VPN기반의 안전한 VoIP 시스템 설계 및 구현

방제완*, 박정용**, 권지웅***, 이상진*, 류대현**
*고려대학교 정보경영공학전문대학원
**한세대학교 컴퓨터공학과
***(주)XNsystems
e-mail:jwbang@korea.ac.kr

Design and Implementation of Secure VoIP based on VPN

Je-wan Bang*, Jung-yong Park**, Kwon JiWoong***,
Lee, Sangjin*, Dae-Hyun Ryu**
*Graduate School of Information Management and Security,
Korea University
**Dept of IT, Hansei University
***XNsystems

요 약

VoIP 서비스는 인터넷을 기반으로 하므로 인터넷망에서 발생하는 보안 위험이 내재해 있고, 서비스가 실시간으로 이루어진다는 특성으로 인해 기존의 보안 솔루션으로 이러한 보안 위험을 해소하기는 어렵다. 따라서 VoIP 망 구축 초기단계부터 정보보호를 고려하여 보안대책을 세우고 이를 반영하는 것이 비용과 보안 효과 측면에서 바람직하다. 본 논문에서는 상용 VPN 제품에 공개 프로젝트인 SIP VoIP Gateway 'Asterisk'을 연동하여 사용자 인증과 데이터 기밀성을 효과적으로 수행하기 위한 VoVPN(Voice over Virtual Private Network)을 설계하고 구현하였다.

1. 서론

VoIP 서비스는 인터넷을 기반으로 하므로 인터넷망에서 발생하는 보안 위험이 내재해 있고, 서비스가 실시간으로 이루어진다는 특성으로 인해 기존의 보안 솔루션으로 이러한 보안 위험을 해소하기는 어렵다. 인터넷 전화 서비스는 패킷 형태로 인터넷에 노출되므로 기존 전화 서비스보다 보안이 취약하고 공격 가능성이 높다. 또한 시스템 정보와 IP 주소가 쉽게 노출될 수 있는 가입자단의 IP 전화기 프로토콜 취약점이 다수 보고되고 있는 등 기존에 알려진 VoIP 관련 보안 취약성이 다수 존재한다[1]. 국내 VoIP 서비스 업체에서는 VoIP 관련 게이트웨이의 해킹으로 인한 불법적인 국제전화 피해사례가 보고되는 등 점차 보안위협이 증대되고 있다.

이에 한국정보보호진흥원에서 2005년 12월 VoIP 정보보호 가이드를 발간하였으며 정보통신부는 2007년 1월3일 한국정보보호진흥원과 한국정보사회진흥원, VoIP 제공사업자, 정보보호사업자 및 학계 등의 전문가와 공동으로 'VoIP 정보보호 추진대책'을 마련하여 발표하였다[1]. 미국의 경우 미국상무국산하 표준기술연구소인 NIST에서 2005년 2월 VoIP 기술 도입에 신중할 것을 경고하였으며, 2005년 5월과 7월 시스코는 IP전화기의 DNS 쿼리 문제와 콜매니저 소프트웨어에 결함이 있음을 밝힌 바 있다.

본 논문에서는 상용 VPN 제품에 공개 프로젝트인 SIP VoIP Gateway 'Asterisk[6]'를 연동하여 사용자 인증과 데이터 기밀성을 효과적으로 보장하는 VoVPN(Voice over Virtual Private Network) 게이트웨이를 설계하고 구현하였다. VoVPN은 VPN의 암호화 통신에 음성 데이터스트림을 통합하여 추가 비용을 절감할 수 있을 뿐 아니라 향상된 보안 수준을 얻을 수 있다. 본 연구에서는 VoIP와 VPN을 통합함으로 완벽한 보안성을 구현하고자 하였으며 IPSec과 SIP/H.323 표준에 따라 다른 VoIP, VPN기기와 연동되도록 하였다. 또한 VPN 게이트웨이에서 SIP/H.323 이나 NAT 변환 기능 및 대역폭 할당 기능 등을 구현하여 보안성을 충족하면서 QoS가 보장되도록 하였다.

