VoIP 시스템에서 SIP를 이용한 보안 인증기법에 관한 연구

이 영 구* · 김 정 재* · 박 찬 길**

A Study on the Secure Authentication Method using SIP in the VoIP System.

Lee, Young Gu · Kim, Jeong Jai · Park, Chan Kil

〈Abstract〉

VoIP service uses packet network of ip-based because that has eavesdropping, interception, illegal user as vulnerable elements. In addition, PSTN of existing telephone network is subordinate line but VoIP service using the ip packet provide mobility. so The user authentication and VoIP user's account service using VoIP has emerged as a problem.

To solve the vulnerability of SIP, when you use VoIP services with SIP, this paper has made it possible to authenticate user's terminal by using proxy server and proxy server by using authentication server. In conclusion, sender and receiver are mutually authenticated. In the mutual authentication process, the new session key is distributed after exchanging for the key between sender and receiver. It is proposed to minimize of service delay while the additional authentication. The new session key is able to authenticate about abnormal messages on the phone. This paper has made it possible to solve the vulnerability of existing SIP authentication by using mutual authentication between user and proxy server and suggest efficient VoIP service which simplify authentication procedures through key distribution after authentication.

Key Words : VoIP, Session Initiation Protocol, Authentication, Proxy

Ⅰ. 서론

IP기반의 VoIP(Voice over Internet Protocol) 서비스는 음성 데이터뿐만 아니라 텍스트, 이미지, 멀티미디어 등 다양한 데이터들을 전송할 수 있고, 인터넷과 연결된 어느 곳에서든지 통신이 가능하기 때문에 모바일 단말기와 비슷한 이동성도 제공한다[1]. VoIP 서비스는 여러 가지의 문제점이 있는데 그 중 하나는 보안과 관련된 문제이다. VoIP 서비스는 IP기반의 패킷망을 사용하기 때문에 도청, 감청, 부정한 사용자 등의 보안상 취약한 요소들을 가지고 있다[2]. 또 기존의 전화회선망 방식인 PSTN은 회선에 종속되어 있는 반면에 VoIP 서비스는 IP 패킷망을 사용하여 이동성을 제공하므로 VoIP 서비스를 이용하는 사용자의 인증과 VoIP 사용자의 과금 서비스

* 숭실대학교 컴퓨터학과
** 한국사이버대학교 교수 (교신저자)

에 대한 문제가 대두되고 있다[3].

최근에는 이러한 문제점을 보완하기 위해 SIP(Session Initiation Protocol)를 사용한다. SIP는 개방형 네트워크를 기준으로 개발되었으며 다양한 멀티미디어 서비스를 쉽게 이용할 수 있고 확장성이 용이한 프로토콜 구조로 되어 있다[4].

SIP는 IP기반의 패킷망을 사용하고 간단한 텍스트형태의 메시지이기 때문에 그에 대하여 공격에 쉽게 노출된다는 한계를 가지고 있다[5]. 대표적인 SIP공격기법으로는 비정상 메시지 공격(Malformed Message Attack), SIP 메시지 폭주 공격(SIP Message Flooding Attack), SIP 스푸핑 공격(Spoofing Attack), DoS 공격(Denial of Service Attack), 도청, 감청 등의 다양한 공격이 존재한다[6]. 이러한 공격기법의 근본적인 문제는 공격자가 정상적인 SIP 통신 패킷을 수정 및 삭제하고 이를 변경하는데 문제가 없기 때문에 발생하는 공격들이다.

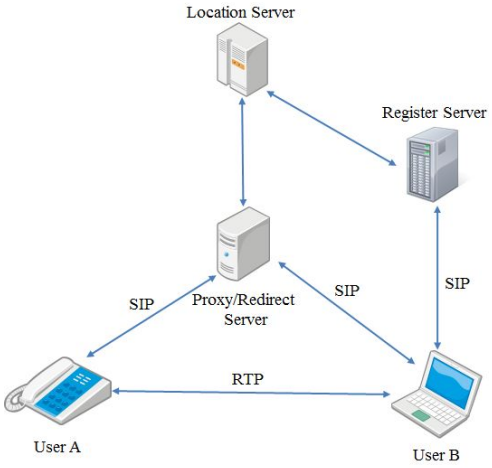
따라서 이러한 SIP 프로토콜의 취약성을 이용한 공격에 대한 능동적인 해결방안의 근본적인 연구가 필요하다. 현재 SIP 서비스는 사용자 등록과정을 통하여 수행하는 Proxy 서버와 각각의 사용자 UA(User Agent)로 구성되며 SIP 호 연결과정을 통하여 사용자들이 RTP 프로토콜을 사용하여 통화를 하는 서비스 구조로 이루어져있다.

