SIP 기반 UC서비스의 보안시스템 설계

윤지상*, 박석천**, 박준식***
*가천대학교 일반대학원 모바일소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)
***인성정보 개발서비스팀장
e-mail : yjs8237@naver.com

Design of Security System of UC Service based on SIP

Ji-Sang Yun*, Seok-Cheon Park**, Jun-Sik Park***
*Dept of Mobile Software, Gachon University
**Dept of Computer Engineering, Gachon University
***Dept of Development Service, In-sung Information co., ltd

요 약

통신기술의 발전으로 사람과 사람의 의사소통에 있어서 IT 기술을 접목시킨 여러 기술들이 발전하고 있다. SIP 기반의 UC 서비스 또한 기업과 고객의 원활한 커뮤니케이션을 위하여 기술이 꾸준히 발전하고 있다. 그러나 UC 서비스 또한 IP 기반의 서비스이기 때문에 여러 가지 보안위협의 노출이 되어 있다. SIP 기반의 서비스는 QoS(Quality of Servic)가 보장되어야 하지만 품질에 중점을 두어 보안위협에 크게 노출 되어 있는 것이 사실이다. 이에 본 논문에서는 SIP 보안 메커니즘인 HTTP Digest 사용자 인증, TLS 홉간 보안, S/MIME을 이용한 단말간의 보안 메커니즘을 적용하고 Virtual Proxy Server 를 이용한 보안 시스템을 설계 하였다.

Ⅰ. 서 론

IT기술의 핵심이라고 할 수 있는 통신기술이 엄청나게 발전하고 있다. 특히 최근에 스마트폰의 도입으로 인해 통신기술의 경쟁력은 이루 말할 수 없이 발전했다고 볼 수 있다. 사용자들이 가장 추구하는 서비스 중에 하나가 바로 편리함 이다. 편리한 IT 서비스를 위해서 무선 네트워크, 블루투스, 센서네트워크, 클라우드 서비스들의 기술발전이 꾸준히 이루어지고 있는 와중에 UC(Unified Communication) 서비스 또한 꾸준한 기술발전이 이루어지고 있다. UC 서비스는 비즈니스 사용자를 위한 서비스라고 할 수 있다. 비즈니스 로직에 맞춘 기술들을 하나의 솔루션으로 통합하고 그 솔루션을 동시에 여러 사람에게 서비스한다. 하지만, 여러 기술이 하나의 솔루션으로 합쳐져 서비스가 이루어지고 있기 때문에 그에 따른 보안측면에서의 단점이 발견되고 있다. 가장 대표적으로 음성보안의 문제가 이슈화 되고 있다. UC서비스에서 사용되는 음성기술은 SIP(Session Initiation Protocol)를 사용하기 때문에 기존 IP기반 보안위협에 그대로 노출되어 있다[1].

SIP 프로토콜 보안 위협의 종류로는 음성패킷을 불법으로 수집·조합해 통화 내용을 재생하는 도청(sniffing) 위협, 비정상 패킷의 다량 발송을 통한 회선 마비 등의 서비스거부(DoS) 공격, 사용자의 등록정보를 조작하거나 추가해 비인가 된 서비스를 이용하는 서비스 오용공격, 호 설정 과정이나 사용자 등록 과정에 개입해 사용자의 세션 제어권한 등을 획득하는 세션 가로채기, 인터넷회선을 공유해 녹음기 등을 통해 발송하는 VoIP(Voice over Internet Protocol) 스팸 등의 SIP 보안위협이 존재한다.

UC 서비스는 비즈니스 로직의 성격이 강하기 때문에 비즈니스업무에 상당히 중요한 부분으로 자리매김하고 있는 보안문제에 있어서 위의 보안위협들은 반드시 대응책을 마련하고 보안위협으로부터 데이터를 보호 할 수 있어야 한다.

따라서, 본 논문에서는 UC 서비스의 보안위협중 SIP 보안 대책 마련을 위하여 Virtual Proxy Server와 SIP 보안 메커니즘을 이용한 보안시스템 설계 방법을 제안한다.