2. 관련 기술

2.1 VPN 기술의 개요

인터넷망은 누구나 쉽게 접속할 수 있고 무한한 확장성을 갖고 있지만, 개인 혹은 기업의 정보가 손쉽게 노출되기 쉬운 환경을 제공한다는 단점도 갖고 있다. VPN은 인터넷과 같은 공중망상에서 사설망을 구축하는 것이므로, 데이터의 보안이 무엇보다도 중요하다. 이를 위해서는 암호화, 사용자 인증 및 액세스 제한과 터널링 기술 등의 기능이 요구된다. 터널링은 VPN을 구현하기 위한 핵심기술이며 라우팅 정보를 포함하는 추가헤더정보로 프레임을 캡슐화하여 전송하면, 캡슐화된 프레임은 추가헤더 정보내의 라우팅 정보를 기반으로 공중망을 경유하여 터널 엔드 포인트로 전송되며, 망의 목적지에 도달한 프레임은 디캡슐되어 최종

목적지로 전송되는 과정을 포함한다.

현재 널리 사용되고 있는 터널링 프로토콜로는 PPTP, L2TP, IPsec 등을 들 수 있다. IPsec은 IP 패킷을 보호하기 위해 보안 방식으로 개발한 인터넷 표준 규약으로서, 최근 발표되고 있는 거의 모든 VPN 제품들은 모두 IPsec을 준수하고 있거나 준수하는 제품을 발표할 예정에 있다.

VPN에서는 데이터가 인터넷이나 ISP의 기간망 등의 공중망을 이용하여 전송되기 때문에 암호화는 중요한 요소기술이다. 인터넷에서 터널링 만으로 패킷의 보안이 완벽하게 이루어질 수 없고 반드시 암호화 알고리즘이 병행적으로 구성하여야 한다. 암호화와 터널링을 동시에 강조하는 이유는, 암호화 기능은 패킷을 암호화하여 외부에 노출되지 않게 하며, 터널링은 패킷을 캡슐화 하여 그 전송경로를 보이지 않게 하여, 각각의 다른 보안 특징을 가지기 때문이다. 터널링 기법을 사용하면, 주소와 라우팅 체계를 외부에 숨길 수 있으며, 이는 하나의 VPN 군 (VPN Community)에서 사용하는 주소와 라우팅 체계가 공중망 또는 다른 VPN 군이 사용하는 것이 가능함을 의미한다. 대부분의 VPN 장비들은 비슷한 수준의 암호화 기능을 제공하고 있으며, DES 와 3DES가 많이 사용되고 있는 암호 알고리즘이다[2].

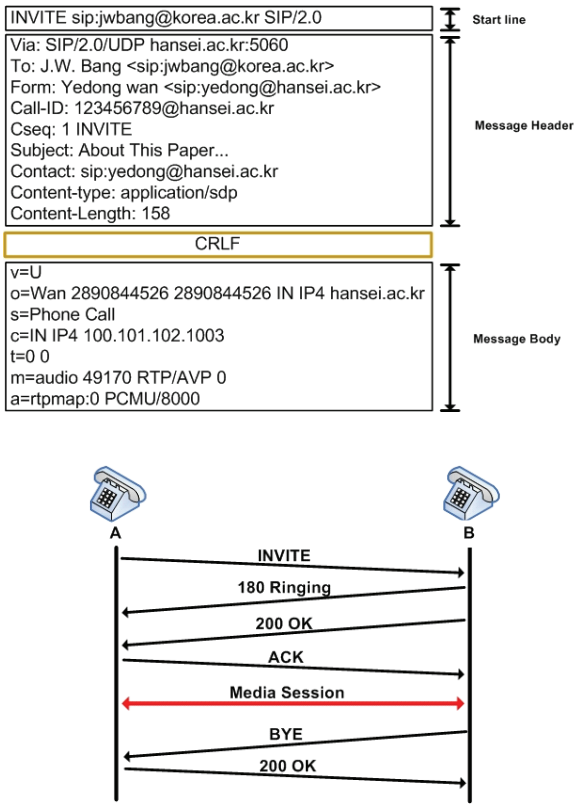
암호화와 함께 언급되는 항목은 각각의 인증된 VPN 사용자들에게 암호화된 인증키를 전달하기 위한 키관리 방식이다. IPsec에서 제안한 방식은 ISAKMP/ IKE(Internet Security Association Key Management Protocol/ Internet Key Exchange)이다.

