한국항행학회 논문지 제12권 제1호 2008년 2월

차세대 네트워크 환경에서의 인터넷전화 서비스를 위한 정보보호 대책 연구

A Study on Information Security policy for VoIP Service in Next Generation Networks

성 경*, 김석훈**

Kyung Sung*, Seok-Hun Kim**

요 약

인터넷 망을 사용하여 음성 서비스를 제공하는 VoIP는 초기의 호기심을 벗어나 이제는 사업의 한 아이템으로 각광 받고 있다. VoIP 기술은 인터넷을 통해 음성 데이터를 전달하는 기술로서 인터넷 전화 서비스가 기존 전화 서비스를 대체할 수 있어 이에 대한 관심이 커졌다. VoIP 기술은 기존 IP 기술을 이용하여 음성통신 서비스를 제공하기 때문에 IP 기반의 위협들을 그대로 상속하며, VoIP 서비스 제공을 위한 신규 기술들로 인해 발생하는 새로운 위협들을 가지고 있다. 따라서 본 논문에서는 VoIP 서비스의 보안위협에 대하여 살펴보고, 보안적용시의 문제점과 고려사항 및 대책에 대하여 제시하였다.

Abstract

VoIP provided voice service using Internet is receiving footlights when it escapes an initial curiosity. VoIP interest became larger, because it can transfer existing phone service and deliver voice data through internet technology. Is inheriting as it is threats of IP base because a VoIP technology provides audiocommunication service taking advantage of an existing IP technology, and have new threats that happen from new know-hows for VoIP service offer. In this paper, presented about problem and consideration and countermeasure of examines about security threat of VoIP service, and applies security.

Key words : VoIP, Security, NGN, BcN, PSTN

I. 서 론

VoIP(Voice over IP) 서비스는 저렴한 통신요금과 부가서비스 제공으로 기존의 일반전화(PSTN)를 대체하는 대중적 서비스로 성장할 것으로 예상되고, 2005년 시장규모는 1,570억원으로 조사되었으며, 오는 2008년까지 연평균성장률(CAGR) 54%를 기록해 2009년에는 9,689억원 규모를 형성할 것으로 전망되고 있다.

음성데이터, 유·무선, 통신·방송 융합형 멀티미디어 서비스를 언제 어디서나 편리하게 이용할 수 있는 광대역통합망(Broadband convergence Network: BcN) 서비스 형태로 진화하고 있다. 특히, 인터넷 전화 서비스가 기존 전화 서비스를 대체할 수 있어 이에 대한

* 목원대학교 컴퓨터교육과(Dept. of Computer Education, Mokwon University)
** (주)파라곤베이스 (Paragonbase co. Ltd.)
· 제1저자 (First Author) : 성 경
· 접수일자 : 2008년 1월 9일

관심이 커지면서 인터넷을 이용한 VoIP(Voice over Internet Protocol) 기술은 유선, 무선, 인터넷들과의 연동하는 단계에서 통합하는 단계로 발전시킬 수 있는 차세대네트워크(Next Generation Network) 환경에서의 킬러 애플리케이션으로 대두되고 있다[1].

VoIP 기술은 기존 IP 기술을 이용하여 음성통신 서비스를 제공하기 때문에 IP 기반의 위협들을 그대로 상속하며, VoIP 서비스 제공을 위한 신규 기술들로 인해 발생하는 새로운 위협들을 가지고 있다. 그 중에서도 공격 가능성 및 피해 규모 등을 고려할 때, 도청, 서비스 거부공격, 서비스 오용공격, 스팸 공격 등은 가장 문제가 될 수 있어 서비스 확산에 장애가 될 수 있다는 문제점이 있다. 기존 전화망의 회선기반 방식과 다르게 VoIP 서비스는 IP 기반의 인터넷 기술을 기반으로 음성통화가 이루어짐에 따라, 인터넷 망에서의 보안위협을 내포하고 있다[2].

따라서 본 논문에서는 2장에서는 VoIP 기술의 기본 개념과 VoIP의 품질보장(Qos, Quality of Service) 특성 및 VoIP 서비스의 보안위협에 대하여 살펴보고, 3장에서 보안적용시의 문제점과 고려사항 및 대책에 대하여 제시한 후 결론을 맺도록 한다.

