VoIP 보안 위협 분석 및 대책 연구

곽진석* 김현철* 이영실* 이훈재**

*동서대학교, **동서대학교 컴퓨터정보공학부

A Study on VoIP Security Risk Analysis and Countermeasure

Hyun Chul Kim* Jin Suk Kwak* Young Sil Lee** Hoon Jae Lee*

*Div. of Computer and Information Engineering, Dongseo University

*Dept. of Ubiquitous and IT, Graduate School of General Dongseo University

E-mail : monkeykjs@naver.com, cnsl@hotmail.co.kr, attract35@hotmail.com, hjlee@dongseo.ac.kr

요 약

VoIP(Voice over Internet Protocol)는 기존의 인터넷망을 이용하여 음성데이터를 패킷단위로 송·수신하여 전화통화를 하는 기술로써, 기존 전화통화 방식보다 비용절감의 이점을 가지며 최근 활성화되고 있는 추세이다. 그러나 최근 VoIP Application을 받을 수 있는 마켓에서의 취약점(누구든지 올릴 수 있다.)을 악용하여 악성코드를 심은 파일을 받게 유도하여 도청을 한 사례, 그리고 DDos 공격으로 인한 마비, 해킹으로 과금 우회 공격 등이 있다. 이를 미루어보아 VoIP에 대한 보안위협에 대한 분석과 대책 마련이 시급한 것으로 사료된다. 이에 본 논문에서는 VoIP 보안 위협에 대해 실제 Soft Phone, Smart Phone App상에서 야기될 수 있는 취약점을 분석하며, 이에 대한 보안 대책을 연구하여 기술한다.

ABSTRACT

VoIP is a technology of voice communication, using the existing internet network which sends and receives voice packets. VoIP has an advantage that VoIP is cheaper than an existing telephony, and the tech is vitalized lately.

But recently you can download Volp Application in the Market that have a vulnerability(Anyone Can Upload). This weakness is wrongfully used that People are downloaded by encouraging about malignant code is planted. Signal intercepts indicates from this case. and paralysis by DDoS Attack, bypass are charged for hacking. Judging from, security threat of VolP analysis and take countermeasures.

In the thesis we analyze the VoIP security caused on 'Soft Phone' and 'Smart Phone', and figure out security policies and delineate those policies on the paper.

키워드

보안 위협, VoIP, SIP, VoIP 어플리케이션

Key word

Security threat, mobile VoIP, SIP, VoIP Application

Ⅰ. 서 론

VoIP(Voice over Internet Protocol)는 기존의 IP Protocol 인터넷망을 이용하여 아날로그 음성신호를 디지털 신호의 음성데이터 패킷 단위로 송 수신하여 전화통화 서비스를 이용할 수 있는 기술이다. 인터넷을 이용한 음성 통화 기술은 90년대 중반 보칼텍(Vocaltec)이라는 이스라엘 회사가 처음 선보였으며, 2005년 8월부터 국내에서 070 전화번호의 인터넷 전화(VoIP)가 상용화되었다. 그러나 방송통신위원회의 보도 자료에 따르면 기존 유선전화의 요금에 비해 저렴하다는 장점에도 불구하고 인터넷 전화의 통화 품질이나 070 식별번호에 대한 부정적 인식, 부가 요금을 청구하는 060 식별번호 혼동 등으로 인해 VoIP 전화 서비스 시장은 초기에 활성화 되지 못하였다.

2007년 말, 인터넷 전화번호 이동제도에 관한 주요 기관 통신 사업자들 간의 합의 후 2008년 3월부터 기존의 전화번호를 그대로 유지하면서, 인터넷 전화로 전환할 수 있게 되었으며, 점차 수요가 증가하기 시작하였다.

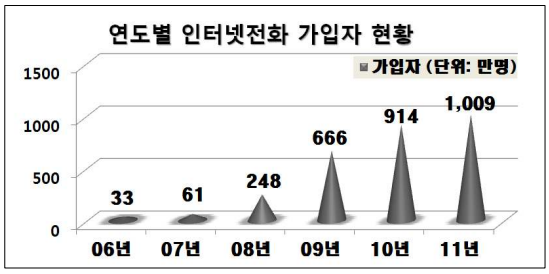

그림 1. 연도별 인터넷전화 가입자 현황[1].

