Gateway 방식에서 SIP Fraud Call 공격기법 관한 연구

양종성*,최형기*,장학범**,강성용*,금기호***
*성균관대학교 이동통신공학과
**성균관대학교 정보통신공학과
***삼성 SDS 인프라 SE3
e-mail : jsyang@hit.skku.edu

A Study on SIP Fraud Call Attack Method and Protect Base on Gateway

Jong-Sung Yang*, Hyoung-Kee Choi*, Hak-beom Jang**, Sung-yong Kang*,ki-ho Gum***
*Dept. Mobile Communication Engineering, Sungkyunkwan University
**Dept. Information and Communication Engineering, Sungkyunkwan University
***Infra SE3 Group , SamsungSDS

요 약

최근 VoIP 서비스는 IP 네트워크의 안정화를 기반으로 국내 기업 Legacy PSTN 시장을 빠르게 대체해 가고 있다. 그러나 VoIP 서비스는 기존 인터넷망에서 발생 할 수 있는 보안 취약성 뿐 아니라 인터넷 전화 트래픽의 통과 문제 및 VoIP 스팸이나 도청 같은 기존에 없었던 새로운 이슈들을 발생 시키고 있다. 특히 SIP 인증 취약점을 이용한 Fraud Call 공격은 VoIP 서비스 사용자로 하여금 원하지 않은 호 및 과금을 대량 발생 시키는 공격기법으로 최근 기업의 피해사례가 늘어 나고 있다. 본 논문은 Fraud Call 의 공격 기법을 분석하고, 호 인증 측면에서의 보안적 대응방안을 기술하고자 한다.

1. 서론

Circuit-Switched Network(Legacy PSTN)는 폐쇄된 Network 환경을 가지며, 단일 서비스(Voice)에 최적화된 구성으로 보안 위협을 최소화 할 수 있다. 이에 반해 IP 서비스는 기술이 표준화되어 있고 개방된 구조로서, 구현된 소프트웨어나 하드웨어에 제약을 받지 않고 목적지 주소만 알고 있으면 아주 적은 비용으로 전 세계 어디서든 접근이 가능하다. 이러한 개방성은 “도청”,”서비스거부공격”,”서비스오용공격”,’세션가로채기” 같은 보안적 위협을 가지고 있으며, IP 기반에 Voice 를 Emulation 한 VoIP 역시 태생적으로 동일한 보안적 위협을 가지고 있다.

IETF 에서 표준화한 SIP(Session Initial Protocol) [1]는일반적으로 Client-Server 환경에서 동작하지만, UAC-UAS 방식으로도 동작이 가능하다. Client-Server 환경은 발신자의 인증을 위하여 ID/Password 기반의 HTTP Digest 메커니즘, 홉간 메시지의 무결성 및 기밀성을 보장하기 위한 TLS(Transport Layer Security)를 정의 하였지만, UAC-UAS 방식은 발신자를 인증할 수 있는 효과적인 메커니즘을 지원하지 않는다. IETF[2]에서는 UAC-UAS 인증을 위하여 RFC3261 를 통해 공인인증서 서명 방식의 S/MIME(Secure/Multipurpose Internet Mail Extension)를 권고하지만 현실적으로 적용하기가 쉽지 않다. 이에 UAC-UAS 방식은 인증을 메커니즘을 구현하지 않는 경우가 대부분이다. 또한 대부분 기업은 기존 투자된 교환기 인프라를 활용하기 위하여 ALL IP telephony 방식이 아닌 Gateway 를 이용한 PSTN 과 SIP 가 혼재된 방식으로 구성하여, 외부에서 SIP 로 접속된 호가 PSTN Re-Routing 될 수 있는 경로를 가지고 있다. 공격자는 이러한 SIP 의 인증 취약점과 PSTN 의 연결 경로를 이용하여, Fraud Call 공격을 시도 한다. 공격이 성공되면 대량의 국제호가 공격 대상자의 내부 Voice 망에서 발생이 되고, 이는 대량의 과금을 발생시키게 된다. 이러한 Fraud Call 은 호 흐름(Call Flow)상 정상적인 외부 발신 형태를 가지므로, 과금이 청구되기 전까지 피해 여부를 파악하기 어렵다. 그러므로 공격자는 최대 1 개월까지 지속적으로 공격을 시도하게 되고 피해가 더욱 커지는 성향을 가지게 된다.

