VoIP 서비스 환경에서의 사용자 접근 통제 및 인증시스템

양호경, 차현종, 한인성, 유황빈
광운대학교 컴퓨터과학과 네트워크 및 정보보호 연구실
pororI2000@nate.com, pororI2000@kw.ac.kr

User Access Control and Authentication System in VoIP Service Environment

Ho-Kyung Yang, Hyun-Jong Cha, In-Sung Han, Hwan-Bin Ryou
Network and Information security Lab, Computer science, Kwangwoon Univ.

요 약

인터넷 상에서 음성데이터를 전달하는 VoIP는 기존의 PSTN망을 대체하는 수단으로 환영받고 있다. 음성데이터를 인터넷 프로토콜 데이터 패킷으로 변환하여 데이터가 일반 IP망에서 전달이 가능하게 해주어 기존 일반 전화망에 비해 요금이 저렴하고 확장성이 뛰어난 특징을 가지고 있다. 이러한 VoIP서비스가 점차 증가함에 따라 보안의 취약점 및 서비스의 질이 저하되는 문제가 발생하고 있다. 이러한 점을 줄이기 위해 본 논문은 기존의 VoIP에 AA(Attribute Authority) Server를 추가하여서 보안성 및 사용자 접근에 차등을 줄 수 있는 인증 시스템을 설계하였다.

1. 서 론

멀티미디어 기술은 네트워킹 기술의 발전에 따라 전 세계가 연결된 인터넷과의 연계가 가속화 되고 있다 오디오, 비디오를 포함한 멀티미디어 데이터를 동일한 IP(Internet Protocol)망을 통해 전송하는 화상회의나 VoIP(Voice over Internet Protocol)와 같은 서비스들에 대한 수요가 빠르게 증가하고 있다 그러나 인터넷 환경에서 시간에 대한 제약이 존재하는 음성이나 영상과 같은 멀티미디어 데이터 서비스를 제공하면서 발생하는 통화 품질 감쇄나 지연 등의 QoS(Quality of service) 문제가 발생되고 있다. 이러한 단점에도 불구하고 비용절감과 기존의 인프라의 효율적 운용, 관리의 편리성, 데이터 통합에 의한 다양한 응용 서비스 제공 등의 효과를 거둘 수 있기 때문에 많은 기업 등에서 큰 관심을 보이고 있는 것이 현실이다 VoIP는 단말 간의 음성 통화를 효율적으로 제공하고 있으나 활성화를 위해서는 다양한 서비스들이 요구된다 부가 서비스의 종류로는 호 전환 무응답 또는 통화 중 착신 전환, 호 예약, 통화 중 대기, 호 필터링과 같은 여러 유형의 서비스를 예로 들 수 있다. 사용자들이 임의의 시간에 사용이 용이한 방법으로 자신이 직접 원하는 서비스를 등록하기 위한 VoIP의 시그널링 프로토콜로서 SIP와 H.323이 각광을 받고 있다.[1]

VoIP는 사용자의 증가가 예상되지만 패킷 망은 보안 측면에서 공개된 네트워크로 누구나 쉽게 접근할 수 있기 때문에 여러 가지 문제점이 발생 할 수 있다 PSTN 망은 물리적으로 접근해야 공격할 수 있는 반면, VoIP는 원거리의 공격자도 네트워크 기술을 이용하여 쉽게 시그널링 메시지의 변조 및 음성 패킷을 도청할 수 있다 SIP는 확장성, 컴포넌트 재사용성 그리고 상호 운용성을 고려하여 IETF에서 표준화를 시작했다 또한 RFC 3261에서는 SIP 보안 기술로 기존의 안정화된 보안 모델의 사용을 권고하고 있다 SIP는 Digest 사용자 인증, TLS, S/MIME을 적용하여 메시지에 대해서 보안 서비스를 제공하고 현재 드래프트 상태인 SRTP(Secure RTP)를 사용하여 미디어 보안을 구현하였다 안정화된 보안 모델의 사용하는데 보안성이 확보된다는 장점이 있지만 사용자들이 사용하기에는 그 품질이 현격하게 떨어져 사용상의 불편함이 존재한다는 단점이 있다[2]

본 논문에서는 VoIP서비스의 증가에 따른 보안적인 문제해결과 사용자 접근권한에 따른 차등 서비스를 제공하기 위한 시스템을 설계하였다 본 논문은 1장에 서론과 2장의 관련연구 3장에 제안기법 4장에 결론으로 구성되

어 있다.

