SIP 기반의 VoIP 보안 시스템 구현

정회원 최 재 덕*, 정 태 운**, 정 수 환*, 김 영 한**

Implementation of a Secure VoIP System based on SIP

Jaedeok Choi*, Taewoon Jung**, Souhwan Jung*, Younghan Kim** *Regular Members*

요 약

본 논문에서는 IETF에서 제안한 SIP 프로토콜의 보안에 대해서 연구하고 이를 기반으로 VoIP 보안 시스템을 설계하여 RFC 3261의 보안 요구 사항 및 방향에 대해서 분석하였다. SIP 보안 메커니즘으로 HTTP Digest 사용자 인증, TLS를 적용한 홉간 보안, S/MIME을 적용한 단말간 보안을 적용하고 미디어 보안으로는 현재 드래프트인 SRTP를 사용하여 구현하였다. SIP 표준 문서에서 제안하고 있는 사용자 인증, 홉간 보안, 단말간 보안을 SIP VoIP 단말 시스템에 적용하고 미디어 보안을 구현함으로써 VoIP 단말 및 프록시 서버 보안 기능을 구현하였다. 또한 SIP 표준에서 제시된 보안 메커니즘의 안전성을 분석하였다.

ABSTRACT

In this paper, a security mechanism for a VoIP system based on SIP was implemented. This was satisfied security requirement of RFC 3261. The SIP standard proposes a HTTP digest authentication for user authentication mechanism, TLS for hop-by-hop security and S/MIME for end-to-end security. SRTP draft was implemented for media security. We also analyzed security of proposed SIP standard.

Ⅰ. 서 론

SIP(Session Initiation Protocol)[1]는 기존 공중전화망(PSTN) 전화 서비스를 초고속 통신망의 보급과 인터넷 응용기술의 발전으로 일반화 되어가고 있는 IP 기반의 VoIP(Voice over IP) 서비스의 시그널링 프로토콜로서 각광받고 있는 프로토콜이다. 과거에 비해 인터넷 전송 속도가 빨라지고 음질 면에 있어서도 많이 향상되어, 저렴한 가격비용으로 점차 VoIP 사용자수는 늘어날 것으로 기대되고 있지만 패킷 망은 보안 측면에서 공개된 네트워크로 누구나 쉽게 접근할 수 있기 때문에 여러 가지 문제점이 발생할 수 있다. PSTN망은 물리적으로 접근해야 공격할 수 있는 반면, VoIP는 원거리의 공격자도 네트워크기술을 이용하여 쉽게 시그널링 메시지의 변조 및 음성 패킷을 도청할 수 있다. 따라서 이러한 공격에 대한 방어와 안전한 VoIP 서비스를 위해서 보안 시스템을 적용할 필요가 있으며 사용자 인증, 메시지 인증과 무결성 보장, 메시지의 기밀성 보장 그리고 음성 데이터에 대한 기밀성을 보장해야 할 필요가 있다.

RFC 3261에서는 SIP 보안 메커니즘으로 새로운 보안 메커니즘의 설계를 지양하고 기존 보안 모델의 사용을 권고하고 있다. SIP 표준문서에 규정된 Digest 사용자 인증[2], TLS[3], S/MIME[4]을 적용하여 SIP 메시지에 대해서 보안 서비스를 제공하고 현재 드래프트 상태인 SRTP(Secure RTP)[5]를 사용하여 미디어 보안을 구현하였다.

본 논문에서는 II장에서 SIP 보안 메커니즘 및 시스템 구조에 대해서 언급하고 III장에서는 구현

* 숭실대학교 정보통신전자공학부 통신망보안 연구실
** 숭실대학교 정보통신전자공학부 네트워크 연구실
(jdchoi@addpac.com, taeun@dcn.ssu.ac.kr, souhwanj@ssu.ac.kr, yhkim@dcn.ssu.ac.kr)
논문번호 : 030048-0203, 접수일자 : 2003년 2월 3일
※ 본 연구는 숭실대학교 교내 연구비 지원에 의해 수행되었습니다.

내용과 동작 결과를 기술하는데 특 , 적용된 보안 메커니즘들에 대해서 안전성을 분석하여 앞으로 보완되어야 할 사항들에 대해 언급하였다.

Ⅱ. SIP 보안 메커니즘 및 시스템 구조

SIP에서는 보안을 위한 새로운 메커니즘을 정의하지 않고 주로 기존에 사용하고 있는 보안 메커니즘을 보안 모델로 제시하고 있으며 여러 가지 다양한 환경과 응용 프로그램에 적용할 수 있는 보안 메커니즘으로 복잡성을 최소화하기 위하여 새로운 기반 구조나 알고리즘의 확장은 지양하고 있다.

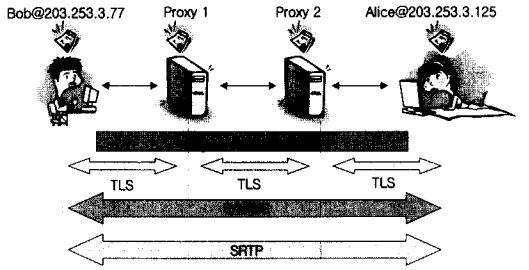


그림 1. RFC 3261을 기반으로 구현된 SIP 보안 메커니즘

그림 1은 RFC 3261을 기반으로 본 논문에서 구현된 SIP 보안 메커니즘을 나타내고 있다. 먼저 사용자 인증은 HTTP Digest 사용자 인증을 사용하고 이후 세션 연결을 위해서 주고받는 SIP 메시지에 대해서는 홉간에 TLS를, 양단간에는 S/MIME을 사용하여 SIP 메시지의 기밀성, 무결성 및 사용자 인증을 제공한다. RTP 패킷 보안을 위한 SRTP는 현재 드래프트 상태이지만 RTP 패킷의 암호화를 통해 음성 보안 서비스를 제공할 수 있기 때문에 적용하였다.

