韓國 컴퓨터情報學會 論文誌
第10卷 第5號, 2005. 11.

2005-10-5-2-15

VOIP 보안 게이트웨이에 관한 연구

박 대 우*

A Study of VoIP Secure Gateway

Dea-Woo Park*

요 약

VoIP 기술을 사용하는 IP 인터넷 전화 통신 서비스에서 기업형 IP-PBX 서비스와 개인형 IP 인터넷 전화서비스의 상호운영은 방화벽에 막혀 통신이 원활하지 못했다. 본 논문에서는 VoIP 보안 게이트웨이를 이용하여 통신 및 보안을 수행하는 방안으로 방화벽에 VPN 전용 터널 개설, 애플리케이션 레벨의 게이트웨이 사용, VoIP 보안 게이트웨이 설정 연결, IP 인터넷 전화 프로토콜로의 변환을 제안한다. 이를 통해 IP 인터넷 전화 프로토콜과 기업형 IP-PBX 서비스가 방화벽을 지나 개인형 IP 인터넷 전화서비스와 상호운영될 수 있도록 하는 VoIP 보안 게이트웨이의 통신 기술에 대한 제안을 한다. 또한 VoIP 보안 게이트웨이의 보안성에 대한 문제점과 해결점을 제시한다.

Abstract

IP-Internet Telephony Service has not yet been achieved that of operating an IP-PBX service and a consumer Internet telephone services using VoIP technologies. In this paper, i suggest that the technologies of the VoIP Secure Gateway have connecting and securing for IP-Internet Telephony Service which makes IP telephony protocols, firewall VPN tunneling, using Application Level Gateway, connection of the VoIP Secure Gateway. I suggest of telecommunication technologies that are enables an enterprise IP-PBX service to interoperate with a consumer IP telephony service through a firewall. Also, I have proposed the solutions of security problems which was the security for VoIP Secure Gateway.

▸ Keyword : 방화벽(Firewall), 보안(Security), IP-PBX, Gateway, VoIP.

• 제1저자 : 박대우
• 접수일 : 2005.10.14, 심사완료일 : 2005.10.28
* 숭실대학교 컴퓨터학과

Ⅰ. 서 론

IP 인터넷 전화서비스는 정부의 허가 기준이 제시되면서 급격하게 발달하고 있다. VoIP(Voice over Internet Protocol) 기술을 사용하는 IP 인터넷 전화 서비스는 IP-PBX(Internet Protocol-Private Branch eXchange) 서비스를 이용하는 기업형 IP 인터넷 전화 서비스와 개인형 IP 인터넷 전화 서비스가 있다.

또한 기업에 대한 IP 인터넷 전화 아웃소싱 서비스(IP Centrex services)는 ISPs(Internet Service Providers) 사업자들에 의해 제공되고 있다. IP-Centrex 서비스의 경우, ISPs 사업자들은 단지 IP-Centrex 서비스만 제공 하는 것이 아니라, 개인형 IP 인터넷 전화서비스도 제공하며, ISPs 사업자들은 기업형 IP 인터넷 전화와 개인 IP 인터넷 전화 사이의 상호 운영을 수행할 수 있다.

그러나 IP-Centrex 서비스와 별개로, IP-PBX서비스는 개인형 IP 인터넷 전화서비스와 상호운영 할 수 없다. 그 이유는 (그림 1)처럼 일반적으로 내부 네트워크를 보호하는 방화벽(Firewall)에 의한 패킷필터링 정책[1]에 의해 통로가 막혀있고, IP 인터넷 전화 프로토콜은 방화벽에 막혀서 통신이 가능하지 않다는 등의 이유로 UDP(User Datagram Protocol)을 기반으로 전화 통신을 하기 때문이다.