본문의 구성은 다음과 같다. 2 장에서는 SIP 의 Client-Server 방식의 Call Flow(HTTP Digest)와 UAC-UAS(미인증)방식의 Call Flow 를 비교한다. 3 장에서는 UAC-UAS 방식에서 발생하는 Fraud Call 의 공격기법을 분석하고 4 장에서 논문의 결론을 맺는다.

2. SIP Call Flow 비교

SIP 에서는 User-Agent, Proxy-Server, Redirect-Server,

Location-server, Registrar 로 총 5 개의 구성요소를 정의한다. User-Agent(UA)는 IP Phone 또는 Gateway 로 구성될 수 있으며, Server 역시 Redirect 또는 proxy 로 구성할 수 있으며 이에 따라 Call flow 가 달라진다. 본문에서는 Proxy-server 를 기준으로 한 Client-Server 방식과 UAC-UAS 방식의 Call Flow 를 기술한다.

2.1 Client-Server 방식 (HTTP Digest)

SIP Client-Server[1] 구성에서 UA 는 Proxy-Server 에 ID/Password 기반 HTTP Digest 인증 메커니즘을 사용하여 Proxy 서버에 등록을 한다. SIP HTTP 인증은 (RFC 2617)의 방식을 따르지만 Digest 인증 방법만을 사용한다. SIP Digest 인증은 사용자에 대한 인증과 재사용 공격만을 방지하며, 메시지에 대한 무결성과 기밀성은 보장하지 않는다.

```
REGISTER sip:172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK200B
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-87RT
To: <sip:36602@172.18.193.187>
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 1 REGISTER
Contact: <sip:36602@172.18.193.120:5060>;user=phone
Expires: 60
Content-Length: 0
```

(그림 1) Register Message

UA 는 그림 (1)_Register Message 를 Proxy-Server 에 보낸다. 이때 Register Message 정보에는 인증정보가 포함 되어져 있지 않다.

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK200B
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-87RT
To: <sip:36602@172.18.193.187>;tag=3046583040568302
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
CSeq: 1 REGISTER
WWW-Authenticate: Digest realm="example.com", qop="auth",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algori
Content-Length: 0
```

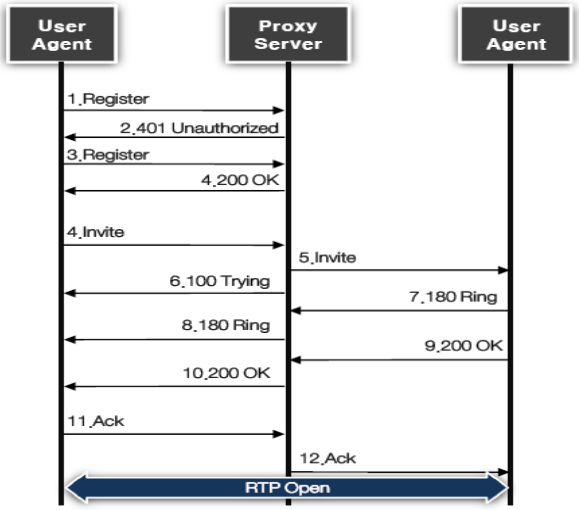
(그림 2) 401 Unauthorized Message

Register Message[1]를 받은 Proxy-Server 는 그림 (2)_401 Unauthorized Message 를 이용하여 UA 에게 Digest Challenge 를 전송한다. 401 Unauthorized message 에는 Challenge 를 위한 nonce 값, qop=auth 등이 포함되어져 있다. qop=auth[1] 는 Server 가 사용자 인증을 제공하겠다는 의미이다.

