VoIP 망에서 SIP 취약점을 이용한 위협의 분석과 대응

김무성*, 문길종*, 양승호*, 노봉남**, 김용민***
*(주)정보보호기술,
**전남대학교 시스템보안연구센터, ***전남대학교 전자상거래전공
e-mail:kimms@infosec.co.kr, alcorjjong@infosec.co.kr, shyang@infosec.co.kr
bbong@chonnam.ac.kr, ymkim@chonnam.ac.kr

Analysis and Countermeasure of Threats using SIP Vulnerabilities on VoIP Network

Mu-Sung Kim*, Gil-Jong Mun*, Seung Ho Yang*, Bong-Nam Noh**,
Yong-Min Kim***
*InfoSec Technology Co., LTD., **SSRC, Chonnam National University
***Dept of Electronic Commerce, Chonnam National University

요 약

VoIP를 위한 개방형 규약 중 SIP는 IETF에서 정의한 시그널링 규약으로 IP 네트워크에서 음성, 영상의 호와 같은 멀티미디어 통신 세션을 제어하기 위해 널리 사용한다. 공격자는 SIP의 취약점을 이용한 전화번호 스캐닝, 사용자 암호를 알아내기 위한 사전공격, 콜 플러딩 공격을 통해 VoIP 서비스 정보를 절취하거나 이용을 방해 할 수 있다. 본 논문에서는 VoIP 환경의 SIP 스캐닝, 콜 플러딩, 그리고 무차별 대입 공격을 분석하고 대응방안을 제시한다.

1. 서론

VoIP(Voice over Internet Protocol)는 음성을 IP 네트워크에서 제공하기 위한 통신 규약이다. VoIP는 PSTN의 단점인 낮은 대역폭을 극복하고, 음성과 데이터로 나누어진 망을 통합하여 높은 대역폭을 가지고 있는 데이터 망을 통해 효율적으로 음성 신호를 전달하는 규약이다. VoIP를 위한 여러가지 개방형 규약들과 표준들이 존재하며, 현재 VoIP 네트워크에서 가장 널리 쓰이고 있는 SIP(Session Initiation Protocol)는 TCP와 같이 양 단말간 세션을 연결하는 과정 및 재전송 기능이 없는 UDP 기반으로 SIP 메시지 조작 및 전송이 쉽다는 취약점이 있다. SIP는 일반적인 요청 혹은 조작된 요청에 대해서도 응답을 보내기 때문에 공격자는 여러 가지 정보를 절취할 수 있다. 예를 들면, 외부의 공격자는 특정 SIP 메소드를 이용한 스캐닝 공격으로 서버의 VoIP 전화번호 정보를 절취 할 수 있다. 또한, SIP 메시지를 조작하여 임의의 호 연결 요청을 생성할 수 있다. SIP에서 사용자 인증이 항상 요구되는 것은 아니며, 만약 인증을 한다고 하더라도 인증을 위한 정보가 대부분 사용자명, 암호와 같은 단순한 정보로 이루어져 있고 암호는 MD5 해쉬 값으로 전송되어 무차별 대입 공격에 취약하다. 사전대입 혹은 해당 통신사업자 혹은 VoIP 서비스 이용회사의 특성을 이용하여 패스워드를 추측할 수 있다.

본 논문에서는 서버에 다수의 요청을 보내어 전화번호 정보를 획득하는 스캐닝(scanning) 공격, 조작된 메시지를 통한 콜 플러딩(call flooding), 암호를 알아내기 위한 무차별 대입(brute force) 공격에 대한 위협을 실험 및 분석하고 이에 대한 대응방안으로 공개형 소프트웨어를 이용한 공격 탐지 방안을 제시한다.

본 논문은 2장에서 SIP 공격의 관련 연구를 제시하고, 3장과 4장에서는 SIP 공격의 실험과 대응방안에 대하여 분석하며, 5장에서 결론을 기술하였다.

2. 관련연구

표 1은 VoIP를 위한 여러가지 개방형 규약들과 표준들을 보인 것이다.