[그림 1]의 국내 인터네 전화 가입자 수 현황에 관한 분석 결과에서 2009년 666만명에서 2011년 1009만 명으로 이용자의 수가 증가하고 있는 것을 확인할 수 있다. 또한, Smart Phone 시장의 활성화로 인해 유료 혹은 무료로 VoIP 전화 서비스를 사용할 수 있는 Application이 증가하고 있으므로 VoIP 전화 서비스 사용자는 현재보다 더 늘어날 것으로 예상된다[2].

그러나 이러한 인터넷 전화 시장 규모의 증가에 비해 VoIP 활성화에 투자되는 노력은 상대적으로 매우 열악한 상황이며, VoIP의 보안을 위한 HTTP Digest 인증, S/MIME, 그리고 Secure RTP, VoIP Firewall 등 다양한 보안 기술 및 제품이 사용되고 있으나, 최근 발생하는 다양한 공격 유형에 능동적으로 대처할 수 있을 정도로 성숙되지는 못한 상태라 할 수 있다, 더불어 NAT 및 보안 설정에 따른 QoS 저하 이슈 등은 앞으로 풀어야 할 숙제로 남아 있다[3].

이에 본 논문에서는 VoIP 서비스 환경에서 현재까지 취약점으로 대표적으로 알려진 5가지 공격 방법 (DoS, Session Hijacking, Eavesdropping, Scanning, VoIP Spam)을 이용한 침해사고 유형에 대하여 기술하고, 자체적인 SIP Server를 구성하여 동일한 무선 인터넷 (Wireless Internet)망에서 Eavesdropping/Sniffing 공격을 가하여 전화 통화 내용 도청 가능 여부를 실험하였다. 또한, 실험을 통해 VoIP Application을 이용한 VoIP 전화 서비스 이용 시 발생 가능한 취약점에 대하여 분석하고 그에 따른 보안대책에 대하여 연구한다.

II. 관 련 연 구

VoIP 기술은 기존의 인터넷망을 이용하여 서비스를 제공하기 때문에 인터넷망에서 발생 가능한 모든 공격들에 노출되어 있다. 이에 본 관련 연구에서 기존의 알려진 5가지 VoIP 공격방법[2][4]에 대해 기술한다.

2.1 DoS(Denial of Service: 서비스 거부 공격)

서비스 거부 공격(DoS)은 특정 사용자가 공격 대상의 시스템을 공격해 해당 시스템의 자원을 부족하게 하여 원래의 기능을 수행하지 못하게 하는 상황을 말한다. VoIP 서비스의 DoS 공격은 VoIP 전화 음성 통신이 원활하게 동작하지 않게 하거나 VoIP 전화 통화 동작중인 상태를 임의적으로 멈추게도 할 수 있다. 대표적인 VoIP DoS 공격에는 일정한 시간에 다량의 메시지를 보내어 VoIP 서비스를 다운시키거나 통화품질을 저하시키는 Flooding 공격과 현재 이루어지고 있는 통화를 강제로 종료시키는 BYE 메시지 공격, CANCEL 메시지 공격 등이 있다.

2.2 Session Hijacking (세션 가로채기)

Session Hijacking(세션 가로채기)은 세션 연결 중인 상태의 사용자에게서 권한을 훔치거나 도용하여 불법적으로 사용하는 방법을 말한다. VoIP 서비스의 Session Hijacking 공격은 전화통화 중인 상태에서 음성 데이터 수신 경로를 변경하여 참여 호스트들의 모든 메시지에 대한 도청이 가능하고 세션 정보를 가로채기 때문에 사용자의 등록정보 역시 유출될 위험을 가지고 있으며 이로 인해 피해자의 과금 회피 등 부가적인 문제 또한 발생할 수 있다.