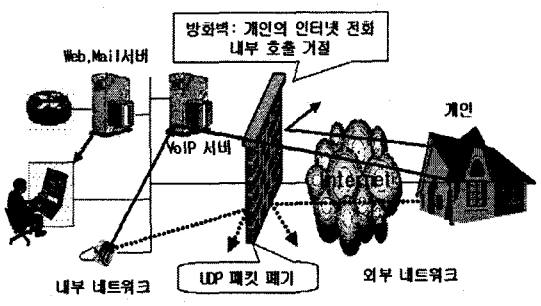

그림 1. IP 방화벽에서 인터넷 전화 호출 거절
Fig. 1 reject calling of Internet phone in Firewall

결국, 기업형과 개인형 IP 인터넷 전화에 대한 상호 운영 서비스는 기존의 전화선들을 사용하여야만 가능하게 되어, IP 인터넷 전화를 이용한 서비스에 차질을 가져오고 있다.

따라서 본 논문에서는, 개인형 IP 인터넷 전화 프로토콜과 기업형 IP-PBX 서비스가 방화벽을 지나 상호 작동될 수 있도록 하는 VoIP 보안 게이트웨이를 이용하는 통신 기술들을 제안하고자 한다. 또한 IP 인터넷 전화 서비스가 발전되기 위해서 해결되어야 할 다른 VoIP 보안 게이트웨이의 보안성에 대한 문제점과 해결점을 제시하고자 한다.

Ⅱ. 관련 연구

2.1 IP 게이트 웨이

IP 게이트웨이는 전화 네트워크와 IP 네트워크를 접속하며, IP 인터넷 전화 이용자와 가입 전화 이용자가 상호 통화할 수 있도록 하기 위해 양쪽의 통신 네트워크를 접속한다. 통신 사업자용과 일반 기업용 장치가 있는데, 통신 사업자용 장치에서는 일반적으로 가입 전화 네트워크에 접속되며, 공통선 신호 네트워크에 접속할 수 있는 기능을 가지기도 한다. 반면, 일반 기업용 장치에서는 PBX와 구내 정보통신 네트워크를 접속한다. 음성 부호화 방식의 표준은 ITU-T 권고 G.729나 G.723.1[2]을 채용하고 있다. 또 전화번호와 IP 주소 변환에는 게이트 키퍼를 이용하기도 한다.

2.2. 방화벽과 인터넷 네트워크와의 연결 정책

내부 네트워크 자원을 보호하는 방화벽 관리자는 보안 정책을 책정하여, 외부의 불법침입으로부터 내부 네트워크 자원을 보호한다. 방화벽의 기본 보안 정책은 내부 네트워크로부터 인터넷으로 나가는 모든 패킷은 허락하고, 외부 인터넷으로부터 접근하는 모든 패킷은 거절한다. 따라서 외부 인터넷네트워크에서 진입하는 패킷을 필터링하여, 불법적인 패킷을 폐기(drop) 시키거나, 인증을 통해 패킷을 허용한다.

하지만 기술적인 예외 사항을 하나 둔다. 즉 SMTP(Simple Mail Transfer protocol)의 TCP(Transmission Control Protocol) 패킷이거나 E-mail 서비스의 프로토콜이다[3]. 이러한 이유로 사용자는 외부 인터넷 네트워크와 내부 네트워크의 TCP 연결은 가능하지 않지만, SMTP를 이용하는 TCP 연결은 가능 하다.

즉 외부 인터넷 네트워크로부터 불법 접근을 막도록 보안 정책을 시행하고 있는 방화벽은 DMZ (Demilitarized Zone)의 E-mail 게이트웨이를 경유한 경우 SMTP, TCP 연결만 유일하게 허용한다.

IP 인터넷 전화 서비스는 외부 인터넷과 내부 네트워크 사이의 방화벽을 통해 상호 연결을 하여야 한다. 방화벽은 TCP/IP의 네트워크에서 허가되지 않는 패킷을 차단하기 위한 보안 정책을 사용하고 있다. 따라서 IP-PBX 서비스를 이용하기 위해 방화벽을 통과하여 개인형 IP 인터넷 전화 서비스와 상호 운영 할 때 생기는 데에서 발생하는 보안상의 문제점들에 대한 해결책이 필요하다.

