韓國 컴퓨터情報學會 論文誌
第11卷 第4號, 2006. 9.

2006-11-4-1-18

VoIP 서비스의 도청 공격과 보안에 관한 연구

박 대 우*, 윤 석 현**

A Study about Wiretapping Attack and Security of VoIP Service

Dea-Woo Park*, Seok-Hyun Yoon**

요 약

Ubiquitous-IT839전략 중에 8대 신규서비스에 VoIP 기술이 들어있다. 본 논문은 VoIP 인터넷 네트워크에 연결된 소프트폰과 LAN 구간과 연결된 인터넷전화 및 디바이스, IP PBX, 기간사업자 망이 연결된 WAN 구간에서의 VoIP 서비스의 도청 실험을 하였다. 실험 네트워크에서 도청 실험을 한 결과 CVE 리스트에 따르는 단말기와 Proxy 및 허브와 같은 VoIP 네트워크의 연결점에서의 취약점이 발견되었고, 해커의 공격에 의한 도청이 성공되었다. 현재 070으로 명명된 VoIP 네트워크에서 각 도청 구간별로 접근제어, 기밀성, 신뢰성, 가용성, 무결성, 부인봉쇄의 6가지 보안기능의 관점에서 도청의 보안방안을 적용하였다. 보안 방안의 적용 후에 도청 실험을 실시한 결과, 패킷에 대한 AES 암호화로 내용의 도청을 방지하였으며, 접근차단과 인증 및 메시지 해시함수 및 착신거절의 사용으로 도청을 예방하였고, 네트워크 모니터링과 감사기록으로 보안성과 감사기록을 유지하여 VoIP 정보보호를 이룩할 수 있었다.

Abstract

VoIP technology is Eight New Services among Ubiquitous-IT839 strategies. This paper tested wiretapping of VoIP service in connected a soft phone and LAN and WAN sections, Internet telephones and a device, IP PBX, a banner operator network to have been connected to VoIP Internet network. As a result of having experimented on wiretapping of VoIP networks, Vulnerability was found, and a wiretapping by attacks of a hacker was succeeded in a terminal and Proxy and attachment points of a VoIP network like a hub to follow a CVE list. Currently applied a security plan of an each wiretapping section in viewpoints of 6 security function of Access Control, Confidentiality, Authentication, Availability, Integrity, Non-repudiation in VoIP networks named to 070. Prevented wiretapping of contents by the results, the AES encryption that executed wiretapping experiment about a packet after application of a security plan. Prevented wiretapping, and kept security and audit log, and were able to accomplish VoIP information protection to network monitoring and audit log by an access interception and qualification and message hash functions and use of an incoming refusal.

▸ Keyword : Hacker Attack, SIP, VoIP Security, Vulnerability, Wiretapping

---

• 제1저자 : 박대우
• 접수일 : 2006.08.05, 심사일 : 2006.09.11, 심사완료일 : 2006.09.22
* 숭실대학교 정보과학대학원 정보보안학과, **청강문화산업대학 컴퓨터소프트웨어과

Ⅰ. 서 론

대한민국은 Ubiquitous-IT Korea의 완성이란 목표를 가지고, IPv6 체제 하의 그림 1.과 같은 USN (Ubiquitous Sensor Network)하에서 BcN(Broadband Convergence Network)을 형성하고 있다. IT839전략에서 8대 신규서비스로 와이브로(WiBro)[1], DMB, 홈 네트워크, 텔레매틱스, RFID 활용, W-CDMA, 지상파 DTV, 인터넷전화(VoIP) 서비스가 있다.

VoIP(Voice over Internet Protocol)는 인터넷전화의 핵심 기술로서 PSTN(Public Switched Telephone Network)를 통해 이루어졌던 음성 서비스를 IP(Internet Protocol)를 사용하여 여러 가지 다양한 서비스로 제공하는 것이다. 음성이 디지털화 되고, 전달체계가 IP화됨으로써 전화는 물론 인터넷 팩스, 웹콜, 통합 메시지 처리, 화상회의 등의 향상된 인터넷전화 서비스가 가능하게 된다.

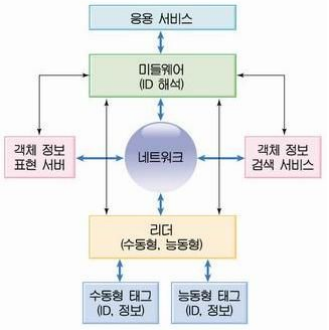

그림 1. 유비쿼터스 센서 네트워크
Fig. 1 Ubiquitous Sensor Network

VoIP 기술은 인터넷뿐만 아니라 사설 IP 기반망, PSTN 또는 이들의 복합 망에서도 연동되어야 하기 때문에 기술 및 프로토콜의 표준화가 중요한데, ITU-T의 H.323과 IETF의 SIP 기반 기술, 그리고 ITU-T와 IETF가 공동으로 개발하는 차세대 VoIP 게이트웨의 MEGACO (Media Gateway Control)[2] 기반 기술 등이 있다.

현재의 인터넷 네트워크에 연결된 노트북이나 PC에서의 프로그램 형태의 소프트폰 형태이거나, 기존의 전화기와 유사한 인터넷전화 형태의 VoIP 서비스를 실시하고 있다. 최근에 VoIP 서비스에 대한 정부의 활성화 대책으로 2006년 말에 상용서비스를 목표로 품질의 개선과 고객확보에 노력하고 있다.

하지만 문제는 보안이다. 개방형 인터넷 기술의 IP 프로토콜을 이용하는 VoIP 서비스는 통화설정 관련한 SIP 패킷 및 음성 패킷을 해커가 불법으로 수집하여 이 패킷을 조합하면 도청이 가능하다. 이러한 도청은 해커가 접근이 용이한 PC나 노트북에서의 소프트폰이나 개인 단말기를 악성코드나 바이러스를 사용하거나 해커가 직접 해킹하여 음성 패킷을 단말기로부터 도청하는 취약점이 존재한다.