1. Digest 사용자 인증

Digest 사용자 인증은 UA-to-Registrar, UA-to-Proxy, UA-to-Redirect 서버간에 적용되어 사용자 인증을 위해서 SIP 보안에 적용하고 있다. Digest 사용자 인증 방법은 challenge-response 형태로서 UAC에서 request 메시지를 보내면 Registrar, Proxy, Redirect 서버에서는 challenge 메시지에 nonce와 같은 랜덤 정보와 realm 정보를 보내주게 되고, 이와 같은 정보를 받은 UAC에서는 서버로부터 받은 정보와 자신의 password, ID값을 사용하여 해쉬함수를 통하여 생성된 인증정보(Credential)를 Registrar, Proxy, Redirect 서버에게 response로 보내게 된다. 이 인증정보는 사용자의 ID와 password 값이 해쉬함수를 통해 생성되었기 때문에 password 추측이 불가능하다. Registrar, Proxy, Redirect 서버에서는 UA로부터 받은 인증정보 값과 자신이 가지고 있는 UA에 대한 정보를 가지고 해쉬함수를 통해 생성된 값을 비교하여 값이 같으면 UA에 대해 인증을 하게 된다. Digest 사용자 인증은 'qop=auth' 옵션 파라미터를 사용하여 인증 정보 생성시 UA에서 cnonce를 사용하여 chosen plain text 공격에 대해서 보호할 수 있다. 또한 Digest 사용자 인증은 REGISTER 메시지를 통해 사용자 등록에만 사용되지 않고 INVITE, ACK, BYE 메시지에도 적용되어 SIP VoIP 시스템에서 세션 연결 시에도 정당한 사용자인지 아닌지 확인할 수 있도록 HTTP Digest 사용자 인증 메커니즘을 확장 적용하였다.

2. Hop-by-Hop 보안

SIP 홉간 보안은 UA-to-Registar, UA-to-Proxy, Proxy-to-Proxy, Proxy-to-UA간에 적용되며 이러한 보안 메커니즘으로는 TLS, IPsec등이 사용된다. RFC 3261에서는 TLS의 구현을 SIP 서버에서 반드시 구현해야 한다고 규정하고 있고 UA에서는 옵션으로 적극 권장하고 있다. 홉간 보안은 보안 채널을 통해 SIP 메시지를 전달하기 때문에 SIP 전체 메시지에 대해서 기밀성과 무결성을 제공하고 인증서를 통해 사용자간에 인증을 제공한다. SIP 메시지 전체에 대한 암호화는 메시지에 대한 기밀성 및 무결성을 완벽하게 보장하여 네트워크 상의 공격자로부터 정보누출을 방지 할 수 있지만 Proxy 서버에서 라우팅을 위한 정보를 나타내는 To, From, Request-URI, Route, Via 등의 헤더를 확인할 수 없어 정확한 메시지 전달이 어렵다는 문제가 있다. 이러한 이유로 TLS 보안 채널은 UA-to-UA와 같이 End-to-End로 적용할 수 없고 SIP 단말간에 홉 단위로 적용하여 보안 서비스를 제공한다. UA에서는 TLS 보안 채널을 통해 SIP 전체 메시지를 암호화해서 전송하게 되고 이 메시지를 받은 Proxy 서버에서는 복호화하여 라우팅에 관한 정보를 확인한 후 다시 다음 홉과 보안 채널을 형성해 SIP 메시지를 암호화하여 전송한다. 그림 2는 TLS를 적용하여 보안 채널을 형성하는 구조를 나타낸다.

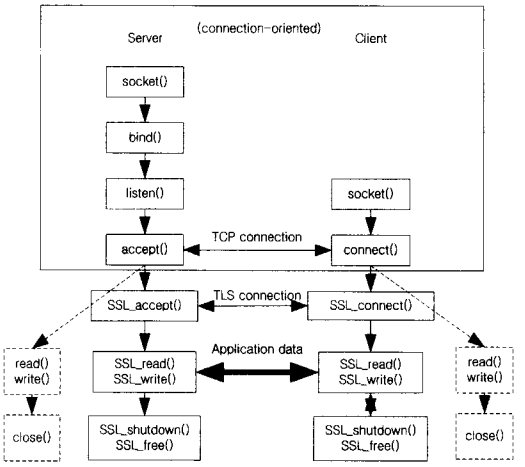


그림 2. TLS를 통한 SIP 메시지 보안

TLS 보안 채널은 TCP Connection이 연결된 후에 형성되기 때문에 UA와 Proxy 서버간에는 TCP Connection이 먼저 이루어져야 한다. UA와 Proxy 서버에서 이렇게 생성된 TCP Client SockID와 TCP Server SockID는 TLS Connection을 위해서 'Hello' 메시지를 주고받으며 핸드쉐이크 과정을 시작하는데 사용된다. 이 과정에서 UA와 Proxy 서버는 상호간에 인증서를 통해 인증을 하고 메시지 전송에 필요한 대칭키 암호 알고리즘, MAC 생성을 위한 해쉬 알고리즘의 종류 등 대칭키 암호 알고리즘 및 MAC 생성을 위한 여러 종류의 파라미터 값을 생성 및 교환하게 된다. RFC 3261에서는 TLS_RSA_WITH_AES_128_CBC_SHA를 반드시 구현해야 한다고 규정하고 있고 호환성을 위해서 TLS_RSA_WITH_3DES_EDE_CBC_SHA 또한 규정하고 있다. TCP Connection에서는 read(), write()를 사용하여 SIP 메시지 전달이 되지만 TLS 보안 채널이 형성된 후에는 SSL_read(), SSL_write() [6]를 사용하여 SIP 메시지의 기밀성 및 무결성을 제공하게 된다.