2.3 Eavesdropping (도청)

Eavesdropping(도청)은 사용자의 동의 없이 통화 내용을 몰래 엿듣는 행위를 말한다. VoIP 서비스 환경에서 시스템 또는 단말의 취약점을 악용하여 사용자간의 통화내용을 도청할 수 있다. 가장 손쉬운 도청 방법으로는 같은 LAN 회선 환경에서 ARP Poisoning 공격을 통해 패킷을 수집하는 방법이다. 수집된 패킷에는 통화 설정 메시지 패킷 및 음성 RTP 패킷, 사용자의 인증정보 패킷 등이 포함 되어 있으며, 불법으로 수집한 패킷 중 음성 RTP 패킷을 분석하여 음성통화내용을 도청하는 것이다.

또한, 동일한 LAN 환경이 아닌, 데이터 암호화 통신을 하는 경우 등 다양한 환경에서 Rouge AP 혹은 Application의 바이러스 및 악성코드 유포 등의 방법 인해 도청이 가능하지만 쉽게 성공하기 어렵다.

2.4 Scanning

스캐닝(Scanning)은 공격자가 공격할 대상을 찾기 위해 각 시스템의 취약점을 탐지하는 공격이다. 스캐닝 공격을 통해 불법으로 취득한 정보로 인가되지 않은 사용자가 VoIP 서비스를 이용하는 정상적인 사용자의 등록정보를 이용하여 서비스를 이용하는 공격이다. 이 방법을 통하여 인가되지 않은 사용자가 정당한 사용자의 VoIP 서비스를 이용하거나, 정당한 사용자의 등록정보 변조하는 등의 피해를 입힐 수 있다.

2.5 VoIP Spam(SPIT: 스팸 전화)

VoIP Spam(스팸 전화)은 상대적으로 저렴한 인터넷 비용과 스팸 발생 자동화 도구를 이용하여 다수에게 대량의 전화 서비스를 발생시키는 것을 말한다. 이러한 VoIP Spam의 발생이 증가할 경우 사생활 침해뿐만 아니라 VoIP 서비스 자체의 신뢰도 역시 하락할 수 있다.

Ⅲ. Eavesdropping(Sniffing) 공격 실험

본 장에서는 VoIP 보안 위협 분석을 위하여 5가지 공격 방법 중 하나인 Eavesdropping 공격을 실험하였다. 실험을 위해 먼저, 자체적인 Astrisk SIP Server를 구축하고 동일한 무선 인터넷망에서 Smart Phone과 태블릿 PC의 VoIP Application을 이용하여 Eavesdropping 공격 실험을 진행하였다. 실험에 사용된 VoIP Application은 인터넷을 통해 쉽게 구할 수 있는 무료 Android VoIP Application을 사용하였다.

3.1 Test 환경

표 1. Test에 사용된 Program

Program	Version
WireShark Tool	Version 1.6.2
Application	Simple SIP Application 1.0

표 2. Test에 사용된 기기

Device	Test Environment
테블릿 PC (갤럭시 탭 10.1)	Android 3.1 nVidia Tegra2 1.0GHz 내장 메모리 32G
Smart Phone (HTC Sensation)	Android 2.3 듀얼코어 1.2GHz 외장 메모리 16G
SIP Server	Centos5.6, Asterisk PBX 1.6.2.7
유/무선 AP	ipTime N6004

그림 2 갤러시 탭 - VoIP Application

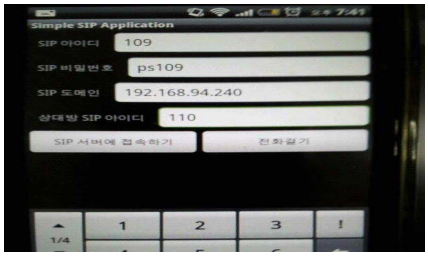

그림 3 센세이션 - VoIP Application

3.2 Packet Capture

사용자가 VoIP 전화 통화를 이용하는 동안 유/무선 AP에 연결된 PC를 통해 전송되는 패킷을 WireShark Tool 등 다양한 패킷 캡처 툴을 이용하여 Capture 가능하다. 본 실험에서는 WireShark Tool을 사용하여 전송되는 패킷을 캡처하였으며, 그 결과를 [그림 4]에 나타내었다.

