SIP 기반 VoIP 서비스 환경에서의 보안성 확보를 위한 사용자 인증 시스템 설계

김철중* 윤성열* 박석천*
* 경원대학교 소프트웨어학부

Design of User Authentication System for Secure Support in VoIP Service Environment Based on SIP

Cheol-Joong Kim*, Sung-Yeol Yun*, Seok-Cheon Park*

* Division of Software, Kyungwon University

요 약

본 논문에서는 SIP 기반의 VoIP 서비스 환경에서 보안성 확보를 위해 속성인증서를 사용한 사용자 인증 시스템을 설계하였다. Redirect Server와 인증 서버를 각 Proxy Server 사이에 두어 인증서의 발급 및 검증, 사용자의 등록 및 관리 기능을 수행한다. 기존에 인증 시스템은 사용자 인증서가 외부에 노출이 되면 심각한 보안상의 문제가 발생할 수 있지만 속성인증서를 사용하면 외부에 노출에도 강력한 보안을 적용할 수 있다. 이에 본 논문에서는 속성인증서를 인증 서버가 발급과 검증을 하므로 안전한 통신 시스템을 구현할 수 있으며, 서비스 사용자를 Redirect Server에 등록 하게 함으로써 불법사용자의 접근을 제한하고, 정상적인 사용자를 인증하여 사용자의 정보보안 및 올바른 서비스의 제공이나 서비스 이용 요금의 과금시 유용하게 사용될 수 있다.

1. 서론

최근 인터넷 관련기술의 급속한 발전으로 데이터, 음성, 영상, 화상 등의 다양한 멀티미디어 서비스는 통합한 개방형 네트워크로 진화하고 있으며 궁극적으로는 모든 미디어가 인터넷으로 수렴되는 NGN(Next Generation Network)으로 발전할 전망이다[1]. 이러한 개방형 네트워크로의 진화는 IP(Internet Protocol)망을 통해 전송하는 화상회의나 VoIP(Voice over Internet Protocol)와 같은 서비스들을 가능하게 한다.

인터넷상에서 음성전화, 화상통신, 멀티미디어 전송 등을 목적으로 IETF의 SIP 시그널링 프로토콜의 경우 내용이 간단하여 개발과 구현이 쉽고, 서비스의 확장성과 포괄성이 뛰어나다. 또한 인터넷 망을 기준으로 만들어진 프로토콜이기 때문에 인터넷의 다양한 멀티미디어 서비스를 쉽게 수용할 수도 있다. SIP구성요소는 UA(User Agent), Proxy Server, Redirect Server, Registrar Server로 구성된다. SIP의 구성 요소는 MIP(Mobile IP)의 홈에이전트(HA), 외부 에이전트(FA) 등과 유사하기 때문에 단말 이동성을 지원해준다. SIP는 기본적으로 단말 이동성 외에 세션 서비스, 개인 이동성 지원이 가능하며, 하위 프로토콜에 독립적이기 때문에 기존의 IP프로토콜이나 다른 IP 응용과 통합이 용이하다. 또한 차세대 네트워크에서는 SIP를 멀티미디어를 위한 시그널링 프로토콜 표준으

본 연구는 BK21의 연구비지원에 의하여 연구되었음

로 채택하고 있다[2].

이 VoIP는 유선전화에서는 문제가 되지 않았던 사용자의 인증 문제나 과금문제 등이 대두되고 있는데, 정상적으로 접근하지 않는 불법 사용자의 구분이나 정상 사용자의 정보를 보호하기 위해서 사용자 인증 시스템이 필요하다. 따라서 본 논문에서는 SIP를 기반으로 하는 VoIP 서비스에서 보안성 확보를 위해 속성인증서를 사용하여 사용자를 인증하는 기법을 제안한다.

2. 관련연구

2.1 SIP 보안 메커니즘

SIP에서는 기존에 유선 전화망에서 사용하고 있는 보안 메커니즘을 주로 사용하고 있으며, 복잡성을 최소로 하기 위해 새로운 알고리즘의 확장은 고려하고 있지 않다.