3. End-to-End 보안

SIP 양단간 보안은 UA-to-UA간에 적용되며 이러한 보안 메커니즘을 위해서 RFC 3261에서는 UA에서 S/MIME을 옵션으로 규정하고 있다. MIME은 SMTP를 확장하여 오디오, 비디오, 이미지, 응용프로그램, 기타 여러 가지 종류의 데이터 파일들을 주고 받을 수 있도록 기능이 확장된 프로토콜이며 응용계층에서 보안을 제공하기 위해 S/MIME이 제안되었다. SIP 메시지 암호화를 위해 새롭게 제시된 S/MIME은 양단간의 메시지에 대한 기밀성과 무결성을 지원할 뿐만 아니라 인증서를 통한 상호간의 인증도 제공한다. SIP 메시지의 S/MIME적용은 SDP 암호화 모드, SIP 전체 메시지 서명 모드, SIP 전체 메시지 암호 및 서명 모드와 같이 3가지로 나뉘어 진다. TLS는 SIP 전체 메시지의 암호화에 대해 홉간 제공하고 Proxy 서버에서 라우팅 정보를 본 후 다시 암호화해서 보내는 메커니즘을 사용하고 있지만 S/MIME은 SIP 전체 메시지를 양단간 암호화에 대한 보안 서비스를 제공하기 때문에 Proxy 서버에서 SIP 메시지 라우팅 관련 헤더들을 볼 수 있어야 한다. 따라서 양단간에 보안 서비스를 제공하기 위해서 라우팅 관련 헤더에 대해서는 기밀성을 제공하지 않고 이 점을 고려하여 SIP에 S/MIME적용에 대해서 RFC 3261은 Tunneling SIP 모드를 적용할 것을 규정하고 있다. 이 Tunneling 모드는 SIP 전체 메시지에 대해서 암호화 및 서명 기능을 제공하기 위해서 Outer 메시지와 Inner 메시지로 구성된다. 그림 3은 암호화와 서명이 적용된 SIP 메시지 형태를 나타낸다.

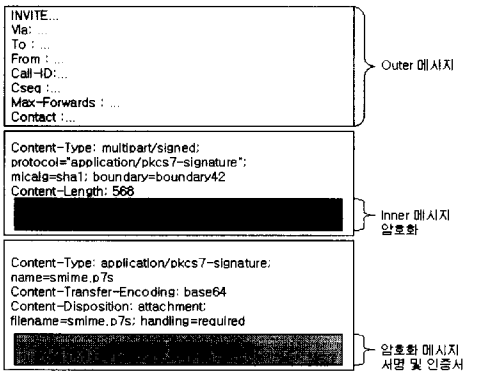


그림 3. S/MIME을 통한 SIP 메시지

위 그림과 같이 Outer 메시지는 SIP 메시지 중에서 라우팅 헤더에 관한 To, From, Call-ID, CSeq, Contact 등과 같이 Proxy에서 라우팅 할 수 있는 헤더로 구성이 되며 Inner 메시지는 SIP 전체 메시지로 구성이 되어 있다. 이렇게 두 부분으로 나누어 S/MIME 적용시 MIME 부분에 해당하는 부분으로 Inner 메시지 부분을 서명 및 암호화하여 SIP 메시지를 보호하게 된다. 그러나 Proxy에서 라우팅을 위

해서 Outer 메시지에 헤더를 그대로 노출시키기 때문에 Inner 메시지의 암호화에 대해서는 한계가 있다. 이는 사실상 SIP 전체 메시지의 암호화에 대한 의미는 없지만 Outer 메시지의 From 헤더에 UAC의 ID는 'anonymous'로 표기를 하고 Contact 헤더에는 UAC의 ID를 생략하여 UAC의 ID와 SDP 메시지의 기밀성을 제공한다. 이와 같이 함으로써 UAS에서는 Inner 메시지를 복호화 한 후에 UAC의 ID를 확인 할 수 있지만 중간 노드에서는 UAC의 ID를 확인 할 수 없게 되어 ID Privacy가 제공된다.

4. 미디어 보안

RFC 3261에서는 SIP 시그널링에 대한 보안만을 고려하며 미디어 보안에 대해서 규정해 놓은 것이 없기 때문에 미디어 보안은 VoIP 시스템에서 실제 두 사용자간에 음성 데이터인 RTP Payload의 암호 및 패킷 인증을 위해서 적용할 수 있는 SRTP 드래프트를 적용하였다. 그림 4는 SRTP의 패킷 형태를 나타내고 있다.