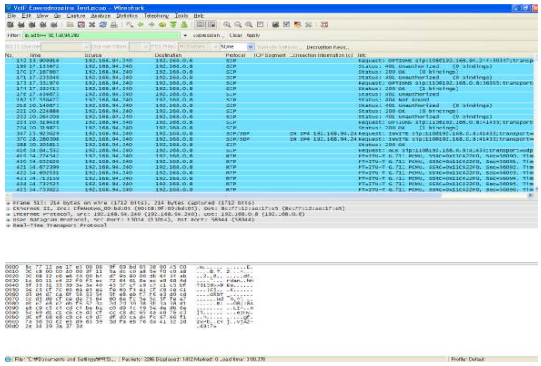

그림 4 WireShark Tool을 이용한 패킷 Capture

캡처된 패킷 분석 결과, Smart Phone과 태블릿 PC가 SIP Server를 통해 세션을 맺는 INVITE, CANCER, ACK, BYE등의 패킷과 음성을 전달하는 미디어 RTP 패킷을 확인할 수 있을 뿐만 아니라 VoIP 전화 통화에서 사용된 음성 코덱의 정보와 Source IP, Destination IP 역시 얻을 수 있다. 또한 수집된 정보들을 통해 패킷의 이동 경로 분석, Protocol Type, Sequence number 등 부가적인 정보 확인 및 분석 가능하다.

본 실험 결과에서는 VoIP 전화통화에 사용된 음성 코덱은 G.711, Source IP는 192.168.0.8, Destination IP는 192.168.94.240을 이용하였음을 확인하였고, 이를 미루어 보아 SIP Server IP가 192.168.94.240임을 추측할 수 있다.

3.3 Eavesdropping Test

[그림 5]는 WireShark Tool로 Capture한 패킷들 중 RTP Type의 패킷들을 모아 WireShark의 VoIP Calls 기능을 이용하여 실행한 결과로, 도청된 Smart Phone 과 태블릿 PC간의 전화 통화 내용을 들을 수 있다.

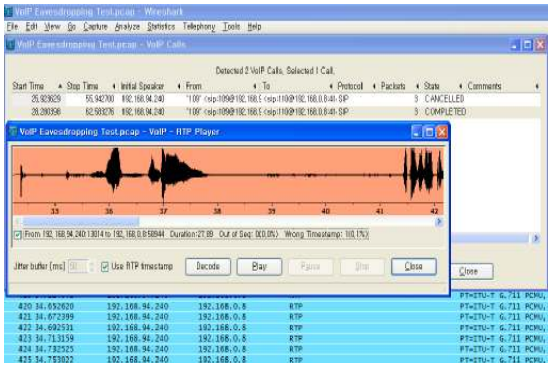

그림 5. RTP 패킷으로 전화 통화내용 도청.

Ⅳ. 보안 대책

VoIP 서비스는 PC based VoIP 서비스와 Mobile based VoIP 서비스(m-VoIP)로 구분되며, 이에 따라 기존 인터넷망에서 발생하는 공격 및 취약점뿐만 아니라 Smart Phone 이용을 통해 발생 가능한 모바일 바이러스/악성코드에 대한 취약점 역시 가지게 된다. 이를 미루어 보아 VoIP 서비스를 위한 보안을 제공할 경우 PC와 모바일 기기에서 보다 능동적으로 적용 및 활용 가능한 추가적인 보안 대책이 시급하다 사료된다.

현재 VoIP 서비스 보안을 위해 제공되는 대표적인 두 가지 방법으로, 첫째, sRTP(secure RTP) 보안을 사용하는 것이다. 기존의 VoIP 통신 세션을 맺은 후 양단간에 음성 패킷을 전송하기 위하여 RTP 프로토콜을 이용하여 보안에 취약하나, sRTP 프로토콜을 사용할 경우 암호화된 패킷이 전송되므로, Eavesdropping 등의 공격을 통해 악의적인 공격자가 패킷을 캡처 또는 수집하더라도 분석이 불가능하다. sRTP 사용을 위한 키 교환 프로토콜로 SDES, MIKEY, DTIS-SRTP을 이용하기를 권장한다. 둘째, VoIP 전화 통신 시 SSL/TLS 보안을 사용한다. SSL/TLS를 통한 Secure Channel을 이용해 SIP 시그널링을 보호함으로써, 통신 간 MOS(mean opinion score)를 향상시킬 수 있다[3][6].

