主題

인터넷전화 서비스를 위한 보안기술

대구가톨릭대학교 컴퓨터정보통신공학부 교수 전 용 희

차 례

1. 서 론

인터넷전화 서비스를 제공하기 위한 대표적인 기술이 VoIP(Voice over Internet Protocol)이다. VoIP 기술에 의한 전화 서비스는 기존의 PSTN(Public Switched Telephone Networks) 서비스에 비하여 경제적이고, 향후 멀티미디어 서비스 지원 등의 특징을 가지기 때문에 보급의 확산이 기대된다. VoIP 기술은 유선에서 뿐만 아니라, 무선에서도 VoIP 기술을 채택하여 유무선 통합의 핵심기술로서 IETF, ITU 등에서 작업이 추진되고 있다[1]. 이와 같이 VoIP 서비스의 확대가 예상됨에 따라 사용자의 인증, 메시지 보호 등 보안 서비스의 중요도가 증대되고 있다[2].

VoIP 서비스가 비즈니스 애플리케이션으로 사용될 때, 고객과 비즈니스 동료와 대화할 수 있는 능력은 비즈니스의 주요 요구사항 이상으로 중요하다. 따라서 VoIP 시스템이 동작하는 것을 보증하는 동시에, 보안은 절대적인 요구사항이다. 인터넷전화 시스템이 바이러스와 해커 공격에 의하여 정지될 수 있기 때문에 네트워크 상의 위협이 서버-기반 IP 사설 교환기를 이용하는 사업자들에게는 큰 문제가 된다. 그러므로 VoIP를 이용한 인터넷전화 서비스를 안전하게 제공하기 위해서는 보안 문제가 하나의 큰 선결과제라 할 수 있다.

국내에서도, 정보통신부 산하 인터넷텔레포니 포럼(VoIP포럼)이 VoIP 보안문제 해결을 위해 노력하고 있다. VoIP 보안 연구반은 SIP(Session Initiation Protocol)의 보안 부분을 중점적으로 연구하고 방화벽과 NAT(네트워크 주소 변환) 장애를 해결하는 방법 및 기밀성 보호방안 등에 대하여 연구를 진행하고 있다[3,4].

본고에서는 VoIP 시스템에서 발생할 수 있는 보안 문제와 표준화 동향 등을 간단히 알아보고, SIP 보안 메커니즘에 대하여 기술하고, 사례 연구로 시스코 사와 체크포인트 사의 VoIP 보안

솔루션을 소개하고자 한다[5,6].

2. 보안 문제

2.1 개요

VoIP 시스템에서, SIP는 세션 설정을 위한 신호 프로토콜이다. 본고에서는 먼저 SIP-기반 음성 네트워크에서 직면하고 있는 여러 가지 네트워크 보안 위협들을 알아본다. 인터넷전화 서비스를 위한 네트워크 상에서, VoIP 네트워크 보안은 다음과 같은 두 가지의 문제를 포함한다.

- 음성 패킷 보안: 애플리케이션 문제에 초점을 둔다.
- IP 보안: 네트워크 혹은 트랜스포트 문제에 초점을 둔다.

인터넷 전화망에서 SIP 전개는 광범위한 네트워크 보안 위협과 공격에 노출된다. SIP 기반 네트워크에 대한 위협으로는 두 가지가 있다: 외부 위협과 내부 위협. 외부 위협은 SIP-기반 호(call) 기간 동안의 메시지 흐름에 참가하지 않는 누군가에 의하여 시작되는 공격이다. 음성과 신호 패킷이 비신뢰 경계를 지나거나, 호 트래픽이 장치 간에, 혹은 참가자 사이에 전달될 때 제 3의 네트워크를 포함하는 경우, 외부 위협이 보통 발생한다. 내부 공격은 SIP 호 참가자에 의하여 보통 개시되기 때문에 훨씬 더 복잡하다.

표 1은 일반적인 네트워크 및 애플리케이션 레벨 보안 문제점을 포함하여 여러 가지 위협을 보여준다[6].