또한 작은 규모의 LAN 환경에서의 리피터나 유선 무선의 허브에서의 도청이 가능하다. 이런 경우 패킷 스니핑 (Sniffing)[3] 도구를 이용하면 VoIP 음성 등 정보를 재생할 수 있을 정도의 도청의 취약점이 존재한다.

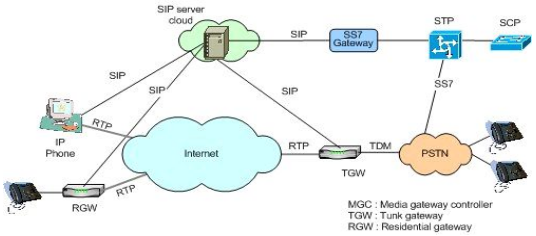

그림 2. SIP를 이용한 VoIP 시스템
Fig. 2 The VoIP system that used SIP

또한 원격지에서 인터넷망을 통해서 VoIP 서비스를 이용할 때에 중간에 라우터와 부속 디바이스에 관한 도청이 가능하다. 라우터를 이용하여 원격지에서의 연결하는 WAN 환경에서는 전용선을 통하는 경우 중간에 연결설정을 하는 링크 부분에서의 도청이 가능하다. 본 논문은 위의 VoIP 서비스 도청에 관한 취약성을 분석하고, 실험실 환경에서 실험을 통해 VoIP 서비스의 도청이 됨을 확인한다.

도청 후에 현재 070으로 명명된 VoIP 네트워크에서 단말기와 라우터 및 LAN과 WAN 구간별로 접근제어, 기밀성, 신뢰성, 가용성, 무결성, 부인봉쇄의 6가지 보안기능의 관점에서 보안 방안을 제시한다. 제시한 보안 방안을 적용한 후에 도청 실험을 실시하여, VoIP 패킷과 메시지에 대한 AES 암호화를 통한 기밀성을 보장하고, 통화내용의 도청을 방지하며, 접근차단과 인증 및 메시지 해시함수 및 착신거절의 사용으로 도청을 예방하고, 네트워크 모니터링과 감사기록으로 보안성과 감사기록을 유지하여 VoIP 서비스의 정보보안에 관한 연구를 한다.

본 논문에서는 이러한 취약점의 확인과 취약점을 보안하는 보안방안을 적용한 상태에서, 도청의 예방 및 차단의 실험 결과를 통해서 VoIP 정보보호를 이룩할 수 있도록 연구하는데 본 논문의 목적이 있다.

II. 관련 연구

VoIP 서비스를 수행 할 때에 도청의 의미와 VoIP 관련 프로토콜[4] 및 도청과 해킹에 사용되는 툴 및 수집된 패킷을 분석하고 정보를 수집하는 네트워크 툴에 관한 관련 연구를 한다.

2.1. 도청

1) 좁은 의미의 도청(Eavesdropping)

정보의 불법적인 가로채기로 정보의 변경을 포함하지 않는 정보의 수신만을 의미하는 말이다. PSTN에서의 음성에 대한 정보의 불법적인 수신을 말한다.

2) 넓은 의미의 도청(Wiretapping)

VoIP서비스의 도청에 해당되는 용어로 네트워크를 거쳐서 송수신하고 있는 데이터를 부정한 방법으로 엿듣는 것이다. 라우터 등의 통신 기기의 유지 보수를 위한 외부로부터 제어할 수 있는 기능을 이용하여 부정적인 접속에 노출되면 정보의 수신뿐만 아니라, 전송되는 정보를 이용하여 정보를 조작하여 사용할 수 있다. 도청에서 이동용 단말을 사용, 수신자의 통신을 도청하는 사례가 증가하고 있고, 디스플레이 장치로부터 누설된 미약한 전자파를 수신하여 표시 내용을 도청하는 수법도 있다.

2.2. H.323, SIP, SDP, RTP, RTCP 프로토콜

1) H.323

서비스 품질이 보증되지 않은 구내정보통신망(LAN)에서의 음성/동화상/데이터 통신을 지원한다. 1996년에 ITU-T가 권고하였으며 파일 전송, 백판(White Board) 등의 데이터 공유를 위한 채널도 규정하고 있으며 그림 3.과 같이 인터넷전화 서비스나 제품에 널리 채용되어 있다.

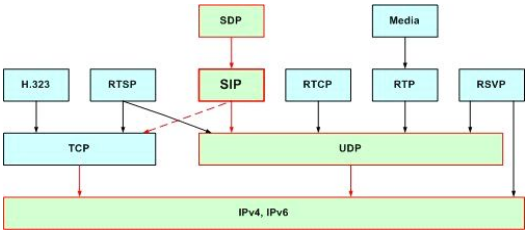

그림 3. VoIP 프로토콜
Fig. 3 VoIP Protocols

2) SIP, SDP

그림 3.에서 SIP(Session Initiation Protocol)는 인터넷상에서 통신하고자 하는 이동 VoIP 단말들이 서로를 식별하여 그 위치를 찾고, 단말 상호간에 멀티미디어 통신세션을 생성하거나 삭제 변경하기위한 절차를 명시한 응용계층의 시그널링 프로토콜이다.

그림 4.에서 창수는 호균에서 SIP 시그널링인 INVITE 패킷을 보내면, 180 Ringing 호를 보내 응답 준비를 하고, 호균은 세션을 연결해도 좋다는 200 OK 호를 보낸다. 이때 SIP은 Request/Response 구조로서 TCP와 UDP에 모두 사용할 수 있으며, 각 사용자들을 구분하기 위해 이메일 주소와 비슷한 SIP URL을 사용함으로서 IP주소에 종속되지 않고 서비스를 제공받는다. SIP는 텍스트 기반이므로 구현이 용이하며, 2002년 7월 RFC3261 표준이 제정되었다.