Ⅱ. 관련 연구

2-1 VoIP 서비스 개념

기존부터 사용되고 있는 데이터통신용 패킷망을 인터넷폰에 이용하는 것으로, VoIP(Voice over Internet Protocol)라고 한다. 음성 데이터를 인터넷 프로토콜데이터 패킷으로 변화하여 일반 전화망에서의 통화를 가능하게 해주는 통신서비스 기술이다. 케이블을 통하여 여러 명이 동시에 사용할 수 있고 확장성도 뛰어나며 기존 전화에 비하여 요금도 훨씬 저렴하다.

신호제어, 미디어 신호 전송, 음성 압축 및 통화품질 보장, 주소 및 번호체계, 이기종망 연동, 응용 및 부가 기능에 해당하는 요소별 기술들의 집합이다. VoIP 시스템은 하드웨어 구현물로 기능상 전송채널과 전송시스템, 호처리 및 제어를 담당하는 교환시스템, 상이한 신호체제를 중계하는 게이트웨이시스템과 사용자 단말시스템으로 구분할 수 있다[3].

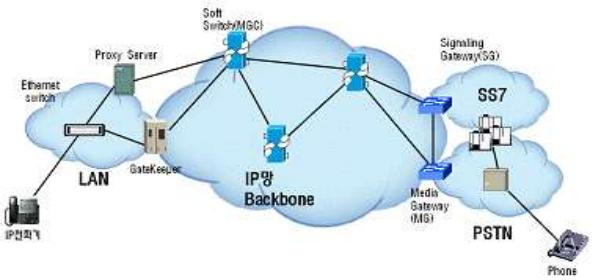

그림 1. VoIP 망 구성도
Fig. 1. VoIP Architecture

2-2 VoIP 음성전송 특징

VoIP의 음성전송 특성을 이해하기 위해 VoIP 통신환경에서 처리되는 과정은 그림 2와 같이 먼저 아날로그 음성 신호를 디지털화하고, 대역 사용의 효율성을 위해서 압축 알고리즘을 적용하여 음성 패킷을 생성한다. 생성된 패킷은 실시간 프로토콜(RTP, Real-time Transport Protocol), UDP 및 IP 헤더를 붙여 해당 네트워크의 전송로 규격에 맞추어 전송된다. 여기서 한가지 주목할 점은 VoIP가 데이터 전송에서 주로 사용하는 TCP 대신 신뢰성을 보장하지 못하는 UDP를 사용한다는 점이다. 그 이유는 신뢰성 제공이 중요한 데이터 전송과는 달리 음성 신호가 갖는 실시간 전달특성(사용자 입장에서는 늦게 전송되느니 차라리 손실이 있는 편이 품질이 좋다고 느끼는 특성)에 기인한 것이다. RTP는 UDP 전송에 대한 최소한의 신뢰성을 부여하기 위한 보완 수단으로 사용하며, RTP 헤더는 패킷 순서 정보를 포함한다[4].

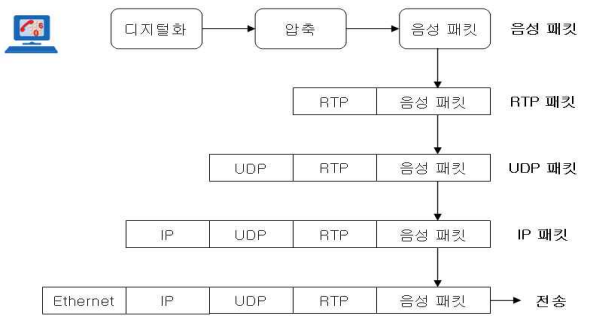

그림 2. VoIP 음성 처리 절차
Fig. 2. Voice Precess Procedure of VoIP

VoIP에서의 통화품질 저하 현상은 데이터 트래픽은 간할적이기는 하나 많은 양의 패킷이 집중적으로 전송하는 반면, VoIP 패킷은 음성의 실시간 전송 특성에 따라 짧은 시간(10~30ms)마다 작은 패킷(수십 바이트)을 주기적으로 전송한다. 이러한 패킷 분포는 전달하는 정보의 특성을 반영한 것으로서, 단순히 선입선출(FIFO)로 서비스 순서를 결정하는 시스템의 경우 데이터 패킷이 제시간에 처리되지 못하고 통화품질에 영향을 받을 정도의 지연을 겪을 수 있음을 보여준다.

2-3 VoIP 보안위협

VoIP 보안 위협은 IP 기반 망에서 발생할 수 있는 모든 보안 위협이 예상 가능하지만, 공격 가능성 및 피해 규모 등을 고려할 때, 도청, 서비스 거부 공격, 서비스 오용 공격, 세션 가로채기, VoIP 스팸으로 크게 분류 할 수 있다[5,6].