위와 같은 보안 문제를 해결하기 위하여, 다양한 제안들이 표준화 단체에서 논의되고 있는데, 주요한 VoIP 보안 관련 표준은 다음과 같다.

- ITU-T H.323: 패킷-기반 멀티미디어 통신 시스템
- ITU-T H.235: H-시리즈 멀티미디어 터미널을 위한 보안과 암호화
- IETF RFC 2543: SIP(Session Initiation Protocol)
- IETF RFC 2543 bis-09: 보안 위협과 메커니즘 기술
- ETSI Tiphon* 보안 프레임워크(*2003년 9월부로 Tispan으로 변경됨)
- 기타 ANSI(American National Standard Institute) 등

2.2 H.323 보안 문제

H.323은 인터넷을 포함한 IP-기반 네트워크 사이의 오디오, 비디오, 데이터 통신을 위한 기초를 제공한다. H.323은 H.225-RAS, Q.931, H.245 RTP/RTCP와 오디오 코덱(G.711, G.723.1 등), 비디오 코덱(H.261, H.263)의 부분들을 포함한다. 미디어 스트림은 RTP/RTCP 상으로 전송되며,

〈표 1〉 네트워크 보안 공격 형태, 문제점 및 솔루션

공격 형태	문제점	솔루션
서비스 거부 공격	인증되지 않은 패킷으로 SIP 프락시 서버나 음성 게이트웨이 장치를 공격하여 서비스 접근 방해	DoS 공격을 예방하기 위한 장치 구성
도청	음성 패킷이나 RTP 미디어 스트림의 비인가된 가로채기 및 신호 메시지의 디코딩	Secure RTP 같은 암호화 기법을 사용 전송 데이터 암호화
패킷 스푸핑	데이터를 전송하는 합법적인 사용자로 가장	호 참가자 사이에 주소 인증을 전송
재생	진짜 메시지의 재전송	암호화 및 메시지 번호 매기기
메시지 무결성	메시지가 전송 도중에 변경되지 않음을 보장	HTTP 다이제스트를 사용 메시지 인증

RTP는 실제 미디어를 운반하고 RTCP는 상태와 제어 정보를 운반한다. 신호 정보는 TCP 상으로 신뢰성 있게 전송된다. RAS(Registration, Admission, and Status), Q.931(호 설정과 종료 관리), H.245(채널 사용과 능력 협상), H.235(보안 및 인증 관리)는 신호를 다루는 프로토콜이다.

이와 같이 H.323은 복잡하며, 동적 포트를 사용하고 복수의 UDP 스트림을 포함한다. 인텔에 의하여 수행된 광범위한 연구에 의하면 H.323의 주요한 보안 관련 문제는 다음과 같다[5]:

- 한 개의 H.323 호는 많은 다른 동시 연결을 가지고 있다. 적어도 두 개의 연결은 TCP이다.
- 한 개를 제외하고 모든 연결은 단명의(동적) 포트에 만들어진다.
- 호는 방화벽 내부와 외부로부터 시작될 수 있다. 컨퍼런스 호를 만들기 위하여, 외부 사용자는 내부 사용자의 데스크톱 시스템과 직접 호를 설정할 필요가 있다.
- 주소와 포트 번호는 다음 상위 연결의 데이터 스트림 내에서 교환된다. 예를 들어, H.245 연결을 위한 포트 번호는 Q.931 데이터 스트림 내에서 확립된다. 이것이 데이터 스트림 내의 주소를 수정해야 하는 주소 번역 방화벽에게 특히 어렵게 만든다. 더욱 문제를 어렵게 만드는 것은, 예를 들어 Q.931 안에서 H.245 연결이 안전해야(암호화되어야) 한다는 것을 기술하는 것이 가능하다.
- 대부분의 제어 정보는 ASN(Abstract Syntax Notation).1로 부호화된다. Q.931 PDU(Protocol Data Unit) 안의 단지 사용자-사용자 정보만이 ASN.1로 부호화되고, 모든 Q.931 PDU의 다른 부분은 부호화되지 않는다. ASN.1은 주소 정보를 위하여 고정된 바이트 오프셋으로 끝나지 않기 때문에, 동일한 목적지에 연결하는 동일 애플리케이션의 동일 버전도 바이트 오프셋을 변경하며 다른 옵션을 포함하기 위하여 협상할 수 있다.

