행정기관 VoIP 서비스에 대한 취약점 공격과 도청 연구

천우성*, 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of Eavesdropping and Vulnerability Attack of Administrative Agency VoIP Services

Woo-Sung Chun*, Dea-Woo Park*

*Dept. of, IT Application Technology, Hoseo Graduate School of Venture

E-mail : deux8522@gmail.com, prof1@hoseo.ac.kr

요 약

행정기관 VoIP 서비스는 현재 PSTN망과 인터넷망을 활용하여 기존 전화망보다 저렴한 가격에 음성통화를 할 수 있게 해주는 서비스로 확대되고 있다. 하지만 공공의 보안이 유지 되어야 할 행정기관 VoIP의 경우 보안취약성에 대한 문제들이 발생하고, 해커의 공격을 받을 가능성이 높다. 본 논문은 행정기관에서 유·무선 인터넷을 이용하여 VoIP 서비스 이용 시 발생할 수 있는 침해사고 유형을 분석하고 도청 공격을 실시하여 취약점을 분석한다. 행정기관용 Smart Phone으로 VoIP 취약점을 분석을 위하여 OmniPeek와 AirPcap 장비가 설치되어 있는 실험실 환경에서 도청 공격을 실시한다. 도청 공격에 따르는 Packet을 분석하고, IP을 확인하여 공격에 의한 침해사고로 도청이 이루어짐을 시험으로 증명한다. 본 논문의 연구는 행정기관뿐 아니라 일반사용자의 Smart Phone과 VoIP 서비스 보안성 강화에 기초자료로 제공 될 것이다.

키워드

VoIP, 행정기관 Smart Phone, 도청 공격, 침해사고, 보안성

Ⅰ. 서 론

그림 1. 인터넷전화 가입자 수 현황

2005년 7월부터 상용 서비스를 시작한 한국의 국내 VoIP(Voice over Internet Protocol)을 사용하는 인터넷전화 서비스 시장은 2006년 말 32만명이 가입하였고, 2010년 9월에는 659만명이 인터넷 전화에 가입하였다. 또한 행정기관에서도 비용절감과 사용의 편리성 때문에 행정기관 VoIP사용이 줄고 있다.

또한 최근 스마트폰 보급의 증가로 인하여, 무료로 제공되는 VoIP 서비스를 이용하면서, 행정기관 사용자를 포함하여 2011년에는 1000만명 이상으로 VoIP 가입자가 증가할 것으로 예상된다.

하지만 국내에서 기업이 자체 구축한 VoIP 사업자의 교환장비가 해킹을 당하는 사고가 있었다. 또한, 네트워크상에서 ARP 스푸핑 공격을 이용한 도감청 및 비밀정보 누출이 가능하기 때문에 이미 1000만 인터넷 전화 가입자 시장에 우려가 실제로 발생한 것이다.

VoIP에서도 7.7. DDoS공격과 3.3 DDoS공격으로 인한 인터넷 대란과 비슷한 방법으로 행정기관에서 사용하는 VoIP 전화와 장비에 대해 대량의 특화된 공격이 발생할 소지는 충분하다. 이런 경우 행정기관의 업무가 마비되면 국가의 행정이 마비되는 사태가 발생 할 수 있다. 더구나 VoIP의 경

우 일반 포털 사이트에서 쉽게 구할 수 있는 해킹 툴로 쉽게 도청이 가능하다.

행정기관에서 VoIP 이용 시 외부에서의 해킹 공격 등으로 침해사고가 발생 할 수 있으므로, 행정기관에서 VoIP 이용시 취약점분석과 해킹공격에 대한 연구가 필요하다.

본 논문에서는 행정기관에서 유·무선 인터넷을 이용하여 VoIP 이용 시 발생할 수 있는 침해사고 유형을 분석하고 도청, 세션, VoIP 스팸 등에 대한 공격을 실시하여 공격 성공이 되는 취약점을 분석한다. VoIP 침해사고에 따른 공격 유형별 보안성 강화를 위한 보안 대책을 제시한다.