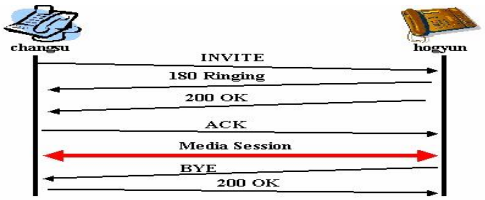

그림 4. SIP의 동작 순서
Fig. 4 Operation order of SIP

SDP(Session Description Protocol)는 멀티미디어 세션 및 관련 스케줄 정보를 기술하기 위한 아스키 문장 기반의 프로토콜이다. 멀티미디어 세션은 지속 시간 동안 일단의 매체 스트림으로 정의되고, 세션이 진행되는 시간은 연속적일 필요는 없다. SDP 정보 내용은 세션의 이름과 목적, 세션 진행 시간, 세션 구성 매체, 매체 수신 정보 등이 포함된다.

3) RTP, RTCP

RTP(Real-Time Transport Protocol)는 실시간으로 음성이나 동화를 송수신하기 위한 트랜스포트층 통신 규약으로 RFC 1889에 규정되어 있다. 자원 예약 프로토콜(RSVP)과는 달리 라우터 등의 통신망 기기에 의지하지 않고 단말 간에 실행되는 것이 특징이다. 보통 사용자 데이터그램 프로토콜(UDP)의 상위 통신 규약으로 송신 측은 타임스탬프(Time Stamp)를 근거로 지연이 큰 패킷을 포기할 수 있다. 또 수신 측에서 전송 지연이나 대역폭 등을 점검한다.

RTP(Rapid Transport Protocol)는 오디오, 비디오, 시뮬레이션 데이터와 같은 실시간 스트리밍 데이터를 유니캐

스트, 또는 멀티캐스트하기 위한 단대단(end-to-end) 인터넷 표준 프로토콜이다.

RTCP(RTP control protocol)는 인터넷을 통한 영상이나 음성의 스트리밍용 프로토콜 RTP를 제어하기 위한 프로토콜이다. RFC 1889에 RTP와 함께 규정되어 있으며 IETF 표준으로 되어있다. 전송 지연 등을 점검해서 RTP를 이용하는 응용 프로그램에 이러한 정보를 알리는 기능을 실현한다.

2.3. 도청을 위한 공격 툴

1) Cain & Abel v2.9.[5]

Cain은 표준 윈도우 LANMAN 및 NTLM 암호 표식을 포함해서 로컬 윈도 시스템에 캐시화, 암호화, 해시화된 다양한 암호 및 마이크로소프트 아웃룩, 인터넷 익스플로러, MSN 익스플로러 및 OS등의 고유한 암호들을 해독하고 마이크로소프트의 Kerberos와 같은 윈도 네트워크 인증 프로토콜을 처리한다.

네트워크 패킷을 스니핑하여 여러 가지 다양한 시스코 암호, 라우팅 프로토콜 해시, VNC 암호, RADIUS 쉐어드 시크리트(RADIUS Shared Secrets), MS SQL 서버 2000 그리고 MySQL 암호를 해독할 수 있다. 그리고 IKE 미리 공유된 키까지 해독하고 IKE를 사용하여 비밀 키를 교환 및 업데이트하는 IPSec VPN에 침입한다.

암호 해독 이외에도 무선 LAN 탐지 툴, 해시 계산기 및 ARP Cache poisoning Tool(침입자가 보다 쉽게 전환된 환경에서 탐지 능력을 발휘할 수 있도록 LAN상에서 트래픽을 다른 방향으로 돌리는 데 사용할 수 있음)이 정교한 GUI로 포함되어 있다. 사전대입이나 무차별대입을 통한 크랙기능을 제공한다. 스크램블된 비밀번호를 해제하고 캐시에 저장된 비밀번호를 추출한다.

2) Ethereal 0.99.0[6]

네트워크 인터페이스로부터 활동 중인 패킷 데이터를 캡처하여 캡처된 패킷 데이터를 열고 저장한다. 캡처된 많은 다른 캡처 프로그램들로부터 패킷 데이터를 인 포트하고, 익스 포트를 한다.

많은 기준에 대해서 패킷을 필터링하고, 필터들에 근거한 패킷 표현을 칼라로 표현하고, 다양한 통계를 생성한다. 그리고 매우 상세한 프로토콜 정보를 가지고 패킷들을 표현한다. Ethereal 설치 전에 윈도우에서 패킷을 캡처해 주는 툴인 WinPcap를 먼저 설치해야 한다(LINUX에서는 Libpcap)[7]. 따라서 Ethereal은 공격 툴이기도 하면서 패킷과 네트워크의 모니터링 툴이라고도 할 수 있다.

2.4. 패킷과 네트워크 모니터링 툴

1) MRTG(Mutli Router Traffic Grapher)[8]

네트워크 장비 상태를 점검하기 위한 트래픽의 양을 측정 해준다. 또한 장비의 CPU, 메모리, 4~7계층 스위치, 서버와 애플리케이션까지의 다양한 값을 측정해 준다.

MRTG는 라우터에서 가장 중요한 여러 인터페이스들의 'In/Out' 트래픽을 그림 5.와 같이 일간, 주간, 월간, 연간 기준으로 각각 별도의 그래프를 그려주고, 이들의 현재, 평균, 최대치를 한눈에 알 수 있게끔 해주는 툴이다.
MRTG는 네트워크 장비들의 내부 온도를 나타내는 수치를 이용하여 온도 그래프까지 나타내고 있다.

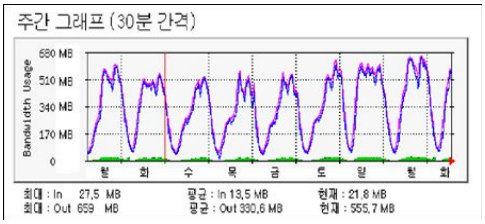

그림 5. MRTG 트래픽 측정 그래프
Fig. 5 MRTG traffic measurement graph

2) NTOP[6]

실시간으로 연결한 각 네트워크 세그먼트에 현재 흐르는 트래픽상의 모든 세션과 통계를 제공하고 가상 LAN이나 OSPF등 현황을 파악한다. 네트워크 장비의 잘못 설정된 사항 뿐 아니라 통신 애플리케이션 단계에서 문제가 발생한 부분의 트래픽 상황 파악을 통해 네트워크를 최적화하고 오남용을 방지하고 네트워크 효율성을 높이는데, 충분히 필요한 정보를 제공한다.