또한 stateful inspection을 위하여 방화벽에서는 패킷을 분해(disassemble)할 수 있는데, 제어 스트림의 ASN.1 부호화로 패킷의 분해가 쉽지 않게 된다. 여기서 stateful inspection 방식은 패킷 헤더 안의 출발지, 목적지 주소 정보와 포트 번호 뿐만 아니라, 패킷의 내용까지를 보고 훨씬 더 정교하고 복잡한 검사를 수행하는 패킷 필터링 방법이다.

3. SIP 보안 메커니즘

SIP을 위하여 필요한 기본적인 네트워크 보안 서비스는 <표 1>에서 기술한 것과 같이, 메시지의 비밀성과 무결성을 유지하고, 재생 공격이나 메시지 스푸핑을 방지하고, 세션 참가자의 인증과 비밀성을 제공하고, 서비스 거부(DoS: denial of service) 공격을 방지하는 것이다. SIP은 어떤 민감한 헤더 필드 및 메시지 몸체의 흡별 및 종단간 암호화를 위하여 여러 가지 보안 메커니즘을 제공한다. 어떤 메커니즘들은 HTTP 인증이나 신뢰 연결장치의 다른 변종을 포함하여, 프로토콜에 구축된다.

트랜스포트나 네트워크 계층 보안은 메시지 기밀성과 무결성을 보장하기 위하여, SIP 신호 트래픽을 암호화한다. IP 보안(IPSec)은 트랜스포트 계층 보안을 제공하는 네트워크 보안 메커니즘이다.

3.1 인증

SIP 사용자-에이전트 클라이언트를 포함하는 호 동안, 공격자는 클라이언트의 실제 신분을 위

조하여 사용자로 가장할 수 있다. 인증(authentication)은 사용자 혹은 클라이언트가 합법적인지 검증하기 위한 메커니즘을 제공한다. SIP 네트워크에서는, 인증이 사용자 에이전트와 프락시 사이에서 발생할 수 있다. 여기서 프락시 서버는 자신으로부터 "invite" 메시지를 처리하기 전에 사용자 에이전트가 인증할 것을 요구한다. 비슷하게, 사용자 에이전트는 프락시의 인증을 요구하거나 서버를 변경(redirect)할 수 있다.

SIP은 인증에 사용될 헤더를 정의한다. 권한검증(authorization) 헤더는 SIP 메시지의 컴포넌트 간 계산된 서명을 포함한다. 이 헤더는 프락시 사이를 통과하면서 변화하지 않으며, 다음으로 구성되어 있다: 논스(nonce), 영역(realm), 요구 방법(사용자-에이전트 클라이언트에 의하여 발송되는 요구 메시지의 형태), 요구-방법 버전 및 권한검증 형태. 또한 프락시에게 자신을 식별하기 위하여 SIP 사용자 에이전트에 의하여 사용되는 프락시-권한검증 헤더가 있다. 이것은 인증 형태, 사용자 에이전트의 신용장(credential), 혹은 요구되는 자원의 영역을 포함한다.

3.2 권한검증

일단 인증이 이루어지면, 해당 신분(ID)이 요구하는 서비스를 사용하는 것이 허용되는지를 결정해야 한다. 신뢰적인 인증에도 불구하고, 파티가 요구하는 서비스의 전부 혹은 일부를 사용할 허가를 가지지 않을 수 있으며, 추가적인 권한검증이 요구된다.