- 도청 : LAN 구간에 대한 도청, WAN 구간에 대한 도청, 단말기 도청
- 서비스 거부 공격 : 시스템 자원고갈, 회선자원 고갈, 해킹을 통한 시스템 장애
- 서비스 오용 공격 : 등록정보 변조, 관리상의 오류공격, 시스템 해킹을 통한 설정 변경
- 세션 가로채기 : Invite 세션 가로채기, SIP 하이잭킹
- VoIP 스팸 : Call 스팸, IM 스팸, Presence 스팸, 피싱
- 패스워드 취약점 : 스위치의 기본설정되는 로그인 및 패스워드(admin/admin, root/root 등) 사용에 따른 취약점으로 포트 감시를 통한 대화 도청 가능
- IP 주소 매핑 정보노출 : VoIP를 사용하는 다른 가입자의 식별번호(전화번호 등)를 알면 대상 장비에 호를 시도하고, 프로토콜 분석을 통해서 상대방 전화기의 IP 주소를 알수 있음.
- 웹 서버 인터페이스 : VoIP 교환기와 단말기는 원격관리를 위해 웹 서버 인터페이스를 갖는 경우가 많으나, 공격자에게 기밀 정보를 얻기 위해 평문 HTTP 패킷들을 가로챌 수 있는 빌미 제공.
- IP 전화기 넷마스크 취약성 : IP 전화기의 서브넷 마스크와 라우터 주소를 수정하여 장비가 보내는 패킷을 공격자의 MAC 주소로 송신할 수 있도록 할 수 있음.

Ⅲ. VoIP 정보보호 대책

3-1 VoIP 보안 적용시 고려사항

1) Qos : 방화벽 및 NAT 서버는 네트워크에서는 병목구간이 되는 경우가 많으며 VoIP와의 호환을 위하여 방화벽은 패킷 내부 검사작업을, NAT 서버는 빈번한 VoIP 패킷의 주소 변환 작업을 수행해야 한다. 이러한 동작은 또한 VoIP의 지연, 지터, 손실을 증가시키는 결과를 가져와 전체적인 통신품질을 저하시키며, 나아가 통화량이 증가하거나 악의적인 공격으로 인하여 호 요청 패킷들이 폭주하게 되면 서비스 거부로 이어질 수 있다. VoIP의 Qos 보장을 위해서는 방화벽 및 NAT 서버에서 Qos를 고려한 장비의 처리용량 업그레이드가 요구된다.

2) VoIPSec : VoIP 보안 서비스 제공을 위하여 IPSec을 적용할 경우에는 기밀성 및 인증을 위한 별도의 추가 헤더가 필요하며, 이로 인해 가뜩이나 낮은 VoIP의 실효 대역폭을 더욱 더 떨어뜨려 결국은 수십 바이트 음성 패킷을 전송하기 위해 수백 바이트의 헤더를 부가해야 하는 비효율적인 통신환경을 초래한다. 그리고 IP 헤더 내부의 정보가 암호화됨에 따라 Qos 지원 라우터가 RTP 패킷 특성을 확인할 길이 없어져 Qos 지원 라우터의 이점을 무력화 시킨다. 현재 이러한 문제들은 패킷 헤더의 압축 및 RTP를 대상으로 암호 및 인증 기능을 제공할 수 있는 SRTP 적용 등을 통해서 상당부분을 해결할 수 있지만, 아직은 많은 연구가 필요한 부분이다.

3) 전력 장애와 백업 시스템 : 기존 전화기는 전화선 자체에 공급되는 전원으로 동작되기 때문에 전력 장애가 발생하더라도 동작에 지장을 받지 않지만, VoIP 단말기는 별도의 전원이 필요하기 때문에 전력

장애는 곧 서비스 불가를 의미한다. 단말기 외에 IP PBX, 스위치 등의 장비에도 무정전 전원 장치를 설치하는 등의 별도의 고려사항이 필요하다.

