사용자 접근권한 인증을 이용한 안전한 VoIP 시스템 설계*

양호경** · 김진묵*** · 유황빈** · 박춘식****

요 약

VoIP 서비스는 아날로그인 음성 신호를 디지털 신호로 변환한 후 패킷으로 구성하여 사용자에게 음성정보를 전달해주는 서비스로 기존의 음성전화 서비스에 비해 요금이 저렴하고 확장성이 뛰어난 장점을 가지고 있다. 그러나 VoIP 서비스는 기존의 음성전화 서비스(PSTN)에 비해서 열악한 통화품질과 보안측면의 취약성을 포함한 시스템 구조를 갖는다. 이와 같은 문제점을 보완하기 위해 TLS 서비스를 도입함으로서 보안성을 높였지만, 실제적인 시스템에서는 QoS 문제점이 발생하므로 보안적인 측면과 QoS를 동시에 만족시킬 수 있는 VoIP 보안 시스템 개발이 필요하다. 본 논문에서는 기존 VoIP 세션 설정단계에 AA 서버를 추가하여 사용자의 접근에 따른 차등 서비스를 제공함으로서 보안과 사용자에 따른 서비스를 제공할 수 있는 사용자 권한 인증 VoIP 시스템을 제안한다. 본 논문에서 제안한 시스템은 TLS 기술을 추가한 시스템보다 빠른 QoS를 제공하면서 비슷한 보안성을 제공한다는 이점을 가지고 있다. 또한 사용자별 다양한 부가서비스를 제공할 수 있다.

Design of User Access Authentication and Authorization System for VoIP Service

Ho Kyung Yang** · Jin-Mook Kim*** · Hwang-bin Ryou** · Choon-Sik Park****

ABSTRACT

VoIP is a service that changes the analogue audio signal into a digital signal and then transfers the audio information to the users after configuring it as a packet; and it has an advantage of lower price than the existing voice call service and better extensibility. However, VoIP service has a system structure that, compared to the existing PSTN (Public Switched Telephone Network), has poor call quality and is vulnerable in the security aspect. To make up these problems, TLS service was introduced to enhance the security. In practical system, however, since QoS problem occurs, it is necessary to develop the VoIP security system that can satisfy QoS at the same time in the security aspect. In this paper, a user authentication VoIP system that can provide a service according to the security and the user through providing a differential service according to the approach of the users by adding AA server at the step of configuring the existing VoIP session is suggested. It was found that the proposed system of this study provides a quicker QoS than the TLS-added system at a similar level of security. Also, it is able to provide a variety of additional services by the different users.

Key words : VoIP, AA인증

---

* 이 논문은 2007년도 광운대학교 연구년 지원에 의해 연구 되었음.
** 광운대학교 컴퓨터과학과
*** 선문대학교 교양학부 IT교육원
**** ETRI 부설연구소

1. 서 론

인터넷의 발달로 전 세계가 연결되고 이에 따라 멀티미디어 기술과의 연계가 가속화되고 있다. 대표적으로 IP(Internet Protocol)망을 통해서 오디오, 비디오 등을 포함한 멀티미디어 데이터를 전송하는 VoIP(Voice over Internet Protocol)와 같은 서비스들에 대한 수요가 빠르게 증가하고 있다[1].

그러나 기존의 전화선망인 PSTN은 물리적으로 접근해야 공격할 수 있는 반면, 인터넷 환경에서 멀티미디어 데이터 서비스는 QoS(Quality of service)문제 및 보안 취약성이 발생할 수 있다. 특히 VoIP는 원거리의 공격자도 네트워크 기술을 이용하여 쉽게 시그널링 메시지의 변조 및 음성 패킷을 도청할 수 있다는 취약점을 갖는다. 이를 해결하기 위해 SIP와 같은 안들이 제안되었다. 하지만 SIP와 같은 대안은 사용자의 편의성이 감쇠되는 부작용을 가지고 있다[2].

본 논문에서는 기존에 TLS 기반 시스템에서 추가하지 않은 VoIP세션 설정단계에 AA 서버를 추가하고자 한다. 이를 통해서 사용자의 접근에 따른 차등서비스를 제공하고 보안성을 높이며 QoS를 보장할 수 있는 안전한 VoIP 시스템을 제안하고자 한다.