Ⅱ. 관 련 연 구

2.1 UC 기술 개요

UC란 여러가지 통신 기술을 하나로 통합한 시스템이라고 할 수 있다. UC서비스 에는 현재 E-mail, 전화, 컨퍼런싱, 인스턴트 메시지 등 정보전달의 어플리케이션 기술 통합에서 ERP (Enterprise Resource Planning)와 같은 기업 비즈니스 어플리케이션까지 IP기반의 시스템으로 구성되어 있다. UC서비스의 간단한 예로, 외부로부터 받은 업무나 기술요청, 서비스요청 업무를 내부 직원 혹은 외근

자에게 업무를 전달하기 위해서 UC서비스가 사용되고 있다[2].

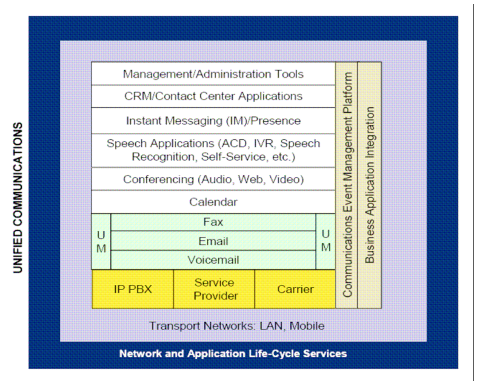
통합 커뮤니케이션의 주요기능은 다음 표1과 같다.

<표 1> UC 주요기능

	기 능	설 명
	VoIP	SIP 기반의 Call 서비스
	메신저	메신저를 통한 Instance Messaging, Click to Call 서비스
	컨퍼런싱	영상회의, 다자간통화 서비스
	E-mail	E-mail 서비스

UC 시스템을 구축하기 위해서는 IP-PBX와 같은 하드웨어와 각 솔루션에 맞게 구성 된 어플리케이션 소프트웨어가 필요하다. 그리고 각 해당 기업의 비즈니스 로직에 맞춘 기업 솔루션의 성격이 강하다 보니 해당 기업의 맞는 비즈니스 프로세스에 따라 시스템의 구조와 어플리케이션이 달라지는 특성이 있다.

다음 그림1은 “한국 인터넷 데이터 센터” (IDC :Internet Data Center) 에서 정의하고 있는 통합커뮤니케이션 플랫폼이다[6].



(그림 1) 통합 커뮤니케이션 구조

2.2 SIP 보안 위협 분석

SIP(Session Initiation Protocol) 는 IP 기반의 프로토콜이기 때문에 보안위협으로부터 노출되어 있다. SIP(Session Initiation Protocol) 보안위협요소 중 통합커뮤니케이션 서비스에 가장 큰 영향을 미치는 위협요소는 다음과 같다.

- 도청 (Sniffing) 위협
  사용자의 통화 내용을 공격자가 청취할 수 있다.
- 서비스거부 (DoS) 공격
  SIP 서비스 관련 시스템 또는 단말을 공격하여 정상적인 SIP 서비스를 받지 못하게 한다.
- 서비스 오용공격
  SIP 서비스를 공격자가 세션가로채기 등의 공격방법으로 서비스를 오용하는 방법이다.
- 세션 가로채기
  SIP 호 설정 과정에서 공격자가 개입을 하여 도청 또는 서비스를 오용하는 방법으로 1차적인 공격의 위험과 2차적인 공격의 위험이 같이 공존한다.

위와 같은 보안위협요소들은 비즈니스 통합커뮤니케이션 서비스를 이용함에 있어 보안적인 측면에서 가장 위험하고 중요한 요소들이다.

2.3 보안 프로토콜 개요

본 논문에서 제안하는 보안시스템의 보안프로토콜은 사용자 인증을 위한 HTTP Digest 인증 프로토콜, 홉간 보안을 위한 TLS(Transport Layer Security) 프로토콜, 단말간의 End-to-End 보안을 위한 S/MIME(Secure/Multipurpose Internet Mail Extensions) 프로토콜을 이용한다. 또한, 보안프로토콜을 이용하여 UC 시스템 에서 효율적으로 보안시스템을 설계하기 위한 Virtual Proxy 시스템을 이용한다.