2.3 방화벽과 IP 인터넷 전화 프로토콜

IP 인터넷 전화 서비스에서 호출에 대한 응답은 방화벽이 외부 인터넷 네트워크로부터 H.323 또는 SIP(Session Initiation Protocol)[4]과 같은 IP 인터넷 전화 프로토콜이 통과하도록 한다. SIP은 인터넷 멀티미디어 회의, IP 인터넷 전화, 멀티미디어 배포 등을 지원한다. SIP은 멀티캐스트와 유니캐스트을 통한 통신 교섭을 허용하며, 프록시와 리다이렉트 등의 방법을 이용하여 사용자 이동성을 지원한다. 따라서 IP 인터넷 전화 프로토콜이 SMTP와 유사한 호출 신호 프로토콜의 TCP라면 하위계층 프로토콜과 독립적으로 사용할 수 있다.

하지만 웹 브라우저의 HTTP(Hypertext Transfer Protocol)의 업 링크, FTP(File Transfer Protocol), IP 인터넷 전화 서비스 등은 보안의 취약성을 갖는다. 따라서 방화벽 관리자는 외부 인터넷과 내부 네트워크의 TCP 연결은 방화벽에 적용할 보안 정책에는 알맞지 않는다고 생각한다.

IP 인터넷 전화 서비스는 리얼타임 통신을 규정하고 있지만, 이것은 음성미디어 패킷 전송에 있어 TCP 보다는 UDP 사용이 더 효율적으로 여겨진다. 결국, IP 인터넷 전화 프로토콜의 호출 신호 프로토콜의 UDP를 사용하므로, 음성 미디어 프로토콜은 (그림 2)와 같은 영향을 미칠 수도 있다. 즉 방화벽은 내부 네트워크와 외부 인터넷의 터미널 사이의 통신에 대한 UDP 패킷의 통과를 허락할 수 있다.

UDP 패킷은 TCP처럼 3 핸드 세이크나 연속번호를 가지고 있지 않으므로, TCP 패킷보다 많은 UDP 패킷을 만들 수 있다. 이 이유로 각 UDP 패킷의 주소 소스 필드는 주의 깊게 조사하여야 한다. 하지만 보수적인 정보 보안을 관리하는 방화벽은 UDP 패킷을 거절한다.

IP 인터넷 전화 프로토콜의 연결은 다른 하나의 문제점을 갖고 있다. 전형적인 IP 인터넷 전화 시스템의 사용은 호출 신호의 다른 프로토콜인 SIP, H.323을 사용한다. 그리고 미디어통신은 RTP (Real-time Transport Protocol)를 사용한다. RTP 패킷은 목적지 IP 주소의 라우터 및 각 호출의 포트 번호에 사용된다. 그런데 IP 인터넷 전화 시스템은 반드시 넓은 범위의 포트번호를 사용한다.

일반적인 방화벽의 인터넷 보안정책은 넓은 범위 포트 번호를 허용하지 않는다[5]. 따라서 IP 인터넷 전화의 통신과 보안에 대한 해결책이 필요하다.

III. VoIP 보안 게이트웨이

IP 인터넷 전화 서비스를 활성화시키기 위해서는 위에 제기된 방화벽과의 통신 및 보안에 관한 문제점들에 대한 해결책이 필요하다. 이 해결책의 방법 중 하나는 VoIP 게이트웨이를 사용하는 것이다. 다음은 IP 인터넷 전화 서비스를 위해 방화벽을 통과하는데 따른 문제점과 이에 대한 해결 방법을 제시한다.

