VoIP 환경의 SIP에서 악의적인 사용자를 차단하기 위한 보안성이 강화된 사용자 인증 프로토콜 제안

장승철, 전문석
숭실대학교 일반대학원 컴퓨터학과
E-mail : lagris@naver.com, mjun@ssu.ac.kr

Suggest to improve security to user authentication protocol what block a malicious user for SIP in VoIP Environment

Seung-Chul Jang, Moon-Seog Jun
Dept of Computer Science, Soongsil University

요 약

최근 기존 PSTN망을 이용하던 음성전송방식이 VoIP 기반의 인터넷 전화 서비스로 바뀌어가고, 그 사용수도 늘어가는 추세이다. 그와 동시에 악의적인 사용자에 의한 도청, 피싱 등의 사건이 일어나면서 VoIP 보안 이슈가 늘어가고 있다. 본 논문에서는 이러한 보안 이슈들에 대한 해결책으로 SIP의 사용자 인증을 신뢰받는 기관에서 UA를 인증하여 사용자 인증에 대해 안정성을 강화하는 보안 프로토콜을 제안한다.

1. 서론

최근 인터넷의 급속한 발전으로 전 세계가 인터넷 망을 통하여 하나로 이어지게 발전되었다. 이런 인터넷의 발전에 힘입어 기존 PSTN(Public Switched Telephone Network)망으로 통신하던 음성통신이 IP(Internet Protocol)을 이용해 음성통신을 시도하게 되었고, 음성데이터를 패킷으로 변환하여 음성통신을 하는 VoIP(Voice Over Internet Protocol)이 등장하게 되었다. VoIP는 기존 인터넷 망을 사용하기 때문에 회선 사용 비용 절감과 웹 콜 센터, 영상통화 등 각종 서비스 제공이 가능하다. 그러나 기존 PSTN망의 경우 물리적인 접근으로만 도청이 가능했었던 반면에 VoIP의 경우 인터넷 망을 사용하기 때문에 보안상의 공격에 쉽게 노출이 되고, 그 이외에 여러 가지 보안상 취약점을 가진다.

VoIP에서 보안상 고려되어야 하는 부분으로 사용자 인증과 음성통신시의 음성데이터에 대한 부분이 있다. 그중 사용자 인증이 되지 않는다면 악의적인 사용자에 의하여 VoIP 서비스의 불법적인 이용 등의 문제점이 발생할 수 있다. 그렇기에 세션 연결을 설정하는 과정에서 사용자 인증이 제공되어야 한다. VoIP에 사용되는 세션연결 프로토콜로는 ITU-T의 H.323 표준과 IETF의 SIP(Session Initiation Protocol)가 있다. 그중 H.323이 주로 사용되었으나 최근에는 세션연결 설정 동작이 간단하고 확장성이 높은 SIP 프로토콜의 사용이 증가하고 있다. SIP 표준문서인 RFC 3261에서는 사용자 인증을 위하여 HTTP Digest 인증 기법의 사용을 권고하고 있다.

HTTP Digest 인증 기법을 사용할 경우 사용자를 인증 할 수 있지만 몇 가지 보안상의 취약점을 가진다. 첫째로, HTTP Digest 인증 기법은 상호 인증이 취약하여 Server Spoofing 공격에 취약점을 가진다. 둘째로, UAC와 outbound 프록시 서버와의 인증은 제공하나 inbound 프록시 서버와의 인증은 제공하지 않는 문제점을 가진다.

본 논문에서는 다음의 문제점을 해결하기 위하여 신뢰받는 인증기관으로부터 UA(User Agent)를 인증하는 보안성이 강화된 사용자 인증 프로토콜을 제안한다.

2. 관련연구

2.1. SIP

SIP 프로토콜[1]은 음성 및 멀티미디어 통신 세션을 생성하거나 삭제 변경하기 위한 절차를 명시한 응용 계층의 시그널링 프로토콜이다. 이는 사용자/서버 방식으로 TCP와 UDP프로토콜 모두 사용 가능하고 구현이 용이하다는 장점을 가지고 있다. SIP는 음성 통신 서비스에서의 유연성과 확장성을 제공하며 H.323에 비해 간편한 프로토콜 작동 구조로 구성되어 있다. SIP 세션 설정 및 통신 과정은 사용자가 프록시 서버에 등록하는 과정부터 시작된다. SIP 프록시 서버는 사용자로부터 호 연결 및 해제 요청을 대행해 주는 역할을 한다. Location Server와 Proxy Server는 물리적으로 동일한 서버에 동작을 한다. 소규모 LAB 환경에서는 프락시 서버, Location Server, Registrar Server가 하나의 서버로 운영된다. 각 사용자가 콜을 하기 이전에 자신의 위치정보를 Location 서버에 제공하는 그림이다. 이들 정보에는 자신의 SIP 어드레스와 IP 어드레스 정보 등이 포함된다.