NTOP은 특정 포트나 프로토콜(UDP, 1434port)의 과부하에 대해 하나의 화면에서 보여주며, 또한 시스템별로 DoS 공격을 감지하기 위해 맺어진 세션을 모두 확인하고 세션을 맺은 시스템에 대한 정보를 얻을 수 있다.

네트워크 내에서 인터넷공유 등 인가되지 않은 라우팅 기능을 하는 PC나 장비를 찾아낼 수도 있다. 또한 스니핑을 위한 인터페이스(Promiscuous Mode)를 감지해 관리자가 쉽게 해킹에 대응할 수 있다.

2.5. AES[7]

AES(Advanced Encryption Standard)는 미국 국립표준 기술연구소(NIST)가 데이터 암호화 표준인 DES를 대체할 차세대 국제 표준 암호로 대체하는 순서 공개형의

블록 암호화를 사용한 대칭 키 암호 방식이다. 블록 길이는 128비트이고, VoIP 메시지를 암호화하는데 사용되며, 키의 길이는 128/192/256 비트 중에서 선택 가능하며 주요 평가 항목은 안정성과 암호화의 처리 속도이다. NIST는 2000년에 'Rijndeal'을 최종 채택하였다. 이 알고리즘은 스마트카드 등과 같은 제한된 환경을 포함하여 하드웨어나 소프트웨어로 구현하기 쉽다.

III. VoIP 도청 취약성에 대한 공격

VoIP 서비스에서 보안의 가장 큰 취약성은 도청이다. 본 논문은 VoIP 서비스를 위해 사용되는 단말기와 라우터 및 시스템 디바이스, 구내 네트워크인 LAN과 원격지의 WAN 구간에서의 도청 환경을 구성하고 실험실에서의 도청을 실시한다.

VoIP 도청 Test의 근거자료로는 CERT에서의 취약성 공고 자료를 조사하였으며, 이 자료를 근거로 하여 취약성을 공격하고 분석하여 공격을 통한 결과를 나타낸다.

3.1. VoIP 단말기과 디바이스의 도청

VoIP 서비스를 위하여 인터넷 네트워크에 연결된 노트북이나 PC에서의 프로그램 형태의 소프트폰이나, 인터넷전화를 대상으로 취약점 스캔을 실시한다. 발견된 취약점을 이용하여 인터넷 네트워크로부터 현재 070 전화번호로 명명된 H.323 또는 SIP와 같은 세션연결제어 프로토콜을 통하여 RTP 데이터 패킷을 이용하여 정보를 전송하면서 단말기에서 도청을 실시한다.

1) Test 환경 구성

❖ **Attacker 시스템 사양**

Windows XP Professional(SP2)(OS), Intel Pentium 2.66GHz(CPU), 448 RAM(Memory), 60GB(HDD)

❖ **Target(Victim) 시스템 사양**

Windows XP Professional(SP2) (OS), Intel Pentium 2.66GHz(CPU), 448 RAM(Memory), 40GB(HDD)

❖ **VoIP PBX 및 단말기 사양**

IP PBX, Linux Redhat 9.0(OS), Asterisk 1.2.9, LinkSys IP Phone SPA941(IP Phone)

2) Test Network 구성

그림 6.과 같다.

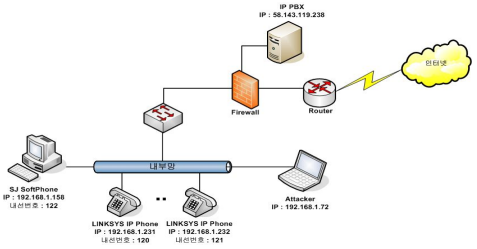

그림 6. 단말과 디바이스 도청 시험 환경

Fig. 6 Terminal and Device Wiretapping Test environment

3) Attack Tools

❖ Rserver를 이용하여 특정 포트를 열어 공격 대상 컴퓨터를 원격제어를 할 수 있다.

❖ SiVuS를 이용하여 VoIP 취약점을 스캔한다.

4) Attack

가) SiVuS 툴을 이용하여 특정 네트워크의 인터넷 전화기 유무를 스캐닝한다.

나) Rserver 프로그램을 이용하여 소프트폰이 설치된 개인 사용자의 PC를 해킹한다.

다) 공격exe 파일과 함께 공격 exe파일을 실행할 수 있는 배치파일을 만든다.

라) 두 파일을 하나의 알집exe로 묶은 후 공격 대상자에게 알집 exe파일을 보낸다.

마) Rserver가 실행되면 원격에서 Rviewer를 실행시켜 원격에서 공격대상 컴퓨터를 제어한다.

바) Ethereal, Cain과 같은 스니핑 툴을 공격대상 시스템에 설치하여 음성파일 또는 패킷들을 도청한다.

5) Attack 결과

VoIP 단말에서 전송 정보에 대한 메시지를 도청하였다. Attack 결과로 정보 전송자의 개인정보 및 정보의 불법적인 사용에 대한 피해를 야기할 수 있다.

3.2. LAN 구간 도청

인터넷 네트워크에 연결된 구내 네트워크인 LAN구간에서 현재 070으로 명명된 서비스에 대한 취약점을 발견한다. 공격은 VoIP 로컬망 내 호스트에 스니핑 도구를 설치하고, ARP Cache poisoning을 시행하여, LAN에서 발생하는 VoIP 패킷을 스니핑 한 후 툴을 통해 재생하여 음성 정보에 대한 도청을 실시한다.

1) Test 환경 구성

❖ Attacker 시스템 사양

Linux RedHat 9.0(OS), Intel Pentium 2.66GHz (CPU), 448 RAM(Memory), 60GB(HDD)

❖ Target(Victim) 시스템 사양

Windows XP Professional(SP2) (OS), Intel Pentium 2.66GHz(CPU), 448 RAM(Memory), 40GB(HDD)

IP PBX와 VoIP 단말기 사양

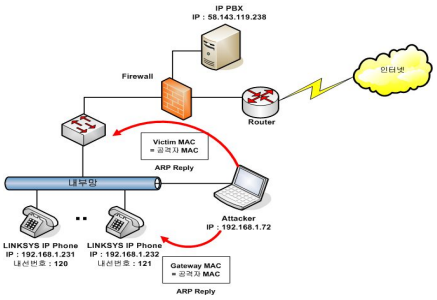

그림 7. LAN에서 원격제어를 통한 도청

Fig. 7 Wiretapping through remote controls at LAN

IP PBX, Linux Redhat 9.0(OS), Asterisk 1.2.9, LinkSys IP Phone SPA941(IP Phone)

2) Test Network 구성도

그림 7.과 같다.