3.3 IPSec

IPSec은 IP 계층에서 보안 기능, 인증 및 암호화를 제공한다. 세 개의 프로토콜이 IPSec 구현에 사용 된다:

- 암호화 보안 페이로드(ESP: Encapsulating Security Payload) 프로토콜: 선택적인 인증과 재생-탐지 서비스를 가진 데이터 기밀성과 보호를 제공하는 보안 프로토콜이다. ESP는 사용자 데이터를 완전히 캡슐화 한다. ESP는 독자적으로나 인증 헤더와 결합하여 사용될 수 있다[7].
- 인증 헤더(AH: Authentication Header) 프로토콜: AH는 패킷 인증 서비스를 제공하며, 독자적으로나 ESP와 함께 사용된다[8].
- 인터넷 키 교환(IKE: Internet Key Exchange) 프로토콜: IKE는 키를 요구하는 서비스를 위하여 공유 보안 정책과 인증키를 확립하기 위하여 사용된다. 어떤 IPSec 트래픽이 통과될 수 있기 전에, 모든 라우터, 방화벽이나 호스트는 피어(peer)의 신원을 검증할 수 있어야 한다. 이것은 양 호스트에 사전에 공유된 키를 수동적으로 넣거나, 인증기관(CA) 서비스, 혹은 DNS(Domain Name System) 보안을 통하여 가능하다[9].

IPSec은 네트워크 암호화 및 인증을 수행하기 위하여 많은 옵션들을 제공한다. 모든 IPSec 연결은 암호화, 무결성 및 인증성(authenticity)을 제공할 수 있다. 보안 서비스가 결정될 때, 두 통신 노드는 암호화를 위하여 DES(Data Encryption Standard) 같은 암호화 알고리즘, 무결성을 위한 안전한 해시 알고리즘(SHA: Secure Hash Algorithm)과 같은 사용하고자 하는 알고리즘을 결정하여야 한다. 알고리즘에 대하여 결정한 후, 두 장치는 세션키를 공유하여야 하며, 두 VoIP 엔티티 사이에 보안연계(SA: Security Association)가 확립되어야 한다.

4. 사례 연구

4.1 시스코

시스코(Cisco) 사의 VoIP 인프라 솔루션은 전화 서비스를 제공하기 위하여 SIP를 이용한 voice-over-packet 네트워크 설계가 특징이다. SIP 기반 voice-over-packet 네트워크를 구현하기 위하여, SIP 지원 IP 전화기, 시스코 IOS(Internetwork Operating System)를 수행하는 SIP-실행 게이트웨이, 소프트웨어, SIP 프락시 서버 및 방화벽을 포함한다. 이런 컴포넌트들은 기존 전화망과 통합될 수 있는 SIP-기반 VoIP 솔루션을 제공하기 위하여 함께 동작한다.

4.1.1 SIP-실행 VoIP 제품상의 보안 특성

(1) SIP 프락시 서버

SIP 프락시 서버는 인증, 권한 검증 및 IPSec을 지원한다. SIP 프락시 서버는 외부 RADIUS(Remote Authentication Dial-In User Service) 서버나 프락시 자체에서 인증을 제공하기 위하여 구성될 수 있다. 프락시는 적절한 RADIUS 서버와 결합하여 세 가지 형태의 인증 메커니즘을 지원 한다:

- CHAP(Challenge Handshake Authentication Protocol) 패스워드 인증
- HTTP 다이제스트 인증
- HTTP 기본 인증

CHAP-패스워드 인증은 인증자(authenticator)와 그 피어에게만 알려진 "비밀" 키에 의존한다. CHAP은 점차적으로 변하는 식별자와 가변 수하값(challenge value)의 사용을 통하여 피어에 의한 재생 공격에 대하여 보호를 제공한다. 반복되는 수하의 사용은 어떤 단일 공격에 노출되는 시간을 제한하기 위함이다.