각 사용자와 서버들은 서로의 위치를 알아내기 위해 DNS와 Location Server를 통해 서로의 정확한 위치 정보를 받게 된다. 이를 이용하여 각 사용자들은 처음 Invite를 하는 경우 Location Server를 통해 필요한 상대방의 위치정보를 획득하여 사용자들이 서로 호 설정을 할 수 있도록 도움을 준다.

SIP 메시지는 TEXT 기반 메시지 형태로 구성되어있다. 구체적인 내용을 보면 기존의 HTTP 언어 형태의 메시지 구조를 사용한다. 메시지의 구분과 형태는 다음과 같다.

- Register : SIP 클라이언트들은 반드시 Registrar 서버에 자신의 위치 정보를 제공해야 한다. 즉, 자신의 SIP 어드레스와 IP 어드레스 정보 등을 등록해야 한다.
- Invite : SIP 세션을 시작할 때 즉, 콜을 만들 때 사용자(UAC)가 서버 쪽으로 전송하는 메시지이다. 경우에 따라서는 상대 사용자(UAS) 쪽으로 바로 전송 할 수도 있다.
- ACK : 사용자는 Invite 메시지에 대한 최종 Response 메시지를 받고 그 Response에 대해 ACK를 회신한다. Response가 Success 또는 Fail 이라도 자신의 Invite에 대한 최종 Response 에 대해 ACK로 회신한다.
- BYE : 클라이언트가 콜을 종료할 때 서버에서 해당 콜이 종료되었음을 알릴 때 사용한다.

위에서 설명한 4가지 메시지 이외에도 여러 메시지를 통해 SIP 통신 과정을 지원하게 된다. 이는 대략 10단계의 호 설정 과정을 수행하며 이때 발생하는 상태코드의 순서는 정해져 있다. 이러한 과정을 다시 종류별로 4단계로 표현하게 되면 다음과 같이 표현할 수 있다.

1단계 : 자신을 등록 하는 Register 단계.
2단계 : 다른 사용자와 통화를 하기 위해 Invite를 요청하는 단계와 부가적인 Ringing, Trying, OK, ACK 단계를 통해 호 설정을 하려고 하는 단계.
3단계 : 호 설정 단계들이 마무리가 되면 RTP/RTCP 단계를 통해 사용자간 쌍방향 통신을 하는 단계.
4단계 : RTP통신 단계를 종료시키고 다시 대기상태로 들어가는 Bye, OK 단계를 거쳐 사용자는 다시 대기 상태로 유지되는 단계.

2.2. H.323 프로토콜

H.323 프로토콜은 터미널, 게이트웨이, 게이트키퍼, MCU(Multipoint Control Unit)으로 구성되고, 각 구성요소들은 비디오, 오디오, 데이터, 통신제어, 그리고 호 제어로 분류되는 정보 스트림의 전송을 통해서 통신한다.

H.323 터미널은 실시간 양방향 통신을 제공하는 클라이언트로서, 시스템 제어장치와 H.225.0계층, 네트워크 인터페이스, 그리고 오디오 코덱 장치는 필수적으로 제공해야 하고, 화상 및 데이터통신 기능 등은 선택적으로 사용한다[1].

게이트웨이는 LAN과 SCN(Switched Circuit Network) 사이에 위치하여, 두 네트워크간의 호 설정과 해제를 담당하는 호 시그널링(H.225.0 - Q.931, Q.2931 등), 전송 형식(H.225 - H.221), 통신절차(H.245 - H.242) 사이의 차이점을 보상해준다.

게이트키퍼는 선택사양으로서 게이트키퍼가 존재할 경우 주소변환과 수락제어, 터미널의 등록과 인증, 대역폭 제어, 지역 관리 기능을 제공해야 하고, 선택적으로 호 제어와 호 인증, 대역폭 관리, 호 관리 등을 제공할 수 있다.