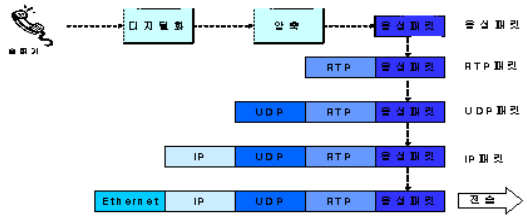
본 논문의 구성은 제 2장에서 관련연구로서 인터넷 전화 시스템의 기반을 이루는 VoIP, 세션초기화를 위한 SIP, 공개키 기반 인증서 기술인 PKI, 속성인증서 등의 기반기술에 대해 기술하였다. 제 3장은 제안 시스템의 구조 및 동작과정에 대해서 설명하였다. 제 4장에는 성능분석에 대한 내용으로 기존의 보안기술이 추가되지 않은 VoIP 시스템, TLS 기술을 추가한 VoIP 시스템과 본 논문에서 제안한 방법에 대한 비교를 하였다. 마지막은 본 논문에 대한 결론으로 구성하였다.

2. 관련 연구

2.1 VoIP

VoIP란, 음성 데이터를 데이터 패킷으로 변환하여 일반 전화망에서 통화가 가능하도록 해주는 통신 서비스이다. 이렇게 함으로써 기존의 전화망 서비스에 비해 요금이 저렴하고 여러 명이 동시에 사용 할 수 있고 확장성도 뛰어나게 된다. 이를 위해서 사용되는 대표적인 프로토콜로 SIP, H.323, MGCP, MEGACO 등이 있다[1].

VoIP의 음성전송 특징은 먼저 아날로그 음성 인소를 디지털화하고, 대역 사용의 효율성을 위해서 압축 알고리즘을 적용하여 음성 패킷을 생성한다. 생성된 패킷은 실시간 프로토콜(RTP : Real-time Transprot Proticil), UDP 및 IP 헤더를 붙여 해당 네트워크의 전송 규격에 맞추어 전송한다[13].

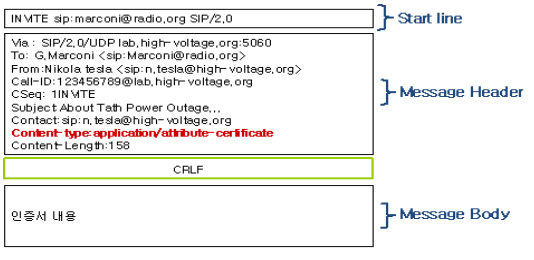


(그림 1) VoIP 음성처리절차

2.2 SIP

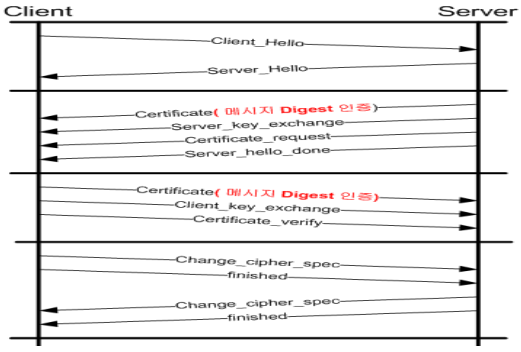
SIP는 Text기반의 프로토콜이다. SIP 메시지는 클라이언트에서 서버로 보내는 요청(request)과 서버에서 클라이언트로 보내는 응답(response)으로 구성된다.

사용하는 메시지들은 (그림 2)와 같이 공통으로 start-line과 하나 이상의 메시지 헤더 필드들, 그리고 SDP로 구성된다[7].



(그림 2) SIP 메시지 구성

SIP는 IETF에서 개발한 IP전화 통신 신호 프로토콜로서, 적용된 보안 기술은 크게 Hop-by-Hop 보안과 End-to-End 보안 기술로 분류될 수 있다. Hop-by-Hop 보안에는 digest 인증, TLS, IPSec 등의 기술이 포함되며, End-to-End 보안은 S/MIME을 적용한다[6, 8, 14].