프락시는 HTTP 다이제스트 인증과 HTTP 기본 인증을 지원한다. 두 개의 인증 메커니즘은 RFC 2617에 기술된 것과 같이 수행된다[10]. 외부 RADIUS 서버와 결합하여, CHAP-패스워드 인증이 지원된다. HTTP 다이제스트 인증을 사용하여, 패스워드는 네트워크 사이에 평문으로 절대로 전송되지 않고, 사용자 패스워드의 MD5(Message Digest 5) 다이제스트로 항상 전송된다. 이렇게 하여, 네트워크 상의 스니핑 트래픽은 패스워드를 식별할 수 없다. RADIUS-지원 인증을 위하여, SIP 사용자-에이전트 클라이언트(UAC: user-agent client) 패스워드는 RADIUS 서버에 저장된다. 프락시-지원 인증을 위하여, UAC 패스워드는 MySQL 데이터베이스 안의 가입자 테이블에 저장된다.

(2) 인증과 권한검증

SIP 프락시 서버에서 수행되는 디폴트 인증 스킴은 HTTP 다이제스트 인증이다. SIP 프락시 서버가 HTTP 기본 인증을 지원하나, 안전한 인증 메커니즘으로는 권고되지 않는다. 프락시에서 수행되는 인증 메커니즘은 MySQL 데이터베이스를 질의(query)하기 위한 키로 권한검증 헤더나 프락시-권한검증 헤더에서 찾아진 사용자 이름을 사용한다. 만약 RADIUS 서버가 인증을 수행하기 위하여 사용된다면, 사용자 이름이 SIP 프락시 서버에서 RADIUS 서버까지 속성 값 쌍의 하나로 전달된다.

인증된 사용자는 자동으로 권한검증 되며, SIP 프락시 서버에서 추가적인 권한검증 단계는 수행되지 않는다.

(3) 접근 목록

구성(configuration) 파일내의 SIP 프락시 서버 접근 통제 디렉티브(directive)가 서버에 대한 접근을 결정한다. 다양한 기준에 따라서 접근이 허가 또는 거절될 수 있다. SIP 프락시 서버 구성 파일내의 허용(Allow) 및 거절(Deny) 디렉티브가 클라이언트의 호스트명이나 호스트 주소에 기반하여 서버에 대한 접근을 허용하거나 거절한

다.

- Allow: 어떤 호스트가 서버의 영역을 접근 가능한지 결정한다. 접근은 호스트명, IP 주소, IP 주소 범위, 혹은 환경 변수에서 포획된 클라이언트 요구의 다른 특성에 의하여 통제될 수 있다. 서버 접근에 대하여 특정 호스트나 호스트 그룹을 허용하기 위하여, 호스트는 다음의 포맷 중에서 기술될 수 있다: (부분적) 도메인 이름, 완전한 IP 주소, 부분 IP 주소, 네트워크/넷마스크 쌍, 네트워크 CIDR(Classless Inter-Domain Routing) 사양서.
- Deny: 호스트명, IP 주소, 혹은 환경 변수에 기초하여 제한을 가지고 서버에 대한 접근을 허용한다. 인수는 Allow의 인수와 같다.
- Satisfy: 두 가지 형태의 접근 통제(허용 및 거절) 및 인증 조사를 위한 접근 정책을 결정한다. 파라미터는 "all" 혹은 "any"이다. 만약, "all"이 기술되면, 전송 호스트는 "허용"되고 인증된다. 만약 "any"가 기술되면, 전송 호스트가 접근 통제 "allow"나 인증 조사를 통과하면 접근이 허락된다.
- Order: 기본 접근 상태와 허용과 거절 디렉티브가 평가되는 순서를 제어한다. 유효한 순서로는 다음과 같이 세 가지가 있다: 거절-허용, 허용-거절, 상호 실패.