본 논문에서는 기존의 SIP프로토콜의 취약점을 해결할 수 있는 기술과 SIP Proxy 서버와 사용자 간의 전송되는 패킷에 대하여 기존의 인증 기술인 HTTP Digest를 통하여 사용자 인증을 제공한다. 또한 Proxy 서버들의 인증을 위하여 인증 서버를 두어 상호인증을 통하여 더욱더 안전한 SIP 인증 기법을 제안한다. 그리고 SIP 세션 설정 시 인증된 Proxy 서버가 세션키를 분배하여 통화 중에 발생하는 비정상 메시지, 호 종료 메시지(BYE) 등을 인증하는데 사용하여 추가적인 인증절차가 없이 사용하는 인증 기법을 제안한다.

Ⅱ. 관련연구

2.1 SIP(Session Initiation Protocol)

SIP는 사용자간의 멀티미디어 전송을 위한 세션의 개시, 변경, 폐지를 정의하는데 사용된다[7]. <그림 1>은 SIP 서비스의 구성도이다. 사용자(User Agent)와 SIP 서버들로 구성되고 SIP 메시지를 통하여 호 연결 및 해제를 수행한다.



<그림 1> SIP 구성도

① UA(User Agent)

VoIP 서비스를 사용하는 사용자를 UA라 부르고 SIP 메시지를 생성하는 요청사용자(UAC : User Agent Client)와 수신된 메시지에 응답하는 응답 사용자(UAS : User Agent Server)로 구성된다.

② Proxy 서버(Proxy Server)

Proxy 서버는 User가 요청한 호 요청에 대하여 UAS의 위치를 등록 서버나 DNS를 통하여 해당 정보를 요청한다. 그리고 해당하는 Proxy 서버로 SIP 호 요청 정보를 전달한다. Proxy 서버는 SIP 요청은 수행하지 않고 단순

허 UA로부터 발생한 호 요청에 대한 응답 또는 포워딩만 수행한다.

③ 재지정 서버(Redirect Server)

재지정 서버는 User의 요청에 응답하지만 메시지를 포워딩 할 수 없다. 따라서 User의 최종위치를 SIP 호 연결을 요청한 User로 보내고 수신한 메시지가 전달되어야 하는 새로운 노드의 주소를 알려주는 역할을 수행한다.

④ 위치 서버(Location Server)

위치 서버는 도메인 내에 속하는 사용자의 위치를 기록하고 알려주는 역할을 수행한다.

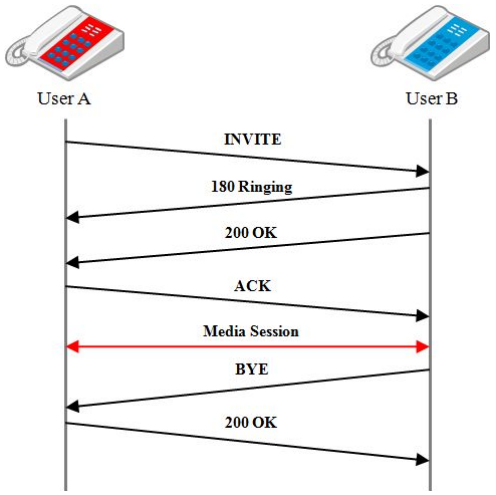
⑤ 등록 서버(Registrar Server)

등록 서버는 E-Mail 형태의 SIP 주소로 구분된 사용자 정보를 관리하고 사용자의 인증과정을 제공한다. 인증과정을 통하여 인증된 사용자의 요구에 따라 사용자 정보를 제공해주는 역할을 수행한다.