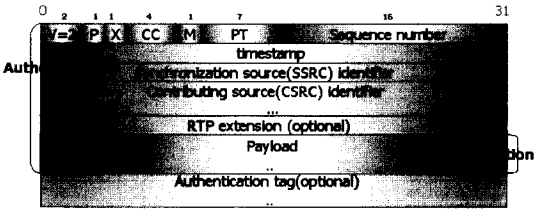


그림 4. SRTP 패킷 형태

SRTP 위 그림과 같이 RTP 패킷의 Payload 부분을 AES Counter 모드[7]를 사용하여 암호화하고 'Authentication tag'를 통해 암호화된 Payload 부분을 포함한 전체 RTP 패킷의 무결성을 HMAC-SHA1을 통하여 제공하게 된다. 두 UA 간에 세션키는 여러 Key 교환 메커니즘을 사용할 수 있지만 현재 드래프트로 나와 있는 MIKEY (Multimedia Internet Keying)[8]에서 정의하는 Key 교환 메커니즘을 사용하여 Key 교환이 이루어질 수 있다.

5. 보안 기능이 추가된 SIP 시스템 구조

구현된 SIP 시스템의 프로토콜 구조는 그림 5와 같다. 최하위 계층인 sipstack 부분은 표준 프로토콜의 syntax와 encoding 기능을 하는 부분으로 SIP 헤더를 구성하고 파싱하는 부분이다. 이 부분에 구현된 모듈은 SIP URI 모듈과 SIPS URI 모듈로 구성되며, SIP 헤더 및 SIP 메시지를 구현한다.

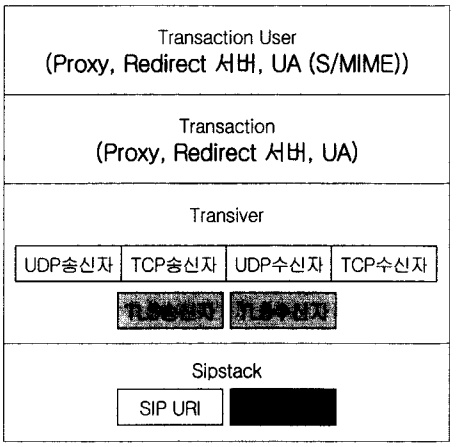


그림 5. 구현된 SIP 프로토콜의 구조

중간 계층인 transceiver 부분은 표준 프로토콜의 전송계층을 설계한 부분으로 목적지를 결정하고, 전송/수신 방법을 결정한다. transceiver 계층에서는 TLS를 지원하기 위한 TLS 송신자모듈과 TLS 수신자모듈을 설계해야 한다. transaction 부분은 표준 프로토콜의 transaction 계층을 구현한 부분으로 transaction, 재전송, time out등을 관리하여 상위계층으로 전달한다. 마지막으로 최상위 계층인 transaction user계층은 논리적인 부분으로 transaction 계층에서 올라온 메시지별 상태를 관리한다. 본 논문에서 고려한 모델은 중간 계층인 transceiver 부분까지는 모든 서버들이 같은 모듈을 사용할 수 있도록 설계하였으며, transaction 계층부터는 각각의 application별 기능을 갖도록 설계하였다. 즉 모든 서버 및 UA는 SIPS 기법과 TLS, 그리고 Digest 인증 기법을 지원하도록 설계하였다.

5.1. 보안 기능이 추가된 sipstack과 transceiver

sipstack과 transceiver의 주요 구성 요소는 그림 6과 같이 database, sending transceiver, receiving transceiver, creating으로 설계한다. 각각의 요소는 메시지 처리시에 다음과 같이 작동한다.

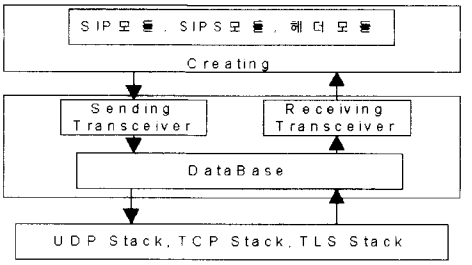


그림 6. sipstack의 구조

UDP, TCP, TLS 스택을 통하여 수신된 메시지를 데이터 베이스에 저장하고 receiving transceiver를 통해 creating 모듈로 전달한다. creating에서는 SIP와 SIPS 그리고, 헤더모듈을 참조하여 메시지를 재구성하여 sending transceiver를 통하여 전송하고 이때 URI가 SIPS이면 TLS 스택을 통하여 응답을 보낸다. 각각의 flow는 그림 7과 그림 8에 보여진다.

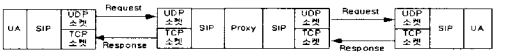


그림 7. 일반 SIP 메시지 처리 절차

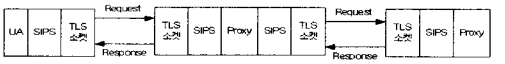


그림 8. TLS 적용 SIP 메시지 처리 절차

5.2 보안 기능이 추가된 Proxy의 구조

Proxy 서버의 transaction을 관리하기 위한 구조는 그림 9와 같다. Proxy 클래스는 Proxy 서버 전체의 상태를 관리하고, Registrar 서버는 REGISTER 메시지를 받아 인증 정보를 통해 사용자 인증을 하고, DataContainer는 operator를 통해 들어오는 각 메시지의 정보를 관리한다.