III. 보안 시스템 설계

3.1 UC 서비스 보안 시스템 구성

SIP 보안을 위한 새로운 메커니즘을 정의하지않고 기존에 SIP 보안으로 사용하고 있는 보안 메커니즘을 모델로 제시하였다. 또한 Virtual Proxy Server 로 UA-to-Proxy, Proxy-to-UA 간의 인증을 한번 더 거치게 되는 모델이다.

Public 망에서 들어오는 패킷에 대한 보안도 유지할 수 있으며 기업 사설망의 Proxy 서버의 부하를 줄이기 위해 Virtual Proxy Server 에서 일련의 인증과정이 순차적으로 진행된다.

UC시스템의 경우 모바일을 통한 시스템 접근이 있기 때문에 송신단말 사용자와 Proxy 서버간의 인증만 이루어지지 않고, 수신단말 사용자와 Proxy 서버간의 인증도 이루어진다.

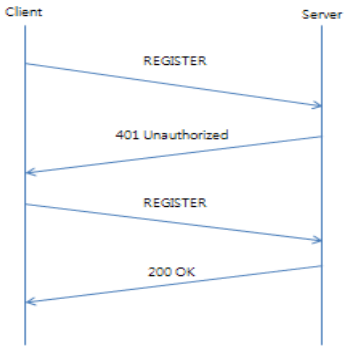
(그림 2) UC 서비스 시스템 구성도

위 그림 2 에서는 UC 서비스의 전체 시스템 구성을 간략적으로 표현한 그림이다.

3.2 UC 서비스 보안 시스템 기능 분석

- HTTP Digest 사용자 인증

  HTTP Digest 사용자 인증 방법은 그림 3과 같이 최초의 사용자가 서버에게 Request 메시지를 보내면 서버에서는 challenge 메시지에 nonce 와 같은 랜덤 정보와 realm 정보를 보내주게 되고, 이 정보를 받은 사용자(UAC)에서는 서버로부터 받은 정보와 자신의 Password, ID 값을 이용하여 해쉬함수를 통해 생성된 인증정보를 서버에게 보내게 된다. 서버는 사용자(UAC) 에게 받은 정보를 가지고 해쉬함수를 통해 생성된 값을 비교하여 값이 같으면 인증을 하게 된다[3].



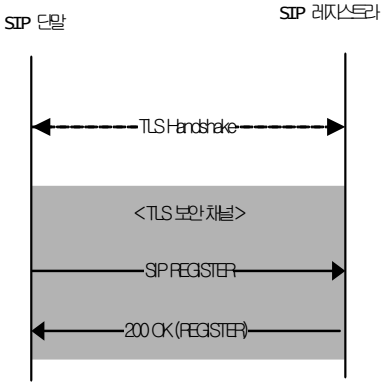
(그림 3) HTTP Digest 인증 절차

- TLS 보안

  RFC 3261에서는 TLS 의 구현을 SIP 서버에서 반드시 구현해야 한다고 규정하고 있고 UA 에서는 옵션으로 적극 권장하고 있다. UA-to-Register , UA-to-Proxy, Proxy-to-Proxy 등 홉간의 보안 메커니즘으로는 TLS와 IPSec등이 사용된다.

  TLS는 SIP 메시지에 대한 암/복호화를 통해 홉간(Hop-by-Hop) 신뢰구간을 형성하며, SIP 메시지에 대한 기밀성과 무결성을 제공한다.

