행정기관 인터넷전화 보안 대응 모델 개발 연구

박대우* · 양종한**

*호서대학교 벤처전문대학원

**한국정보화진흥원

A Study on Voice over Internet Protocol Security Response Model for Administrative Agency

Dea-Woo Park* · Jong-Han Yang**

*Hoseo Graduate School of Venture, **National Information Society Agency

E-mail : prof1@paran.com · yjh@nia.or.kr

요 약

행정기관 인터넷전화를 구축하여 사용하는 국가정보통신서비스 `C'그룹 사업자에는 KT, SK브로드밴드, LG유플러스, 삼성SDS 4개 사업자가 있다. 행정기관 인터넷전화에 대한 공격을 대비하여 보안 대응 모델에 대한 연구가 필요하다. 본 논문에서는 행정기관 인터넷전화 사업자 별로 보안 대응 대책을 내용으로 조사 분석한다. 행정기관 인터넷전화 보안 침해 모델 개발 연구를 위해 국정원의 5가지 보안 위협에 대해 기밀성을 중심으로 우선순위를 설정하여 ①불법 도청 ②호 가로채기 ③서비스 오용 ④서비스거부 공격 ⑤인터넷전화 스팸 공격에 대한 공격 시나리오 작성하여 분석한다. 행정기관 인터넷전화 보안 대응 모델 개발 연구는 보안 위협별 보호 기술 분석과 보안 침해 단계별 대응 체계 연구를 통해 단계별 대응 모델 개발 연구를 한다.

ABSTRACT

Voice over Internet Protocol calls using administrative agency to build a national information and communication service, `C 'group, providers, the KT, SK Broadband, LG U+, Samsung SDS, as there are four operators. To prepare for an attack on Voice over Internet Protocol for administrative agency, security is a need for research to support the model. In this paper, the Internet telephone business of Administrative Agency to investigate and analyze the specific security measures to respond. Should set priorities around confidentiality about five security threats from NIS to Study of Voice over Internet Protocol Security Response Model for Administrative Agency. ① Illegal wiretapping, ② call interception, ③ service misuse, ④ denial of service attacks, ⑤ spam attacks, write about and analyze attack scenarios. In this paper, an analysis of protection by security threats and security breaches through a step-by-step system to address the research study is a step-by-step development of the corresponding model.

키워드

Administrative Agency Voice over Internet Protocol, VoIP Security, Eavesdropping Attack, Hacking

Ⅰ. 서 론

인터넷전화(VoIP: Voice over Internet Protocol)는 기존의 인터넷망을 활용하여 전화망인 PSTN(Public Switched Telephone Network)망보다 저렴한 가격에 음성통화와 부가서비스를 할 수 있게 해주는 서비스이다.

2005년 7월부터 상용 서비스를 시작한 국내 인터넷전화 서비스 시장은 2008년 약 2,791억원에서 2009년에는 약 4693억원 규모로 성장하였다. 2006년 7월 070식별번호 부여 등으로 인터넷전화 서비스가 본격화 되어 인터넷전화 가입자 및 유선 가입자 추이는 2008년 약 315만명, 2010년 약 956만명으로 2011년 현재 천만명이상이 가입하고 있

다[1].

정부는 통신비 20%이상 절감을 목표로 2013년까지 모든 행정기관의 전화망을 인터넷전화로 바꾸고 있다. 2009년 행정기관에서 인터넷전화 도입 및 운영 지침서를 마련하고 국가정보통신서비스 `C'그룹사업자인 KT, SK브로드밴드, LG유플러스, 삼성SDS를 통해 행정기관에 인터넷전화를 구축하고 있다[2][3].

본 논문은 인터넷환경에서 이루어지는 행정기관 인터넷전화의 취약점을 분석하고 가지고 있기 때문에 행정기관 인터넷전화 보안 침해 모델 개발 연구를 하고 보안 대응 모델 개발 연구를 한다.

Ⅱ. 관련연구

2.1 행정기관의 인터넷전화 이용 유형

국가정보통신서비스 인프라를 통하여 인터넷전화서비스를 구축하고, 이용기관은 국내/국제/이동통화나 SMS, 영상 등을 서비스를 이용할 수 있게 한다. 국가정보통신서비스 `C'그룹을 이용하여 인터넷 기반의 기관간통화, 국내통화, 국제통화, 이동통화 및 문자, 영상통화 등을 인터넷전화 이용유형을 가진다.

2.2 인터넷전화 서비스 관련 보안 침해사고

2009년 10월 17일 국내 별정사업자에 구축된 교환기의 해킹으로 몰디브와 소말리아에 국제전화가 사용되면서 약 1.1억원 이상의 피해 발생시켰다. 해킹 당한 교환기(게이트키퍼)는 인가된 장비의 통화만을 허용하는 접근제어 기능을 미 설정한 상태에서 외부 해커(중국 소재)에 의해 국제전화 무단 사용하여 피해를 발생시켰다[4][5].