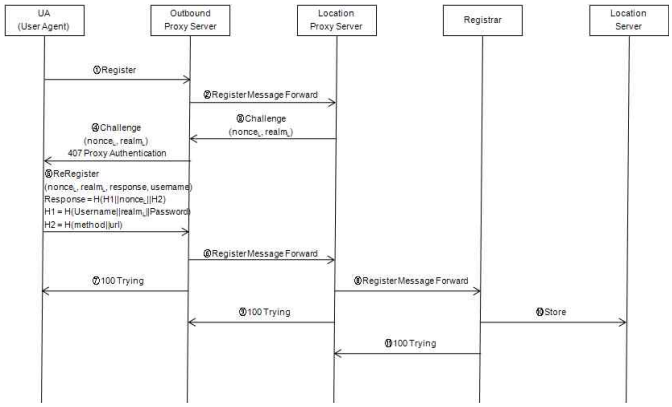
MCU는 다중점 회의를 지원하는 단말로, 하나의 MC(Multipoint Controller)와 하나 이상의

MP(Multipoint Processor)로 구성되어야 한다. 집중형 다중점 회의를 지원하는 MCU는 하나의 MC와 오디오, 비디오, 데이터 MP로 구성된다.[1]

3. 보안성이 강화된 사용자 인증 프로토콜 설계

본 논문에서 제안하고자 하는 사용자 인증 프로토콜은 기존 Outbound Proxy Server 내에 존재하던 Location Server를 외부의 신뢰받는 기관에 두어 Location Server가 UAS와 UAC를 상호인증하게 하여 내부자 공모나 악의적인 사용자의 비정규 사용을 막고자 하였다.

3.1. UAC 등록과정

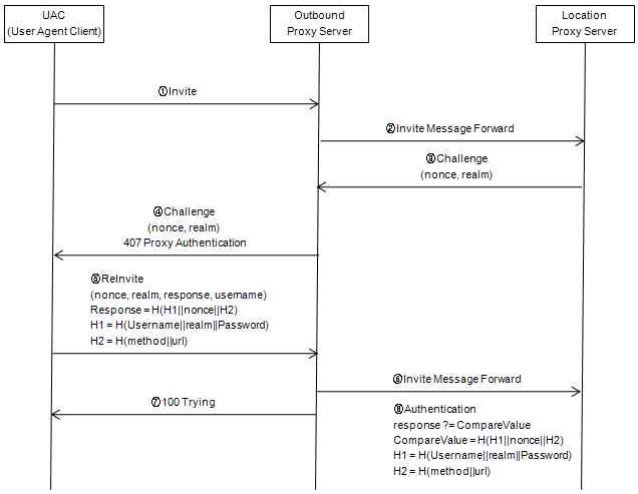


[그림 1] UAC 등록과정

UA(User Agent)를 등록한다는 것은 UA의 논리적 주소(address of record)와 실질적인 주소(contact address)간의 바인딩 정보를 생성하고 Location Server에 등록하는 것이다. 그림 1 은 Location Server에 UA를 등록하는 과정을 표현한 것이다. UA가 Outbound Proxy Server에 등록(Register) 메시지를 요청하면 Location Proxy Server의 인증을 위하여 등록 메시지를 포워딩하고 Location Proxy Server는 realm값과 nonce값을 Challenge 메시지를 Outbound Proxy Server를 통하여 UA에게 전송한다. Challenge 메시지를 통해 전달된 realm값과 nonce값을 HTTP Digest를 이용해 암호화하고 다시 Location Proxy Server에 전송한다. Location Proxy Server는 자신이 가지고 있는 값(ID, PW, realm, nonce)를 이용해 해쉬 후 전송받은 값을 비교하여 UA를 인증한다. UA의 인증 후 Registrar를 통해 Location 정보를 저장한다.