2.2 SIP 메시지 교환

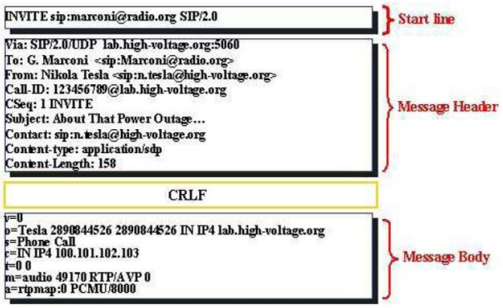
SIP 메시지 교환은 <그림2>와 같이 User간의 세션을 설정하고 종료하는 그림이다. UserA가 UserB로 세션을 설정하기 위하여 INVITE 메시지를 생성하여 전송한다. UserA에 속한 Proxy 서버는 UserB가 위치한 Proxy 서버로 INVITE 메시지를 포워딩한다. 100 Trying 메시지는 자신이 다음 목적지로 포워딩 사실을 알려주는 메시지이다.

INVITE 메시지를 받은 UserB가 속한 Proxy 서버는 위치 서버를 이용하여 UserA의 위치를 확인 하고 수신된 INVITE 메시지를 UserB에 전달한다. UserB는 UserA로부터 연결이 들어와 벨이 울리고 있다는 180 Ringing 메시지를 전달한다. UserB는 수신확인을 위해 200 OK 메시지를 전송하고, 200 OK 메시지를 받은 UserA는 ACK 메시지를 UserB에 보냄으로써 세션을 설정하는 과정을 마치고 RTP를 사용하여 데이터를 주고받는다. 세션의 종료는 종료를 원하는 어느 한쪽이 BYE 메시지를 보내고, 그에 대한 응답으로 200 OK 메시지를 전송함으로써 이루어진다[3].



<그림 2> SIP 동작 순서

<그림 3>은 SIP 메시지 형식이다. Start line에는 요청할 Method와 SIP URI가 위치하고 Header에는 세션을 제어하기 위한 값들이 세팅된다. Message body에는 Header에서 Content type에 설정된 내용이 들어간다.

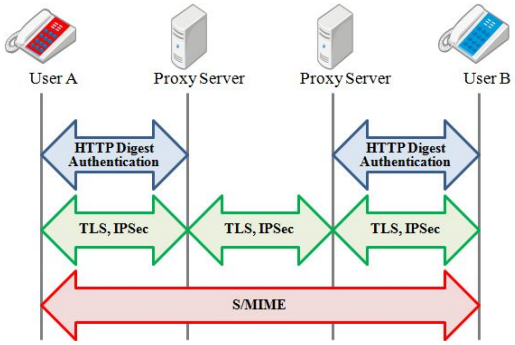


<그림 3> SIP 메시지 형식

2.3 SIP 보안 기술

기존의 SIP에서는 보안 메커니즘은 <그림 4>와 같이 VoIP의 특성상 빠른 전송을 목적으로 하고 있기 때문에 복잡성을 최소화하기 위해 새로운 기반구조나 알고리즘 확장을 가급적 사용하지 않는다.

SIP 기반의 VoIP 서비스 환경에서는 사용자 인증을 위해 HTTP Digest 인증 기법을 사용한다. 그리고 보안 메커니즘으로는 S/MIME, TLS, IPSec을 이용한다[8].



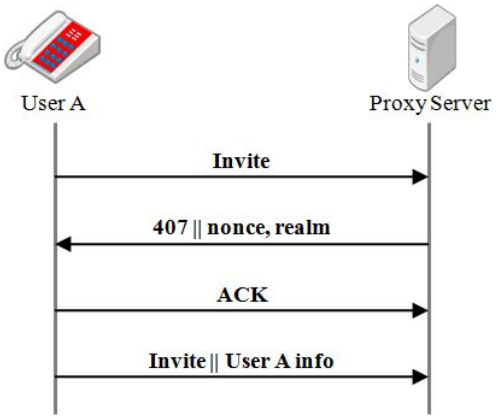
<그림 4> SIP기반의 보안 메커니즘

① HTTP Digest 사용자 인증

HTTP Digest 인증은 <그림 5>와 같이 HTTP 기본 인증이 사용자 이름과 패스워드를 암호화 하지 않고 전송하는 문제점을 보완하기 위하여 만들어진 메커니즘이다. UserA와 각 SIP 서버간에 적용되어 사용자 인증을 위해서 SIP 보안에 적용하고 있다. 사용자 인증을 위하여 사용자와 Proxy 서버 사이에 사전에 공유하고 있는 패스워드와 등록서버로부터 받은 임의의 값을 사용하여 해쉬함수를 기반으로 MD5나 SHA-1 Digest를 전송한다[8].