다음의 예에서, company.com 도메인은 접근이 허용되고, 모든 다른 호스트는 접근이 거절된다. 예: Order Deny, Allow/ Deny from all/ Allow from company.com

(4) IP 보안

비보호 혹은 비신뢰 네트워크 상으로 VoIP 트래픽과 같은 민감한 정보 전송을 위하여, IPSec은 IPSec 장치나 피어 사이에 교환되는 IP 패킷들을 보호하고 인증하는 네트워크 계층 보안 프로토콜로써 동작한다. IPSec은 IPSec 피어 장치 사이의 보안 연계를 설정하기 위하여 두 가지 방법의 키 관리를 제공 한다:

- 수동 키잉: 키는 관리자에 의하여 수동으로 설치되거나 배치된다. 수동 키잉은 공격자가 프락시 서버나 게이트웨이의 통제권을 얻거나. 보안 구성 파일을 읽을 수 있거나, 트래픽 교환에서 사용된 키에 대한 접근을 얻을 수 있는 공격에 취약하다.

〈표 2〉 SIP-실행 IP 전화기의 네트워크 보안 문제점

보안 관심사	솔루션
TFTP(Trivial FTP) 도청: SIP 전화기는 TFTP 요청이 구성 파일과 펌웨어 이미지를 다운로드하도록 한다. TFTP는 파일이 암호화되지 않은 채로 전송되기 때문에 안전하지 않다.	방화벽으로 보호되는 TFTP 서버를 이용하여 방화벽을 통하여 FTP 요청을 한다.
DHCP(Dynamic Host Configuration Protocol) 스푸핑: SIP 전화기는 DHCP 요청으로 IP 주소, 게이트웨이, 부트 서버 등을 얻도록 한다.	안전한 DHCP 서버가 방화벽 뒤에서 보호된다. 정적 IP 전화 주소기법은 안전하다.
비암호 RTP 미디어 스트림	안전한 IPSec VPN 터널링
Telnet	전화기 구성파일 안에서 Telnet을 불가능하게 하거나 이 특권을 네트워크 관리 워크스테이션에만 허용한다.
인증과 권한검증	전화기와 SIP 프락시 서버 사이 HTTP 다이제스트를 통하여 이루어 질 수 있다. SIP IP 전화기는 INVITE, BYE, CANCEL과 같은 방법을 인증할 수 있다.

· 자동 키잉: 키가 IKE 프로토콜을 사용하여 보안 연계를 형성하는 장치사이에 협상된다. 자동 키잉은 수동 키잉보다 훨씬 더 안전하다. 자동 키잉은 연결을 중지하거나 관리자 간섭의 필요 없이 몇 시간마다 혹은 몇 분마다 변경될 수 있다.

4.1.2 SIP-실행 IP 전화기

표 2는 SIP-실행 IP 전화기를 관리하는데 있어서의 보안 관련 사항이다[6].

4.2 체크포인트

본 절에서는 체크포인트(Check Point)사의 VoIP 보안 특징을 제시한다. VoIP 연결을 안전하게 만들기 위하여 방화벽을 위한 위치는 여러 가지가 가능한데, 게이트키퍼, 터미널 혹은 게이트웨이를 보호할 수 있게 위치할 수 있다. 터미널 클라이언트는 보호 지역이나 다른 비신뢰 네트워크에 위치할 수 있다. VoIP 호는 많은 연결로 이루어져 있다. 방화벽은 어떤 다른 파티 사이에도 위치할 수 있다. 중요한 문제는 연결의 상황을 이해하는 것이다. 이것은 데이터 및 신호 연결을 포함한다.

체크 포인트 구조는 QoS(Quality of Service) 솔루션과 VoIP 보안 특성을 통합하는 것을 허용하고 있다. FloodGate-1은 VPN(Virtual Private Network), 사설 WAN과 인터넷 링크를 위한 정책-기반 QoS 솔루션이다. VoIP를 위하여 LLQ(Low Latency Queueing)라고 하는 메커니즘을 채택하여 고정 비트율 애플리케이션을 위하여 가장 좋은 지연을 얻도록 한다. 체크 포인트 게이트웨이를 사용함으로써 DOS 공격과 호 hijacking 등의 공격을 방지할 수 있음을 보여주고 있다[5].