```
REGISTER sip:172.18.193.187:5060 SIP/2.0
Via: SIP/2.0/UDP  172.18.193.120:5060;branch=z9hG4bK1DEA
From: "36602" <sip:36602@172.18.193.120>;tag=98AS-89FD
To: <sip:36602@172.18.193.187>
Call-ID: A9EEC728-495E11D6-8003AD63-F55A9C4
User-Agent: Cisco-SIPGateway/IOS-12.x
Authorization: Digest username="36602", realm="example.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:172.18.193.187",
response="dfe56131d1958046689d83306477ecc"
CSeq: 2 REGISTER
Contact: <sip:36602@172.18.193.120:5060>;user=phone
Expires: 60
Content-Length: 0
```

(그림 3) Register Message For Response

Challenge 를 받은 UA 는 자신의 ID 및 Password 등의 정보를 기반으로 Response 값을 만들어 그림 (3)_Register Message 값을 만들어 전달하고, Proxy-Server 의 승인을 받으면 Registration 이 완료 된다.

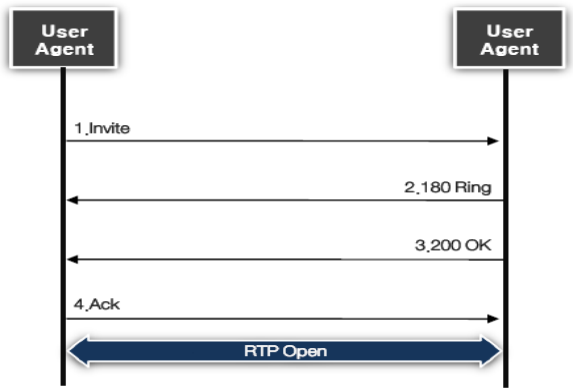


(그림 4) Client Server 방식의 Call Flow

Proxy-Server 에게 인증 받고 등록이 된 UA 는 그림 (4)와 같이 정상적인 SIP Signaling[3]을 통하여 RTP(Realtime Transport Protocol)를 개방한다.

2.2 UAC-UAS 방식

UAC-UAS 구성 시 공인인증서 기반의 S/MIME 를 사용한다면 사용자 인증을 제공할 수 있으나, 모든 UAC 가 공인인증서를 가지기에는 현실적으로 어렵다. 그래서 SIP 구성 환경에서는 사용자 인증과정을 구현하지 않는 경우가 대부분 이다.

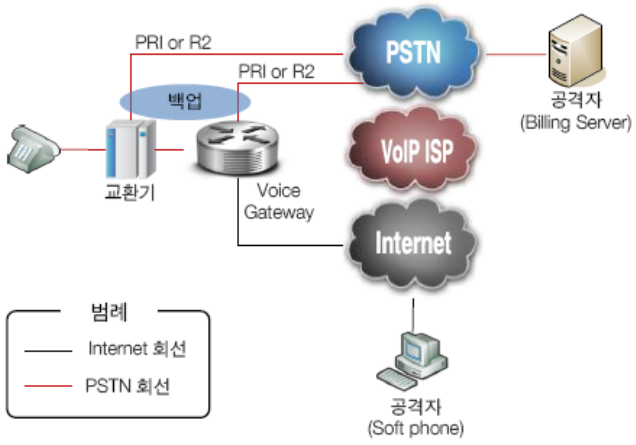


(그림 4) UAC-UAS 방식의 Call Flow

이에 UAS 는 그림(4)와 같이 자신에게 요청 되어지는 Invite Message 를 사용자 인증 없이 100% 수용한다.

3. SIP Fraud Call 공격 기법

일반적으로 SIP Fraud Call 공격 대상이 되는 네트워크 구성은 그림(6)과 같다. 내부 전화 네트워크는 기존 교환기를 사용하고, Outbound Call 을 위해 Voice Gateway 를 사용하여 VoIP 사업자와 SIP 연동을 구성한다. Voice Gateway 는 내부 교환기와 PRI,R2 등 PSTN 회선을 사용하여 연동하고, SIP 장애를 대비하여 PSTN 경로를 추가적으로 구성하여 이중화 한다.