2.2 VoIP

본 연구에서는 VoIP 시스템의 구축을 위해 공개 프로젝트인 VoIP Gateway ‘Asterisk[6]’를 활용하였다. ‘Asterisk’는 게이트웨이간 통신과 end-to-end 호 연결 설정을 위해 SIP(Session Initiation Protocol)을 사용하고 있다[3].

SIP은 인터넷 기반 멀티미디어 세션의 설정, 세션 정보 교환 및 해지 기능을 제공하는 응용 계층의 시그널링 프로토콜로 VoIP 외에도 인스턴트 메세징 및 프리젠스 서비스와 같은 다양한 인터넷 응용 개발에 사용 된다. 또 한 IP에 기반하므로 H.323과 같이 상호 운용성을 고려할 필요가 없으며 H.323에 비해 프로토콜 구조가 간단하여 디코딩이나 디버그 및 확장이 용이하다.

SIP의 동작을 (그림 1)에 표시하였다. 먼저 A는 INVITE method를 이용해서 B와 같이 통화할 수 있도록 요청한다. 이 과정에서 SIP body에 A의 media type 정보가 같이 전달된다. INVITE 메시지가 B의 전화기에 전달되면 전화벨을 울리고 그 상태를 다시 A에게 알려준다. B가 전화를 받으면 통화를 하려는 의지가 있다는 메시지를 B의 media type과 함께 A에게 전해준다. A는 ACK 메시지를 보냄으로써 통화를 시도하는 media type의 일치를 알리며 양측 간의 미디어 전송이 이루어진다. 통화가 끝난 뒤 B가 수화기를 내림으로 BYE method가 A에게 전달되고 세션을 끝내는 BYE method 요청이 처리되었음을 알리는 메시지를 보냄으로 세션을 마치는 과정으로 이루어진다.



(그림 1) SIP의 동작

2.3 VoVPN

VoIP 시스템이 안전하게 운용되기 위해서는 사용자 인증, 시그널링 메시지나 미디어 스트림의 암호화 및 무결성 등의 보안이 필수적이다[4]. 이러한 VoIP 시스템의 보안을 위한 접근 방법에는 크게 2가지가 있을 수 있다.

첫 번째 방법으로 VoIP 프로토콜에 내장되어 구현 보안 기능을 제공하는 것이다. 이는 각 프로토콜에 맞는 최적의 암호화/인증 방법을 적용할 수 있으므로 보다 효과적인 보안을 제공할 수는 있으나, 각 프로토콜마다 자체의 보안 메커니즘을 따로 설계한다는 비효율성이 따르며 또한 충분한 분석을 통해 검증되지 않은 새로운 보안 프로토콜을 사용한다는 것은 상당한 위험 부담이 따른다.