  TLS는 TLS 레코드 프로토콜과 TLS 핸드셰이크 프로토콜의 두 개의 계층으로 구성된다. TLS 레코드 프로토콜은 DES(Data Encryption Standard)와 같은 일부 암호화방식을 이용하여 접속 보안을 제공한다. TLS 레코드 프로토콜은 또한 암호화 없이도 사용될 수 있다. TLS 핸드셰이크 프로토콜은 데이터가 교환되기 이전에 서버와 클라이언트가 서로를 인증하고, 암호화 알고리즘 및 암호 키를 결정하게 해준다[4][5].



(그림 4) TLS 보안 시나리오

그림 4와 같이 홉간의 TLS Handshake가 이루어지고 나서 TLS 보안채널이 형성된다. 보안채널이 형성되고 나면 정상적인 SIP 메시지를 전송할 수 있다[5].

- S/MIME 보안

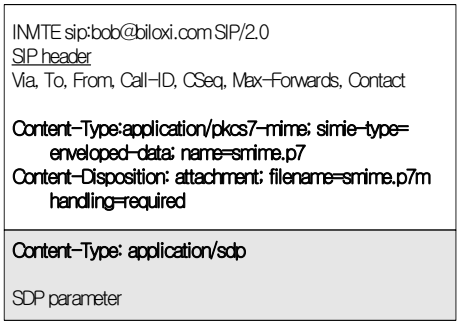
  RFC3261 에서는 UA에서 S/MIME을 옵션으로 규정하고 있다. S/MIME 은 단말과 단말간의 메시지에 대한 기밀성과 무결성을 지원하며, 인증서를 통한 인증도 제공한다.

  S/MIME에서 인증서는 사용자 인증, SIP 메시지의 서명에 사용되는 키(Key) 정보와 SIP 메시지 암호화에 사용되는 대칭키를 암호화하는 키 정보를 갖고 있다.

  인증서는 공인 인증 기관을 통해서 획득하여야 한다. 그러나 공개키 기반 구조 환경이 구축되어 있지 않을 경우에는 사용자 자신이 사설 인증서를 만들어 사용할 수 있다.

  사용자 인증은 인증서와 SIP 메시지의 필드가 같은지를 비교하여 이루어진다. SIP 메시지를 암호화하기 위해서는 상대방 인증서를 알고 있어야 한다. 상대방의 인증서에는 SIP 메시지를 암호화하는 대칭키 보호에 사용될 공개키가 포함되어 있다[3][5].

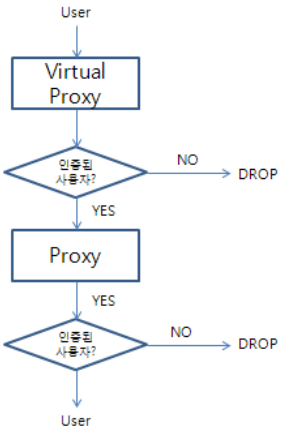
SIP 메시지안에 있는 SDP 메시지에 대해서 암호화를 적용할 수 있으며 SDP 암호화를 적용한 S/MIME 형태는 그림 5와 같다[5].



(그림 5) SDP 암호화를 위한 S/MIME

3.3 UC 서비스 보안 시스템 인증 절차 설계

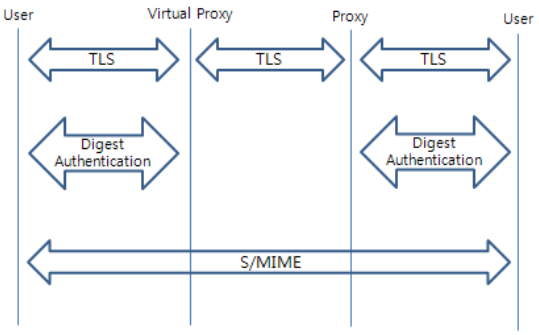
UC 서비스 보안시스템을 구성하는 인증 절차는 사용자와 서버간의 인증보안, 홉간의 보안채널 형성, 송신단말과 수신단말의 보안적용을 바탕으로 구성된다. 이밖에 E-mail, 영상 컨퍼런싱, 메신저를 통한 Instance Messaging 또한 위와 같은 보안 프로토콜을 적용한 시스템으로 구성한다.