한편, AP를 이용해 무선인터넷을 이용하는 사용자들은 VoIP 서비스 보안을 위하여 공개형 AP 보다는 암호화 인증기능이 있고, 인터넷 제공자를 알 수 있는 보안 AP를 사용하도록 권고되고 있다. 그러나 보안 AP 역시 기존의 Rogue AP 공격에 대한 취약점을 가지므로, Rogue AP 공격에 대한 새로운 대처 방안이 필요하다 사료된다. 그 한 예로 Radius AAA인증 기능을 들 수 있다. Radius(Remote Authentication Dial-In User Service)는 분산된 전화 접속/원격 애겟스 네트워킹에 대한 승인, 식별, 인증 및 계정 서비스를 제공하기 위한 산업 표준 프로토콜로, 이 중 AAA 인증 기능은 Authentication, authorization, Accounting의 약자로 Radius Server 자체에서 제공되는 기능 중 하나이다. Radius 서버로 AP 사용자 인증 기능을 사용할 경우 Rogue AP를 차단하여 공격을 막을 수 있다. 이를 토대로 Radius AAA 인증 서버를 이용한 사용자 인증 방안을 현재 SSL/TLS 보안에 접목시킬 경우 보다 안전한 무선 인터넷을 이용 할 수 있을 것이다. 또한 이는 VoIP 서비스의 보안을 향상시킬 수 있는 길이라 생각된다.

Ⅴ. 결 론

본 논문에서 VoIP 서비스의 보안 취약점 분석을 위하여 SIP Server를 구축하여 무선 인터넷망에서 Eavesdropping 공격을 실험하였으며, 그 결과 현재 마켓이나 인터넷을 통해 무료로 제공되고 있는 기존의 VoIP Application은 유/무선 AP에서 수집한 패킷으로 분석/조합하여 쉽게 도청이 가능함을 확인할 수 있다.

VoIP는 기존의 통화 보다 요금이 저렴하며 VoIP를 사용할 수 있는 기기들의 종류가 점차 다양해지고 발전하는 점 등의 이유로 추후 VoIP 서비스를 이용하는 사용자는 급격히 증가할 것으로 예상되는 만큼 VoIP 서비스를 이용하는 사용자를 위해 기존의 VoIP 서비스 취약점에 대한 보안 대책뿐만 아니라 새롭게 등장하고 있는 공격 기술에 대응할 수 있는 보안 기술의 개발과 더불어 보다 향상된 QoS를 제공할 수 있도록 적극적인 노력이 필요하다.

참고문헌

[1] 통신정책과, “인터넷전화 가입자 1,000만명 돌파 ” 방송통신위원회 보도자료, p.1 - 4, 2011.07.04.

[2] 천우성, 박대우, 양종한, “ Smart Phone VoIP 서비스에 대한 공격과 도청 연구“ 한국정보진흥원, p.1 - 7, 2011.

[3] 금융보안연구원 취약성 분석팀, “금융부문 보안 가이드(5종)”, 금융부문 VoIP 보안 가이드 , p.3 - 42, 2010.12.

[4] 박진범, 백형구, 원용근, 임채태, 황병우, “VoIP 보안 취약점 공격에 대한 기존 보안 장비의 대응 분석 연구,” 정보보호학회논문지, 제17권 제5호, p.1-9, 2007.10.

[5] KISA, "정보보호뉴스 05“, www.kisa.or.kr, p.9 , 2007.05.

[6] 신영찬, 김규영, 김민영, 김중만, 원유재, 류재철, “VoIP를 위한 보안 프로토콜 성능평가“, 정보보호학회논문지 제18권 제3호, p.109-120, 2008. 06.