Ⅱ. 관련 연구

2.1. 행정기관 VoIP

행정안전부에서는 행정기관의 인터넷전화 도입 및 운용을 위한 지침을 마련하여 각 기관에 배포했다. 인터넷 전화 서비스 인프라는 대국민서비스 제공 및 국가기관에게 인터넷전화 서비스 제공을 위한 국가기관 전용의 인프라를 의미하며, 이용기관은 인터넷전화 서비스 사업자가 제공하는 IP 인프라를 활용함으로써 인터넷 전화 서비스를 이용하게 된다.

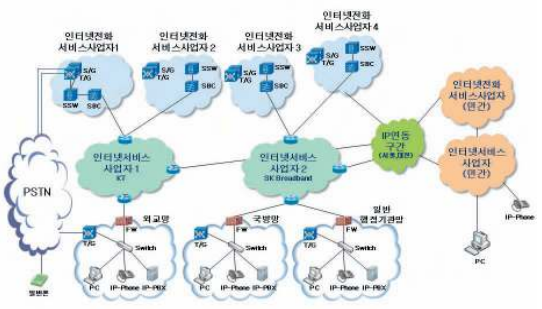

그림 2. WiBro 망 구성도

그림 2는 행정기관 인터넷전화 서비스 구성을 나타낸다. 현재 행정기관 인터넷전화 서비스를 위한 C그룹 사업자는 4개 사업자(KT, SKT, LG 텔레콤, 삼성SDS)가 선정되어 있으며, 각 사업자는 B그룹 사업자의 인터넷망을 사용해 각 기관에 행정기관 인터넷 전화 서비스를 제공하게 된다. 그리고 도입, 운용 지침에서는 이용 기관별 특성에 따라 시스템 구축을 위한 세 가지 모델을 제시하고 있으며, 각 기관은 내부 전화망 교체 계획에 따라 세 가지 모델 중 한 가지를 선택해 구축할 수 있다[1].

2.2. VoIP

VOIP 서비스인 인터넷 전화는 IP 네트워크상으로 음성 및 팩스 데이터를 전송하는 기술로 인터넷 망을 기반으로 하는 음성 응용서비스이다[2].

인터넷전화에 대한 정의는 시기별로 기관별로 조금씩 다르지만 ITU에 따르면 인터넷 전화는 “인터넷 프로토콜을 활용하여 주로 음성형태의 정보를 교환하는 것으로 정의된다. 인터넷전화망은 크게 Gatekeeper(G/K)와 Gateway(G/W) 그리고 초고속 인터넷가입자망 및 백본망으로 구성된다. G/K2)는 인터넷전화 교환기로 호제어, 중계, G/W 및 단말기 상태관리, 빌링 지원 및 다양한 부가서비스 제공 기능을 담당한다.

G/W는 IP망과 PSTN과의 연동을 위한 장비이며, PSTN 교환기의 중계 트래픽과 패킷 전송망 트래픽 간의 미디어 변환(음성 ↔ 데이터) 기능을 수행한다[3].

2.3. VoIP 전화 보안위협

VoIP 전화의 보안위협은 크게 네 가지로 나누어볼 수 있다. 해킹을 통한 통화내용에 대한 불법 도청, 불법광고 전송을 위한 스팸 발송, 요금을 지불하지 않고 인터넷 전화를 불법적으로 사용하는 서비스 오용 공격이 있을 수 있다.

① 불법 도청 : 해킹도구를 통하여 통화내용을 불법으로 도청하는 공격으로서, 기업 내부 등같이 회선을 공유하는 동일한 LAN환경에서 인터넷 전화와 컴퓨터를 사용하는 경우 제한적으로 도청이 가능할 수 있다. 다만, 가정용 ADSL과 같이 LAN 환경이 아닌 경우, 서로 다른 LAN 상호간, 인터넷 전화와 컴퓨터 이용 인터넷망이 분리된 경우, 신호교환장비(IP-PBX)를 통해 일반전화로 인터넷 전화 서비스를 하는 경우, LAN에 연결된 단말에 MAC 인증을 하거나 암호화 통신을 하는 경우에는 도청이 어렵다[4].