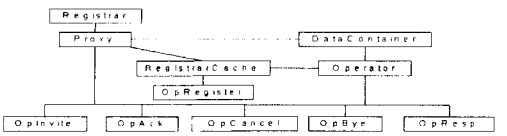


그림 9. Proxy 구조

REGISTRER 메시지의 처리는 OpRegister에서 처리하고, 처리 절차는 미리 Registrar 서버에 등록된 정보를 통해 사용자 인증을 하고 등록되어 있으면 100 Trying을 송신하고, 등록되어 있지 않으면 WWW-Authenticate 헤더를 붙여 401 응답을 보낸다. 401응답을 받은 UA가 다시 Authorization 헤더를 붙여 등록한다. INVITE 메시지의 처리는 OpInvite에서 메시지가 들어올 경우 INVITE 메시지가 SIP URI인지 SIPS URI인지 확인하여 올바른 메시지 일 경우 100 Trying 응답을 보내고, Record-Route 헤더를 붙이고, Via 헤더를 추가하여 전달한다. ACK 메시지의 처리는 OpAck에서 처리하고, 주요 처리 방법은 메시지의 Via를 떼어내고 Record-Route를 보고 전달한다. BYE와 CANCEL 메시지 처리는 각각 OpBye와 OpCancel에서 하는데, Route 헤더를 보고 전달한다.

5.3 보안 기능이 추가된 Redirect 서버의 구조

보안 기능이 추가된 Redirect 서버는 TLS 연결을 통하여 SIPS INVITE 메시지 요청이 있을 경우, CONTACT 리스트를 검사하여 URI가 SIPS인 URI에 우선 순위를 주어 TLS 연결을 보장토록 설계한다.

5.4 보안 기능이 추가된 UA의 구조 및 기능

UA의 구조는 그림 10과 같이 사용자 인터페이스에서 단말의 기능설정, 사용자 이벤트 발생을 처리하여 이벤트 프로세스 큐에 넣어 준다.
이벤트 프로세스 쓰레드에서는 사용자가 요청한 이벤트를 상태를 관리하는 모듈에서 처리 할 수 있도록 큐에 넣어 주는 역할을 하며, 상태 관리 모듈은 SIP request와 response에 따라서 각각의 상태를 유지변경하는 기능, 을 한다. 이러한 UA의 동작은 시그널링 부분을 처리하는 SIP와 미디어 송수신을 처리하는 RTP, SRTP 부분으로 구분된다. SIP 에서는 사용자 이벤트에 따라서 request를 전송하거나, 수신된 request에 대한 response를 만들고 만약 사용자가 S/MIME, TLS을 사용한다고 하면 SIP message의 암호화와 복호화를 수행하게 된다. 여기서 S/MIME은 단말간 보안에 속하게 되므로 실제 단말 측만 필요한 모듈이 된다. 또한 미디어 전송을 위한 모듈인 RTP/SRTP 모듈은 일반적인 경우 RTP

를 이용하여 음성을 송·수신하는 기능을 하며, 사용자가 미디어에 대한 보안을 하겠다고 하는 경우 SRTP를 이용하여 송·수신한다.

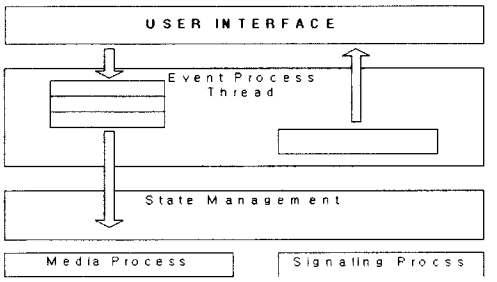


그림 10. 단말기의 설계 및 구조

Ⅲ. SIP 기반의 보안 시스템 구현 결과

본 논문에서는 RFC 3261에서 권고하는 있는 보안 사항과 미디어 보안을 위해서 드래프트 SRTP의 내용을 구현하였으며 결과적으로 SIP 사용자 인증, 메시지의 기밀성 및 무결성 그리고 음성 데이터의 암호화 및 패킷 인증을 구현하였다.

1. 시스템 구현환경

본 논문에서는 VoIP 보안 시스템을 구현하기 위하여 Windows 2000 운영체제로 하는 UA를 구현하였으며 SIP 서버는 Redhat 7.1 운영체제를 사용하였다. 컴파일러는 MS Visual C++ 6.0과 gcc 2.96을 사용하였고 네트워크는 일반적인 IP 네트워크를 이용하였다. SIP 보안 메커니즘을 위한 모듈은 Openssl[9] 프로젝트의 공개 소스를 이용하였는데 리눅스와 윈도우 운영체제를 지원한다.