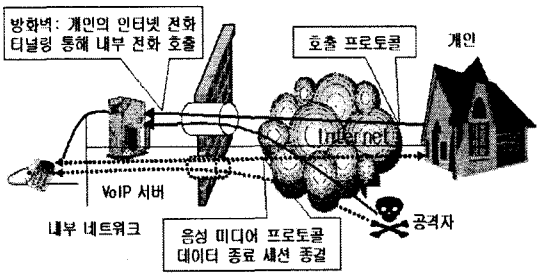

그림 2. IP 인터넷 전화 프로토콜의 방화벽 통과
Fig. 2 accept Internet Telephone Protocol in Firewall

3.1 전용 터널 개설

(그림 2)와 같이 방화벽에 VPN 전용 터널을 개설[6]하여 IP 인터넷 전화 서비스 전용의 터널을 만드는 것이다. 이러한 VPN 터널의 방법은 다음과 같다.

1) 방화벽이 지정된 IP 인터넷 전화 신호 프로토콜을 VPN 터널링에 통과하도록 보안 정책을 설정한다.

2) IP 인터넷 전화 신호 프로토콜은 통신파라미터에 포함되는 정보 세션의 교환과 이용하는 포트 번호에 사용된다.

3) 이 방법은 정보 세션의 획득으로 방화벽의 보안 정책 룰의 삭제와 추가에 사용 된다.

4) 음성 미디어 프로토콜은 IP 인터넷 전화 신호를 확인 호출하는 동안 만 통과된다.

5) 호출이 끝났을 때 음성미디어 프로토콜이 통과 후, 책정된 룰에 의해 VPN 터널링은 닫히고 방화벽의 보안 정책에서 적용되었던 룰은 지워진다.

하지만, 이 방법을 사용하여 생길 수 있는 취약점으로는 외부의 공격자가 속임 신호 프로토콜을 이용하여 방화벽을 통과 할 수 있고, IP-PBX의 IP 주소와 IP 인터넷 전화 터미널이 노출될 수 있다.

3.2 애플리케이션 레벨 게이트웨이 사용

IP 인터넷 전화 시스템은 애플리케이션 레벨 게이트웨이(Application Level Gateway)[7]를 사용한다. 애플리케이션 레벨 게이트웨이는 인터넷과 내부네트워크 사이의 IP 인터넷 전화를 위한 호출의 중계 역할을 한다. 만약 공격자가 IP 인터넷 전화 시스템을 공격할 때 방화벽은 공격자의 통과를 허용함으로써 이 시스템을 방어를 해 주지 못하는 점이 있기 때문이다.

이 부분은, IP-BPX와 IP 인터넷 전화 서비스 시스템의 공통적인 문제이다. 즉 이 문제들은 IP 인터넷 전화 프로토콜이 방화벽의 보안 정책에 연동되지 못함으로 발생하는 것이다.

지능화된 VoIP 보안 게이트웨이는 방화벽과 공통된 구성방식의 IP 인터넷 전화 프로토콜을 만든다. 이것은 보안을 약화시키지 않는 TCP의 기본 애플리케이션의 전형적인 룰에 대한 최소한의 추가사항만을 요구하고 있다. (그림 3)에서 VoIP 보안 게이트웨이 기술을 나타내고 있다.

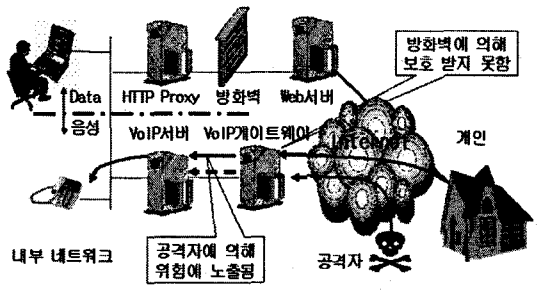

그림 3. VoIP 게이트웨이
Fig. 3 VoIP Gatewayf

3.3 보안 게이트웨이 설정 연결

IP 인터넷 전화 서비스는 SIP과 H.323의 UDP 패킷과 TCP 연결을 기본으로 한다. 그리고 방화벽의 보안 정책은 이 패킷들을 VPN 터널링의 방법으로 통과하도록 하는 것이다. 그런 까닭에 IP 인터넷 전화 서비스 프로토콜이 방화벽을 통과하여 작동하는 것이 가능하다.