4.2.1 H.323용 방화벽 보안 특징

방화벽은 H.323 기반 프로토콜을 위하여 다음과 같은 동작을 수행 한다:

· H.323 메시지의 해석(parsing)이 방화벽 커널에서 수행된다. 이것은 다음을 포함 한다: H.225 RAS 메시지 해석, Q.931 메시지 안의 설정 및 연결 명령 해석, H.245 프로토콜 명령 해석
· Fast start 명령 해석, H.225 메시지 안의 H.245 캡슐화
· H.323 신호 문맥과 H.245에 기초하여 열린 RTP/RTCP 포트 상의 stateful inspection 동작 수행.

방화벽은 H.225 Q.931 포트를 동적으로 개방한다. 이 이벤트에서 방화벽은 동적 포트 할당의 기본 동작 훨씬 이상으로 보안 제한을 시행 한다:

-제어-데이타 연결 관계성 항상 시행
-H.323 서비스는 한 가지 형태의 연결이 다른 것과 서로 독립적으로 존재하는 것을 허용하지 않는다. 시스템은 제어 연결 안에 어떤 데이터 연결을 위한 협상이 보이지 않으면 그 연결을 개설(open)하는 것을 허용하지 않는다.

· 방화벽은 게이트키퍼의 직접 및 간접 라우팅 모드를 지원함으로써, 네트워크 구조에서 높은 레벨의 융통성을 허용하고 있다:
  - Direct(RAS 메시지만)
  - 호 설정(Q.931)
  - 호 설정 및 호 제어(Q.931과 H.245)
· 게이트웨이 지원 라우팅 모드:
  - 호 설정(Q.931)
  - 호 설정 및 호 제어(Q.931과 H.245)
· 신호의 다른 부분은 다른 엔티티에 의하여 행해지기 때문에, 방화벽은 핸드오버 도메인 상에서 보안 제한을 시행한다. 방화벽은 비-VoIP 통신을 허용하기 위하여 신호 프로토

콜의 변경(redirection) 능력을 남용하는 가능성을 없앤다.

H.323 로깅으로 다음과 같은 로그를 생성 한다:

- 호(call) 로그: 모든 로그 항목은 각 메시지의 호 로깅과 전화번호를 포함하여, IP 소스와 목적지, H.323 프로토콜 형태를 포함한다.
- 설정 메시지 로그(H.225, Q.931)
- 등록 로그(H.323 전화 번호 포함)
- 상세한 기술과 함께 거절(reject) 로그

4.2.2 SIP용 방화벽 보안 특징

방화벽은 SIP VoIP 세션을 위하여 다음과 같은 보안 옵션을 제공 한다:

- 규칙-기반 SIP 지원
- 멀티미디어 형태와 관련 미디어 포트를 결정하기 위한 SIP 헤더 해석 능력
- SDP 헤더에 지시된바와 같이 RTP/RTCP 포트를 열고 그런 연결의 상태를 모니터할 능력
- SIP 서비스는 항상 제어-데이터 연결 관계성을 실행한다. SIP 서비스는 한 형태의 연결이 다른 것과 독립적으로 존재하는 것을 허락하지 않는다. 이것이 빌링(billing) 프로세스의 보안과 무결성을 보증한다.
- RFC에 의한 SIP 프로토콜 호 흐름을 검정하며, 상태 외 SIP 메시지를 탈락시킨다.
- SIP 핸드오버 도메인 객체를 정의할 수 있는 능력으로, 비-VoIP 통신을 허용하기 위하여 신호 프로토콜의 변경 능력을 남용할 가능성을 없앤다.
- 광범위한 SIP 프로토콜 특성 집합을 취급한다 : re-invite 메시지, hold, 및 Call conference

SIP 로깅으로 다음과 같은 로그를 생성 한다:

- 호(call) 로그: 모든 로그는 SIP URL과 전화번호를 포함한다.
- 등록 로그(SIP URL 포함)
- 상세한 기술과 함께 거절(reject) 로그

5. 맺음말

VoIP 트래픽의 양이 전통적인 회선 교환기에서 차세대 소프트 스위치로 이동함에 따라서 엄청나게 증가되고 있다. VoIP 기술로 부가-가치 서비스가 상대적으로 쉽게 제공될 수 있고, 비용 절약의 장점이 증명됨으로써 산업계에서 VoIP 장비의 빠른 구축을 위한 주도적인 힘으로 작용될 것이다.