Ⅲ. 행정기관 인터넷전화 보안 침해 모델 개발 연구

3.1 행정기관 인터넷전화 보안 위협 도출

2010년 국정원에서 CDMA의 도청문제로 보안 위협을 발견하였다. 인터넷전화의 취약점으로는 비 암호화문제, 패킷 스니핑 및 스푸핑, 인증을 우회하거나 BruteForce 공격과 같은 행정기관 인터넷전화 보안 위협을 도출한다[6][7].

국가정보통신 인프라 및 행정기관 인터넷전화 보안 위협 도출은 국정원의 VoIP에 대한 5가지 보안 위협에 대해 기밀성을 기반으로 우선순위를 설정하면 ① 불법 도청 ② 호 가로채기 ③ 서비스 오용 ④ 서비스거부 공격 ⑤ 인터넷전화 스팸 공격으로 구분하여 볼 수 있다[8][9].

국정원의 기준에 의하여 행정기관 인터넷전화에 가해질 수 있는 보안 위협을 정리하면 불법도청, 호 가로채기, 서비스 오용, 서비스거부 공격, 인터넷전화 스팸 공격이다[10][11].

3.2 행정기관 인터넷전화 보안 침해 시나리오

행정기관 인터넷전화 환경을 이용하여 SIP기반 요청메시지를 보내 DoS 공격을 유발하거나, DoS 공격을 할 수 있다. 스니핑이나 스푸핑을 이용하여 서비스 오용 공격으로 사용자 정보 변조, 과금 우회/회피할 수 있으며, 불법적으로 도청을 할 수 있는 침해 시나리오를 도출한다. 그림 1과 같이 테스트베드를 구성하고 행정기관 인터넷전화 보안 침해 시나리오를 도출한다.

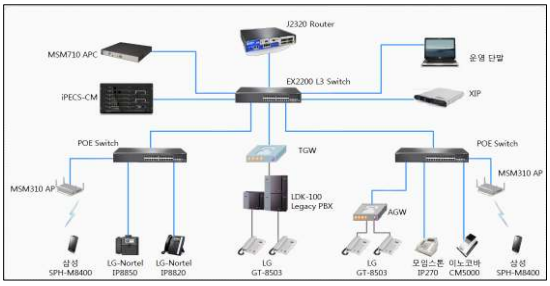

그림 1. 행정기관 인터넷전화 기본기능 시험 환경 구성도

국정원의 행정기관 인터넷전화 5가지 보안위협에 대해 공격시나리오를 작성하고 다음과 같이 실험하였다.

■ 불법도청

SK브로드밴드는 그림 2와 같이 불법 도청 구성도를 구성하여 국가·공공기관 보안 가이드라인 적용 여부(호 교환)에 따라, ① 암호화 기능이 적용된 단말 간 시험통화 수행 ② 동일 네트워크 안에서 미러링을 통해 시험통화 패킷 수집 ③ TLS Handshake 과정 확인을 하고 있다.

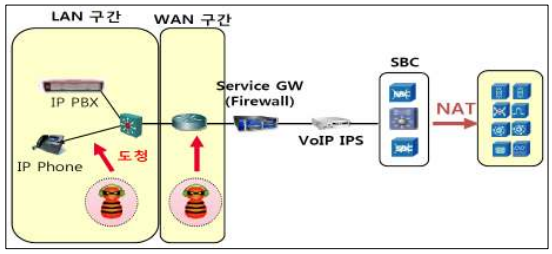

그림 2. SK브로드밴드 불법 도청 구성도

또한, 음성 통화의 경우, ① 암호화 기능이 적용된 단말 간 시험통화 수행 ② 동일 네트워크 안에서 미러링을 통해 시험통화 패킷 수집 ③ 음성통화 과정 확인을 하고 있다.

■ 호 가로채기

KT에서는 공격탐지 구성도를 구성하여 호 가로채기에 Call Hijacking 공격 시나리오를 작성하

였다.

통화시도 시 위변조된 301/302 메시지로 수신자의 통화를 공격자로 돌리는(redirection)공격에서 redirect poison tool 을 이용하여 지속적으로 301/302 메시지를 SIP Server로 송신하여 테스트하고 공격자 PC에서 스크립트를 실행하여 Call-Hijacking 차단 로그를 확인한다.

■ 서비스 오용

KT에서는 서비스 오용 구성도를 구성하여 서비스 오용 공격 중 관리상 오류 공격(SIP server 우회 공격) 시나리오를 실시한다.

① SIP 서버 우회 : 보안장비에 등록되지 않은 SIP Server를 경유하여 SIP 메시지를 전송한다.

② 내부 사용자 위장 : 보안장비에 등록되지 않은 IP, URI로 Outbound SIP 메시지를 전송한다.

③ 공격자 PC에서 스크립트 실행하여 SIP서버 우회 차단로그를 확인한다.