3) Attack Tool

❖ ca_setup.exe : 패킷 스니핑과 패스워드 크래킹 등 다양한 기능이 포함된 통합 해킹 툴로서 스위칭 환경에서의 스니핑 및 각종 프로토콜에 대한 디코드가 가능하다.

4) Attack

가) 내부망의 취약한 PC를 공격하여 패킷을 스니핑할 수 있는 Ca_setup.exe 프로그램을 설치하여 실행한다.

나) 스니핑 하려는 victim PC의 IP를 선택한 후 ARP Cache Poisoning을 실행한다.

다) Attacker는 Target(Victim)에게 Gateway Mac주소 =Attacker Mac주소라는 정보를 포함한 ARP Reply를 전송한다. Gateway에게는 Target(Victim) Mac주소 =Attacker Mac주소라는 정보를 포함한 ARP Reply를 전송한다.

라) Target(Victim)은 수신한 ARP Reply 정보를 이용하여 자신의Mac Table에 있는 Gateway의 Mac정보를 변경, Gateway는 수신한 ARP Reply정보를 이용하여 자신의 Mac Table에 있는 Target(Victim)의 Mac정보를 변경한다.

마) Target(Victim)은 VoIP 폰을 이용하여 통화할 때 변경된 Gateway의 Mac주소(=Attacker의 Mac주소)로 패킷을 전송한다.

바) Target(Victim)의 패킷을 스니핑한 Attacker는 올바른 Gateway로 패킷을 Forwarding, Gateway는 Proxy Server로 패킷을 전송한다.

사) 패킷을 받은 Proxy Server는 Gateway로 응답 패킷을 전송한다.

아) Gateway는 Proxy Server의 응답 패킷을 Target (Victim)으로 전송할 때 변경된 Target(Victim)의 Mac주소 (=Attacker의 Mac주소)로 전송한다.

자) Gateway에서 Target(Victim)으로 전송되는 패킷을 스니핑한 Attacker는 패킷을 Target(Victim)으로 Forwarding한다.

차) 이 해킹과정을 통하여 Attacker는 패킷을 Target(Victim)에서 Proxy Server로 전송되는 모든 정보 데이터를 스니핑 할 수 있다.

5) Attack 결과

LAN 구간에서 VoIP 서비스의 전송 정보에 대한 메시지를 도청하였다. Attack 결과로 LAN 구간에서 취약점이 발견되고, 정보 전송자의 개인정보 및 정보의 불법적인 사용에 대한 피해를 야기할 수 있다.

3.3. WAN 구간 도청

VoIP 서비스의 중요 구성 요소인 Proxy 서버를 해킹하여 SIP 메시지를 변조하여 음성 데이터가 공격시스템을 경유하도록 하여 통화 내용을 도청한다. Registrar 서버를 해킹하여 등록정보를 변조하여 음성 데이터가 공격 시스템을 경유하도록 하여 도청한다. 마지막으로 라우터 및 네트워크 시스템 해킹을 통하여 경유하는 모든 트래픽을 수집하고, 트래픽 중 음성 트래픽을 필터링하여 재생하는 방법이 있다.

그러나 사용자 VoIP 트래픽들이 모아지는 WAN 환경의 단일 백본 링크에서 특정 사용자의 음성 트래픽을 추적하는 일은 쉽지 않다. VoIP 상용서비스를 제공하는 백본은 MPLS 등 QoS가 보장될 수 있는 VoIP 전용의 폐쇄망으로 기간사업자에 의해 운영되므로 물리적, 논리적 접근이 어려워 스니핑 공격뿐만 아니라 상대적으로 기타 위협에 노출되기 쉽지 않다.

1) Test 환경 구성

❖ Attacker 시스템 사양

Linux RedHat 9.0(OS), Intel Pentium 2.66GHz (CPU), 448 RAM(Memory), 60GB(HDD)

❖ Target(Victim) 시스템 사양

IP PBX, Linux Redhat 9.0(OS), Asterisk 1.2.9

2) Test Network 구성도

그림 7.과 같다.

3) Attack Tool

❖ Ca_setup.exe

4) Attack

가) SIP 서버 해킹 후, 공격자는 SIP 메시지를 변조하여 원하는 목적지로 전송한다.

나) Registrar 서버 해킹 후, 공격자는 등록정보를 변조하여 원하는 목적지로 전송이 가능하다.

다) 라우터 및 네트워크 시스템 해킹 후, 공격자는 경유하는 모든 트래픽을 수집하고, 그 중 음성 트래픽을 걸러내어 통화내용을 도청한다.

5) Attack 결과

위의 공격은 실제 기간사업자망에 대한 해킹 공격을 시도하였으나, 실험실 밖에서의 실제 기간사업자망에 대한 법률적 현실적 제약으로 공격에 성공을 하지 못하였다. WAN 구간에서 공격이 성공되면 네트워크 시스템을 거치는 모든 메시지에 대한 도청이 가능하므로, 정보전송자와 수신자 모두의 개인정보 및 정보의 불법적인 사용에 대한 대규모의 피해를 야기할 수 있다.

Ⅳ. VoIP 도청 공격의 보안방안

4.1. VoIP 도청 공격의 취약점

표 1.에서는 VoIP 서비스를 이용할 때 도청의 취약점으로 나타난 CVE(Common Vulnerability and Exposures) 리스트[9]이다. 표 1.에서 나타난 취약점에 대한 해커의 공격에 대해 VoIP 보안 방안들이 필요하다.