<표 1> VoIP 개방형 규약 및 표준

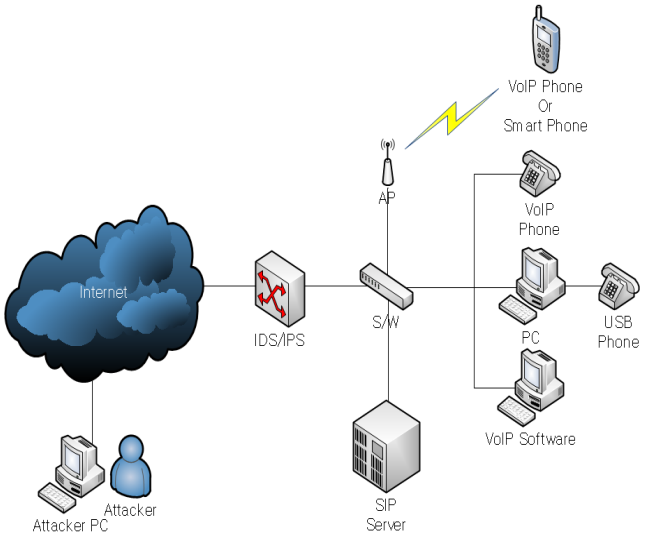
규약	기관	설 명
H.323	ITU-T	패킷 네트워크에서 AV(Audio- Visual) 통신 세션을 제공하기 위해 개발
IMS	3GPP	IP 멀티미디어 서비스를 전달하기 위해 개발된 프레임워크
MGCP	IETF	IP 네트워크와 PSTN에서 미디어 게이트웨이를 제어
SIP	IETF	IP 네트워크에서 음성, 비디오 콜들과 같은 멀티미디어 통신 세션들을 제어
RTP	IETF	인터넷 상에서 음성과 비디오를 전달
SDP	IETF	스트리밍 미디어 시작 값을 표현

패킷 네트워크에서 AV(Audio-Visual) 통신 세션을 제공하기 위한 H.323[1], IP 멀티미디어 서비스를 전달하기 위한 프레임워크인 IMS(IP Multimedia Subsystem), IP 네트워크와 PSTN에서 미디어 게이트웨이를 제어하기 위한 MGCP (Media Gateway Control Protocol)[2], IP 네트워크에서 음성, 비디오 호(call)들과 같은 멀티미디어 통신 세션들을 제어하기 위한 SIP(Session Initiation Protocol)[3], 인터넷 상에서 음성과 비디오를 전달하기 위한 RTP(Real-time Transport Protocol)[4], 스트리밍 미디어 시작 값을 표현하기 위한 SDP(Session Description Protocol)[5] 등이 있다.

SIP 관련 위협 및 대응방안에 대하여 RFC 3261에서는 SIP 보안 메커니즘으로 HTTP Digest, S/MIME, TLS, SIPS URI 등을 제시하였다. Aegean 대학에서는 SIP 메시지 조작에 대하여 IPsec, TLS, S/MIME 적용과 플러딩 공격에 대하여 올바른 장치 설정을 대응방안으로 제시하였다[6]. 또한, SIP 시그널링 공격에 대한 대응방안으로 IP 인증과 사용자의 인증을 위한 Checker 헤더를 제시하였고[7], SIP 취약점에 대한 대응 방안으로 비정상 행위를 효율적으로 탐지하는 기술을 수행하는 상태정보 기법과 사용자와 프록시 서버 간 인증을 통한 안전한 SIP통신 환경에 대한 프로토콜을 제시하였다[8]. 그러나, 기존에 제안한 프로토콜들을 현재의 VoIP 환경에 적용하기 위해서는 많은 시간과 서버, 단말의 교체 및 설정이 필요하다.

3. 위협 행위의 실험 및 분석

본 장에서는 서버에 다수의 요청을 보내어 전화번호 정보를 획득하는 스캐닝 공격, 조작된 메시지를 통한 콜 플러딩, 암호를 알아내기 위한 무차별 대입 공격에 대한 위협을 실험하고 분석한다.