(그림 6) UC 서비스 보안 시스템 인증 절차

사용자가 Proxy Server를 통한 UC 서비스 보안 시스템 인증 절차를 그림 6과 같이 설계 하였다. Virtual Proxy Server를 통한 인증으로 WAN, PSTN, 모바일 망을 통해 접속을 시도하는 사용자에 대해 최초 인증을 시도하고, 인증이 이루어진 사용자에 대한 인증은 내부 Proxy Server를 통해 재인증이 이루어진다. 재인증을 통해 기업 관계자와 일반 사용자를 구분하고 인증 보안 신뢰성을 높일 수 있다.

시스템상의 모든 Proxy Server 는 Virtual Proxy Server를 통해 모든 통신이 이루어지고 Virtual Proxy Server에서는 SIP 세션관리 , 인증 관리, 패킷 제어 관리등 UC 서비스의 보안관련 기능을 제어하게 된다.



(그림 7) 보안시스템 프로토콜 구성

그림 7 은 UC 서비스 보안프로토콜의 전체 구성을 나타낸다. 홉간의 보안은 TLS 프로토콜을 사용하고, 사용자와 서버간에 인증은 HTTP Digest 인증을 사용한다. 사용자와 사용자의 End-to-End 보안은 S/MIME 프로토콜을 사용하여 보안시스템을 설계한다. Virtual Proxy Server 를 통하여 기존 SIP 모델에서 고려되지 않는 네트워크 패킷의 정보를 통한 사용자 인증, 혹은 모바일연동 관련 패킷에 대한 사용자 인증이 더욱 더 신뢰성 있게 이루어진다 [7].

Ⅳ. 결 론

현재 UC 시장이 급격히 증가하고 있다. 이러한 현재 상황에서 UC 기술들은 보안적인 측면보다는 편의성만 추구하는 기술에만 치우쳐있다. 특히 UC 서비스는 기업의 비즈니스 측면의 솔루션 성격이 강하기 때문에 일반 사용자들이 사용하는 솔루션보다 보안적인 부분이 더욱 강화 될 필요가 있다.

본 논문에서는 SIP기반의 UC 서비스의 보안 요소를 고려한 시스템을 제안하였다. UC 서비스 또한 SIP 기반 서비스를 바탕으로 한 솔루션이기 때문에 SIP보안 메커니즘에 중점을 두었다. 기존의 SIP 보안 메커니즘에 Virtual Proxy Server 시스템을 추가 함으로써 인증 관련 부분을 한층 더 강화 할 수 있고, UC 시스템에 있어서 가장 중요한 인증, 데이터보안을 더욱 더 효과적으로 유지할 수 있도록 하였다. 향후 연구로는 SIP 보안 메커니즘을 제외한 다른 기술부분에 보안 메커니즘에 대해 연구를 진행 할 계획이다.

참고문헌

[1] 김태수, 이형우 “VoIP 서비스 보안을 위한 Virtual SIP Proxy 시스템” , 2009

[2] 서정민, 김종락, 김수현, 송영호, 정준환, 정구민 “IP텔레포니 기반의 통합 커뮤니케이션 개발” , 2009

[3] 최재덕, 정태운, 정수환, 김영한 “SIP 기반의 VoIP 보안 시스템 구현” , 2003

[4] 윤석웅, 정현철, 차설매, 추경호, 박한, 백재종, 송주석, 유형선 “모바일 환경에서 적용 가능한 SIP기반 인터넷전화(VoIP)보안 통신 프로토콜 성능 평가” , 2011

[5] TTA “SIP 보안 정보통신단체표준” , 2004

[6] 김영욱 “Unified Communications 2008 ~ 2011 Forecast and Analysis IDC Korea” , 2008

[7] 장유정, 정수환, 문형권, 최재덕, 원유재, 조영덕 “SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법” , 2007

[8] 이형우 “SIP 프로토콜 상태정보 기반 공격 탐지 기능을 제공하는 가상 프록시 서버 설계 및 구현” , 2008