다음 그림 1은 SIP 보안 메커니즘을 나타낸 것이다.

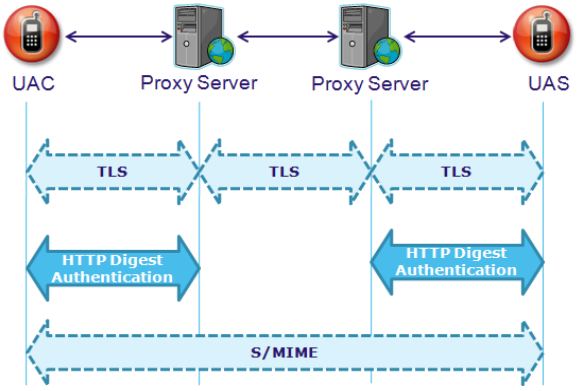

그림 1. SIP 기반의 보안 메커니즘

SIP 환경에서는 발신자를 인증하기 위한 기법으로 DKIM[3] 기법과 유사한 Authenticated Identity 기법[4]이 있다. 하지만 이기법은 SIP 환경에서의 전 구간에서 적용하기 어렵다. 따라서 그림 1과 같은 SIP 기반의 VoIP 환경에서는 발신자 및 발신경로를 인증하기 위해 HTTP digest 사용자 인증 기법과 TLS(Transport Layer Security)[5] 및 S/MIME (Secure Multi-Purpose Internet Mail Extensions)을 이용한다.

UAC(User Agent Client)와 UAS(User Agent Server) 양 단간의 보안을 위한 S/MIME과 각 홉간 보안을 위한 TLS가 선택적으로 적용 가능하다. 또한 UA와 Proxy 서버 간에는 HTTP digest 인증이 필수로 적용된다.

2.2 Digest 사용자 인증

Digest 사용자 인증은 UA-to-Registrar, UA-to-Proxy, UA-to-Redirect Server간에 적용되어 사용자 인증을 위해서 SIP 보안에 적용하고 있다. Digest 사용자 인증 방법은 challenge-response 형태로서 UAC에서 request 메시지를 보내면 Registrar, Proxy, Redirect Server에서는 challenge 메시지에 랜덤하게 생성된 정보 및 Server 정보를 보내주게 되고, 이와 같은 정보를 받은 UAC에서는 서버로부터 받은 정보와 자신의 password, ID값을 사용하여 해쉬함수를 통하여 생성된 인증정보(Credential)를 Registrar, Proxy, redirect Server에게 response로 보내게 된다. 이 인증정보는 사용자의 ID와 password값이 해쉬함수를 통해 생성되었기 때문에 password 추측이 불가능하다. Registrar, Proxy, Redirect Server에서는 UA로부터 받은 인증정보 값과 자신이 가지고 있는 UA에 대한 정보를 가지고 해쉬함수를 통해 생성된 값을 비교하여 값이 같으면 UA에 대해 인증을 하게 된다.

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[6].

3. SIP 기반의 VoIP 서비스 환경에서 사용자 인증 시스템 설계

본 논문에서 제시하는 SIP 기반의 VoIP 서비스 환경에서는 모든 메시지를 SIP를 이용하여 응용계층에서 전송한다. SIP 메시지를 암호화해서 전송하지 않으면 외부적인 공격에도 쉽게 노출되고, 정상 사용자가 아닌 불법 사용자가 네트워크의 자원을 불법으로 사용할 수 있다. 따라서 현재 이 시스템에 접속하는 단말이 정상 사용자인지 불법 사용자인지를 인증하는 과정이 필요하게 되었고, 본 논문에서는 사용자 인증 시스템을 속성 인증서를 사용하여 설계하였다.