(그림 6) 공격대상자의 일반적 SIP 구성

3.1 취약점

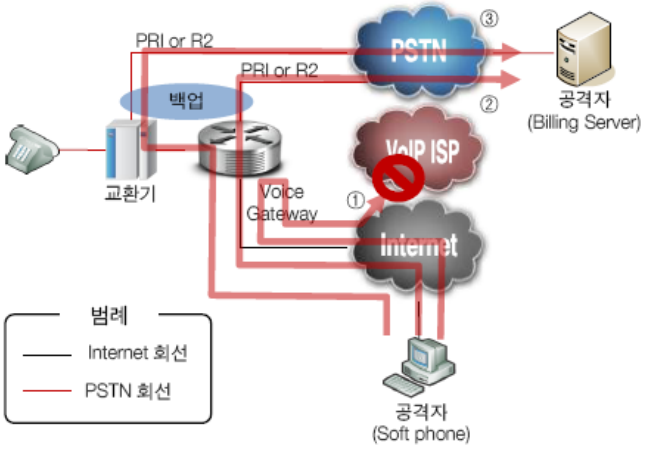
그림(6)의 구성에서 Fraud Call 에 대한 3 가지 취약점을 발견 할 수 있다. 첫째 Voice Gateway 는 공인 IP 를 사용하므로 전세계 어디에서나 접속이 가능하다. 공격자는 Voice Gateway 를 찾아 내기 위하여 위치, 시간, 비용에 구애 받지 않고 Scanning 이 가능하다. 둘째 SIP 는 UAC-UAS 방식의 경우 앞에서 설명 한 바와 같이 발신자의 인증을 거치지 않고 호를 접속 시킨다. 셋째 Voice Gateway 는 Outbound 호를 위하여 PSTN 백업경로, 교환기 연결 PSTN 경로, ISP 와의 VoIP(SIP) 연동을 위한 인터넷 경로를 가진다. 이 중 VoIP 연결 경로를 제외한 나머지 PSTN 연결 경로는 인증을 거치지 않고 호 발신이 가능한 경로이다. 이러한 경로들은 공격자가 인증을 거치지 않고 과금이 가능한 Outbound 호를 생성시 킬 수 있는 취약점을 가진다.

3.2 Scanning

공격자는 Voice Gateway 를 찾아내기 위하여 불특정 공인 IP 를 대상으로 Invite Message 를 전송한다. 이때 목적지 E.164 번호(전화번호)는 공격자가 구성한 Billing Server 이다. Billing Server 는 대량 과금을 발생시키고 추적을 피하기 위하여, 공격자 및 공격대상자 외 제 3 국에 위치 시킨다. 공격자는 Invite Message 전송 한 후 SIP Response Message 로 응답하는 Client 를 검색 한다. Client 가 Voice Gateway 가 아닐 경우 Response Message 가 없을 것이고, Voice Gateway 일 경우 UAC-UAS 방식에서는 인증절차가 없으므로 호의 성공 여부에 관계 없이 Response Message 로 응답 할 것이다. Response Message 를 응답한 Client 는 SIP 가 동작하는 Client 이고, 이는 공격 대상이 된다.

3.3 Call Route Scanning

공격 목표 Voice Gateway 를 찾아낸 공격자는 Billing Server 로 호를 연결시켜 과금을 발생 시키기 위한 Call Routing 경로를 검색 한다. 그림(7)에 ①번 경로와 같이 SIP 경로는 일반적으로 VoIP ISP 에서 인증과정을 거치거나 ISP 에서 부여한 E.164 번호를 확인 하므로 공격자가 해당 경로를 이용하는 것은 매우 어렵다.



(그림 7) Fraud Call 공격경로

이에 공격자는 발신자 인증절차가 없는 PSTN 으로 연결된 경로를 찾아내기 위하여, 국제전전화 Dialing Pattern 을 이용하여 호 연결을 시도한다. 예를 들어 Billing Server 가 남아프리카공화국에 있고 Billing Server 번호가 27-1-234-5678 이라면, 공격자는 001(국