2. 구현 내용 및 동작 결과

2.1. Digest 사용자 인증

Digest 사용자 인증을 이용하여 REGISTER 메시지뿐만 아니라 INVITE, ACK, BYE 메시지와 같은 call 과정에서 필요한 메시지에도 Digest 사용자 인증을 적용하였다. 그림 11은 UA가 Registrar 서버에 등록을 한 후 실제 call을 하는 모습을 나타낸 그림이다.

```
Protocol  Info
SIP/SDP Request: INVITE sip:1001@203.253.3.125;transport=tcp;user=phone, with ses
SIP     Status: 407 Proxy Authentication Required
TCP     1096 > 5060 [ACK] Seq=1830297402 Ack=2723882445 Win=16165 Len=0
SIP     Request: ACK sip:1001@203.253.3.125;transport=tcp;user=phone
TCP     5060 > 1096 [ACK] Seq=2723882445 Ack=1830297724 Win=10224 Len=0
SIP/SDP Request: INVITE sip:1001@203.253.3.125;transport=tcp;user=phone, with ses
TCP     5060 > 1096 [ACK] Seq=2723882445 Ack=1830298624 Win=13500 Len=0
SIP     Status: 100 Trying
TCP     1096 > 5060 [ACK] Seq=1830298624 Ack=2723882698 Win=17520 Len=0
SIP     Status: 180 Ringing
TCP     1096 > 5060 [ACK] Seq=1830298624 Ack=2723882952 Win=17266 Len=0
SIP/SDP Status: 200 OK, with session description
TCP     1096 > 5060 [ACK] Seq=1830298624 Ack=2723883579 Win=16639 Len=0
SIP     Request: ACK sip:1001@203.253.3.125:5060;maddr=203.253.3.125
TCP     5060 > 1096 [ACK] Seq=2723883579 Ack=1830299309 Win=15300 Len=0
SIP     Request: BYE sip:1001@203.253.3.125:5060;maddr=203.253.3.125
TCP     5060 > 1096 [ACK] Seq=2723883579 Ack=1830299733 Win=17100 Len=0
SIP     Status: 407 Proxy Authentication Required
TCP     1096 > 5060 [ACK] Seq=1830299733 Ack=2723884001 Win=16217 Len=0
SIP     Request: BYE sip:1001@203.253.3.125:5060;maddr=203.253.3.125
TCP     5060 > 1096 [ACK] Seq=2723884001 Ack=1830300420 Win=18900 Len=0
SIP     Status: 200 OK
```

그림 11. SIP Request 메시지에 적용된 Digest 사용자 인증

위 그림에서는 INVITE, BYE 메시지에 대해서 Proxy 서버는 407 Proxy Authentication Required 메시지를 보냄으로써 사용자 인증을 요청한다. 이에 대해 UA는 인증 정보를 생성해 메시지를 재전송하는 것을 볼 수가 있다. 그러나 200 OK에 대한 ACK 메시지에 대해서는 UA에서 인증 정보를 포함하여 보내기 때문에 Proxy 서버에서는 407 Response를 보내지 않는다.

2.2. Hop-by-Hop 보안

Hop-by-Hop 보안을 위해서 본 논문은 TLS 보안 메커니즘을 적용하여 SIP 메시지의 기밀성 및 무결성을 제공하고 서버의 인증서를 통해서 서버에 대해 인증하는 서버 인증 모드를 구현하였다. TLS 보안 메커니즘은 서버와 UA 모두에서 사용자의 설정에 따라 동작이 가능하고 사용 알고리즘은 TLS_RSA_WITH_ AES_128_CBC_SHA와 TLS_RSA_WITH_3DES_EDE_CBC_SHA을 서버에서 사용자 설정에 의해 선택할 수 있도록 하였다. 인증서는 가상 CA를 구성하여 생성 배포된 사설 인증서를 사용하였다. 그림 12는 TLS를 통해서 SIP 메시지들에 대해 보안 서비스가 제공된 그림이다.
각 SIP 메시지들은 실제 네트워크 상에서 Application Data로 나타나고 패킷의 내용은 그림 아래 부분과 같이 SIP 메시지가 암호화되어 알아볼 수가 없다. 각 TLS Application Data 옆에는 실제 어떤 SIP 메시지인지 표기를 하였다.

2.3. End-to-End 보안

UA 단말간 보안을 위해 S/MIME을 적용하여 단말간 SIP 메시지에 대해 기밀성, 무결성 및 인증서를 통한 사용자간에 인증을 제공하였다. S/MIME은 RFC 3261에서 언급한 SDP 암호화, SIP 메시지 서명, SIP 메시지 암호 및 서명에 대해서 각각 사용

자 설정에 의해 적용되도록 구현하였으며 메시지 암호 알고리즘은 RC2, 3DES를 적용하였다. 인증서는 가상 CA로부터 각 사용자는 인증서를 받아 사용자는 상대방의 인증서에 대해서 검증을 할 수 있도록 하였다. 그림 13은 S/MIME 모드 중 SIP 메시지 암호 및 서명 모드가 적용된 모습을 나타낸다.

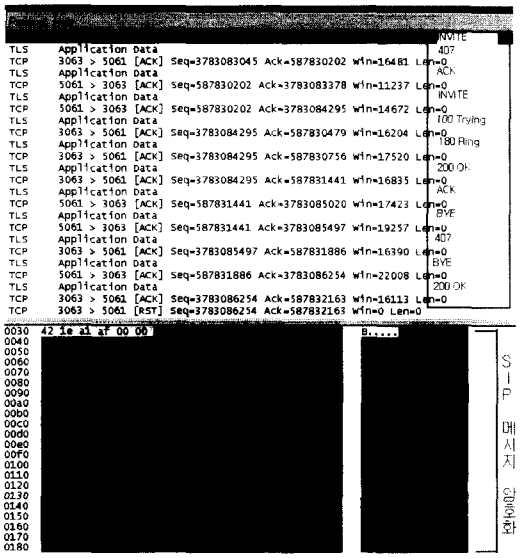


그림 12. TLS가 적용된 SIP 메시지

위 그림에서 INVITE 메시지의 From 헤더의 사용자 ID는 "anonymous"로 표기되어 있으며 Contact 헤더에는 사용자 ID의 내용이 없어 ID Privacy를 제공하며 SIP 메시지에 대해서 서명이 적용되었다. S/MIME이 적용되면 그 길이가 5~6배 증가하여 위와 같이 패킷이 나뉘어 전송되는 것을 볼 수 있다.