인증은 시도-응답(challenge-response)형태로 UserA에서 request 메시지를 보내면 등록 서버에서 request 메시지에 랜덤 정보(nonce와 realm)를 보내주게 된다. 이러한 정보를 받은 UserA는 서버로부터 받은 정보와 자신의 정보를 사용하여 생성된 HTTP Digest 인증정보를 각 서버에 응답으로 보낸다.

각 서버는 UserA로부터 받은 정보와 자신이 가진 UserA 정보를 가지고 생성된 값을 비교하여 같은 값이면 UA를 검증한다. 이러한 HTTP Digest 사용자 인증은 INVITE, ACK, BYE 메시지 등에도 적용되어 SIP를 사용하는 VoIP 서비스 시스템에서 세션 연결 시에도 정당한 사용자 여부를 확인할 수 있다. HTTP 인증은 SIP단말, Proxy 서버, 등록 서버에서 구현되어야 한다[9].



<그림 5> HTTP Digest 인증

② 홉간(Hop by Hop) 보안

SIP 시스템에서 UA와 각 서버간에는 TLS, IPSec 등의 홉간 보안 기법이 적용된다. 홉간 보안은 TLS 보안 채널을 통하여 SIP 메시지를 전달하므로 기밀성과 무결성을 제공하며 사용자간 인증은 인증서를 통해 제공한다[10,11].

③ 양단간(End to End) 보안

양단 채널인 UA-UA간에는 S/MIME 보안 기법이 옵션으로 적용된다. S/MIME은 양단간의 메시지에 대한 기밀성과 무결성, 인증서를 통한 상호간 인증을 제공한다. SIP에서는 SIP 암호화 모드, SIP 전체 메시지 서명 모드, SIP 전체 메시지 암호 및 서명모드로 구분되어 사용된다.

2.4 VoIP 서비스의 공격유형

VoIP 서비스에서 SIP 메시지를 위·변조를 통한 사용자의 프라이버시를 침해하거나 부정한 사용자가 정상적인 시스템으로 위장하는 등 여러 가지 공격유형이 존재한다. <표 1>은 SIP 기반의 VoIP 서비스에서 위협유형과 위협내용을 나타낸다[12].

<표 1> 위협유형과 위협내용

위협유형	위협 내용
스푸핑	TCP/IP 프로토콜의 약점을 악용, 발신주소를 조작하여 정상의 사용자로 위장
스니핑	트래픽을 불법으로 재생이나 정보를 수집하는 행위
중간자 공격	부정한 제 3자가 양단간 통신에 개입하여 권한이나 정상의 시스템으로 참여하려는 공격
세션 가로채기	공격자가 세션에 개입하여 불법 정보를 발생시킬 수 있도록 하는 공격
악의적인 호 발생	양단간의 정상적인 통화에 개입하여 악의적인 패킷을 통화중에 삽입하여 통신을 방해
서비스 거부	SIP 서버와 같은 주요 시스템의 자원을 고갈시키거나 독점, 파괴하여 서비스를 제공받지 못하도록 무력화하는 공격
재사용 공격	권한이 없는 공격자가 정상적으로 사용된 데이터를 복사하여 나중에 그대로 사용하여 합법적인 사용자로 가장하려는 공격

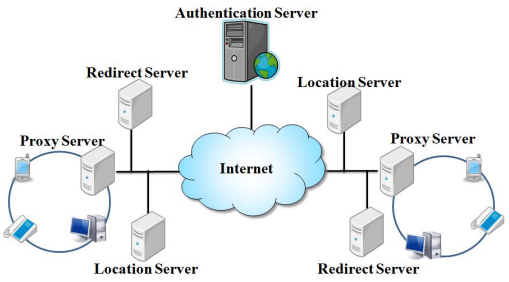
Ⅲ. SIP를 이용한 안전한 인증기법

본 논문에서 제시하는 SIP기반의 VoIP 서비스 환경에서는 모든 메시지를 SIP를 이용하여 응용계층에서 전송한다. SIP 메시지를 암호화하여 전송하지 않으면 외부적인 공격에 취약하고, 정상의 사용자가 아닌 불법적인 사용자가 네트워크의 자원을 불법으로 사용할 수 있다.