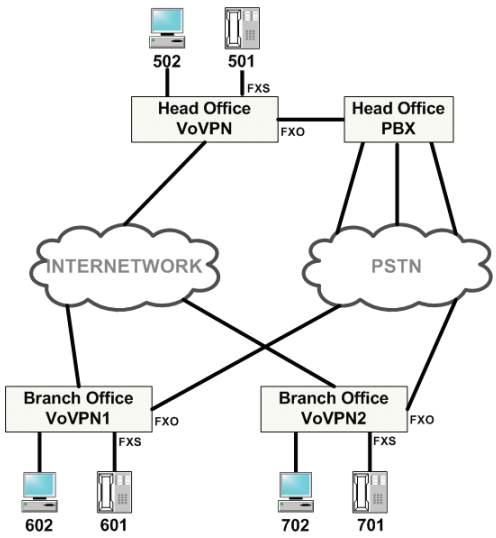
두 번째 방법으로 IPSec이나 TLS와 같이 잘 정립되어 있고 널리 사용되는 보안 인프라를 재사용하는 것이다. 이는 보안 전문가들에 의해 검증된 기존의 보안 인프라를 재사용함으로써 안정성을 보장받고 개발 기간을 단축시킬 수 있으며, 중복 투자를 피할 수 있으므로 대부분의 응용 프로토콜에서 추구하는 가장 일반적인 접근 방법이다. ITU-T나 IETF에서도 기본적으로는 가능한 한 기존의 보안 프로토콜을 재사용하는 것을 권고하고 있다.

VoIP 시스템의 보안은 또한 보안이 적용되는 구간에 따라 홉 대 홉 보안과 종단간 보안으로 구분할 수 있다. 홉 대 홉 보안은 IP 패킷이 전송되는 각 링크 상의 모든 트래픽을 전부 암호화 시키거나 MAC을 걸어주는 방법이다. 비

록 종단간 경로의 중간 장비들에서 복호화 후 다시 암호화가 일어나므로 보안상 취약점이 될 수 있으나 헤더를 포함한 전체 패킷을 보호할 수 있다는 장점이 있다. 이 목적으로 IPSec이나 TLS 등이 사용될 수 있다. 그러나 TLS는 TCP 위에서만 동작하므로 적용에 제한이 있으므로 IPSec이 가장 일반적인 솔루션이 될 것이다. 실제로 대부분의 프로토콜에서 홉 대 홉 보안을 위해서는 IPSec을 권고하고 있다[5].

RTP/RTCP는 H.323이나 SIP, RTSP 등 대부분의 VoIP 시스템에서 미디어 스트림의 전송을 위해 공통적으로 사용하는 프로토콜이다. IETF의 RTP/RTCP 표준문서에는 기본적으로 보안을 위해 IPSec과 같은 하위계층의 보안 인프라를 사용하는 것을 전제로 하고 이러한 보안 인프라가 일반화되기 전에 사용될 목적으로 자체 프로토콜에서 PEM 방식의 변형으로 DES-CBC로 암호화 하는 방법을 제시하고 있다[9].

위에서 언급했듯이 ITU나 IETF에서 다양한 방법으로 제안되고 있고, 그것을 바탕으로 VoIP 시스템의 음성 보안 구현에 가장 효과적으로 접근할 수 있는 보안 기술을 적용하여야 한다. 그래서 본 연구에서는 기존의 보안 인프라를 최대로 활용할 수 있는 VPN 프로토콜인 IPSec을 이용하여 데이터 기밀성을 보장하는 VoVPN 시스템을 구현하였다.



(그림 2) 망 구성

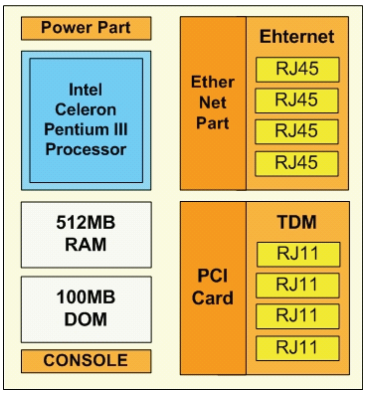
3. VoVPN의 설계 및 구현

3.1 망구성

본 연구에서는 (그림 2)와 같이 본사에 여러 지사가 연결되는 방식으로 망을 구성하였다. VoVPN 게이트웨이의 내부 FXS 단자를 통해 VoIP 통화가 가능할 뿐만 아니라 연결된 PC의 Soft VoIP 폰으로도 보안 통화가 가능하도록 하였다. 또한 FXO 단자를 통해 PSTN이나 PBX와 연동함으로 공공망을 이용한 통화나 음성 사서함 및 자동 응답 기능을 가능하도록 하였다. 그리고 공공망에서 걸려온 전화를 본/지사로 포워딩 가능하게 함으로 완벽한 보안 통화망을 구현할 수 있도록 하였다.