VoIP 기술에 대하여는 많은 기술적인 논의가 있어 왔어나, VoIP 기술의 보안 측면은 완전하게 연구되지 못한 상태에 있다. 여기에는 여러 가지 이유가 있다: 첫째는 VoIP가 낮은 가격에서 값싼 장거리 전화 서비스를 제공하기 위하여 주로 사용되어 왔으며, 소비자들은 보안 문제보다는 음성 품질에 더욱 관심을 가져왔다. 둘째는 인터넷 기술이 발전함에 따라서 보안 기술도 여전히 변하고 있고, 시장에서는 다른 제조사로부터의 다른 제품과 솔루션들이 있어, 유일한 보안 표준을 구현하는 것을 어렵게 만든다는 것이고, 마지막으로 개방된 IP 환경에서 공격 유형을 예측하고 VoIP 네트워크와 컴포넌트의 보안을 관리하는 것이 어렵다는 것이다[11].

이러한 맥락에서 VoIP 네트워크에서 보안 문제와 기술에 대한 국내 연구가 필요하다고 사료된다. 주요 연구 분야로는 정보보증(IA: Information Assurance), 취약성 시험, 인터넷 인프라 보안 영역 등이 있겠다.

참 고 문 헌

[1] 강태규, 김도영, 김봉태, "유무선 통합 네트워크에서의 VoIP를 위한 공통 논리 기능 구조 분석", 전자통신동향분석, 제 17권 제 5호, pp.47-54, 2002년 10월.

[2] 임채훈, "VoIP 시스템에서의 보안기술", (주) 퓨처시스템 자료.

[3] 국내 기술정책동향, VoIP 포럼, http://www.kisa.or.kr/K_trend/KisaNews/200112/infosec_trend_in.html

[4] 정수환, 차세대 VoIP 보안 구조 및 프로토콜 (프리젠테이션 자료), 2002. 4.25.

[5] Check Point NG FP2, VoIP Security white paper, VoIP Security Features.

[6] Cisco Systems, White Paper, Security in SIP-Based Networks.

[7] RFC 2406,IP Encapsulating Security Payload, Nov. 1998, http://www.ietf.org/rfc/rfc2406.txt?number=2406

[8] RFC 2402, IP Authentication Header, Nov. 1998, http://www.ietf.org/rfc/rfc2402.txt?number=2402

[9] RFC 2409, The Internet Key Exchange, Nov. 1998, http://www.ietf.org/rfc/rfc2409.txt?number=2409

[10] RFC 2617, Proxy Chaining and Policy Implementation in Roaming, June 1999, http://www.ietf.org/rfc/rfc2617.txt?number=2617

[11] Call for papers, The first International Workshop on Security in VoIP Networks, SVoIPNet 2004. To be held in Aug.2004, Portugal.

전 용 희

1971. 3~1978.2 고려대학교 전기공학과

1985. 8~1987.8 미국 플로리다공대 대학원 컴퓨터공학과

1987.8~1992.12 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사

1978. 1~1978.11 삼성중공업(주)

1978.11~1985.7 한국전력기술(주)

1989.1~1989.6 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA

1989.7~1992.9 미국 노스캐롤라이나주립대 부설 CCSP(Center For Comm. & Signal Processing) RA

1992.10~1994.2 한국전자통신연구원 광대역통신망연구부 선임연구원

1994.3~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수

2000.1~현재 한국통신학회 학회지 편집위원

2001.3~2003.2 대구가톨릭대학교 공과대학장 역임

2004.2~현재 한국전자통신연구원 정보보호연구단 초빙연구원

관심분야 : 네트워크 보안, 통신망 성능분석, QoS 보장 기술