중간자 공격이나 스푸핑, 악의적인 호 발생, 세션 가로채기, 재사용 공격 등 Proxy 서버에 대한 공격들이 늘어나고 불법적인 사용자나 공격자가 Proxy 서버로 위장하는 공격도 발생한다. 따라서 Proxy 서버간에서도 인증서버를 두어 각 Proxy 서버에 대한 상호인증을 통하여 Proxy 서버가 인증한 단말기에 대해서는 정상적인 서비스를 사용할 수 있도록 제안한다. 그리하여 부정사용자의 네트워크 사용을 방지하고 도청 및 감청을 예방할 수 있게 한다.

3.1 인증 서버를 이용한 SIP 구성

제안하는 시스템은 각 User 단말이 Proxy 서버와 연결되어 있고 각 Proxy 서버는 사용자 인증서버에 연결되어 있다.



<그림 6> 제안 시스템 구성도

<그림 6>에서 나타낸 것처럼 시스템에 참여하는 Proxy 서버는 인증 서버에 연결되어 있고 인증서버는 Proxy 서버를 통하여 연결된 각 User의 인증을 수행한다. 제안된 시스템 구조에서는 인증은 크게 두 가지로 구분된다. User와 Proxy 서버간의 인증과 Proxy 서버간의 인증으로 구분될 수 있다. 첫째로 User와 Proxy 서버간의 인증은 불법적인 사용자나 공격자가 서버에 접근하여 서버의 정보를 조작이나 유출하는 것을 방지하기 위한 인증이다. 두 번째 인증은 Proxy 서버와 인증 서버간의 인증이다. 이 절차는 송신지 Proxy 서버와 수신지 Proxy 서버를 상호인증을 함으로써 공격자가 Proxy 서버로 위장하거나 감청, 도청을 시도할 경우를 예방하기 위하여 필요하다.

3.2 SIP 사용자 인증

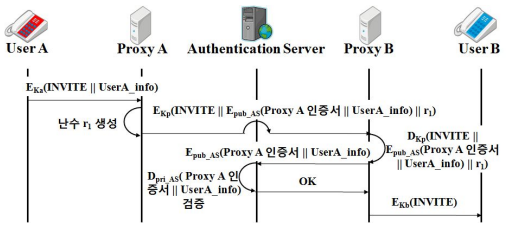
제안하는 SIP 메시지 교환은 인증 서버를 추가하고, Proxy 서버가 User를 인증하고 Proxy 서버를 인증 서버가 인증하는 절차를 수행하고 있다. 또한 상호인증을 통하여 송·수신 측을 모두 인증하여 안전한 SIP 인증 기법을 설계하였다. 제안하는 SIP 메시지 교환은 송신측 인증, 수신측 인증, 키 교환, 호 종료 메시지 교환으로 분류할 수 있다. 제안하는 SIP 인증 기법을 이해하기 위하여 용어 설명을 <표 2>에서 보여주고 있다.