(그림 3) SIP보안기술

2.3 PKI

PKI(공개키 기반구조)는 신뢰할 수 있는 기관에서 부여된 한 쌍의 공개키와 개인키로 구성된 키쌍을 이용하여 사용자를 인증하는 구조이다. 이를 통해서 안전하고 은밀하게 데이터나 자금을 교환할 수 있게 해준다.

PKI는 한 개인이나 기관을 식별할 수 있는 디지털 인증서와, 인증서를 저장했다가 필요할 때 사용하는 디렉토리 서비스를 제공한다.

PKI에서 사용하는 인증서의 종류에는 X.509인증서, SSL인증서, SET인증서, S/MIME인증서, IPSec인증서 등이 있다. 이 중에서 X.509인증서가 주로 사용되는데, 1995년 이후 만들어진 X.509 v3 인증서가 ITU-T에 의해 표준으로 인정되고 있다.

2.4 속성인증서

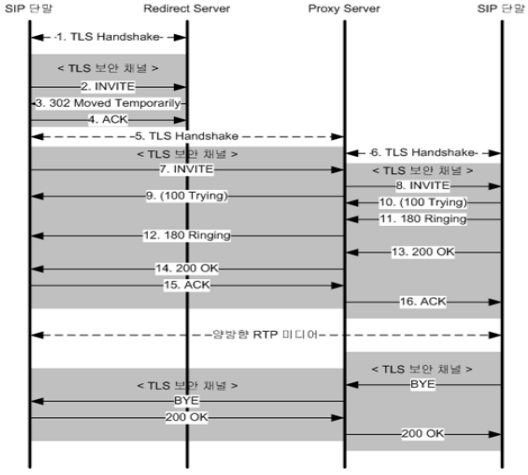
공개키 인증서와 유사한 구조를 가지며 공개 키 정보를 포함하는 대신 객체의 소속, 역할, 보안 수준, 권한 정보 등의 속성을 포함하는 인증서이다[10]. 본 논문에서는 ATM과 같은 고속 통신망에서 셀 데이터 전송 시에 셀 데이터를 실시간으로 암호화/복호화를 수행하는 효율적이고 신뢰성 있는 데이터 보안 장치를 구현함을 목적으로 한다.

〈표 1〉 속성인증서 프로파일

필 드	설 명
Version	버 전
Holder	소유자
Isuser	발행자
Signature	사용되는 전자서명 알고리즘
SerialNumber	일련번호
Fanaldate	유효기간
Attributes	속성 정보들
Extensions	확장 필드들

2.5 TLS 보안기법

TLS는 SIP 단말들간에 적용되는 보안 메커니즘으로 SIP 메시지 전송시 TLS 보안 채널을 형성해 SIP 메시지에 대해서 기밀성 및 무결성을 제공한다.



(그림 4) TLS를 사용한 세션연결과정

(그림 4)의 과정에서 나타나듯이 각 단말을 연결할 시 TLS Handshake라는 과정을 거쳐서 새로운 보안 채널을 생성하게 되고 많은 계산량을 필요로 하게 된다[5, 11].

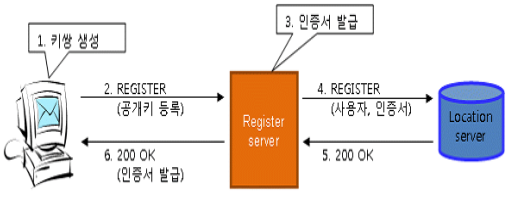
3. 제안기법

제안 기법을 구성하기 위해서는 다음과 같은 선행 사항이 필요하다.

- AA 서버와 KMS 서버는 사전에 인증작업을 거치게 되고 서로의 공개키 값을 알고 있다.
- 사용자는 PKI인증기법을 기반으로 사용자는 공개키와 개인키를 생성해서 KMS 서버에 공개키를 등록하면서 인증서 발급을 요청한다.
- KMS 서버는 인증서발행 시 AA 서버의 공개키 값을 포함하여 전송해 준다.