3.1 시스템 구성

본 논문에서는 각 UA 단말이 Proxy Server와 연결되어 있고 각 Proxy Server는 사용자 인증서버에 연결되어 있다. 이 사용자 인증서버는 속성인증서를 발급하고 검토하는 서버로써 Redirect Server에 연결되어 있다. 그림 2는 전체 VoIP 시스템 구성도이다.

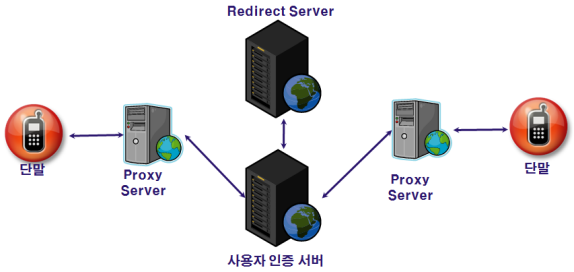

그림 2. 제안한 VoIP 시스템 구성도

제안 시스템을 적용하기 위해서는 인증된 Proxy Server와 인증서버, 그리고 Redirect Server가 필요하다. 따라서 사전에 공개키의 교환이 이루어 져야 하는데 이에 대한 조건은 다음과 같다.

1. 인증 서버와 Redirect Server는 인증절차를 사전에 실시하여 서로의 공개키 값을 알고 있다.

2. 서비스에 등록되지 않는 사용자는 기본적으로 본 서비스를 제공받지 못하므로 Redirect Server에 등록 절차를 거칠 때 Proxy Server의 공개키를 등록시킨다.

3.2 제안 시스템 서비스의 흐름도

위에 조건을 만족하는 UAC, UAS, Proxy Server A, Proxy Server B, 인증서버 및 Redirect Server를 이용하여 UAC가 UAS에게 RTP세션을 열기위해 INVITE메시지에 UAS의 Proxy Server 주소를 담아 보낸다. 그림3은 제안 시스템 서비스의 흐름도이다.

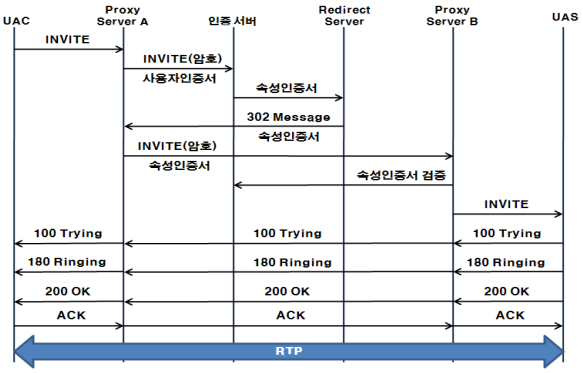

그림 3. 제안한 시스템 서비스의 흐름도

먼저 UAC가 UAS에게 INVITE메시지를 보냄으로써 연결시도를 하려 할 때 Proxy Server A는 받은 INVITE 메시지를 인증 서버의 공개키로 암호화 하여 사용자인증서를 생성 후 전송한다. 인증서버는 Random R 값을 생성하여 Redirect Server의 공개키로 암호화한 속성 인증서를 발급한다. Redirect Server는 302 메시지 안에 UAS와 연결되어 있는 Proxy Server B의 IP와 공개키를 Proxy Server A의 공개키로 암호화하여 인증서버에서 전송받은 속성인증서와 함께 전송한다. Proxy Server A는 수정된 INVITE 메시지를 Proxy Server B의 공개키로 암호화하고 속성인증서와 함께 Proxy Server B로 전송하고, Proxy Server B는 전송받는 INVITE 메시지를 해석하고 수신된 속성인증서를 인증 서버에 검증 요청을 한다. 검증이 되었다면 UAS로 원래의 INVITE 메시지가 전송되고 RTP(Real Time Protocol) 세션이 개시된다.

그림 4는 메시지의 전송 시 필요한 공개키와 R

값의 흐름도 이다.