2. 관련연구

2.1 VoIP

기존에 데이터 통신을 위해 사용하고 있는 데이터통신용 패킷망을 인터넷폰에 이용하는 서비스 이다. 음성 데이터를 인터넷 프로토콜 데이터 패킷으로 변환하여서 일반 전화망에서 통화가 가능하게 해주는 통신 서비스 이다. 기존에 전화망 서비스에 비해 요금이 저렴하고 케이블을 통해서 여러명이 동시에 사용 할 수 있고 확장성도 뛰어나다. 사용되는 프로토콜로는 SIP와 H.323등이 있다.[1]

2.2 SIP 보안

2.2.1 End-to-end보안

SIP의 End-to-end보안에서는 통신 당사자들의 단대단 보안을 제공하는 것으로 basic, digest인증 S/MIME 같은 보안기법이 사용된다 basic이나 digest인증기법은 사용자와 메시지에 대한 인증은 보장하나 전달되는 메시지의 무결성과 기밀성은 보장해 주지 못하는 단점이 있다.[3] S/MIME기법은 모든 프로토콜에 적용 할 수 있고 암호화와 전자 서명의 기능도 제공 받을 수 있는 장점이 있는 반면 서버간의 인증이 없을 시에는 악의적인 라우터로 메시지가 전달 될 수 있는 단점이 있다[4]

2.2.2 Hop-by-hop보안

Hop-by-hop보안에서는 IP패킷이 전송되는 각 단계의 모든 트래픽을 통째로 암호화 시키어서 통신을 해주는 방법으로 전체적인 내용을 암호화해서 보낸다는 점에서 보안성이 높다고 할 수 있다. 대표적인 보안 기법으로는 TLS, IPsec가 있다. TLS는 SSL을 표준화 시킨 것으로 TCP상의 응용 프로토콜에 대한 암호화나 무결성 등의 보안 서비스는 제공해주는 Client-Server기반의 보안 기법이다. 단점으로는 TCP상에서만 응용 될 수 있기 때문에 UDP같이 멀티미디어 프로토콜에서 널리 사용되는 것에는 적용 될 수 없다는 단점이 있다[5] IPsec은 IP패킷에 대한 인증 암호화, 접근제어 등 다양한 보안서비스는 제공해 주는 것으로 IP계층 위에서 작동되기 때문에 TCP나 UDP등 전송프로토콜에 관계없이 적용 가능하다. 그러나 IPsec의 키 관리 프로토콜인 ISAKMP/IKE가 지나치게 무거워 무선 단말과 같은 환경에서는 구현이 어렵다는 문제점이 있다.[6][7][8]

2.3 속성인증서

속성 인증서는 전자 상거래 응용에서 다양한 목적을 갖는 정보 보호 서비스 증가에 따라서 기존의 신분 확인을 위한 인증서를 사용하지 않고 환경에 따라 특별한 역할을 하는 인증서를 발행해 주는 것을 뜻한다. 이 인증서는 해당 목적만으로 사용되고 신분 확인용 인증서에 비해서 짧은 생명주기를 갖게 된다. 속성인증서는 신분확인용 인증서와 함께 사용될 수 있고 이것의 응용분야는 네트워크 접근제어, 컨텐트 접속에 따른 과금, 웹 페이지 접근제어 등 여러 가지 분야에서 다양하게 사용되고 있다.[10]

3. 제안기법

제안 기법을 하기 위해서는 다음과 같은 선행사항이 필요하다.