다음 과정은 서비스를 사용하기 전에 사용자를 등록하는 과정이다. 등록 서버에서 사용자에 대한 인증서를 발급해 주고, Location 서버에 이 내용을 저장한다. 등록 서버와 Location 서버는 물리적으로 같은 시스템으로 구성한다.

사용자가 등록 서버에 등록하고 인증서를 발급받는 과정은 (그림 5)와 같다.



(그림 5) 사용자 등록과정

1. 사용자는 키쌍(개인키, 공개키)를 생성한다.
2. 등록 서버에 공개키를 전송하여 등록한다.
3. 수신된 공개키를 기반으로 인증서를 발급한다.
4. Location 서버에 사용자 정보와 인증서를 저장한다.
5. 등록 서버로 저장완료 메시지를 전송한다.
6. 발급된 인증서, 프록시서버 인증서와 함께 등록완료 메시지를 전송한다.

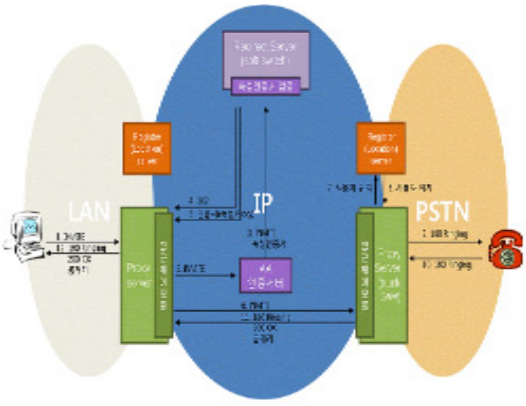
```
// 클라이언트의 사용자 등록 알고리즘
int Proxy_Regist_user()
{
        KEY                 user_Key ;
        CERTIFICATE         user_cert ;

        if(!(GenerateKeyPair(user_Key)))
                return Key_Generate_FAIL ;
        else
        {
                if( ! (Transmit( user_Key.Public_Key ))
                        return Key_Transmit_FAIL ;

                if( !(Receive_Certificate( user_cert ))
                                return
 Certificate_Receive_FAIL ;
        }

        return SUCCESS ;
}
```

(그림 6) 사용자등록 알고리즘

VoIP 환경에서 데이터를 주고받기 위해서는 세션연결과정을 거쳐야 한다. 다음은 세션 연결을 위한 처리 절차를 설명하였다.

1. 개인(사용자)인증서를 프록시 서버의 공개키로 암호화하고 이를 INVITE의 메시지에 포함하여 전송한다.
2. 프록시 서버는 사용자를 확인하고 AA 서버에게 사용자인증서와 프록시에 대한 인증서를 INVITE 메시지와 함께 전송한다.
3. AA 서버는 사용자를 확인 한 후 속성인증서를 발급한 후 프록시 서버의 인증서와 속성인증서를 포함해서 리-다이렉트 서버에 INVITE 메시지와 함께 전송한다.

4. 속성인증서를 확인한 후 수신측 프록시 서버의 인증서와 주소에 관한 메시지를 전송한다.
5. 송신측 프록시 서버는 인증서에서 얻은 공개키 값을 가지고 INVITE 메시지를 암호화하여 전송한다.
6, 7. 등록 서버에서 사용자 위치를 전달 받는다.
8, 9. Ringing(108)
10. 정상적으로 연결되었다는 200 OK 메시지를 전송한다.
11. 정상적으로 연결되었다는 200 OK 메시지를 전송한다.