<표 2> 용어정리

Symbol	Definition
Ka	Proxy A와 UAC간의 키
Kb	Proxy B와 UAS간의 키
Kp	Proxy A와 Proxy B간의 키
Pub_AS	인증서버의 공개키
Pri_AS	인증서버의 개인키
E	암호화
D	복호화
Ks	난수 r1, r2에서 생성된 키
info	UA가 생성한 HTTP Digest

3.2.1 송신측 인증

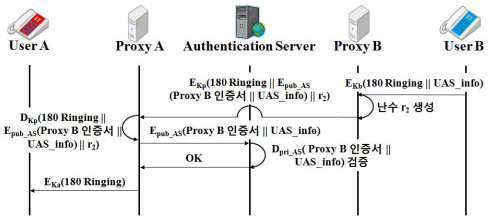
송신측 인증은 <그림 7>과 같이 UserA가 UserB와 연결을 하기 위해 INVITE 메시지를 보낸다. 이 때 연결을 시도하는 UserA에 연결된 Proxy A는 INVITE 메시지에 HTTP Digest를 요청한다. UserA는 Proxy A에게 INVITE 메시지에 HTTP Digest를 같이 보내고 Proxy A는 UserA로부터 받은 INVITE 메시지에 포함된 HTTP Digest를 검증한다. UserA가 검증되면 난수 r1을 생성하고 UserA의 HTTP Digest와 자신의 인증서를 포함하여 인증서버의 공개키로 암호화하여 보낸다. Proxy A로부터 메시지를 받은 Proxy B는 인증 서버의 공개키로 암호화된 부분을 인증 서버에게 검증요청을 한다. 인증 서버는 Proxy A의 인증서와 UserA를 검증하고 Proxy B에게 검증결과를 응답한다. Proxy B는 검증결과를 보고 정상적인 사용자가 검증되면 INVITE 메시지를 UserB에게 전송한다.



<그림 7> SIP 송신측 인증

3.2.2 수신측 인증

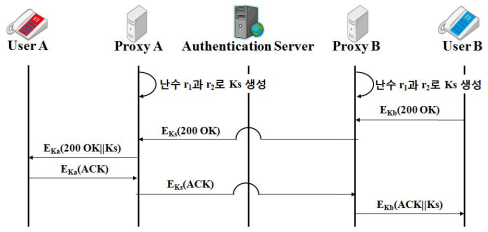
수신측 인증은 <그림 8>과 같이 UserB가 180 Ringing 메시지를 전송할 때 Proxy B는 UserB의 HTTP Digest를 요청한다. UserB는 Proxy B에게 180 Ringing 메시지에 HTTP Digest를 붙여 보내고 Proxy B는 UserB를 검증한다. UserB를 검증한 Proxy B는 난수 r2를 생성하고 Proxy A에게 자신의 인증서와 UAS의 HTTP Digest, 난수 r2를 인증 서버의 공개키로 암호화하여 전송한다. Proxy B로부터 메시지를 받은 Proxy A는 인증 서버로 암호화된 부분은 인증 서버에게 검증을 요청한다. 인증 서버는 Proxy B의 인증서와 UserB를 검증하고 Proxy A에게 검증결과를 응답한다. Proxy A는 검증결과를 보고 정상적인 사용자가 검증되면 180 Ringing 메시지를 UserA에게 전송한다.



<그림 8> SIP 수신측 인증

3.2.3 세션키 교환

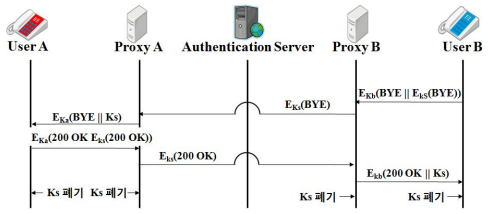
세션키 교환은 <그림 9>과 같이 송신측과 수신측을 상호인증과정에서 Proxy 서버가 분배한 난수 r1과 r2를 가지고 세션키 Ks를 생성한다. UserA에게는 200 OK 메시지를 전송할 경우 Ks를 같이 넣어 보내고 UserB에게는 ACK 메시지를 전송할 경우 Ks를 같이 넣어 보낸다.



<그림 9> SIP 세션키 교환

3.2.4 호 종료 메시지

<그림 10>과 같이 호 종료 메시지나 통화 중에 발생하는 비정상적인 메시지를 전송할 경우 앞에서 분배한 세션키를 이용한다. 전송하는 측의 User가 호 종료 메시지나 비정상적인 메시지를 보낼 경우 그 메시지를 분배한 세션키로 암호화하여 전송한다. 메시지를 받은 Proxy 서버는 분배한 세션키 Ks를 확인하고 Ks로 암호화된 메시지를 수신측의 Proxy 서버에게 보낸다. 수신측의 Proxy 서버는 Ks로 암호화되어 있는 것을 검증하고 User에게 호 종료나 비정상적인 메시지를 전송한다.



