SIP 기반의 확장 보안 메커니즘 설계

이근호[O] 이송희 김정범 김태윤
고려대학교
{root1004[O], pine, qston, tykim}@netlab.korea.ac.kr

The Design of SIP based Extension Security Mechanism

Keunh-Ho Lee[0] Song-Hee Yi Jeong-Beom Kim Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

최근 인터넷 관련 기술의 급속한 발전으로 데이터, 음성, 화상 등의 다양한 멀티미디어 서비스가 통합된 개방형 네트워크로 진화되어지고 있다. 모든 미디어가 인터넷으로 수렴되는 NGN(Next Generation Network)으로 발전할 전망이다. 개방형 네트워크는 다양한 유무선 통합망의 융합화에 따른 통신망간의 간섭이 증가하고 네트워크 접속점 중심의 통신망간 접속구조가 확대되어 지금까지의 시스템 보안 위주의 단순한 보안 기술을 적용하기가 어려웠다. 따라서 네트워크 노드간을 효율적으로 보호하는 네트워크 중심의 보안 기술이 필요한 시점이다. 이에 본 논문은 IETF에서 제안한 텍스트 기반 응용 계층의 접속제어 프로토콜로 실시간 미디어 통신을 위한 차세대 인터넷 프로토콜로 주목받고 있는 SIP(Session Initiation Protocol) 시스템을 분석하고, SIP 기반의 보안 메커니즘인 IPSec에서의 확장 보안 메커니즘을 설계하였다.

1. 서 론

최근에는 기존의 전화망을 이용한 데이터 전송에 관한 연구가 활발히 진행중이다. 통신 사업자, 인터넷 서비스 제공자, 산업체 및 일반 이용자의 관심이 고조되고 있는 VoIP 기술은 인터넷의 최대 응용 서비스로서 급부상함과 동시에 고속으로 시장이 성장·확산되고 있는 분야이다. VoIP의 성장 배경에는 VoIP가 기존의 인터넷 서비스 사업자들이 구축한 인터넷망을 이용함으로써 비록 이용 편리성이나 품질에 일부 문제가 있더라도 무료 또는 기존의 PSTN에 비해 낮은 가격으로 전화 서비스를 제공할 수 있었던점과 IP 기반망을 이용한 음성의 비용이 기존의 전화에 비해 보다 빠른 속도로 낮아지고 있는점 등이 작용했다고 할 수 있다. 최근에는 VoIP가 단순히 값싼 요금의 전화 서비스 제공에 머물지 않고 음성과 데이터를 통합한 부가 서비스 제공에 역점을 두는 추세이다. VoIP는 인터넷의 IP 계층을 사용하여 음성을 전송하는 기술을 말한다. VoIP는 아날로그의 신호를 디지털 신호로 변환한 후, 패킷으로 구성하여 IP망인 인터넷을 통해 수신측까지 전달하는 것을 의미한다[2].

음성 패킷만을 전송하던 과거의 음성망을 데이터의 전송을 통한 멀티미디어 기능을 제공할 수 있는 멀티미디어 망으로 발전되어 가고 있다. 음성에 관한 연구 분야인 VoIP 분야는 크게 세가지로 구분할 수 있다. ITU-T의 H.323과 IETF의 SIP(Session Initiation Protocol)과 ETSI 의 TIPHON(Telecommunication and Internet Protocol Harmonization Over Networks)으로 나눌 수 있다. 본 논문에서는 IETF에서 제안한 SIP 기반 보안 메커니즘의 확장 모델을 설계하였다. SIP은 보안을 위한 새로운 메커니즘을 정의하지 않고 주로 기존에 사용하고 있는 보안 메커니즘을 사용한 보안 모델을 제시하고 있다.

HTTP 나 SMTP에서 사용하고 있는 digest 인증 방법과 end-to-end 메시지 암호화를 위한 방법으로 S/MIME을 이용하고 있다. 제안 모델은 IPSec이나 TLS와 같은 네트워크나 트랜스포트 계층 보안 프로토콜을 적용하여 hop-by-hop 간의 메시지에 대한 비밀성과 무결성을 지원하도록 설계하였다.