(그림 7) 세션연결과정

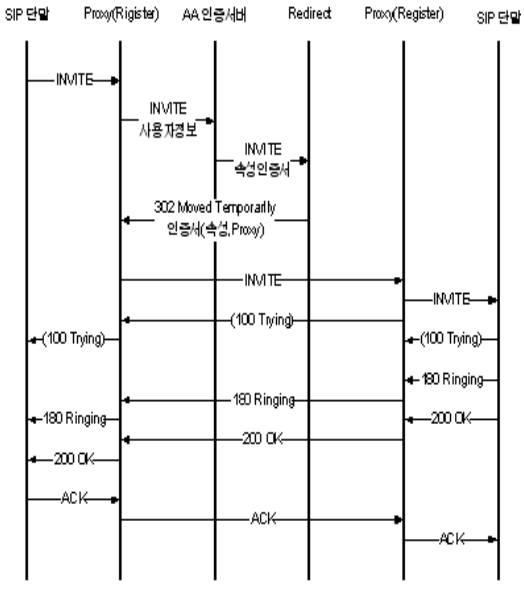
(그림 7)과 같이 개인(사용자)은 다른 사용자에게 메시지를 보내기 위해서 세션연결과정을 거치게 된다. 사용자는 프록시 서버에게 개인을 인증할 수 있는 인증서를 INVITE 메시지에 포함하여 전송한다. 이때, 사용자는 등록과정에서 전송받았던 프록시 서버의 인증서에 포함된 공개키를 사용해 메시지를 암호화하여 전송한다.

프록시 서버는 사용자의 인증서를 확인하여 사용자 신분을 확인한다. 그리고 AA 서버에게 사용자인증서와 프록시 서버 인증서를 INVITE 메시지에 포함하여 전송한다. AA 서버는 사용자를 계정 정보를 확인한 후, 사용자가 가진 권한에 적합한 속성인증서를 발급한다. 그리고 프록시서버 인증서와 속성 인증서를 INVITE 메시지에 포함해 리-다이렉트 서버에 전송한다.

리-다이렉트 서버는 속성 인증서를 검증하고 검증 결과가 올바른 경우에만 수신측 프록시 서버 인증서와 주소 정보를 메시지에 포함시켜 전송해 주게 된다.

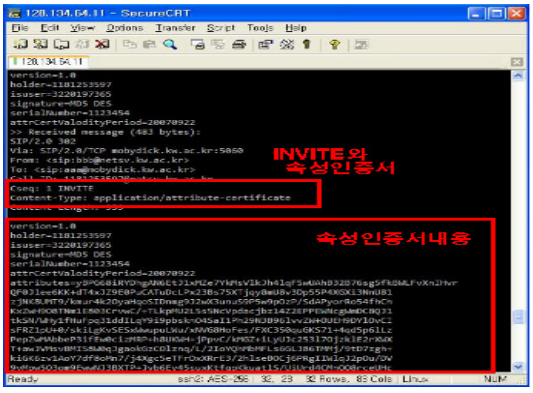
송신측 프록시 서버는 수신측 프록시 서버의 인증서에서 공개키 값을 확인하여 그 공개키를 사용해서 암호화해서 전송한다. 사용자는 등록 서버에서 세부적인 전송 위치를 습득하고 해당 시스템으로 전송한다. 이때, 연결이 올바르게 성립되면 200 OK라는 응답메시지를 전송하고, 세션을 연결을 마친 후 데이터를 전송한다.

(그림 8)은 세션 설정단계부터 등록 서버에 인증서의 등록과 AA서버로부터 인증을 받거나 리-다이렉트 서버에서 처리되는 과정을 절차적으로 나타내고 있다.



(그림 8) 데이터 흐름도

(그림 9)는 제안하는 시스템에서 사용하는 INVITE 메시지의 전송과정과 내용을 보이고 있다.



(그림 9) 제안시스템 INVITE 메시지전송

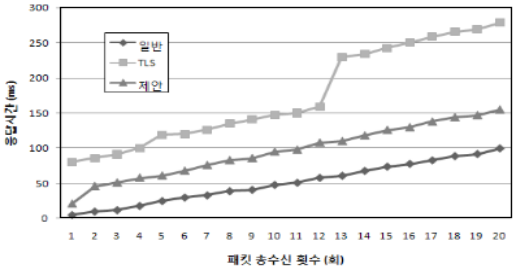
4. 성능분석

본 장에서는 구현된 SIP프로토콜 기반의 VoIP 시스템을 이용한 실험을 바탕으로 일반적인 VoIP 시스템과, TLS가 적용된 시스템, 제안 시스템의 실험 결과에 대해 기술한다. 실험에서는 CALL을 하는 INVITE 명령을 기준으로 하였고, 사전에 계정등록이 이루어져 있다고 가정하였다.