일반적으로 방화벽에 의하여 승인된 TCP 연결이 트랜스포트로 변환되는 것[8]으로 HTTP나 FTP와 같은 인터넷 애플리케이션 서비스에 사용된다. 본 논문에서는 이 기능을 이용하여 접근 통제를 실시하고자 한다.

(그림 4)에서 VoIP 보안 게이트웨이는 DMZ의 내부 네트워크와 종단 게이트웨이 사이에서 릴레이 게이트웨이로 사용한다.

주요 개념은 내부 네트워크와 DMZ의 게이트웨이1과 게이트웨이2로부터 TCP를 연결하고 이 연결을 제어하는 것이다. 보통 TCP 송신은 리얼타임 애플리케이션의 송신 지연의 원인이 된다.

LAN(Local Area Network) 환경에서 TCP 연결은 신뢰성 있는 송신을 제공하기는 하나, 패킷을 잃게 되는 경우도 있다. 이 때에는 외부에서 침입하여 불법적인 접근으로부터 내부 네트워크를 보호하는 방화벽이 VoIP 서비스에 대한 필터링 법칙을 단순화하게 하는 것이 중요하다.

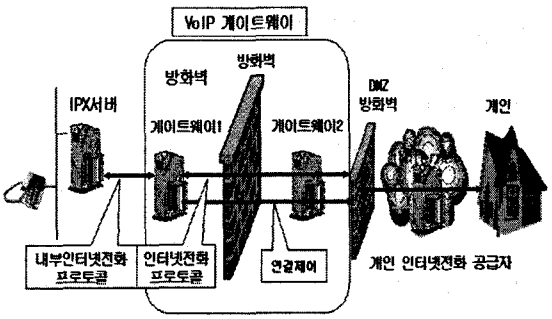

그림 4. VoIP 보안 게이트웨이
Fig. 4 VoIP Secure Gateway

VoIP 서비스를 위해 네트워크 통신을 수행할 때, VoIP 보안 게이트웨이는 2개 TCP 연결을 사용한다. 하나는 신호 호출 프로토콜이고, 다른 하나는 음성 미디어 프로토콜이다. 이 방식은 방화벽이 필터링 보안 규칙을 정하는 있어서, 두 개의 서로 다른 포트를 사용하는 게이트웨이1과 게이트웨이2로부터 TCP 연결을 허락하게 하여 보안을 유지시키게 하는 방법이다.

3.4 IP 인터넷 전화 프로토콜 설계

방화벽에서의 보안 정책은 외부 인터넷과 내부 네트워크 사이의 패킷의 통과는 막는다. 하지만, 게이트웨이2로 호출 패킷이 들어오면, 내부 네트워크의 IP 인터넷 전화 프로토콜로 변환 시키는 것이다. 이때 내부의 IP 인터넷 전화 프로토콜을 메타 IP 인터넷 전화 프로토콜이라고 하자.[9]. IP 인터넷 전화 프로토콜은 내부 네트워크의 호스트로부터 직접 IP 인터넷 전화 프로토콜이 통과하는 것을 막는다. 게이트웨이2는 IP 인터넷 전화통신에 대한 메시지가 들어오는 것을 감시하다가, 이것을 IP 인터넷 전화 프로토콜 메시지로 재구성한다. 이 메시지들은 이미 보안 정책에 룰로 설정되어 있는 방화벽을 통과하여 게이트웨이1인 교체 게이트웨이로 보내진다. 다음에 게이트웨이1은 내부 IP 인터넷 전화 프로토콜을 사용하여 내부 네트워크에 IP 인터넷 전화 통신을 수행한다.

이 프로세스가 진행되는 동안에 입증되지 않는 불법 프로토콜 메시지는 여과되어진다. 게이트웨이2도 들어오는 미디어 메시지와 게이트웨이1에게 포워딩되는 필터링 되는 패킷을 감시한다.