(그림 1) 위협 행위의 VoIP 네트워크 구성도

공격 실험을 위한 VoIP 네트워크 구성은 그림 1과 같다. SIP 서버는 공개용 소프트웨어를 이용하였고, 서버에 저장된 사용자 계정은 암호가 없는 사용자 계정과 암호를 지정한 사용자 계정으로 구성된다. 서버는 사설주소와 공인 주소를 가지며, 공격자는 외부의 다른 공인 주소를 갖는다. 공격 탐지 및 검증을 위해 공개형 IDS인 Snort를 이용하였다.

3-1. 전화번호 스캐닝

SIP 요청 메소드 중, "*OPTION*"은 서비스의 가용성을 질의하는데 쓰인다. VoIP 단말과 서버는 주기적으로 이 메소드를 이용하여 서비스 가용 여부를 체크한다. 사용자 단말이 SIP 서버로 특정 전화번호에 대하여 "*OPTION*" 메소드를 이용한 요청을 보낼 경우, SIP 서버는 이 전화번호의 가용성 여부에 대한 응답을 전송한다. 그림 2는 위협행위 네트워크 환경에서 공격자가 발생한 스캐닝 공격 패킷을 보인 것이다.

응답 코드로 "*200 OK*"가 전송되는 경우, 전화번호가 유효한 것을 알 수 있으며, 그렇지 않을 경우는 "*404 Not found*" 응답이 전송된다. 공격자는 이 메소드를 이용하여 서버 내의 전화번호 리스트를 획득 할 수 있다.

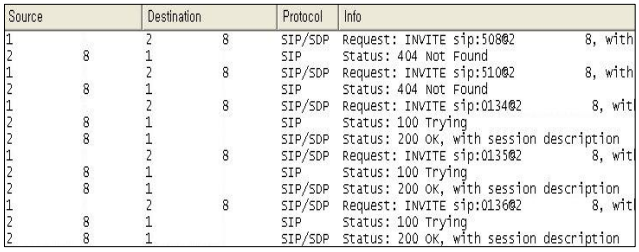
Source	Destination	Protocol	Info
1 2 8	1	SIP	Request: OPTIONS sip:507@2 8
2 8	1	SIP	Status: 404 Not Found
1 2 8	1	SIP	Request: OPTIONS sip:508@2 8
2 8	1	SIP	Status: 404 Not Found
1 2 8	1	SIP	Request: OPTIONS sip:510@2 8
2 8	1	SIP	Status: 404 Not Found
1 2 8	1	SIP	Request: OPTIONS sip:0134@2 8
2 8	1	SIP	Status: 200 OK
1 2 8	1	SIP	Request: OPTIONS sip:0135@2 8
2 8	1	SIP	Status: 200 OK
1 2 8	1	SIP	Request: OPTIONS sip:0136@2 8
2 8	1	SIP	Status: 200 OK
1 2 8	1	SIP	Request: OPTIONS sip:3001@2 8
2 8	1	SIP	Status: 200 OK

(그림 2) *OPTION* 메소드를 이용한 전화번호 스캐닝

3-2. 콜 플러딩

SIP 요청 메소드 중, "*INVITE*"는 호를 생성하는데 쓰인다. 서버에 암호가 없는 계정이 있다면, 공격자는 SIP 메시지를 조작하여 이 계정에 대한 호를 생성 할 수 있다.

전화번호가 존재하지 않는 경우 응답 코드로 "*404 Not Found*"가 전송되며, 존재하는 경우 응답 코드로 호 연결을 시도하는 "*100 Trying*"과 호 연결이 완료됨을 알리는 "*200 OK*"가 전송된다. 호 연결 과정이 완료되면 해당 호 연결 요청을 받은 전화기는 벨이 울린다. 전화번호를 계속적으로 변경하여 요청을 생성하면 사용자의 업무, 서비스 방해가 될 수 있다.