4.1 패킷 송수신횟수 별 응답시간 비교

아래 (그림 10)은 VoIP 시스템 상에서의 INVITE 횟수 별 응답시간을 비교한 그래프이다.

각 20개의 INVITE 메시지에 대한 응답시간을 측정한 결과 일반적인 시스템의 경우 1개의 메시지당 평균응답시간이 5~6ms이다.



(그림 10) INVITE 횟수별 응답시간

제안하는 시스템은 일반 시스템보다 응답시간이 늦었지만, TLS 기반 시스템보다는 응답시간이 짧다는 결과를 얻을 수 있었다. 이는 TLS의 특성상 VoIP 세션설정을 하기 이전에 여러 단계의 핸드셰이크 과정을 거치기 때문에 응답 시간이 길어진 것으로 보인다.

반면에 제안 시스템은 세션설정 초반의 속성인증서 검증과 적용과정을 거치면 일반 보안기술이 적용되지 않은 시스템과 거의 비슷한 응답시간을 갖는다.

4.2 각 시스템의 보안적 측면 비교

4.2.1 기밀성

VoIP 시스템에 대한 기밀성 침해 공격으로는 음성 호나, 음성 호를 위한 신호의 가로채기 등이 있다. 음성 세션도청은 공격자가 수신자를 가장하여 패킷 정보를 받을 수 있다.이러한 정보가 공격자에게 유출되면 음성통화자의 프라이버시가 침해될 수 있다. <표 2>에 도청공격 가능 여부에 대한 결과를 나타내고 있다.

일반 시스템과 비교하여 TLS 기반 시스템과 제안 시스템은 일반 도청이 불가능하고 인증을 기반한 도청에 대해서 부분적인 공격 가능성을 지니고 있다.

〈표 2〉 도청공격 가능여부비교

구 분	동일 네트워크상에서의 음성 세션 도청	가입자 인증에 의한 음성 세션 도청
일반시스템	가 능	가 능
TLS 기반시스템	불가능	부분적 가능
제안시스템	불가능	부분적 가능

4.2.2 무결성

VoIP 시스템에 대한 무결성을 침해하는 공격을 통해서 VoIP 스팸 공격이나 위조된 통화시도(Spoofing

Call), 변조된 RTSP 삽입을 통한 음성통화 방해 공격 등이 가능하다.

〈표 3〉 메시지 공격 가능여부 비교

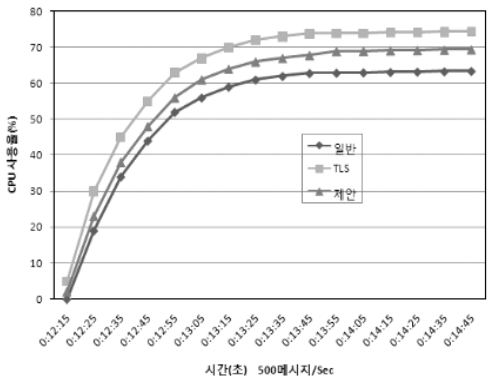
구 분	위조된 통화시도 공격	RTSP 삽입을 통한 음성통화 방해 공격
일반시스템	가 능	가 능
TLS 기반시스템	불가능	불가능
제안시스템	불가능	불가능

<표 3>의 위조된 통화시도 공격으로는 다량의 위조된 INVITE 메시지를 짧은 시간 내에 보냄으로써 정상적인 업무가 불가능하도록 하는 공격이다.

일반 시스템은 위조된 메시지가 도착할 수 있기 때문에 공격이 가능하지만, TLS 기반 시스템이나 제안시스템의 경우에는 메시지를 수신하기 이전에 세션을 설정하거나 속성인증서를 검증하는 단계를 갖는다. 그러므로 위조된 통화시도 공격이나 RTSP 삽입을 통한 음성통화 방해 공격이 불가능하다.

4.2.3 가용성

DoS 공격은 한꺼번에 다량의 데이터 패킷을 전송하여 시스템 내에 자원의 사용이 요구될때 사용하지 못하도록 하는 공격 기법이다.