<그림 10> SIP 호 종료

Ⅳ. 성능분석

제안시스템은 VoIP 서비스에서 User와 Proxy 서버를 송신측과 수신측을 인증하는 상호인증을 통하여 정상적인 사용자를 구분하고 악의적인 공격자에 대한 공격을 예방하는 시스템이다. 기존의 인증 시스템은 User에 대해서 송신측 Proxy 서버가 인증을 수행하는 방식이고 Proxy 서버도 송신측만을 인증하는 단방향 인증이므로 하나의 Proxy 서버라도 공격자에게 공격을 당할 시에는 도청이나 감청 등의 공격이 발생할 수 있다.

<표 3> 기존 시스템과 제안 시스템 비교

	기존 SIP	제안하는 SIP
사용자인증	O	O
Proxy서버인증	X	O
상호인증	X	O
비정상 메시지 공격 탐지	X	O
중간자 공격 탐지	X	O
스푸핑 공격 탐지	X	O
세션 가로채기 공격 탐지	X	O
재사용 공격 탐지	X	O
기밀성	X	O
성능(안전성)	낮음	높음

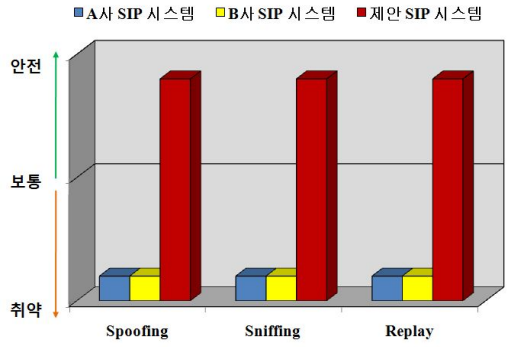
<표 3>은 기존의 SIP 인증과 제안시스템에서의 SIP 인증을 비교한 것이다. 제안하는 시스템은 인증 서버를 사용함으로써 Proxy 서버에 대한 확실한 인증을 수여하고 Proxy 서버가 세션키를 생성하여 호 종료 메시지(BYE)나 비정상 메시지 등과 같은 통화절차를 종료하거나 방해하는 메시지가 발생할 경우 두 Proxy 서버가 생성한 세션키 Ks로 암호화하여 메시지를 전송함으로써 기밀성을 제공할 수 있으며 추가적인 인증절차를 수행할 필요가 없이 인증할 수 있다. 또한 세션 설정시 중간자 공격이나 스푸핑 공격, 재사용공격, 세션 가로채기 공격

등이 발생하였을 때, HTTP Digest를 같이 전송함으로 Digest 생성시 발행한 난수를 확인하여 공격을 탐지할 수 있어 안전하다.

그리고 인증서버에 User의 Digest를 저장하여 사용자 간의 과금이나 부가서비스 이용에 대한 분쟁을 적게 만들 수 있다.

<그림 11>은 기존 SIP 시스템과 제안하는 SIP 시스템에 대한 안전성을 비교한 것이다.

기존의 SIP 시스템은 빠른 전송을 목적으로 하고 있기 때문에 안전성은 고려하지 않았다. A사의 보안 메커니즘은 S/MIME 이용하고 있으며, B사의 보안 메커니즘은 TLS, IPSec를 이용한 방법으로 안전성을 제공하고 있다. 그러므로 제안하는 시스템과의 안전성 비교에서 Spoofing공격, Sniffing공격, Replay 공격을 비교한 결과 제안하는 시스템이 안전성이 뛰어나다.



<그림 11> 안전성 비교

V. 결론

본 논문은 VoIP 서비스에서 부정 사용자 및 악의적인 공격자를 방지하고 탐지하기 위하여 SIP 기반에서 동작하는 상호인증 시스템을 제안하였다. 개방된 인터넷망을 통한 VoIP 서비스는 복제 단말기나 부정사용자에 대해 송·수신자 모두를 인증하는 인증절차가 필요하다. 또한 공격자가 Proxy 서버에 대한 공격과 위장을 통하여 감청이나 도청 등의 공격을 수행하더라도 인증 서버가 Proxy 서버의 인증함으로써, 감청이나 도청 등을 예방할 수 있어 개인의 프라이버시를 보장할 수 있다. 제안된 상호인증 서비스는 인증 서버의 도입과 상호인증에 따른 속도적 문제점을 보안하기위한 성능의 평가, 문제 분석 등의 연구가 계속되어야 한다.