-AA서버와 KMS서버는 사전에 인증작업을 거치게 되고 서로의 공개키 값을 알고 있다

-사용자는 PKI인증기법을 기반으로 사용자는 공개키와 개인키를 생성해서 KMS서버에 공개키를 등록하면서 인증서 발급을 요청한다.

-KMS서버는 인증서발행 시 AA서버의 공개키 값을 포함하여 전송해 준다.

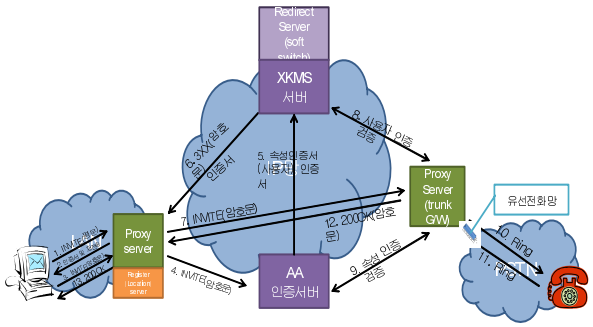

그림1 세션연결과정

그림 1의 세션연결과정을 설명하면 다음과 같다.

1. “Hello"메시지와 인증서 전송
2. Proxy Server는 인증서로 사용자 확인 후 응답메시지

전송
3. 응답 메시지에서 얻은 공개키로 암호화해서 “INVITE"메시지 전송
4. SIP의 “INVITE"메시지와 Random number R, 해쉬 값(R)이 포함된 공개키 인증서를 전송
5. 사용자 확인 후 사용자에 대한 속성 인증서와 Random number R, 해쉬 값(R)을 포함한 인증서를 전송 (SOAP)
6. Redirect server(SMS인증서버)는 AA 서버에서 받은 사용자 인증서에 대해서 인증을 거친 후 해당 사용자에 상대방 주소와 인증서를 전송
7. 인증서에서 얻은 정보로 공개키 암호화 후 전송(속성 인증서의 holder필드, inuser필드 포함)
8. SMS서버에 송신자의 인증을 검증(hoder 필드 값으로 인증서 유효성 검증)
9. AA서버에 송신자의 속성 인증을 검증
10. Ringing(108)
11. Ringing(108)
12. 정상적으로 연결되었다는 뜻의 “200 OK" 전송
13. 정상적으로 연결되었다는 뜻의 “200 OK" 전송
14. 호설정 확인메시지 ACK전송(사용자->프락시서버)
15. 호설정 확인메시지 ACK 전송(프락시->프락시)

SIP에서 통신을 하기 위해서는 호 연결과정이라는 과정을 거쳐야 한다. 이때 송/수신자 정보 및 암호기법 통신방법 등의 여러 가지 정보가 유출될 수 있기 때문에 안정한 호 설정을 해 주어야 한다. 기존에 VoIP 환경에서 SIP프로토콜 호 설정과정을 기반으로 인증서버와 KMS서버가 추가되어 인증과정을 거치게 된다.