2. 관련연구

2.1 SIP 시스템 구성요소

SIP는 ITU-T의 H.323에 대응되는 프로토콜로서 단말간 또는 사용자들간에 기존의 VoIP 서비스뿐만 아니라 다양한 서비스의 호 설정 프로토콜이다[1]. 즉 SIP 는 peer-to-peer 시그널링 프로토콜이며 E-mail과 유사한 주소체계 형태의 동일 식별자를 이용하여 언제, 어디서나 음성 통화 서비스를 비롯한 E-mail 인스턴트 메시징 서비스 등을 제공 받도록 한다. 또한 SIP를 이용하여 세션을 설정할 때 세션 파라미터를 협상함으로써 사용자의 능력에 따라 서비스가 지원된다. 세션에 참여하고 있는 수신측은 원치 않는 호출자에 대한 거부, 원치 않는 서버에 대한 거부, 음성메일로의 전환과 같은 필터링 기능을 제공 받는다. SIP 사용자는 자신의 휴대폰 번호, 사무실 번호, 집 전화번호, E-mail 주소 등을 서버에 등록 할 수 있으며 이 등록된 전화 및 응용 서버에 모든 Call이 전달되는 forking 기능을 수행한다. SIP 는 HTTP의 많은 부분을 이용하고 있기 때문에 프로토콜의 메시지는 텍스트로 구성되는 텍스트 기반 프로토콜이고 메시지의 종류는 메소드와 그에 대한 응답으로 구성되는 Request/Response 형식이다. SIP 표준에서 제공하는 메소드는 INVITE, ACK, CANCEL, BYE, REGISTER, OPTION이 있으며 응답 시에는 HTTP와 유사하게 숫자

를 갖는 메시지를 전송한다. SIP 메시지 형식은 HTTP와 동일하게 헤더와 바디로 구성되고 헤더와 바디는 CR/LF로 구별된다.

SIP는 크게 User Agent와 서버로 구성된다. SIP User Agent는 호출자 기능을 수행하는 UAC와 수신자 기능을 수행하는 UAS(User Agent Server)로 분류된다. SIP 서버는 SIP Registrar, SIP Redirect Server, SIP Proxy Server로 구성된다. SIP Registrar는 SIP 사용자의 등록 및 호를 받을 수 있는 위치 등록 기능을 수행한다. SIP Redirect Server 는 UAC로부터 호 설정 요청을 받으면 수신자의 위치정보를 찾아서 UAC에게 전달함으로써 UAC가 다시 호설정 요청을 한다. 반면에 SIP Proxy Server 는 UAC로 부터의 호설정 요청을 받으면 수신자의 위치정보를 파악하고, 그 정보를 UAC에게 알려주는 것이 아니라 그 호설정 요청을 파악된 위치정보 상의 서버에게 전달함으로써 UAC와 UAS 기능을 수행한다[2].

SIP 프로토콜의 기본 특성으로는 먼저 TCP, UDP 등 하위 레벨의 트랜스포트 프로토콜과 독립적으로 동작하며, 사용자뿐만 아니라 미디어 스토리지 서비스 등의 응용 엔터티도 세션에 참가할 수 있고, 유니캐스트 혹은 멀티캐스트 세션을 생성할 수 있다. 세션 설정 및 해지를 위해 제공되는 기능으로는 SIP 사용자 식별(SIP Addressing), 서버 위치 파악(Location), SIP 메시지 전달(SIP Transaction), 세션에 초청(Invitation), 수신자 위치 파악(SIP User Location), 세션 정보 수정 그리고 사용자 등록(Registration)이 있다.

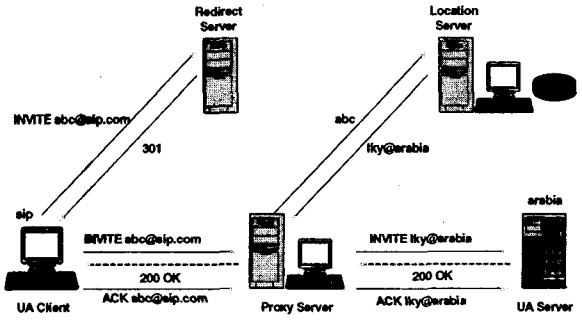


그림 1 SIP 시스템의 구성 요소

2.2 SIP 보안 메커니즘

SIP에서의 신호에 대한 보안은 크게 End-to-End 보안과 Hop-by-Hop 신호 보안으로 구분할 수 있다.

End-to-End 보안 메커니즘으로는 basic, digest 인증, PGP등이 있다. Hop-by-Hop 신호 보안에서의 메커니즘으로는 IPSec, TLS가 있다. SIP에서의 인증 프로토콜로는 Basic, Digest, PGP를 사용한다. 현재 SIP에서는 PGP는 사용하지 않고 있다.

SIP 보안에서는 기본적으로 메시지에 대한 비밀성과 무결성을 지원해야 한다. 메시지 변조와 같은 공격으로부터 보호하고, 메시지에 대한 인증을 통해 공격을 차단해야 한다.