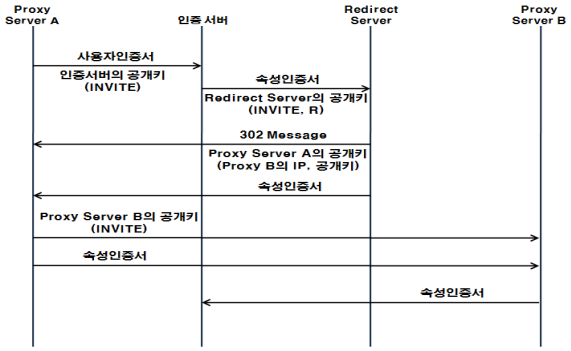

그림 4. 공개키와 R값의 흐름도

속성인증서를 생성할 때 인증서버에서 생성하는 R 값은 Random 값으로 속성인증서가 한 번의 인증 과정이 끝나면서 소멸되고, 다음에 다시 콜을 개시할 때 새로 속성인증서를 발급하게 되는데, 이때 새로운 R값이 재 생성되기 때문에 기존에 발급된 속성인증서로는 인증이 불가능 하다.

이 시스템은 기존에 사용자 인증에서 문제점으로 여겨졌던 TLS 보안의 무리한 오버헤드문제를 보완할 수 있고, 속성인증서의 사용으로 일정 시간이 지나면 인증서의 유효기간이 만료되어 속성인증서가 외부에 노출 되더라도 안전하게 서비스를 이용할 수 있다.

또한 사전에 등록된 사용자만이 이 서비스를 이용할 수 있으므로 유료 서비스의 사용이나 서비스 이용 요금의 과금을 처리할 때 사용될 수 있다.

4. 결론

본 논문에서는 SIP 기반의 VoIP 서비스 환경에서 보안성 확보를 위해 속성인증서를 사용한 사용자 인증 시스템을 설계하였다. 기존에 인증 시스템은 사용자 인증서가 외부에 노출이 되면 심각한 보안상의 문제가 발생할 수 있지만 속성 인증서를 사용하면 외부에 노출에도 강력한 보안을 적용할 수 있다. 이에 본 논문에서는 속성인증서를 인증서버가 발급과 검증을 하므로 안전한 통신 시스템을 구현할 수 있고, 서비스 사용자를 Redirect Server에 등록 하게 함으로써 불법사용자의 접근을 제한하고, 정상적인 사용자를 인증하여 사용자의 정보보안 및 올바른 서비스의 제공이나 서비스 이용 요금의 과금시 유용하게 사용될 수 있다.

[참고문헌]

[1] 이근호, 이송희, 김정범, 한상범, 김태윤, "VoIP를 위한 보안 기술 현황과 전망", 한국통신학회지, 제 19권 8호, 2002.8

[2] 성경, 김석훈, 박길하, "차세대 네트워크 환경에서의 보안성 지원을 위한 SIP 기반 VoIP 시스템", 한국해양정보통신학회 논문지, Vol.10 No.12, 2006

[3] 장유정, 정수환, 문형권, 최재덕, 원유재, 조영덕, “SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법”, 한국통신학회논문지, ‘07-8 vol. 32 No. 8

[4] J. Peterson, C. Jennings, “Enhancements for Authenticated Identity Management in the SIP,” IETF RFC 4474, August 2006.

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

[6] 강명희, 유황빈, "IPSec-VPN 시스템에서의 속성 인증서를 이용한 사용자 접근 제어 방안", 정보보호학회논문지, Vol.14 No.5, 2004

[7] 양호경, 차현종, 한인성, 유황빈, "VoIP 서비스 환경에서의 사용자 접근 통제 및 인증시스템", 한국컴퓨터종합학술대회 논문집, Vol.32 No.1, 2007

[8] 최재덕, 정태운, 정수환, 김영한, "SIP 기반의 VoIP 보안 시스템 구현", 한국통신학회논문지, 제29권 9B호, 2004.9

[9] Ramsdell B, "S/MIME Version 3 Message Specification," RFC 2633, IETF, JUNE 1999.