IP 인터넷 전화 프로토콜은 TCP 연결위에 송신되도록 설계한다. IP 인터넷 전화 프로토콜의 TCP 연결은 게이트웨이1의 내부 네트워크 지역으로부터 게이트웨이2인 DMZ 지역으로 인정된다. 이 TCP 연결은 보통 전형적인 방화벽의 보안정책으로 설정하여 인정한다. 따라서 통과되는 TCP 연결은 보안 방화벽으로 통과되는 VoIP 통신이 된다.

Ⅳ. VoIP 보안 게이트웨이

본 논문에서 외부 인터넷으로부터 내부 IP 인터넷 전화 시스템을 향하여 오는 패킷과 방화벽을 통과하는 불법적인 접근으로부터 정보 시스템을 보호하는 VoIP 보안 게이트웨이를 제안한다.

4.1 VoIP 보안 게이트웨이의 특징

VoIP는 보안 게이트웨이는 두 가지의 특징이 있다. 첫째는 방화벽 관리자가 VoIP 통신을 위해 인터넷으로부터 내부 네트워크를 통과시키기 위한 패킷에 대한 정책 구성이 필요하지 않다는 것이다. 둘째는 DMZ 네트워크의 게이트웨이 지역에서 유일하게 받아들여지는 호출이라는 것이다.

만약 VoIP 게이트웨이가 악의적인 해커로부터 공격을 당한다면 방화벽은 내부 네트워크와 게이트웨이 서버로부터 접근 제한을 하여 스스로를 보호한다. 또한 VoIP 보안 게이트웨이 시스템은 들어오는 프로토콜 메시지를 종료시키고, 메타 IP 프로토콜 메시지로 변환시킨다.

게이트웨이1은 메타 IP 인터넷 전화 프로토콜을 변화시킬 수 있는데, 이것은 SIP과 H.323이다. 즉 IP-BPX 시스템의 VoIP 프로토콜에 포함된 것이다. 이 방법은 인터넷의 사용으로부터 다른 상이한 내부 네트워크의 사용이 IP 인터넷 전화 프로토콜이나 인터넷으로부터 다른 내부 네트워크의 IP 버전으로 사용되어 진다.

4.2 VoIP 보안성 평가

VoIP 보안 게이트웨이를 이용하는 IP 인터넷 전화 서비스에 대한 보안성을 향상하기 위해, 보안성의 6가지 기준인 접근제어, 기밀성, 신뢰성, 가용성, 무결성, 부인봉쇄[10]에 대하여 살펴본다.

PSTN(Public Switched Telephone Network) 시스템은 전화업무의 신뢰성을 목적으로 하였다. 따라서 통신라인은 물리적으로 안전한 보안 레벨에서 만들어 졌다. 그 후로 개발된 IP 인터넷 전화 시스템은 공개된 통신기반의 IP 네트워크를 사용하게 되었는데, IP 인터넷 전화서비스는 PSTN과 같은 높은 레벨의 보안 레벨은 이루지 못했다.

표 1. VoIP의 보안기능
table.1 Security functions in VoIP

보안	VoIP의 보안기능
접근제어 (Access Control)	호출허용과 특별한 서비스
기밀성 (Confidentiality)	데이터통신의 기능 비밀, 프로토콜 파라메터 호출활동
신뢰성 (Authentication)	접근, VoIP 서버, 메시지의 신뢰
가용성 (Availability)	네트워트 접근 방해와 DoS 공격에 대한 대응
무결성 (Integrity)	해커의 세션에 대한 대응, 지연공격
부인봉쇄 (Non-repudiation)	일어나기 쉬운 세션 로그 이용

〈표 1〉에서는 VoIP 보안 게이트웨이를 이용하는 IP 인터넷 전화 서비스는 보안을 강화시키기 위한 접근제어, 기밀성, 신뢰성, 가용성, 무결성, 부인봉쇄의 6가지 보안 기능을 나타내었다.