2.4. 미디어 보안

음성 통화 보안을 위해서 SRTP를 적용하여 RTP Payload 암·복호화는 AES SIC 모드로 구현하였고 RTP 패킷 인증은 HMAC-SHA1을 사용하였다. 키 분배에 관해서는 두 사용자가 공유한 키를 이용하여 세션키를 생성하는 방법을 취하였다. 도청 프로그램을 이용하여 SRTP를 적용할 때와 적용하지 않았을 때 보안이 적용되었는지 확인 할 수 있었다.

3. SIP 보안 안전성 분석

본 절에서는 구현한 SIP 보안 시스템을 바탕으로

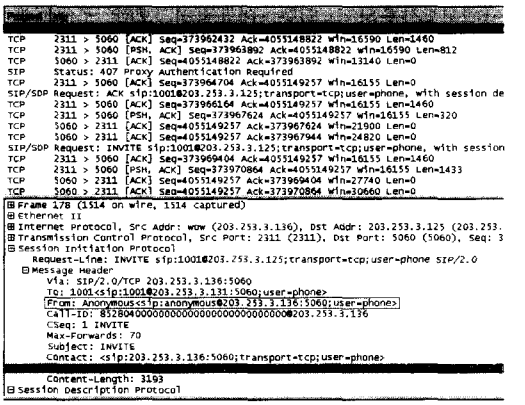


그림 13. SIP 메시지 암호 및 서명 모드가 적용된 SIP 메시지

RFC 3261에서 제시하고 있는 SIP 보안에 대해서 논의하려고 한다.

3.1. Digest 사용자 인증

Digest 사용자 인증은 사용자의 ID, password와 SIP 서버로부터 받은 랜덤 정보로 MD5 Digest 알고리즘을 통해 인증 정보를 생성해 SIP 서버로부터 사용자 인증을 받는 메커니즘이다. 이 방법은 기존의 Basic 인증 방법보다는 password를 평문으로 보내지 않기 때문에 보다 안전하고 qop=auth 값을 통해서 UA에서 인증 정보 생성시 cnonce를 사용함으로써 chosen plaintext 공격법으로부터 보호할 수 있다. 또한 SIP REGISTER 메시지에만 국한되어 사용자 인증이 제공되는 것이 아니라 INVITE, ACK, BYE 메시지에도 사용자 인증이 제공되기 때문에 SIP call 과정시에도 정당한 사용자에게만 call을 연결할 수 있도록 기존의 HTTP Digest 사용자 인증을 확장하여 적용하였다. 그러나 Digest 사용자 인증 방법은 메시지에 대해서 무결성을 제공하지 않기 때문에 메시지 변조 공격과 공격자가 무작위로 password를 입력하여 나온 response를 가지고 password를 알아내는 dictionary 공격에 대해 취약점을 갖고 있다.

3.2. TLS 적용을 통한 Hop-by-Hop 보안

TLS는 SIP 단말들간에 Hop-by-Hop 구간에 적용되는 보안 메커니즘으로 SIP 메시지 전송시 TLS 보안 채널을 형성해 SIP 메시지에 대해서 기밀성 및 무결성을 제공한다. TLS 보안 프로토콜의 안전성에 대해 현재까지 특별한 문제가 없으며 여러 분

야에서 사용되고 있는 대표적인 보안 프로토콜로 은행 뱅킹 시스템이 그 좋은 예라 할 수 있다. SIP 메시지는 중간에 여러 노드를 거쳐서 메시지가 전달되므로 홉간 보안을 위해 TLS가 적용되어 SIP 메시지가 전달될 때에는 각 노드마다 SIP 메시지를 복호화해야 하는 과정이 필수적이므로 공격자에게 공격의 위험성이 있다.

3.3 S/MIME 적용을 통한 End-to-End 보안

S/MIME은 SIP UA 단말간 보안 메커니즘으로 End-to-End 간에 SIP 메시지에 대해서 기밀성, 무결성 그리고 인증서를 통한 사용자 인증을 제공한다. S/MIME 보안 프로토콜 또한 그 안전성에 대해서는 아직까지는 큰 문제가 없는 보안 프로토콜로 여러 분야에서 사용되고 있다. 그리고 S/MIME을 SIP 보안 시스템에 적용함에 있어 RFC 3261에서는 라우팅 헤더에 관한 문제 때문에 메시지 형태를 Outer 메시지와 Inner 메시지로 구분하여 암호 및 서명을 적용하는데 이 부분에서 취약점이 있을 수 있다. 만약에 UAS와 Proxy 서버 사이에 TLS 또는 IPsec이 적용되지 않는다면 S/MIME에서는 라우팅 헤더에 대해서는 메시지 변조 유무를 확인 할 수가 없어 변조된 Record-Route, Via를 이용해 SIP 메시지를 멀리 우회시킨다거나 악의적인 라우터로 보낼 수 있다.

3.4. SRTP 적용을 통한 미디어 보안

미디어 보안으로 현재 드래프트 상태인 SRTP를 사용하여 RTP Payload 암·복호화 및 RTP 패킷 인증과 같은 보안 통화 서비스를 제공한다. 각 알고리즘으로 AES, HMAC-SHA1은 현재 그 안전성에 있어서 다른 알고리즘보다 그 우수성을 인정받고 있는 알고리즘들이기 때문에 보안상 취약점을 발견하기 힘들다. 그러나 현재 드래프트 상태이기 때문에 SRTP에 대한 안전성 분석과 키 분배에 관한 MiKey에 대해서 표준화 작업이 우선적으로 이루어져야 한다.