(그림 11) DoS 공격에 대한 CPU 사용률

(그림 11)에서 보이는 바와 같이 제안 시스템에 대한 실험에서는 초당 500개의 메시지를 보내어 DoS 공격을 가장하였다. 일반 시스템은 처음 CPU 사용률이 0.02%였으며, 공격에 대한 반응으로 최대 62%까지 증가하였다. TLS 시스템의 경우 처음 5%였으며, 공격 이후에는 최대 75%까지 상승하는 것을 볼 수 있었다. 그리고 제안 시스템의 경우 TLS 기반의 시스템보다는 적은 값으로 처음에는 2%였으며, 공격 이후에는 최대 69%까지 상승하였다.

〈표 4〉 가용성에 대한 공격가능여부 비교

구 분	자원고갈공격	계정잠금공격
일반시스템	가 능	가 능
TLS 기반시스템	가능(피해가 가장 큼)	가 능
제안시스템	가능(피해는 세 시스템 중 중간수준)	가 능

자원고갈 공격은 VoIP 서비스 망이 정상적으로 동작하지 못하도록 하는 공격이다. 공격자가 UDP, ICMP, Echo, TCP Syn 패킷 등을 조작하여 공격할 수 있으며 불필요한 패킷들을 공격 대상 시스템에 집중적으로 보냄으로써 시스템 자원을 고갈시키는 공격기법이다.

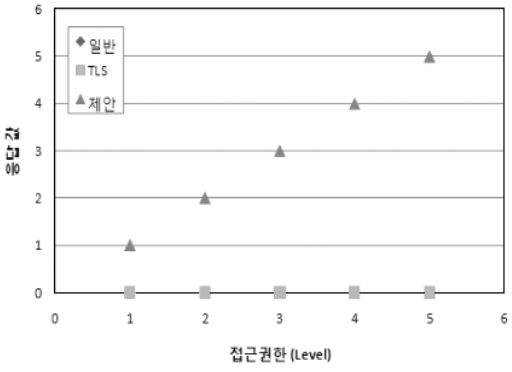
TLS 기반 시스템과 제안 시스템은 일반 시스템에 비해 세션설정을 할 때 자원을 많이 사용하기 때문에 취약성이 높다.

계정잠금공격은 시스템에 수차례 잘못된 로그인을 시도하여 계정이 잠기도록 해서 지정된 잠금해제 시간이 지날 때까지 시스템에 접속하지 못하도록 하는 공격기법이다. 그러므로 시스템 자체의 계정에 대한 공격은 모든 시스템이 취약하다.

4.3 각 시스템의 장/단점 비교

일반 시스템과 TLS 기반 시스템, 그리고 본 논문에서 제안한 시스템에 대한 접근권한별로 시스

템의 리-다이렉트 서버와 프락시 서버에서의 응답 값을 비교하였다. 이 응답 값으로 접근에 대한 제어를 할 수도 있으며, 부가 서비스에 대한 사용권한을 제어할 수도 있다. 일반적인 VoIP와 TLS를 기반 시스템에서는 접근권한에 대한 아무런 응답 값을 얻을 수 없었다. 하지만, 제안 시스템은 접근 권한별로 같은 레벨의 응답 값을 얻을 수 있었다.



(그림 12) 접근권한별 응답 레벨값 비교

<표 5>는 각 시스템에 대한 장/단점을 비교한 결과이다.

〈표 5〉 각 시스템의 장/단점 비교

구 분	장 점	단 점
일반 시스템	- 빠른 응답속도 - 시스템 부하	- 보안성 취약
TLS 기반 시스템	- 보안성 뛰어남	- 느린 응답속도 - 많은 시스템 부하 발생
제안 시스템	- 사용자별 접근 제어 가능 - 다양한 부가 서비스 제공 - 높은 보안성	- 속성 설정단계 요구

일반적인 VoIP 시스템의 경우 빠른 응답 속도와 시스템에 적은 부하를 주는 반면, 보안성이 매우 취약하다. 그러나 TLS 기반 시스템은 뛰어난 보안성을 제공할 수 있는 대신에 세션 설정 시 서버마다 TLS 세션이 설정되어야 하기 때문에 응답속도가 느리고, 일반 시스템보다 시스템에 많은 부하가 발생하게 된다. 마지막으로 제안 시스템의 경우 적절한 보안성을 제공할 수 있으며, TLS 기반 시스템보다 시스템에 발생하는 부하를 줄일 수 있다.