3.2. UAC 인증과정

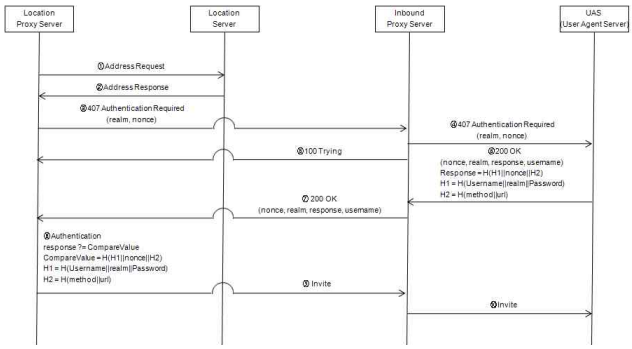
기존의 UA(User Agent)인증은 Outbound Proxy Server에서 HTTP Digest 인증 과정을 통하여 UAC를 인증하였으나 본 논문에서 제안한 프로토콜은 Location Proxy Server를 통하여 인증을 하게 된다. Location Proxy Server를 신뢰받는 기관으로 하여 UA를 인증하기에 내부자 공모나 악의적 사용자에 의한 비정규 접근을 방지할 수 있다. 그림 2는 UAC(User Agent Client)의 인증과정을 나타낸 것이다.



[그림 2] UAC 인증과정

UAC가 UAS를 Invite하기 위하여 Outbound Proxy Server에 Invite 메시지를 전송한다. 전송된 메시지는 Location Proxy Server의 인증을 위하여 Location Proxy Server에 포워딩되고 Location Proxy Server는 도메인 영역 값인 realm과 서버측에서 임의로 생성하는 32비트 값인 nonce를 407 Proxy Authentication Required 메시지의 헤더에 포함하여 UAC에 전송한다. UAC는 전송 받은 값과 Username, MD5로 암호화된 패스워드를 이용하여 MD5 또는 SHA-1으로 DIgest를 생성한다. 생성된 Digest를 Invite 메시지의 Authorization에 포함하여 Location Proxy Server로 재전송한다. Location Proxy Server에서 realm과 nonce, username, 서버간 공유되어있는 사용자 패스워드를 사용해 Digest를 생성한 후 전송받은 Invite메시지의 내의 Digest를 비교하여 인증한다.

3.3. UAS 인증과정



[그림 3] UAS 인증과정

UAC에서 전송받은 Invite메시지를 참조하여 UAS에 대한 Location 정보를 획득하기 위하여 Location Server에 주소를 요청하고, 실질적인 주소를 받는다. 획득한 주소의 Inbound Proxy Server로 407 Authentication Required 메시지의 헤더에 realm과 nonce값을 포함하여 전송하고 UAS에서 407 Authentication Required 메시지를 보낸다. UAS는 realm, nonce, Username, 패스워드를 이용하여 Digest를 생성하고, 생성된 Digest를 Inbound Proxy Server를 거쳐 Location Proxy Server로 전송한다. Location Proxy Server는 UAS의 Username과 패스워드, realm, nonce를 사용하여 Digest를 생성하고, 전송받은 Digest와 비교하여 인증이 되면 Invite 메시지를 Inbound Proxy Server를 통해 UAS에 전송한다.

4. 결론

본 논문에서는 서비스 공급자의 내부자 공모나 악의적 사용자의 위장 공격 및 비정규적 사용을 막기 위하여 신뢰받은 기관에 Location Proxy Server를 두어 UA(User Agent)를 상호 인증하는 프로토콜을 제안하였다.

본 논문에서 제안한 신뢰받은 기관에 Location Proxy Server를 두어 상호 인증을 할 경우 악의적인 사용자의 공격에 대한 안전성과 서비스의 신뢰성을 가질 것이다.

추후에 본 논문에서는 해당 프로토콜을 구현하고 패킷의 부하와 보안 안정성에 대한 성능평가를 할 예정이다.

참고문헌

[1] '주간기술동향', 한국전자통신연구원, 제1063호, 2002.

[2] D.Malas. SIP performance metrics. Internet draft draft-malas-performance-metrics-06.txt(work in progress), IETF, 2007.

[3] 이형우, SIP 프로토콜 상태정보 기반 공격 탐지 기능을 제공하는 가상 프록시 서버 설계 및 구현, 한국인터넷정보학회, 인터넷정보학회논문지, 제9권 제6호 2008.12, pp. 37~48(12pages)

[4] 윤하나, 이형우, SIP 공격 대응을 위한 보안성이 강화된 Stateful SIP 프로토콜, 한국콘텐츠학회, 한국콘텐츠학회논문지, 제10권 제1호 2010.1, pp. 46~58(13pages)