② 스팸 발송 : 불특정 다수에게 음성광고 메시지를 전송함으로써 사생활을 방해하거나 프라이버시를 침해하는 VoIP 스팸공격은 기존 일반전화 및 이동전화에 비해 상대적으로 발송 비용이 저

렴하고, 프로그램화된 자동화 도구를 통해 불특정 다수에게 대량 스팸 발송이 가능하다는 특성을 지닌다.

③ 서비스 오용 : 정상적인 사용자의 등록정보를 조작하거나, 추가시켜 통화요금을 지불하지 않고 불법적으로 서비스를 이용하거나, 사용자 정보를 변경하여 인터넷전화를 악용하여 사용할 수 있다 [5].

Ⅲ. 행정기관 VoIP 서비스 공격

3.1. 행정기관 VoIP 서비스 Sniffing 공격 실험

그림 3. 행정기관 VoIP 공격 실험 환경

행정기관 VoIP 서비스 Sniffing을 하기위해서 VoIP의 Packet을 캡처하기 위해서 다음 그림 3와 같은 대학원 랩의 연구실 실험 환경을 구성하였다.

행정기관에서 사용하는 스마트폰의 VoIP 어플을 이용해 상대방 스마트폰에 VoIP 인터넷 전화를 연결하여 통화를 한다. 이때, OmniPeek와 AirPcap 장비가 설치가 되어있는 노트북을 이용을 하여 행정기관 VoIP를 하고 있는 행정기관용 스마트폰의 Packet을 OmniPeek를 이용해 캡처를 한다.

행정기관 VoIP의 Packet을 캡처하기위해 다음과 같이 실험 환경을 구성 하였다.

- AirPcapNX : 802.11 무선 네트워크 패킷 캡처
- Vega X : 안드로이드 2.2, CPU 1GHz, 512MB RAM
- Galaxy S : 16GB 내장 메모리, 안드로이드 2.2, CPU 1GHz, 512MB RAM
- OmniPeek : Version 6.5.1

행정기관용 Smart Phone으로 행정기관 VoIP 음성 통신을 하고 있을 때, AirPcapNX을 이용하여 중간에 패킷을 가로채기를 할 수 있다. 이때 OmniPeek를 이용하여 캡처된 패킷을 분석을 할 수 있다.

Ⅳ. 행정기관 VoIP 도청 및 Packet 분석

다음은 행정기관용 Smart Phone으로 행정기관 VoIP를 사용할 때 패킷을 캡처하는 실험이다. 실험방법은 그림 4와 같이 행정기관용 Smart Phone에서 메신저 어플리케이션을 다운받아 설치한 후 대화하는 도중에 AirPcapNX로 무선패킷을 캡처한다.

그림 4. VoIP 통화

AirPcap으로 패킷을 캡처 후 OmniPeek를 이용하여 패킷을 분석한다.

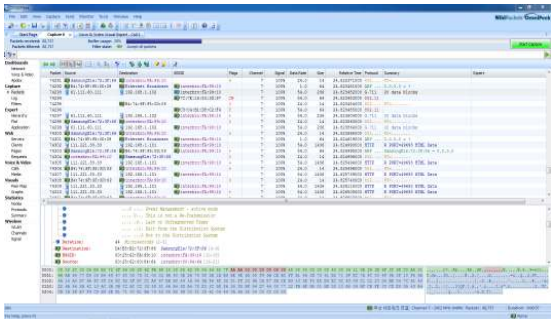

그림 5. VoIP Packet 흐름 분석

그림 5을 보면 IP주소가 192.168.1.102인 Galaxy S와 IP 주소가 192.168.1.101 인 Vega X가 직접 연결하지 않고 61.111.60.111와 111.221.33.33 IP 주소를 통하여 VoIP 통화를

하는 것을 볼 수 있다.

