 스캐닝은 SIP 메시지에 대한 모니터링과 SIP 메시지 위·변조를 통한 IP 대역 스캔 공격이었다. 이러한 측면에서 VoLTE 스캐닝에 대한 탐지를 위·변조된 SIP 탐지와 대량의 SIP 메시지 전송 탐지, 두 가지 방법으로 제시하고자 한다.

(1) 위·변조된 SIP 메시지 탐지

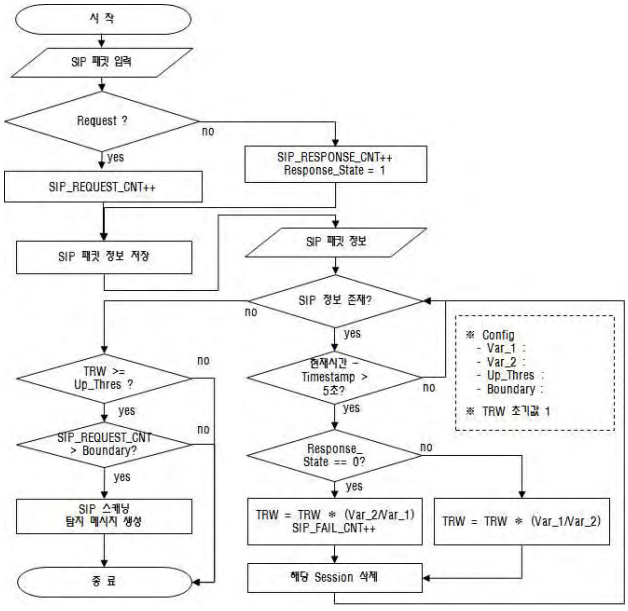
Registration 시 Service-Route 헤더 값에 대한 노출은 S-CSCF IP 주소를 도메인 형태의 URI로 변경하는 것으로 쉽게 대응할 수 있지만 SIP 메시지를 위·변조하여 전송하는 공격에 대한 탐지는 다음과 같은 알고리즘이 필요하다.

(그림 5) Refer 메시지 위·변조 탐지 알고리즘

이 알고리즘은 LTE 기반의 가입자 번호를 조회하여 실제 Refer 메시지 내 발신번호와 동일한지 비교해보고 일치하지 않는 경우 탐지정보를 생성하는 알고리즘이다. 이렇게 함으로서 Refer 메시지가 공격자에 의해 위·변조 되었는지 탐지할 수 있다.

(2) 대량의 SIP 메시지 전송 탐지

네트워크상의 탐지 시스템 입장에서는 공격자가 단말의 SIP 메시지를 모니터링 하는 것은 알 수 없지만, IMS 망 스캐닝을 위해 대량의 SIP 메시지를 IMS 망으로 전송하는 것은 아래와 같이 탐지가 가능하다.



(그림 6) SIP 스캐닝 탐지 알고리즘

이것은 TRW(Threshold Random Walk) 방식을 사용하여 SIP 요청에 대한 응답이 없는 경우를 카운트하고, 설정한 임계치를 넘는 경우 스캐닝 탐지정보를 생성하는 알고리즘이다. TRW는 두 개의 변수를 사용하여 메시지 하나당 증가폭을 결정하며, SIP 응답이 없는 경우만 증가시킴으로서 스캐닝 여부를 판단하게 된다. 그리고 TRW가 임계치를 넘는 경우 SIP 요청의 개수에 따라 SIP 스캐닝 탐지 정보를 생성한다.

6. 결론

이동통신 망의 발전에 따른 4G 기술의 도입으로 인해 우리 생활은 이전보다 훨씬 편리해졌다. 하지만 새로운 기술의 발전에 따라 보안 위협을 유발하는 수법 또한 발전하고 있다. 특히 현재 상용화되어 있는 VoLTE 서비스의 가입자는 갈수록 증가하고 있으나, 이동통신 망은 폐쇄망이라는 인식으로 인해 보안에 대한 충분한 고려가 이루어지지 않고 구축되었으며, 서비스 거부 등 여러 악의적인 공격에 매우 취약한 것이 현실이다. 특히 텍스트 기반의 SIP 프로토콜을 사용한다는 특징은 기존의 3G 음성통화에서 보다 더 큰 보안 위협의 가능성을 안고 있다.

본 논문에서는 VoLTE 보안 위협 중 가장 기본이 되는 스캐닝 공격 위협 및 탐지 방안에 대해 살펴보았다. 하지만 더 중요한 것은 스캐닝을 통해 알아낸 정보를 악용하여 오과금 유발, 통화 불능 등 실제 VoLTE 서비스에 영향을 주는 공격들에 대한 방어이다. 따라서 이동통신 망은 폐쇄망이라는 인식에서 벗어나 어떤 공격들이 잠재되어 있는지 고찰하고 미리 방어할 수 있는 대책 마련이 시급하다.

ACKNOWLEDGMENT

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음"(13-912-06-001, 4G 망 공격/비정상 트래픽 탐지 및 대응 기술 개발)

참고문헌

[1] Infonetics Research, Mobile VoIP and Subscribers Worldwide and Regional Market Size and Forecasts, June 2013.

[2] 김무완, 우노 신타로, 이토우 료조우, 나카무라 미츠히로, "IMS(차세대 네트워크 서비스 제어 기술, IP MULTI MEDIA SUBSYSTEM)", 광문각, Nov, 2008

[3] 3GPP, "IP Multimedia Subsystem (IMS); Stage 2 (Release 12)" TS 23.228 V12.4.0, Mar, 2014

[4] M.Poikselka, H. Holma, J. Hongisto, J. Kallio, A. Toskala, Voice over LTE (VoLTE), Willy, Feb, 2012

[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP : Session Initiation Protocol", RFC 3261, June 2002.

[6] D. Willis, B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration", RFC 3608, October 2003

[7] R. Sparks, "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003