SIP에서는 여러 보안 메커니즘을 적용한다. SIP 메시지 전체에 대한 암호화는 메시지에 대한 비밀성을 보장하여 네트워크 상의 정보 누출을 방지하지만 프락시 서버에서 라우팅을 위한 정보를 나타내는 헤더를 확인 할 수 없어 정확한 메시지를 전달하지 못한다.

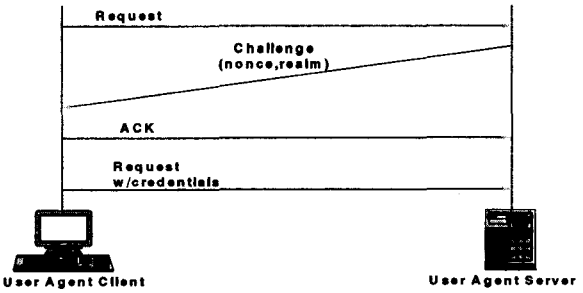


그림 2 SIP Authentication

따라서 프락시 서버와 SIP UA간에 서로에 대한 신뢰하기 위한 방법으로 하위-레이어 보안 메커니즘인 IPSec[6]나 TLS[7]와 같은 네트워크나 트랜스포트 레이어 보안 프로토콜을 적용한다. IPSec이나 TLS는 Hop-by-Hop의 메시지의 비밀성과 무결성을 지원한다.

End-to-End는 암호화 방법을 사용하여 프락시에서 SIP 메시지를 변경하거나 분석 할 수 있도록 라우팅 관련 헤더 부분을 제외하고 암호화하여 전송한다. S/MIME은 End-to-End 간의 메시지에 대한 비밀성과 무결성을 지원하기 위해 메시지 암호화를 위해 새롭게 제시하고, 또한 인증서를 통한 상호간의 인증도 제공할 수 있다.

MIME은 SMTP를 확장하여 오디오, 비디오, 이미지, 응용프로그램 등 여러 종류의 데이터 파일을 주고받을 수 있도록 기능이 확장된 프로토콜이지만 보안 메커니즘을 가지고 있지 않다. 이러한 이유 때문에 응용 계층에서 보안 제공을 위해 S/MIME 형태로 전송한다. S/MIME는 모든 프로토콜에 적용할 수 있고 또한 암호화와 전자서명 기능도 제공한다.

SIP 메시지는 텍스트 기반이므로 MIME 형태로 전송되기 때문에 S/MIME을 사용하여 End-to-End 간의 비밀성과 무결성을 지원한다.

SIP에서는 메시지 변조를 통한 서비스 방해나 Replay 공격을 방지하기 위해 메시지에 대한 인증 메커니즘을 지원하고 있으며 이를 위해 HTTP에서 사용하는 인증 방법인 basic인증과 digest 인증[8]법을 적용하고 있다[9].

3. SIP 기반의 확장 보안 메커니즘

3.1 제안된 메커니즘을 위한 프로토콜

- IPSec AH 프로토콜

IP 인증 헤더(Authentication Header:AH) 프로토콜은 IP 데이터그램에에 대해 무결성, 인증, 재전송 공격 방지 등과 같은 세가지 보안 서비스를 제공하기 위해 사용된다 이러한 보안 서비스 중 재전송 공격 방지는 SA(보안 연계)를 생성할 때 수신자가 선택적으로 이용할 수 있도록 하고 있다.

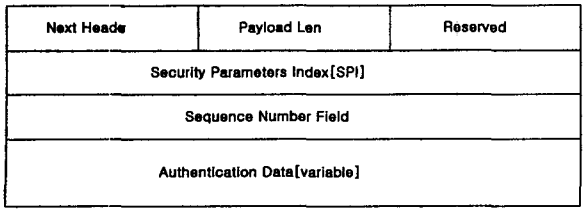


그림 3 AH 데이터 형식

- IP ESP(Encapsulating Security Payload) 프로토콜

IP ESP 프로토콜은 IP 데이터그램에 기밀성, 무결성, 인증, 재전송 공격 방지등과 같은 네가지 보안 서비스를 제공하기 위해 사용된다. 그러나 IP 데이터 그램에 대한 기밀성만을 제공하기 위해 이용될 수 있다. ESP 내에 두 개의 모드가 정의되는데 하나는 터널-모드이고 다른 하나는 트랜스포트-모드이다. 터널-모드는 ESP 헤더 내 IP 데이터그램 전체에 대한 캡슐화를 수행하는 모드이고, 트랜스포트-모드는 ESP 내의 상위 계층 프로토콜에 대한 캡슐화를 수행하고 평문 형태인 IP헤더를 붙이는 모드이다.