5. 결 론

VoIP 서비스는 인터넷의 IP 프로토콜을 사용하여 음성을 전송하는 기술로 기존의 음성전화 서비스(PSTN : Public Switched Telephone Network)에 비해서 열악한 통화품질의 문제점을 가지고 있어 QoS 중심의 VoIP 서비스의 경우에는 보안측면이 배제된 비효율적인 구조를 가지고 있었다고 할 수 있다. 이런 보안적 취약점을 해결하기 위해 TLS 서비스를 추가시켜 보안성을 높였지만 실제 사용시 가장 중요한 QoS에 많은 걸림돌이 된다는 문제점이 있었다. 따라서 본 논문에서는 기존에 VoIP 세션 설정단계에 AA 서버를 추가하여서 사용자의 접근에 따른 차등서비스를 제공하고 나아가 보안성을 추가한 인증 시스템을 제안하였다. 각 서버간의 TLS 세션 설정을 위한 핸드셰이크 과정 대신, 공개키 기반의 공인 인증서와 속성 인증서를 통한 사용자별 접근 제어를 함으로써 보안성을 제공하면서 QoS를 유지할 수 있도록 하였다. 구현을 통해 실험한 결과 기존의 보안이 적용되지 않은 시스템에 비해 QoS는 떨어졌으나 TLS 기술을 추가한 시스템보다 빠른 QoS를 제공하면서 비슷한 보안성을 제공한다는 것을 알 수 있었다. 또한 사용자별 다양한 부가서비스를 제공할 수 있다는 것을 알 수 있었다. 향후에는 기존 VoIP 서비스와 비슷한 정도로 QoS를 높일 수 있는 방법에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] 김영한, 고석갑, “VoIP 기술 개요 및 표준화 동향”, 정보처리학회지, 제8권, 제2호, pp. 10-21, 2001.

[2] 정수환, 홍기훈, 박성준 “VoIP 보안기술”, 한국통신학회지, 제19권, 제2호 pp. 193-203, 2002.

[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) 퓨처시스템자료.

[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, 제8권, 제2호, pp. 27-33, 2001.

[10] 김경남, 강명희, 유황빈, “속성 인증서를 이용한 웹 서비스 접근 제어 방안”, JCCI, 2003.

[11] Baugher, M. et at., “The Secure Real-time Transport Protocol”, July 2003, IETF draft-ietf-avt-srtp-09.txt, Work in Progress.

[12] Housley, R.etal., “Internt X.509 Public Key Infrastructure : Certificate and CRL Profile”, IETF RFC 3280, April 2002.

[13] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP : A Transport Protocol for Real-time Application”, RFC 1889, Audio/Video Transport Working Group, January 1996.

[14] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, “SIP : session initiation protocol”, Request for Comments(Proposed Standard) 2543, Internet Engineering Task Force, March 1999.

양 호 경

2005년 광운대학교 컴퓨터 소프트웨어학과(공학사)
2007년 광운대학교 컴퓨터 공학과(공학석사)
2008년 광운대학교 방위사업학과 재학중

김 진 묵

1998년 배재학교 컴퓨터과학과 (이학사)
2000년 배재대학교 컴퓨터 과학과(공학석사)
2006년 광운대학교 컴퓨터 과학과(공학박사)
2008년~현재 선문대학교 교양대학 IT교육원 전임강사

유 황 빈

1968년 인하대학교 전자공학과 (학사)
1975년 연세대학교 전자공학과 (공학석사)
1984년 경희대학교 전자공학과 (공학박사)
1981년~현재 광운대학교 컴퓨터소프트웨어학과 교수

박 춘 식

1981년 광운대학교(학사)
1983년 한양대학교 전자통신전공(석사)
1995년 일본동경공업대학교 정보보호전공(박사)
1982년~1999년 한국전자통신연구원 부장
2000년~현재 한국전자통신연구원 부설연구소 책임연구원