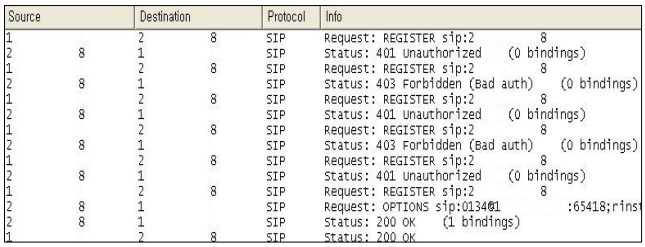


(그림 3) *INVITE* 메소드를 이용한 콜 플러딩

3-3. 무차별 대입 등록 공격

SIP 요청 메소드 중, "*REGISTER*"는 단말이 서버에 등록 할 때 사용된다. 공격자는 SIP 메시지를 조작하여 허위 등록을 하거나, 암호를 알아내기 위해 무차별 대입 공격을 할 수 있다.

서버는 단말의 등록 요청에 대하여 응답코드로 "*401 Unauthorized*"를 전송함으로써 암호를 요구하며, 단말의 재등록 요청의 암호가 맞지 않을 경우, 응답으로 "*403 Forbidden (Bad auth)*"이 전송한다. 무차별 대입 등록 공격이 발생되면 "*403 Forbidden (Bad auth)*" 응답코드가 대량으로 발생하게 된다.



(그림 4) *REGISTER* 메소드를 이용한 무차별 대입 등록 공격

4. 위협 대응방안

본 장에서는 3장에서 실험한 공격에 대해 IDS/IPS의 임계치를 이용한 탐지 및 차단 방안을 제시한다.

현재 VoIP 서비스 제공 업체들은 UDP 기반의 SIP를 사용하고 있으며, 단순한 암호기반으로 인증을 수행한다. 관련연구에서 제시한 방법들을 적용하기에는 많은 시간과 자원이 소비된다. 또한, TCP 기반으로 시그널링 처리를 하면, 공격자에 대한 추적은 쉽지만, TCP기반으로 적용된다 하더라도 암호를 알아내기 위한 무차별 대입 공격에 대한 방어는 임계치에 의한 탐지 및 차단이 필요하다. 본 논문에서는 3장에서 분석한 결과를 바탕으로 공개형 IDS인 Snort형식의 규칙을 생성하여 탐지 및 차단 한다.

4-1. 임계치 측정 방법

본 논문에서 제시한 SIP 공격 위협을 탐지하기 위한 임계치는 공격자 IP를 기준으로 측정하였다. 또한 임계치는 정상적인 VoIP 통신에서 각 메소드에 대한 패킷 발생량을 고려하여 설정하였다. 표 3은 일반 및 공격 상황에서의 임계치이다.

<표 3> 일반 및 공격 상황 임계치

(단위 : 건수/초)

일반		공격	
분류	임계치	분류	임계치
가용성 여부 체크	1/60 혹은 1/30	전화번호 스캐닝	30/3
호 연결 요청	1건	콜 플러딩	30/3
사용자등록	1건 혹은 2건	무차별 대입등록 공격	5/60

일반적으로 정상적인 사용자의 단말은 약 1분에서 30초 간격으로 "OPTION" 메소드를 이용한 가용성 체크 패킷을 발생하는데 공격 도구를 이용한 SIP 스캐닝 공격은 3초에 30건 이상의 패킷을 발생한다. 또한, 정상적인 사용자는 한 번에 한 건의 호 요청을 발생하지만 공격 도구를 이용한 콜 플러딩 공격은 3초에 30건 이상의 패킷을 발생한다. 마지막으로 공격자가 암호를 알아내기 위해 여러 번 등록 요청 패킷을 발생 하거나 공격 도구를 이용한 무차별 대입 등록 공격 패킷을 발생 할 경우 60초에 5건 이상의 패킷을 발생한다.