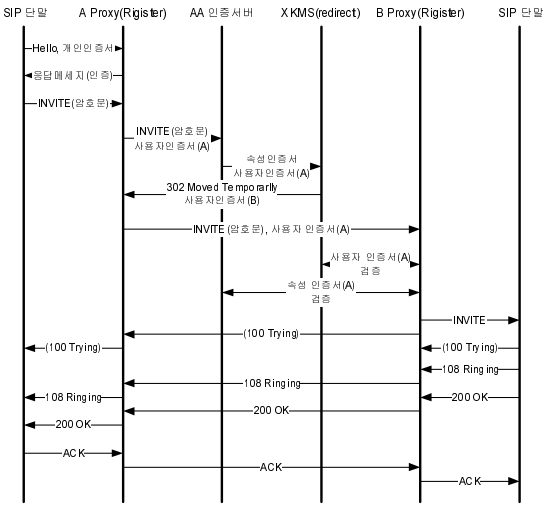

그림 2 서비스 흐름도

그림 2와 같이 우선 사전에 각 서버들끼리는 인증작업을 거치게 되고 서로의 공개키 값을 공유하게 된다. 호 설정 단계에서 처음에 송신자는 Proxy Server에다가 Hello메시지와 자신의 인증서를 보내주게 되고 Proxy Server서버는 그 인증서를 확인 한 후 메시지가 암호화 돼서 와야 한다는 응답메시지를 전송해 주게 된다. 사용자는 응답메시지에서 프락시 서버의 공개키를 얻어서 암호화를 해서 INVITE메시지를 전송한다. 메시지를 전송하기 전에 그 공개키를 기반으로 자신의 개인키를 생성해 주게 된다. Proxy Server는 AA Server에 INVITE메시지와 Random number R, 해쉬값(R)이 포함된 공개키 인증서를 전송해 준다. 그 인증서로 사용자를 확인 한 후 AA Server는 속성인증서와 Proxy Server에서 전송받은 내용을 전송해 주게 된다. SMS 서버는 그 내용을 받아서 사용자 인증서의 내용과 속성 인증서에 관한 내용을 검토한 후 상대방의 주소값과 인증서를 전송해 주게 된다. Proxy Server는 상대방의 인증서에서 얻은 공개키로 암호화 한 후 전송을 해주게 된다. 수신측 Proxy Server는 SMS 에 송신자에 대한 인증을 거치게 된다. 또한 AA Server에 송신자의 속성 인증에 대해서 검증을 거치게 된다. 이 과정을 마치면 Proxy Server는 PSTN망으로 메시지를 전송해 주게 되고 전화망인 PSTN망에서는 벨소리로 이것을 전달해 주게 된다. 그 과정이 올바르게 성사되면 호가 연결되었다는 의미로 200 OK라는 응답메시지가 전송이 되게 되고 송신측에서는 메시지를 잘 전송 받았다는 의미로 ACK를 전송해 주게 되고 이것으로 호 연결이 되게 된다. 안전한 호 설정을 마치면 RTP 프로토콜로 데이터를 전송하기 시작하게 된다.

4. 결 론

기존의 인터넷망을 사용하여서 음성데이터를 전송하는 VoIP 서비스는 기존의 PSTN망을 대체하는 수단으로 환영받고 있다. 이러한 VoIP서비스가 증가함에 따라서 QoS와 보안이라는 문제점이 대두되기 시작하였다. 본 논문에서는 기존에 VoIP세션 설정단계에 AA Server를 추가하여서 사용자의 접근에 따른 차등서비스를 제공하고 보안성을 추가한 인증 시스템을 설계하였다. 향후 연구에서는 QoS를 높일 수 있는 방법에 대한 연구가 필요할 것이다.

참고문헌

[1] 김영한, 고석갑, “VoIP 기술 개요 및 표준화 동향”, 정보처리학회지 제8권 제 2호, pp 10-21, 2001.3.
[2] 정수환, 홍기훈, 박성준 “VoIP 보안기술”, 한국통신학회지, 제 19권 제2호 pp193-203, 2002.2.
[3] RFC 2617, "HTTP Authentication : Basic and Digest Access Authentication", IETF, 1999.
[4] RFC 2402, “IP Authentication Header”, IETF IPSec WG., 1998.
[5] RFC 2246, “The TLS Prototol Version 1.0”, IETF TLS WG., 1999.
[6] 임채훈, “VoIP 시스템에서의 보안기술”,(주)퓨쳐시스템자료
[7]RFC 3261, SIP: Session Initiation Protocol, Jane 2002.
[8] Session Initiation Protocol(sip) Working Group, http://www.ietf.org/html.charters/sip-charter.html
[9] 이종화, 안상현, “SIP 기반 차세대 응용 기술, 정보처리학회지 제 8권 제 2호, pp27-33,2001.3
[10] 김경남, 강명희, 유황빈, “ 속성 인증서를 이용한 웹 서비스 접근 제어 방안”, JCCI 2003