3-2 VoIP 정보보호 대책

1) 안전한 네트워크 및 시스템 구축 : 사설 IP 망으로 구축하여 내부 VoIP 단말 및 시스템들에 대한 구성정보를 외부에 노출시키지 않는 기법을 적용하고, VLAN 적용을 통해 일반데이터망과 VoIP 망을 논리적으로 분리하여 VoIP 관련 트래픽 이외의 트래픽을 차단하는 기법을 적용한다. 또한, 미디어 채널에 대한 전송매체 공유되는 환경에서의 도청을 방지하기 위하여 더미 허브가 아닌 스위칭 장비를 적용한다. 미디어를 공유하는 경우 인터넷에 공개되어 있는 간단한 VoIP 음성통화 도청 프로그램이 설치된 컴퓨터를 통해 매우 쉽게 도청이 가능하기 때문이다.

2) VoIP 장비 접근제어 : VoIP 단말에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술을 적용한다. VoIP 단말기에서 수신하는 호설정을 위한 제어 메시지가 정당한 교환시스템으로부터 전송된 것인지 검증하기 위하여 교환시스템을 인증하고 그렇지 않은 트래픽은 차단한다. 그리고 통화를 하는 합당한 상대방으로부터의 트래픽은 허용하고, VoIP 단말기를 관리하기 위한 관리시스템이 정당한지 여부를 검증하기 위한 관리시스템을 인증하고 그렇지 않은 관리신호는 차단한다.

VoIP 교환시스템에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술로 인증을 우회하는 악의적 공격을 방지하기 위하여 발신자 및 발신경로를 인증하고 인가되지 않은 트래픽을 차단하고, 교환시스템 관리를 위한 관리시스템 및 원격 관리자의 트래픽은 허용한다. 네트워크 장비에 대한 악의적 공격자의 접근을 차단할 수 있는 접근제어 기술을 적용하는 방법으로 네트워크 장비 관리를 위한 관리시스템 및 원격 관리자의 트래픽은 허용하도록 한다.

송신자 IP 주소를 변조하여 공격패킷을 전송하는 스푸핑 공격을 차단하기 위해 스푸핑 패킷 차단 기술을 적용한다.

3) 네트워크 접근제어 : 사업자 네트워크에 대한 악의적 공격자의 접근을 차단할 수 있는 침입차단 기술을 적용하는 방법으로 일반적으로 알려진 공격을 수행하는 공격자 트래픽을 차단하고, VoIP 서비스에 대한 악의적 공격자 트래픽을 차단한다. VoIP 서비스가 활성화 됨에 따라, 교환시스템 및 VoIP 사용자를 대상으로 하는 공격이 증가할 것으로 예상되기 때문에 LAN, WAN 네트워크에 악의적 공격자의 접근을 차단할 수 있는 침입차단 기술을 적용한다.

LAN 네트워크에 정당한 사용자만이 데이터를 송수신할 수 있도록 MAC(Medium Access Control) 주소를 인증하고, 접근제어 할 수 있는 기술을 적용한다.

4) 네트워크 연동 구간 접근제어 : WAN 연동에 있어서 사업자간 상호 인가된 트래픽 이외의 데이터가 전송되지 않도록 접근제어 기술을 적용하고, VoIP 사업자간 인가된 호제어 메시지 이외의 데이터가 송수신되지 않도록 접근제어 기술을 적용한다.

3-3 VoIP 정보보안 권고사항

1) 음성과 데이터 네트워크를 각각의 서브넷 할당을 통해 논리적으로 분리하고, 각 서브넷에 별도의 DHCP 서버를 적용하면 데이터 침입탐지와 VoIP 방화벽 침해방지를 효율적으로 수행할 수 있다.

2) VoIP 게이트웨이는 데이터 네트워크로부터 유입되는 허가 받지 않은 VoIP 프로토콜을 수용하지 않기 위해 사용자에 대한 강력한 인증과 접근제어를 사용해야 한다.

3) 운용기관은 자신의 정보, 시스템 운용, 필수 기능들에 대한 자신의 지식과 훈련 수준, 보안 실행·제어·정책·구조에 대한 자신들의 성숙도 및 관련 보안 위협에 대한 자신들의 이해도에 맞추어 이러한 사항들을 조심스럽게 살펴야 한다.

4) 119 긴급 서비스 통신 등과 같은 특별 서비스를 고려해야 한다.

5) 정전 시에도 계속적인 운용을 보장하는 추가적

인 전력 백업 시스템에 대한 비용을 고려할 필요가 있다.

6) 보안이 중요한 환경에서는 일반 PC 기반 소프트폰 시스템을 사용하지 않아야 한다.

3-4 VoIP 정보보호를 위한 제안 구조

VoIP망의 보안체계를 구축하면 다음과 같이 네트워크 서버군 및 엑세스망에 보안시스템을 구축하고, 보안이벤트 발생, 트래픽 소통상황, 시스템 자원 사용을 탐지 및 모니터링하여 종합적으로 분석 및 대응할 수 있는 통합보안관리시스템(ESM)의 구축이 필요할 것이다.