4-2. 규칙생성

<표 2> 공격 탐지 규칙

공격종류	탐지규칙
전화번호 스캐닝	alert udp any any -> $SIP_server_IP $SIP_server_Port (content:"OPTIONS"; depth:7; pcre:"/^OPTIONS\s+sip\x3a[^\r\n\s]+\x40[^\r\n\s]+\s+SIP\x2f2\x2e0/i"; threshold: type both, track by_src, count 30, seconds 3;)
콜 플러딩	alert udp any any -> $SIP_server_IP $SIP_server_Port (content:"INVITE"; depth:6; pcre:"/^INVITE\s+sip\x3a[^\r\n\s]+\x40[^\r\n\s]+\s+SIP\x2f2\x2e0/i"; threshold: type both, track by_src, count 30, seconds 3;)
무차별 대입등록 공격	alert udp $SIP_server_IP $SIP_server_Port -> any any (content:"SIP|2f|2.0 403 Forbidden |28|Bad auth|29|"; nocase; depth:32; threshold: type both, track by_dst, count 5, seconds 60;)

표 2는 각 공격을 탐지하기 위한 규칙을 생성한 것이다. SIP_*server* 변수는 SIP 서버의 주소를 의미하고, SIP_*server_Port*는 SIP 서버가 사용하는 포트를 의미한

다. 차단을 위해서는 *alert*를 *drop*으로 변경하면 된다.

4-3. 적용 결과

Snort에 생성한 규칙을 적용하여 공격을 효과적으로 탐지할 수 있었다. 그림 5의 각 항목은 탐지명, 공격자 주소, 공격자 포트, 공격대상 주소, 공격대상 포트이다.

Register Brute Force Attack Detection	2	8	UDP/5060	1		UDP/20244
Call Flooding	1		UDP/14732	2	8	UDP/5060
Extension Scanning	1		UDP/14646	2	8	UDP/5060

(그림 5) Snort 공격 탐지결과

본 논문에서 SIP 공격 위협에 대응하기 위해 제시한 탐지 규칙을 적용한 공개형 IDS를 이용하여 공격을 탐지하는 것이 새로운 프로토콜을 적용하는 것 보다 시간과 비용 측면에서 더 효과적이다.

5. 결론

본 논문에서는 VoIP 환경에서 발생할 수 있는 전화번호 정보를 획득을 위한 스캐닝 공격, 조작된 메시지를 통한 콜 플러딩, 암호를 알아내기 위한 무차별 대입 공격에 대해 살펴보고, 이러한 공격 위협들의 대응방안 도출을 위해, H.323, IMS, MGCP, SIP, RTP, SDP의 VoIP 규약 및 표준에 대해 설명하였다. 또한 공격 실험, 분석 및 대응방안 검증을 위해 테스트베드 환경을 구축하고, 위협을 분석하여 Snort 규칙기반 탐지 및 차단 규칙을 생성하였다. 생성된 규칙이 탐지 및 차단에 효과적임을 확인하였다.

향후 RFC 3261에서 제시한 SIP 보안 메커니즘인 HTTP Digest, S/MIME, TLS, SIPS URI등이 VoIP 네트워크에 적용될 경우 임계치 및 규칙의 수정이 필요하다.

참고문헌

[1] ITU-T, "H.323 : Packet-based multimedia communications systems" Recommendation H.323, ITU-T

[2] F. Andreasen, B. Foster, "Media Gateway Control Protocol (MGCP) Version 1.0", RFC 3435, IETF

[3] J. Rosenberg, et al, "SIP: Session Initiation Protocol", RFC 3261, IETF

[4] H. Schulzrinne et al, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, IETF

[5] M. Handley, V. Jacobson, C. Perkins, "SDP: Session Description Protocol", RFC 4566, IETF

[6] Dimitris Geneiatakis, et al, "SIP Security Mechanisms: A state-of-the-art review", University of the Aegean

[7] 강석인 외 3명, "SIP Signaling 공격에 대한 방어 기법", 한국정보과학회 가을 학술발표논문집 제 35권 제 2호 (D), 2008, pp.40-45

[8] 윤하나 외 1명, "SIP 공격 대응을 위한 보안성이 강화된 Stateful SIP 프로토콜", 한국콘텐츠학회논문지 제10권 제1호, 2010, pp.46-58