IP 네트워크는 PSTN 기반의 네트워크 규정만큼 보안 레벨의 필요성에 대해 규정하지 않았다. 하지만 VoIP 보안 게이트웨이는 IP 인터넷 전화 시스템의 가용성을 개선한다.

웜의 네트워크 혼잡 공격과 DoS 공격 그리고 컴퓨터 바이러스 등은 IP 인터넷 전화서비스에 위협을 주는 심각한 문제다. 특히 전화에서 중요한 비상 호출의 기능이 꼭 필요할 때를 대비하여, 이러한 공격에 대한 방어 문제는 꼭 해결되어야 하는 문제이다. 이 문제들의 대부분은 TCP/IP 기반 네트워크 시스템의 공통 문제로서 IP 전화 기술과 기본 IP 보안기술 통합에 의하여 해결해야 한다.

일반적으로 IPsec 프로토콜과, TLS(Transport Layer Security), S/MIME(Security Services for Multipurpose Internet Mail Extension)들은 암호화와 정보 보안을 위해 사용된다. 또한 시스템의 보안성을 위해 이 보안 툴들이 어떻게 사용되었는지는 일반적으로 알려져 있지 않다. PSTN을 이어받는 각 전화기들의 라인은 하나의 ID인 전화기 번호를 가지고 있는데, 전화기 번호는 전화기에 연결된 라인의 물리적인 위치와 동일하다. 추가로 라인들은 물리적으로 안전한 접근과 전화번호는 전화 업무의 기본적인 통제를 한다.

IP 인터넷 전화 시스템은 전화 번호 대신으로 각 전화번호의 IP 어드레스를 할당한다. 그러므로 공격자들은 쉽게 IP 어드레스를 속일 수 있고, IP 인터넷 전화 서비스는 믿을 만한 P2P(Peer-to-Peer) 서비스를 필요로 한다.

특히 이동 IP 전화와 소프트웨어 IP 전화는 PSTN에 비해 상대적으로 안전하지 못해, 보안의 신뢰 없이는 중요한 정보의 전달은 어렵다 따라서 웹 서비스를 응용한 다른 IP 서비스의 IP 인터넷 전화 서비스를 이용할 때에는 더 확실한 인증이 필요하다.

이러한 경우에 단말 사용자에 대한 비밀 정보의 사용을 위해 앤드 유저(End User) 사이에 인증을 사용한다. 인증 시스템의 예로서 PKI(Public Key Infrastructure)와, IP 인터넷 전화 서비스의 데이터 암호화에 대한 P2P 인증을 사용한다[11]. 즉 전화를 걸때 인증 시스템도 백그라운드에서 동시에 작동 되도록 하면 보안성을 강화하게 될 것이다.

VoIP 보안 게이트웨이를 이용하는 IP 인터넷 전화 서비스의 중요한 보안 문제의 하나는 기밀성이다. 기밀성은 데이터의 내용을 암호화함으로서 미디어 통신의 내용을 암호화하여 전달한다. 또한 공격으로부터 힌트를 줄지도 모르는 IP 주소, 포트 번호, 호출에 사용되는 데이터 포맷 등의 파라메터를 감출 수 있다. 암호 기술은 몇몇 사용자로부터 인터미디어와 스위칭의 멀티플렉싱 미디어의 통신 패킷을 하는데 사용한다.

또한 기밀성은 VoIP 보안 게이트웨이의 호출 활동도 감춘다. 이것은 수신 권한을 넘어선 부가의 송신에 대한 위조 패킷을 방지한다. 하지만 이 방식은 여분의 밴드 폭과 또 다른 컴퓨팅 능력을 요구하여 통신 시스템의 부하를 가중시킨다.

V. 결론

본 논문은 VoIP 보안 게이트웨이를 이용한 IP 인터넷 전화 프로토콜에서의 통신과 보안을 위한 기술들을 제안하였다. 일반적인 방화벽에서의 보안 정책의 룰을 극복하면서 IP 인터넷 전화 프로토콜을 이용하게 하여, IP-PBX와 IP 인터넷 전화 서비스 사이에서 상반된 문제를 해결 하였다. IP 인터넷 전화 서비스 사용자들과 IP-PBXs 파라메터를 변환하는 전략이다.