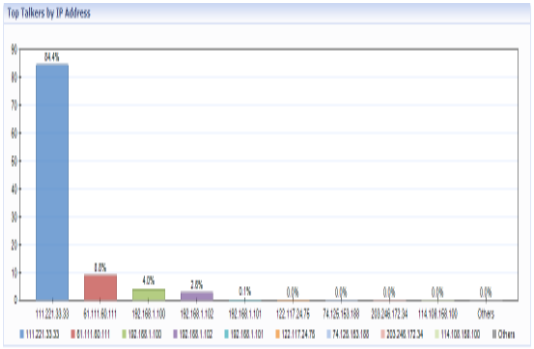

그림 6. VoIP Packet IP당 사용량 분석

이러한 현상은 그림 6에서도 잘 알 수 있다. 그림 6에서 보면 IP 주소가 111.221.33.33이 높은 비율을 차지하며 데이터를 주고 받는 것을 볼 수 있다. 이러한 형태를 볼 때, 행정기관 VoIP 통신시 해당 송수신자와의 직접 연결이 아닌 행정기관 VoIP 업체 서버를 거쳐서 통신하는 것을 유추해 볼 수 있다.

실험을 통하여 얻은 Packet을 분석하여 행정기관 VoIP 사용자가 어떤 대화를 오고 가는지 내용을 분석을 해야 한다.

그림 7. VoIP 통화 내용 분석

그림 7에서는 통화내용을 분석하는 장면이다. 이 논문에서는 총 두 번의 실험을 하였고, 그 중 20초가량 통화 내용이 저장되어 있는 것을 알 수 있다. 이 저장된 VoIP 통화내용은 WMA 파일로 저장 되어있고, 윈도우 미디어 프로그램으로 실행이 가능하여 캡처된 Packet의 내용을 들을 수 있다. 즉 행정기관의 Smart Phone에서 행정기관 VoIP 서비스를 통한 통화 내용에 대한 도청이 가능한 것을 실험으로 증명 하였다.

V. 결 론

본 논문에서는 행정기관 VoIP를 이용하여 행정기관용 Smart Phone의 VoIP 프로그램 접속시 Packet을 분석하고, 저장된 Packet을 이용하여 행정기관 통화내용을 도청을 할 수 있었다.

행정기관 VoIP를 이용시 통화 금액은 상대적으로 저렴하고 행정기관 종사자들이 쉽게 사용 할 수 있다. 하지만, 보안이 취약한 WiFi를 이용하여 행정기관 VoIP를 사용 시, 공격자들은 도청을 통하여 피싱공격, 스팸 등 공격을 할 수 있다. 공격으로 인한 취약점 발생으로 인한 사용자들의 개인정보 유출이나 행정기관의 기밀사항 노출 등의 침해사고 피해를 볼 수 있다.

향후 연구로 행정기관에서 VoIP 사용시 보안 취약점에 대한 보안 대책과 공격에 대한 보안 방어 실험에 대한 연구가 필요하다.

참고문헌

[1] 권성수, 김태완, 양종한, 행정기관 인터넷 전화 : 규격 및 보안 방향성 대한 연구, 정보와 사회, 제14권, PP.29-55, 2008.

[2] 손현구, 이영석, VoIP 이상 트래픽의 플로우 기반 탐지 방법, 정보과학회논문지, 제37권 제4호, pp. 255-316, 2010.08.

[3] 공영일, 인터넷전화의 확산과 통신시장에 대한 함의, PP.39-58, 2009.03.

[4] 조동원, 해킹의 문화정치에서 해킹문화운동으로, 문화/과학, pp.1-29, 2009.08.

[5] 정재훈, 인터넷 전화(VoIP) 보안위협 및 대책, 세상을 이어주는 통신연합, pp.20-23, 2009.

[6] Woo-Sung Chun and Dea-Woo Park, Security Vulnerability Analysis and Forensic Data Research to Attacks on Mobile Stock Trading System in WiBro Network, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.12, pp.291-298, December 2009.

[7] 송진영, 박대우, Smart Phone 인터넷 접속시 패킷 분석 연구, 한국해양정보통신학회논문지, pp.229-232, 2010.10.