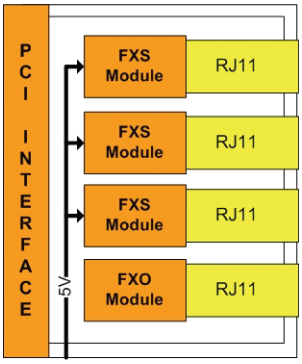
3.2 H/W

VoVPN을 구현하기 위한 하드웨어 플랫폼으로는 상용 VPN인 'XecureVPN 2000'을 활용하였다[10]. 즉 'XecureVPN 2000'의 PCI에 Analog Interface Card를 탑재하여 활용하였다.



(그림 3) 하드웨어 블록도

'XecureVPN 2000'의 메인 보드는 Portwell사의 NAS-3020 모델을 사용하고 있다. NAS-3020 는 (그림 3)에서 보는 바와 같이 CPU는 Intel 사에서 개발한 1.26 GHz의 속도를 가진 Celeron Pentium III 이며 512MB의 RAM과 100MB의 Flash Disk on Module(DOM)로 구성되어 있다.



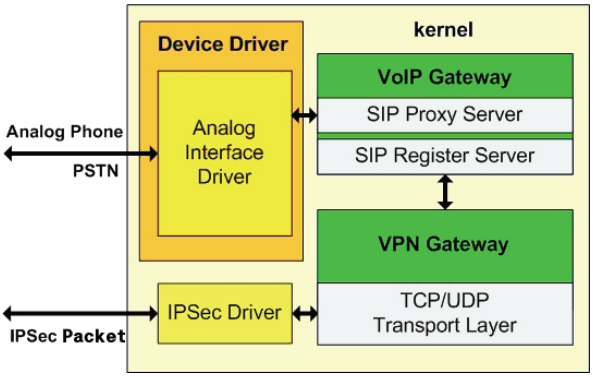
(그림 4) PCI Analog Interface Card 블록도

VoIP Phone과 PSTN망과의 연동을 위한 Analog Interface Card는 Digium 사의 TDM400P 모델을 이용하였다. TDM400P 는 (그림 4)에 나타난 바와 같이 일반 전화기를 연결해 VoIP 망을 이용할 수 있도록 하는 FXS Module과 VoVPN에서 PSTN을 이용할 수 있도록 하는 FXO Module로 구성되어 있다.

3.3 S/W

본 연구에서는 IPSec기반의 VPN에 SIP 기반의 VoIP 게이트웨이 공개 프로젝트 "Asterisk"를 연동하여 VoVPN

을 구현하였다. 소프트웨어 구현 환경은 Linux kernel 2.4.32를 사용하였고 컴파일러로는 GCC를 사용하였으며, 소스 언어는 ANSI-C를 사용하였다.



(그림 5) Software 개념 블록도

본 VoVPN 시스템은 VPN 게이트웨이에서 터널 모드로 동작하며 내부에서 외부로 나가는 모든 패킷에 대해 암호화를 수행한다. IPSec은 IP 계층에서 보안을 수행하기 때문에 상위 서비스인 VoIP 게이트웨이의 통화 개시 및 전송되는 음성 데이터를 터널 모드로 보안이 가능하다. 이를 통한 사용자 패킷의 전체 암호화는 사용자의 IP와 포트 번호, 음성 데이터를 숨길 수 있으므로 공중망에서 사용자의 통화 유무 자체를 은폐시킬 수 있다.