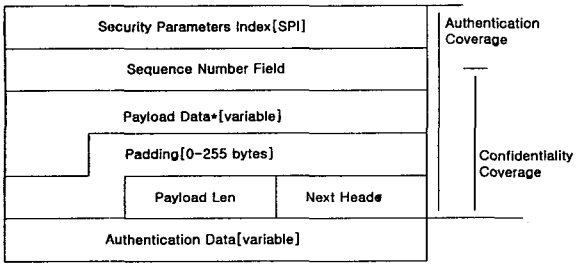


그림 4 ESP 데이터 형식

- Kerberos

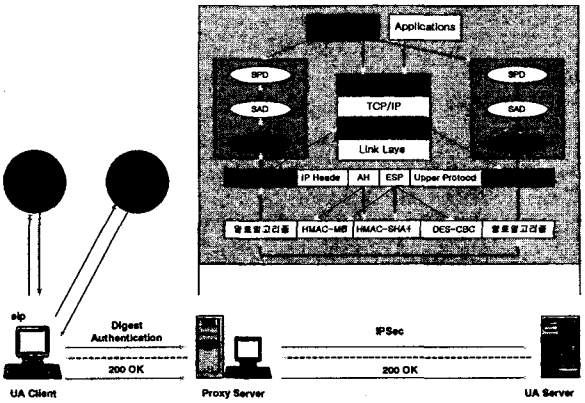
Kerberos는 대칭키 암호 기술과 신뢰된 제 3자를 사용하여 인증 뿐만 아니라 키 설정 서비스를 제공한다.

c=client
s=server
a=client's network address
v=beginning and ending validity time for a ticket
t=timestamp
Kx=x's secret key
Kx,y=session key for x and y
{m}Kx=m encrypted in x's secret key
Tx,y=x's ticket to use y
Ax,y=authenticator from x to y

Kerberos version 5의 메시지는 다음과 같다.
Client to Kerberos : *c, tgs*
Kerberos to client : *{Kc, tgs}Kc, {Tc,tgs}Ktgs*
Client to TGS : *{Ac, s}Kc, tgs, {Tc, tgs}Ktgs*
TGS to client : *{Kc,s}Kc,tgs,{Tc,s}Ks*
Client to server : *{Ac,s}Kc,s,{Tc,s}Ks*

3.2 제안하는 SIP 보안 확장 메커니즘

IPSec은 키관리 프로토콜인 ISAKMP/IKE가 지나치게 무거워 무선 단말과 같은 제한된 환경에서는 구현이 어렵다는 문제점을 극복하기 위해서 대신 키 관리 목적으로 Kerberos 같은 기존의 인증 서버를 사용하여 확장 메커니즘을 설계하였다.



4. 결론

단순한 텍스트 기반에서 다양한 서비스를 제공할 수 있는 VoIP 기술로 발전되면서 SIP 기반에 필요한 보안 메커니즘의 필요성이 대두되고 있다. 본 논문에서는 SIP 기반의 제한된 환경에서 구현이 어려운 문제점을 해결하기 위하여 확장 보안 메커니즘을 설계하였다. 향후 연구에서는 확장된 메커니즘의 QoS를 높일 수 있는 방법의 연구가 필요할 것이다.

참고문헌

[1] Session Initiation Protocol Working Group, http://www.ietf.org/html.charters/sip- charter.html
[2] 김영한, 고석갑, "VoIP 기술 개요 및 표준화 동향", 정보처리학회지 제 8권 제 2호, pp 10-21, 2001.3
[3] M.Handley, H. Schulzrinne, E. Schooler, and J.Rosenberg, "SIP:session initiation protocol", Request for Comments 2543, Internet Engineering Task Force, Mar, 1999
[4] Inmaculada Espigares del Pozo, "An Implementation of the Internet Call Waiting Service using SIP", Master's thesis at Helsinki University of Technology and Polytechnic University of Valencia. December 1999.
[5] 이종화, 안상현, "SIP 기반 차세대 응용 기술", 정보처리학회지 제 8권 제 2호, pp 27-33, 2001.3
[6] RFC 2402, "IP Authentication Header", IETF IPSec WG., 1998
[7] RFC 2246, "The TLS Protocol Version 1.0", IETF TLS WG., 1999
[8] RFC 2617, "HTTP Authentication : Basic and Digest Access Authentication", IETF, 1999
[9] 정수환, 홍기훈, 박성준, "VoIP 보안 기술", 한국통신학회지, 제 19권 제 2호, pp.193-203, 2002.2.