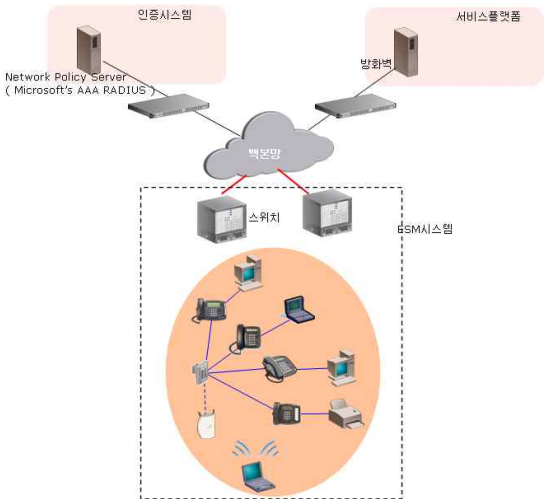

그림 3. VoIP 보안체계 구축
Fig. 3. VoIP Security System Construction

Ⅳ. 결 론

공중전화망과 유·무선 인터넷의 연동이 가능한 인터넷전화 서비스의 피해 파급력은 단일망을 넘어서 통합망에 이르기까지 피해가 확산될 수 있으며 음성 패킷의 전달은 양단간 전화 서비스의 흐름이란 점에서 통화내용이 불법적으로 노출 되는 것을 방지하기 위한 기술 개발의 필요성이 대두되고 있다.

본 논문에서는 VoIP 기술의 개념과 보안적용시 문제점과 대책에 대하여 살펴보았다. VoIP 서비스 사업자들은 보안에 대한 깊은 고려 없이 서비스를 제공하고 있는 실정이기 때문에 보안을 적용하기 위해서는 더욱더 신중한 검토가 선행되어야하고, VoIP 서비스의 다양한 정보보호 대책과 연구가 필요하다.

참 고 문 헌

[1] 국가사이버안전센터, "VoIP를 이용한 인터넷 전화의 이해와 보안대책", NCSC-TR050018

[2] 정보통신부, "VoIP 정보보호 가이드라인", 2006.12.

[3] Time Green and Phil Hochmuth, VoIP security a moving target, Network World, 2004. 10.

[4] Li C, Li S, Zhang D, and Chen G, "Cryptanalysis of a data security protection scheme for VoIP," *IEE Proceedings Vision,Image and Signal Processing,* Feb. 2006.

[5] Steven M. Bellovin, Susan Landau, Matt Bla, "The real national-security needs for VoIP," *Communications of the ACM*, Nov. 2005.

[6] S. Chatterjee, B. Tulu, T. Abhichandani, and Haiqing Li, "SIP-based enterprise converged networks for voice/video-over-IP: implementation and evaluation of components," *IEEE Journal on Selected Areas in Communications,* Oct. 2005.

[7] 구자현, "VoIP서비스 보안 취약성 분석", *한국정보보호학회지,* 제 16권 1호, pp.59~63, 2006.

[8] 박진범 외, "VoIP 보안 취약점 공격에 대한 기존 보안 장비의 대응 분석 연구", *한국정보보호학회 논문지,* 제 17권 5호, pp.57~65, 2007.

[9] 성경, "네트워크 보안성 측정방법에 관한 연구", *한국항행학회 논문지,* 제 11권 1호, pp.79~86, 2007.

[10] 김태훈 외, "중요 정보시스템 위협원에 대한 분석", *한국항행학회 논문지,* 제 11권 2호, pp.203~208, 2007.

성 경(成 鏡)

2003년 한남대학교 컴퓨터공학과 (공학박사)
1994년~2004년 동해대학교 컴퓨터공학과 교수
2004년~현재 목원대학교 컴퓨터교육과 교수
관심분야 : 정보보호 및 정보관리, 컴퓨터네트워크, 신경회로망, 컴퓨터교육

김 석 훈 (金錫勳)

2003년 2월 : 한남대학교 컴퓨터공학과(공학석사)
2006년 8월 : 한남대학교 컴퓨터공학과(공학박사)
2007년 1월~현재 : (주)파라곤베이스 기술마케팅 이사
관심분야 : 모바일 컴퓨팅, VoIP, XML, 웹DB, 정보보호