위와 같이 SIP 기반의 VoIP 보안 시스템에서 시그널링 보안을 위해 여러 가지 보안 메커니즘이 적용되었는데 그 이유는 SIP를 위한 보안 메커니즘이 설계되어 사용된 것이 아니라 기존에 사용되는 보안 프로토콜을 적용하기 때문에 그 어느 하나의 보안 메커니즘으로는 SIP 메시지에 대해서 완벽한 보안 서비스를 제공할 수 없기 때문이다. 여러 보안 메커니즘을 사용하여 안전성을 최대화하기 위한 것이다. 그렇기 때문에 Digest 사용자 인증, SIP 서버간에 TLS 적용에 대해서만 "must"로 구현할 것을 규정해 놓은 RFC 3261을 통해 모든 보안 메커니즘에 대해서 "must"로 규정을 해야만 최상의 보안 서비스를 제공받을 수 있을 것이다. 그러나 이는 단말 등에 추가적인 부하를 생성하므로 통신 환경에 따라 적용 여부가 결정되어야 한다. 또한 앞서 분석한 각 보안 메커니즘을 SIP에 적용하면서 발생할 수 있는 취약점에 대해서도 보다 많은 연구가 수행되어야 할 것이다.

Ⅳ. 결 론

수 차례 걸쳐 지난 2002년 6월 RFC 3261로 표준화 작업이 마무리되어 VoIP의 핵심 시그널링 프로토콜로 사용되는 SIP는 기존의 보안 프로토콜을 사용하여 시그널링을 보호하고 있다. RFC 3261에서는 사용자 인증을 위해 HTTP Digest 메커니즘을 사용하고, SIP 메시지의 기밀성, 무결성을 제공하기 위해 홉간은 TLS를 단말간은 S/MIME을 규정하여 메시지 변조 등에 대해서 보호하고 있다.

본 논문에서는 RFC 3261에서 제안하는 보안 메커니즘을 통해 SIP 메시지 보안과 드래프트인 SRTP를 사용해 미디어 보안을 구현함으로서 앞으로 인터넷상에서의 음성과 화상 연결을 위한 주요 프로토콜로서의 역할을 수행하는 것과 동시에 인터넷상에서 안전한 음성, 화상 통신 환경을 구축하는데 크게 기여할 것이다. 또한 아직 국내에서 개발되지 않은 SIP 기반의 VoIP 보안 시스템 기술 발전에 일조할 것으로 기대된다.

참 고 문 헌

[1] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg "SIP : Session Initiation Protocol," RFC 3261, IETF, JUN 2002.

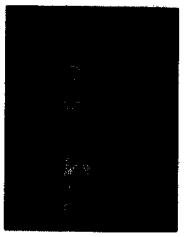
[2] Franks, J, DORNER: "HTTP authentication: Basic and Digest Access Authentication," RFC 2617, IETF, JUNE 1999.

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

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

[5] Baugher, McGrew, Oran, Blom, Carrara, Naslund, Norrman, "The Secure Real-time Transport Protocol," IETF, Internet Draft, December 2002.
[6] Jobn Viega, Matt Messier & Pravir Cbandra, "Network Security with OpenSSL," O'REILLY, 2002.
[7] Chown. p, "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, IETF, JUNE 2002.
[8] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman, "MIKEY : Multimedia Internet Keying," IETF, Internet Draft, September 2002.
[9] Openssl Project, http://www.openssl. org

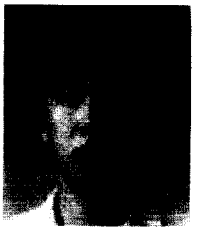
최 재 덕 (Jaedeok Choi) 정회원



2002년 2월: 숭실대학교 정보통신공학과 학사
2004년 2월: 숭실대학교 정보통신공학과 석사
2004년~현재: (주)Addpac Technology

<관심분야> SIP Security, 네트워크 인증, 인증 프로토콜

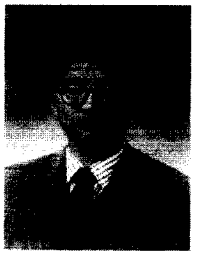
정 태 운 (STaewoon Jung) 정회원



1998년 2월 : 숭실대학교 전기공학과 학사
2000년~2001년 : 동국제강 전기제어팀
2003년 8월 : 숭실대학교 정보통신전자공학부 석사
2003년~현재 : 경봉기술(주)

<관심분야> SIP, 멀티캐스트, Autonomous Decentralized Traffic Management System

정 수 환(Souhwan Jung) 정회원



1985년 2월: 서울대학교 전자공학과 졸업
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임연구원
1996년: 미 워싱턴 주립대 (시애틀) 박사
1997년~현재: 숭실대학교 정보통신전자공학부 부교수

<관심분야> VoIP security, Security Protocol, 사용자 인증, Cryptography

김 영 한 (Younghan Kim) 정회원

1984년 2월 : 서울대학교 전자공학과 졸업
1986년 2월 : KAIST 전기전자공학과 석사
1990년 8월 : KAIST 전기전자공학과 박사
1987년~1994년 : 디지콤 정보통신 연구소 연구부장
1994년 9월~현재 : 숭실대학교 정보통신전자공학부 부교수

<관심분야> 인터넷 네트워킹 (IPv6, QoS, TCP congestion control, multicasting)