제전화코드) +27-1-234-5678 와 같이 국제전화코드를 추가 하여 국제전화 호를 시도 한다. 실패할 경우 다른 국제전화 코드로(002,00755 등) 변경하며 성공할 때까지 호 연결을 시도 한다. 만약 그림(7) ②번과 같이 PSTN 으로의 Backup 경로가 존재 한다면 호는 성공이 될 것이고, 공격자의 Billing Server 에서 과금이 시작 될 것이다. 만약 PSTN 으로의 Backup 경로가 존재 하지 않는다면 공격자는 교환기와 연동된 PSTN 경로를 검색 한다. Voice Gateway 구성에서는 교환기 연동을 PSTN 연결 경로가 반드시 존재 한다. 교환기는 Outbound 경로를 점유하기 위해서는 일반적으로 Access Code 를 사용 하는데. 국내에서는 일반적으로 9 번을 사용한다. 예를 들어 공격자가 9(Access Code)+001(국제전화코드)+27+234+5678 으로 호를 시도 했고, 공격대상자의 교환기가 Access Code 9 번을 사용하며, 011 국제전화 사용이 가능하다면 공격자는 공격에 성공할 것이고, 성공적으로 Billing Server 에서 과금을 유발 시킬 수 있을 것이다. 그림(7)의 ③번 경로이다.

4. 결론

UAC-UAS 의 경우 인증, 암호, 무결성을 제공하기 위하여 S/MIME 사용이 가능하다. 그러나 Smartphone 의 보급 및 IP 네트워크 환경의 안정화를 배경으로 급격히 증가하는 모든 IP Phone 에 대해 공인인증서를 적용하는 것은 현실적으로 불가능하다. 이에 대부분의 ISP 들은 S/MIME 을 적용하지 않는 경우가 많다. Fraud Call 공격은 이런 취약점을 이용한다. S/MIME 적용 없이 Fraud Call 을 대응 할 수 있는 방법은 UAS 가 자신이 수신할 UAS 의 IP 네트워크를 IP Level (L3 Layer)에서 정의 하여 공격자의 IP 를 Filtering 하거나, PSTN 으로 Call Routing 을 제한 하는 방법을 사용할 수 있다.. 그러나 IP Phone 이 급격히 늘어나고 있는 추세에서 위 두 방식은 Fraud Call 방어하기에는 한계가 있다. UAS 가 수신할 수 있는 모든 IP 를 정의하기에는 한계가 있기 때문이다. 이에 대량의 사용자를 빠르게 인증할 수 있는 새로운 보안 메커니즘이 필요하다. 해당 보안 메커니즘은 Voice 환경에 적절하도록 메시지에 대한 암호화 보다는 인증에 대한 효율에 중점을 두어야 할 것이다. 새로운 보안 메커니즘에 대한 연구는 Discussion 으로 남겨둔다.

참고문헌

[1] 한국정보통신기술협회. “SIP 기반 인터넷 텔레포니 프로파일 : 보안 (Internet Telephony profile based on SIP : Security)

[2]IETF RFC1847, “Security Multiparts for MIIME : Multipart/Singed and Multiparr/Encryted

[3]IETF RFC3261, “Session Initiation Protocol”