3.4 성능평가

(그림 2)와 같이 성능 평가를 위한 망을 구성하였으며 VoVPN이 연결된 PC에는 Soft VoIP Phone X-Lite[7]를 사용하였다. SIP Proxy Server를 이용하고 G.723.1 코덱을 사용하도록 설정하였다. 그리고 VoVPN의 FXS 단자에는 일반 Analog 폰을 설치함으로 일반 전화기로 암호화된 VoIP를 사용할 수 있도록 설정하였다.

VoVPN을 통한 음성 통화와 기존 VoIP 통화와의 통화 품질상의 문제점이 없음을 증명하기 위해 암호화된 음성 패킷의 종단간 지연 시간 측정을 위해 네트워크 모니터링 도구인 Ethereal[8]을 이용하여 VoIP 폰에서 음성 패킷을 보내고 되돌아오는 시간(Round Trip Time)을 측정하였다. 측정 결과 암호화한 경우와 그렇지 않은 경우의 전송 지연 차이는 최대 20ms을 넘지 않음을 확인하였다. 지연시간의 대부분은 VPN 터널링을 위한 패킷 캡슐화에 소요되는 지연시간으로 추정된다. 이는 ITU-T에서 제안한 종단간 지연시간 범위인 150ms ~ 200ms를 만족한다[11, 12].

4. 결론

본 논문에서는 상용 VPN 제품에 공개 프로젝트인 SIP VoIP Gateway 'Asterisk[6]'를 연동하여 사용자 인증과 데이터 기밀성을 효과적으로 보장하는 VoVPN(Voice over Virtual Private Network) 게이트웨이를 설계하고 구현하였다. VoVPN은 VPN의 암호화 통신에 음성 데이터스트림을 통합하여 추가 비용을 절감할 수 있을 뿐 아니라 향상된 보안 수준을 얻을 수 있다. 본 연구에서는 VoIP와 VPN을 통합함으로 완벽한 보안성을 구현하고자 하였으며 IPSec과 SIP/H.323 표준을 따라 다른 VoIP, VPN 기기와 연동되도록 하였다. 또한 VPN 게이트웨이에서 SIP/H.323 이나 NAT 변환 기능 및 대역폭 할당 기능 등 구현하여 보안성을 충족하면서 QoS가 보장되도록 하였다.

성능 평가를 위한 시험 결과, 전송 지연 차이는 최대 20ms을 넘지 않음을 확인하였으며, 이는 ITU-T에서 제안한 종단간 지연시간 범위인 150ms ~ 200ms를 만족함을 확인하였다.

참고문헌

[1] VoIP 정보보호가이드, 한국정보보호진흥원, 2005.12
[2] http://www.ietf.org/html.charters/ipsec-charter.html. "IP Security Protocol Working Group".
[3] RFC 3261, M. Handley, H. Schulzrinne, E. Schooler and J. Resenberg "SIP: Session Initiation Protocol". IETF, Jun 2002.
[4] D. Kroeselberg, "SIP security requirements form 3G wireless networks", Internet Draft, IETE, Jan 2001. Work in progress.
[5] R. Blom, E. Carrara and M. Naslund, "Conversational multimedia security in 3G networks", Internet Draft, IETF, Nov 2000. Work in progress.
[6] http://asterisk.org/about. "What is Asterisk".
[7] http://counterpath.com. COUNTERPATH., X-Lite.
[8] http://www.ethereal.com/introduction.html. "Features".
[9] "RTP Profile for Audio and Video Conferences with Minimal Control" RFC 1890, IETF, Jan. 1996.
[10] http://www.xnsystems.com
[11] TIA/EIA/TSB116, Voice Quality Recommendations for IP Telephony, Mar 2001.
[12] A. Percy, Understanding Latency in IP Telephony, Brooktroot Technology.