4.2. VoIP 도청 공격의 보안방안

도청에 대한 보안 방안의 제시에서 보안 기능을 강화시키기 위해 VoIP 서비스의 접근제어(Access Control), 기밀성(Confidentiality), 신뢰성(Authentication), 가용성(Availability), 무결성(Integrity), 부인봉쇄 (Non-repudiation)의 6가지 보안 기능을 취약점이 발견된 도청 시험구간에 적용한 후, 도청시험결과를 표 2.에 나타내었다.

표 1. VoIP 도청의 취약점과 취약 내용

Table. 1 Vulnerability point & contents of VoIP Wiretapping

CVE No.	VoIP 도청의 취약점 대상 과 취약 내용
CVE-2006-0834	UIP1868P VoIP 전화기와 라우터-admin에 대한 디폴트 패스워드에 취약점
CVE-2006-0374	ACT P202S IP폰(1.02.21)의 펌웨어-(1) 원격의 공격자가 UDP 17185포트를 이용하여 VxWorks WDB 원격 디버깅 모드로 직접 접근, 중요한 정보 허용 (2) echo(TCP7)네트워크 데이터 반향 (3) 인증 없이 rlogin 이용하여 접근권한 획득
CVE-2006-0305	Clipcomm CPW-100E VoIP Wireless 헤드셋 폰-TCP 60023 포트 이용, 인증 없이 접근권한 획득
CVE-2006-0302	ZyXel P2000W VoIP 802.11b Wireless 폰-UDP 포트 9090을 이용하여 중요한 정보 획득
CVE-2005-3804	Cisco IP Phone (VoIP) 7920 1.0(8)전화-UDP 포트17185 중요한 정보 획득
CVE-2005-3803	Cisco IP Phone 7920 1.0(8)-SNMP 통신-공격자가 중요한 정보획득
CVE-2005-3724	Zyxel P2000W 버전 1 VOIP WIFI 폰 Wj.00.-UDP 포트 9090을 이용하여 중요 정보 획득
CVE-2005-3723	Hitachi IP 5000 전화 펌웨어1.5.6-SNMP 또는 TCP 포트 3390 중요 정보 획득
CVE-2005-3719	Hitachi IP5000 VOIP WIFI 폰 1.5.6-관리자 패스워드가 "0000"으로 하드코딩 중요정보 획득
CVE-2005-3718	UTStarcom F1000 VOIP WIFI 폰 s2.0-인증 없이 rlogin을 통해 실행
CVE-2005-3717	UTStarcom F1000 VOIP WIFI Phone s2.0- 텔넷 데몬 디폴트 사용자 이름과 패스워드 "password"
CVE-2005-3716	TStarcom F1000 VOIP WIFI Phone s2.0-SNMP 데몬은 공개적인 자격증명서 하드코딩 정보를 획득
CVE-2005-3715	Senao SI-680H Wireless VoIP-UDP 포트 17185를 인증 없이 사용
CVE-2002-0882	Cisco IP 전화기(모델 : 7910, 7940, 7960)의 웹서버-중요 메모리 정보 읽기를 허용
CVE-2002-0881	Cisco IP 전화기(모델 : 7910, 7940, 7960)-디폴트 관리자 패스워드를 사용

1) 표 2.에서 접근제어는 표 1.의 CVE-2006-0305의 취약성에서 VoIP 전화와 무선전화의 단말기에 대한 인증 후, 사용자인증을 받음으로서 접근차단으로 인하여 VoIP 서비스의 도청을 예방 할 수 있다.

2) 표 2.에서 기밀성은 표 1.의 CVE-2006-0834의 취약성에서 전체구간에서, 시그널링인 SIP, SDP와 데이터 전송인 RTP, RTCP 패킷에 대한 메시지의 AES 암호화를 통해 도청을 당하더라도 내용의 판독이 불가하다.

3) 표 2.에서 신뢰성은 표 1.의 CVE-2005-3723의 취약성에서 패스워드의 탈취를 통해서 Spoofing 공격을 하더라도 LAN구간과 VoIP Proxy 서버의 인증 필터링과 해외전화 등의 전송자를 확인하고, 스팸 등에 대한 착신거절을 통해 도청가능 호와 메시지의 필터로 도청 예방을 할 수 있다.

표 2. VoIP 도청구간 별 보안 방안과 도청 결과
table.2 Security plan of a VoIP wiretapping section and the wiretapping test results.

보안 기능	VoIP 네트워크 취약점 도청 구간	VoIP 보안 방안	도청 실험 결과
접근 제어	VoIP 전화, 무선 전화의 단말기	단말기에 대한 인증 후 사용자인증 수행	접근차단으로 도청 예방
기밀성	전체 구간, SIP,SDP, RTP, RTCP 패킷	SIP,SDP, RTP, RTCP 패킷의 AES 암호화	암호화 후 도청 내용 판독 불가
신뢰성	LAN, WAN 구간, VoIP Proxy 서버	서버의 인증 필터링, 해외전화 등의 전송자 확인 및 착신거절	도청가능 호와 메시지의 필터로 도청 예방
가용성	LAN, WAN 구간의 단말기와 라우터	접근 제어와 인증 및 네트워크 모니터링 탐지 대응	도청의 모니터링으로 도청 예방
무결성	전체 구간, 인증과 시그널링에 메시지	메시지 다이제스트 해시 함수 MD5, SHA-1	무결성 보장, 도청 예방
부인봉쇄	LAN, WAN 구간,	Caller_ID, 수신자전화 선택, SIP, RTCP 패킷의 log 감사자료	감사자료를 통해 해킹경로 추적과 도청자료 분석

4) 표 2.에서 가용성은 표 1.의 CVE-2005-3723의 취약성에서 인터넷의 약점인 TCP/IP의 취약점을 이용하여 해커의 도청이나 DDoS공격[10]을 할 때에도 단말기와 라우터 등의 인증과 접근제어를 한다. SBC 장비와 VoIP 네트워크를 모니터링하여 통계적인 방법[11]으로 탐지된 불법적인 침입에 차단으로 대응하여 도청을 예방한다.

5) 표 2.에서 무결성은 표 1.의 CVE-2005-3718의 취약성에서 메시지나 데이터를 위조 변조할 때에 인증과 시그널링에 사용되는 메시지 다이제스트를 위해 해시 함수 MD5, SHA-1 사용하여 무결성을 검증하면 도청이 예방된다.