제안된 기술들이 실제 현장에서 적용되기 위해서는 현실적인 통화의 대역폭 문제, 방문이나 피 방문정보에 대한 기록과 활용, 상호인증에 대한 변수들을 동시에 해결하여야 한다.

또한 IP 인터넷 전화 서비스와 내부 운용에 필요한 보안 문제들을 지적하고, 6가지의 보안 기준에 따라 보안 방법들을 제시하였다. 이러한 문제들은 가용성과, 기반 인증, 그리고 전화의 프라이버시 기능과 관련 있지만, 역시 보안 정책적인 면과 기술상의 문제에 대한 정부 정책과 기준 및 표준화가 꼭 필요하다.

IP 인터넷 전화 서비스는 활동하는 서비스다. 다라서 국가는 전략적인 가이드라인을 제시하고, 공청회를 거쳐, 가장 적절한 IP 인터넷 통신 서비스에 대하여 새로운 가이드라인을 만들어야 한다.

향후 연구 되어야 할 과제로는, 차세대 프로토콜인 SIP 시스템 구축 및 BcN(Broadband converged Network) 개발에 따른 지속적인 VoIP에 대한 업그레이드 방안들이 강구 되어야 할 것이다.

참고문헌

[1] 박대우, "Solalis K4방화벽에 대한 기능별 운영체제 (32비트, 64비트)별 성능비교연구." 한국통신학회논문지, 제28권 제12B호, pp1091-1099, 2003. 12. 30.

[2] http://www.itu.int/itudoc/itu-t/com16/implgd/g7231-02.pdf. 2005.10.

[3] S. Kamara, S. Fahmy, E. Schultz. F. Kershbaum. M. Frantzen. "Analysis of vulnerabilities in Internet firewalls". Computer & Security. Vol 22, No 3, pp214-232, 2003.

[4] W. Stallings. "Cryptography and Network Security, Principles and Practice". Third Edition, Prentice -Hall, October 2005.

[5] W. R. Cheswick and S. M. Bellovin. "Firewalls and Internet Security". 2nd Edition, AT&T Bell Laboratories, 2003.

[6] Tim Mangan, "Using Frame Realy for a VPN" INTERNATIONAL JOUNAL OF NETWORK MANAGEMENT, 11, pp253-257, 2001.

[7] Denis Guster, Charles Hall. A Firewall Configuration Strategy for The Protection of Computer Networked Labs in a College Setting. JCSC 17, 1. October 2001.

[8] 임승린. 박대우. "TCP 사용자 인증 타원곡선 알고리즘 프로토콜의 설계 및 성능 개선에 관한 연구", 한국컴퓨터정보학회논문지, 제9권 제2호, pp7-17, 2004.6.

[9] Noriyuki Fukuyama, Shingo Fujimoto, Masahiko Takemaka. "Firewall-Friendly VoIP Secure Gateway and VoIP Security Issues". FUJITSU Sci. Tech. J., 39. 2, December 2003.

[10] 박대우, "무선방화벽의 설계 및 구현에 관한 연구." 한국컴퓨터정보학회논문지, 제8권 제1호, pp44-50, 2003. 3. 31.

[11] Yongdeug Jung. Deawoo Park. Moonseog Jun. "The Analysis of New Video Conference System for Secure Communications". GESTS International Transaction on Computer Science and Engineering. Vol.2, No.1. 2005.

저 자 소 개

박 대 우

1987년 서울시립대학교 경영학과 졸업 (경영학사)

1995년 숭실대학교 컴퓨터학부 (컴퓨터부전공)

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2003년 숭실대학교 겸임조교수

〈관심분야〉 유비쿼터스, 정보 보안, 인터넷S/W, 시스템 네트워크 보안, 컴퓨터 네트워크, 이동통신 및 IMT-2000 보안, Cyber Reality