참고문헌

[1] 양호경, 차현종, 한인성, 유황빈, “VoIP 서비스 환경에서의 사용자 접근 통제 및 인증 시스템,” 한국컴퓨터종합학술대회 논문집, Vol. 32, No. 1, 2007.

[2] 한국정보보호진흥원, “VoIP 정보보호기술 개발,” 지식경제부, 2009.

[3] 진현철, 김정미, 김종근, “VoIP 서비스의 사용자 인증 기법,” 정보과학회논문지, VOL. 15, No. 8, 2009.

[4] 송유진, 이재용, “SIP-VoIP 보안 인증 모델,” 한국엔터테인먼트산업학회논문지, 제3권, 제3호, 2009.

[5] Ram Dantu, Prakash Kolan “Detecting Spam in VoIP Networks,” SRUTI'05, 2005.

[6] 윤하나, 이형우, “SIP 공격 대응을 위한 보안성이 강화된 Stateful SIP 프로토콜,” 한국콘텐츠학회논문지, 제10권, 1호, 2010.

[7] http://www.voip-forum.or.kr, VoIP 국내표준, “SIP 기반 인터넷 텔레포니 단말,” 2005.

[8] 윤성열, 박석천, “인증 서비스 제공 망에서 VoIP 서비스의 사용자 인증 기법 연구,” 한국인터넷정보학회 학술대회 논문집, 제9권, 1호, 2008.

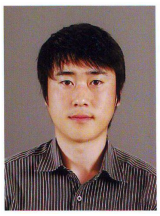
[9] Yacine Rebahi, Dorgham Sisalem and Thomas MageDanz, “SIP SPAM Detection,” ICDT 2006, August, 2006, p. 68.

[10] T. Dierks, C. Allen, “The TLS Protocol Version 1.0,” RFC 2246. January, 1999.

[11] T. Dierks, C. Allen "The TLS Protocol Version 1.0," IETF RFC 2246, January, 1999.

[12] J. Fenton, "Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)," IETF RFC 4686, September, 2006.

■ 저자소개 ■



이 영 구
Lee, Young Gu

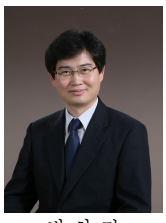
2010년 12월~현재 숭실대학교 컴퓨터학과 박사
2010년 3월 나노웨어주식회사 선임 연구원
2006년 숭실대학교 컴퓨터학과 공학석사
2003년 숭실대학교 전자계산원 공학사

관심분야 : 인터넷 보안, PKI, DRM, 홈네트워크, 멀티미디어 보안
E-mail : ad3927@ssu.ac.kr

김 정 재
Kim, Jeong Jai

2010년 2월 (주) RetailTech 수석 연구원
2005년 숭실대학교 컴퓨터학과 공학박사
1999년 숭실대학교 컴퓨터학과 공학석사
1995년 영동대학교 컴퓨터공학과 공학사

관심분야 : 멀티미디어 보안, 멀티미디어 데이터베이스, DRM, RFID, 멀티미디어 통신
E-mail : argniss@ssu.ac.kr



박 찬 길
Park, Chan Kil

2010년~현재 한국사이버대학교 정보보안학과 교수
2006년 숭실대학교 컴퓨터학과 공학박사
1995년 서울산업대학교 컴퓨터학과 공학석사
1991년 서울산업대학교 컴퓨터학과 공학사
2004년~현재 (사)디지털산업정보학회 이사

관심분야 : 네트워크보안, 유비쿼터스, DRM, E-Learning
E-mail : ckpark@mail.kcu.ac

논문접수일 : 2010년 12월 2일
수 정 일 : 2011년 1월 20일
게재확정일 : 2011년 2월 1일