6) 표 2.에서 부인봉쇄는 표 1.의 CVE-2005-3715의 취약성에서와 인증 없이 임의적인 사용이나 Caller_ID, 수신자전화선택 등을 이용하여 해커의 공격에 이용되는 SIP나 RTCP 패킷의 log 감사 자료를 보관하고 분석함으로써, 차 후 계속되는 공격을 차단할 수 있고, 개인정보보호법이나, 정보통신망보호법에 의한 후속조치를 취할 수 있는 도청에 대한 법적 증거자료로 분석되고 보존한다.

4.3. VoIP 도청 공격의 보안 실험

인터넷 네트워크에 연결된 구내 네트워크인 LAN 구간과 WAN이 연결된 VoIP 네트워크에서 현재 070으로 명명된 인터넷 폰을 설치하고, CVE 리스트에서 발견된 취약점과 도청보안 방안을 구현하여 보안 실험을 하였다.

공격은 VoIP 로컬망 내 호스트에 스니핑 도구를 설치하고, ARP Cache poisoning을 시행하여, LAN에서 발생하는 VoIP 패킷을 스니핑 한 후 Cain툴을 통해 재생하여 음성 정보에 대한 도청여부에 대한 실험을 실시한다.

1) Test 환경 구성

❖ Attacker 시스템 사양

Linux RedHat 9.0(OS), Intel Pentium 2.66GHz (CPU), 448 RAM(Memory), 60GB(HDD)

❖ Target(Victim) 시스템 사양

Windows XP Professional(SP2) (OS), Intel Pentium 2.66GHz(CPU), 448 RAM(Memory), 40GB(HDD)

❖ IP PBX와 VoIP 단말기 사양

IP PBX, Linux Redhat 9.0(OS), Asterisk 1.2.9, LinkSys IP Phone SPA941(IP Phone), VoIP-Soft Phone

2) Test Network 구성도

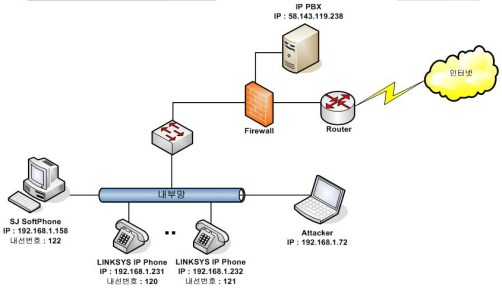

그림 8. VoIP 네트워크의 도청 공격에 대한 보안 시험 환경
Fig. 8 Security test environment about a Wiretapping Attack of a VoIP network

그림 8. 과 같다.

3) Attack Tool

❖ ca_setup.exe : 패킷 스니핑과 패스워드 크래킹 등 다양한 기능이 포함된 통합 해킹 툴로서 스위칭

환경에서의 스니핑을 실시한다.

- ❖ Rserver를 이용하여 특정 포트를 열어 공격 대상 컴퓨터를 원격 제어하는 해킹을 실시한다.
- ❖ SiVuS를 이용하여 VoIP 취약점을 스캔하여 취약점을 공격하여 해킹을 실시한다.

4) Attack

가) 내부망의 취약한 PC를 공격하여 패킷을 스니핑할 수 있는 Ca_setup.exe 프로그램을 설치하고, 스니핑 하려는 victim PC의 IP를 선택한 후 ARP Cache Poisoning을 실행한다. 해킹과정을 통하여 Attacker는 그림 8.에서 Target (Victim)에서 Proxy Server로 전송되는 모든 정보 패킷을 스니핑 한다.

나) SiVuS 툴을 이용하여 특정 망 대역의 인터넷 전화기 유무를 스캐닝하고, Rserver 프로그램을 이용하여 그림 8.의 소프트폰이 설치된 개인사용자의 PC를 해킹한다. Ethereal, Cain 과 같은 스니핑 툴을 공격대상 시스템에 설치하여 음성파일 또는 패킷들을 도청한다.

다) SIP 서버 해킹 후, 공격자는 SIP 메시지를 변조하여 원하는 목적지로 전송하고, Registrar 서버 해킹 후, 공격자는 등록정보를 변조하여 원하는 목적지로 전송이 가능하다. 라우터 및 네트워크 시스템 해킹 후, 공격자는 경유하는 모든 트래픽을 수집하고, 그 중 음성 트래픽을 걸러내어 통화내용을 도청한다.

5) Attack 결과

LAN 구간과 IP PBX 및 VoIP 단말기와 디바이스, WAN 구간에서의 VoIP 서비스의 전송 정보에 대한 도청을 실시하였다. Attack 결과로 WAN 구간과 LAN 구간에서는 그림 9.와 같이 Ethereal을 통해 소프트폰과 해커의 공격에 의한 패킷의 종류와 내용을 정확하게 확인하였다.

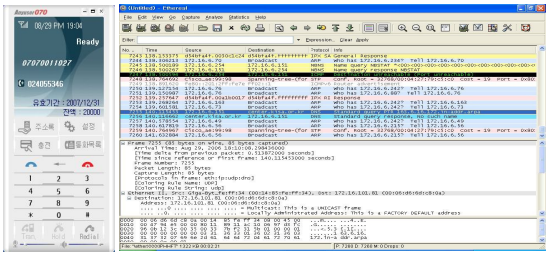

그림 9. 소프트 폰, Ethereal에 의한 공격 및 VoIP의 패킷 캡처

Fig. 9 Softphone, Attacks of VoIP and packet capture by Ethereal

VoIP 네트워크 중간에서 그림 10.과 같이 AES로 암호화된 음성 데이터 패킷을 캡처하였고, 암호화 되지 않는 패킷을 Cain으로 캡처하였다. 두 가지의 캡처된 패킷을 작동시켜 보았을 때, 암호화된 패킷은 물결소리만 들리고 전혀 음성을 해독할 수가 없었으며, 암호화 되지 않는 패킷은 중간 중간에 원음을 해독할 수 있는 자료들이 나왔다.

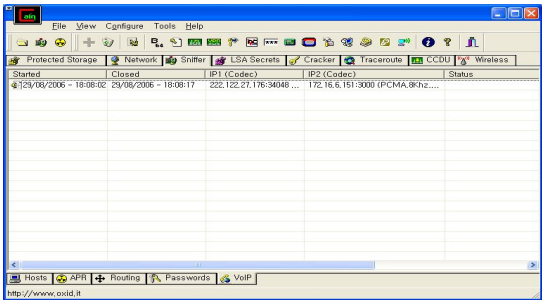

그림 10. Cain이 캡처한 암호화된 음성 패킷의 내용 확인

Fig. 10 Contents confirmation of voice packet encrypted which Cain captured

특히 LAN 구간의 접근제어와 사용자 인증을 실시한 곳에서는 접속 차단으로 패킷을 캡처 할 수 없었지만, 소프트폰 단말기와 중간에 연결 허브에서의 취약점이 발견되어 음성 정보의 패킷이 캡처되었다. 특히 WAN 구간은 기간 사업 네트워크에서의 도청은 이루어지지 않아서 상대적으로 보안이 우수한 것으로 판단되었다.

V. 결론

본 논문은 VoIP 인터넷 네트워크에 연결된 소프트폰과 LAN 구간과 연결된 인터넷전화 및 디바이스, 기간사업자망이 연결된 WAN 구간에서의 VoIP 서비스의 도청 실험을 하였다.

현재 070으로 명명된 인터넷폰과 인터넷전화를 설치하고, VoIP 네트워크에서 IP PBX를 설치하였다. CVE 리스트의 취약점을 연구하고, 공격하여 구현된 도청을 실험 하였다. 실험 네트워크에서 VoIP 서비스의 도청 실험을 한 결과 CVE 리스트에 따르는 단말기와 Proxy 및 허브와 같은 VoIP 네트워크의 연결점에서의 취약점이 발견되었고, 해커의 공격에 의한 도청을 실험한 결과 단말기와 라우터, LAN, WAN 구간에서 도청이 성공되었다.

도청을 성공한 후, 각각의 취약점에 대한 도청의 보안방안을 제시하고 접근제어, 기밀성, 신뢰성, 가용성, 무결성, 부인봉쇄의 6가지 보안 기능의 관점에서 보안방안을 제시하고 각각을 VoIP 네트워크에 적용하였다.

도청 보안 방안을 적용하는 실험은 Ethereal에서 패킷의 분석으로 확인하였으며, 보안 방법으로 제시된 필터링과 접

근제어, 착신거절 설정 등을 시행하였고, 인증 및 검증에 대한 감사 log 기록을 남기고, SIP, RTP 패킷을 AES로 암호화하였다.

Cain으로 AES 암호화된 음성 패킷과, 암호화 되지 않는 패킷을 캡처하여, 두 가지의 캡처된 패킷을 작동시켜 보았을 때, 암호화된 패킷은 물결소리만 들리고 전혀 음성을 해독할 수가 없었으며, 암호화 되지 않는 패킷은 중간 중간에 원음을 해독할 수 있는 자료들이 나왔다. VoIP 네트워크에 대한 접근차단과 Proxy 필터링으로 도청이 예방되었고, 도청가능 호와 메시지의 필터로 해시함수 적용으로 무결성 보장 및 도청 예방 도청이 되었다. VoIP 네트워크의 모니터링으로 가용성이 확보되고, log 기록 등의 감사 자료를 통해 해킹경로 추적과 도청자료 분석으로 도청 예방이 되었다.

따라서 VoIP 네트워크의 도청에 대한 취약점 분석과 해커의 도청 공격에 대한 내용을 확실히 밝혀낼 수 있었으며, VoIP 서비스의 보안 대책에 대한 연구가 되어졌다.

향후 연구 되어야 할 과제로는, 암호화와 접근제어 및 인증과 무결성 검증의 방법을 구체적으로 모듈화하고 SBC나 Proxy Sever에서 SIP 공격이나, RTP Flooding 공격, DoS공격 및 패턴 발견이 않된 해커의 새로운 공격에 대한 방어에도 적용되어져야 할 것이다.

참고문헌

[1] 와이브로 보안기술 해설서. 한국정보보호진흥원. 2006.8.

[2] Edlic Yiu, Edward Yiu, Ljijanu Trakovic. “OPNET Implementation of. Megaco/H.248 Protocol.” opnetwork, 2004.

[3] 박대우, 서정만. “TCP/IP 공격에 대한 보안 방법 연구.” 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.

[4] TTA. 정보통신용어사전. http://word.tta.or.kr/index.jsp 2006.8.

[5] Cain & Abel v2.9. Cain &Abel, http://www.oxid.it/cain.html. 2006.7.

[6] Ethereal-network protocol analyzer Version 0.99.0, Ethereal. http://www.ethereal.com/, 2006.7.

[7] WinPcap. http://www.winpcap.org/install/default.htm. 2006.8

[8] MRTG. http://www.mrtg.co.kr/. 2006.8

[9] NTOP. http://www.ntop.org/download.html. 2006. 8.

[10] W. Stallings. “Cryptography and Network Security, Principles and Practice”. Third Edition, Prentice-Hall, October 2005.

[11] CVE와 Bugtraq. CVE-200x-xxxx. http://cve.mitre.org/cve/, http://www.securityfocus.com/bid/ 2006. 8.

[12] 박대우, 임승린. “해커의 공격에 대한 지능적 연계 침입방지시스템의 연구.” 한국컴퓨터정보학회논문지, 제11권 제2호, pp44-50, 2006. 5. 31.

저 자 소 개

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

<관심분야> 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

윤 석 현

1978년 2월 인하대학교 전자공학과 (공학사)

1982년 2월 연세대학교 전자공학과 (공학석사)

2000년 2월 국민대학교 전자공학과 (공학박사)

1981년 ~ 1993년 동양공업전문대학 전자통신과, 사무자동화과 교수

1996년 ~ 현재 청강문화산업대학 컴퓨터소프트웨어과 교수

관심분야 : 멀티미디어 서비스, ATM 네트워크, 프로토콜 공학, 소프트웨어 공학