■ 서비스거부 공격

KT는 공격탐지 구성도를 설정하고 DoS/Flooding 시나리오를 실시한다.

그림 3과 같이 구성하여 SIP DoS 공격(Invite Flooding)시나리오를 실시한다.

① IPS, SBC의 Invite 메시지 임계값(Threshold)을 확인한다.

② Call Generator를 통하여 Invite 메시지를 생성한다.

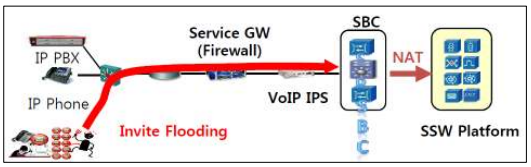

그림 3. SK브로드밴드의 Invite Flooding 구성도

■ 인터넷전화 스팸 공격

KT에서는 인터넷전화 스팸 공격에 대한 구성은 다음과 같다.

① Call Spam으로 동일 발신자로 100건 이상의 실패 또는 짧은 콜을 반복하여 보낸다.

② 메시지 Spam으로 대출이라는 문구를 삽입하여 콜을 실행한다.

③ 공격자 PC에서 스크립트를 실행하여 해당 발신자 콜 스패머로부터 차단 로그를 확인한다.

Ⅳ. 행정기관 인터넷전화 보안 대응 모델 개발 연구

4.1 행정기관 인터넷전화 보안 대응 대책

국가정보통신 인프라 관리기관에서는 매년 주요정보통신기반시설에 대한 보호대책을 수립하여 관계 중앙행정기관에 제출한다.

2001년 정보통신기반보호법 시행 이후, 「정보통신기반 보호법」이 2007년도에 개정되었다. 「정보통신기반 보호법」에서는 보호계획에 포함되어야 할 내용을 다음과 같다.

4.2 행정기관 인터넷전화 보안 장비 대책

행정기관 인터넷전화에 대한 전용 보안장비는 CC인증을 획득한 인터넷전화 전용 보안장비(방화벽, IPS 등)를 도입·사용하여야 한다. 그림 4는 인터넷전화 전용보안장비 구축 개념도이다.

그림 4. 인터넷전화 전용 보안장비 구축 개념도

4.3 행정기관 인터넷전화 보안 위협별 보호 기술

행정기관 인터넷전화는 암호화된 데이터를 주고받는 프로토콜과 제어 신호(SIP) 및 미디어 데이터(RTP), IP-Sec, TLS, DTLS, SRTP 등의 보안 프로토콜과 AES, SEED, ARIA 등의 암호화 기법을 이용하여 데이터를 암호화하고, MIKEY, SDES 등 키 교환 방식을 결합하는 행정기관 인터넷전화의 보안 대응 모델에서 표 1은 국가정보통신 인프라 C그룹 사업자 별 인터넷전화 보안 대응 대책 비교한 표이다.

표 1. 국가정보통신 인프라 인터넷전화 보안 대응 대책 비교

사업자명	서비스 거부공격
A	·네트워크 전용 IPS ·VoIP 전용 IPS
B	·사업자 레벨의 DDoS 대응체계 제공 ·CC인증기반 인터넷방화벽, VoIP IPS, VoIP전용방화벽 등
C	IPS, SBC의 Register/Invite메시지의 임계값(Threshold)확인
D	·3중 방어체계(IPS + F/W + SBC) 구축 ·Rate-Limit, Call Gapping 등 기능 제공
사업자명	**도청**
A	·신호 : TLS ·미디어 : sRTP
B	·신호 : TLS

	·미디어 : sRTP ·AES/ARIA 암호화
C	·신호 : TLS ·미디어 : sRTP ·TLS Handshake
D	·신호 : TLS ·미디어 : sRTP ·AES/ARIA 암호화 ·PKI기반 공인인증서
사업자명	**서비스 오용**
A	·접속 라우터 홉 카운터 제한 ·통화패턴 관리로 임계치 관여
B	공개키 기반의 기기인증서를 통해 상호 기기인증
C	·SIP Invite 메시지 전송, 차단 확인 ·Topology Hiding, 메시지 Digest 확인
D	·네트워크/OS 레벨 접근제어 ·Topology Hiding
사업자명	**호 가로채기**
A	·301/302 메시지 확인 ·단말 로그 분석 ·MD5 부여
B	·Authentication 과정확인 ·MD5 부여 ·TLS Handshake
C	·Authentication 과정확인 ·MD5 부여 ·TLS Handshake
D	·TLS 시그널링 ·PKI 인증서 ·SIP 인증 ·3단계 인증서(Root, 공인 인증기관, 장비)
사업자명	**인터넷 전화스팸**
A	VoIP 전용 IPS
B	·기관의 VoIP IPS 및 VoIP전용방화벽 등
C	Source IP Blocking, Source Port Blocking, Source ID Blocking 동작 확인
D	·TLS 기반의 암호화 서비스 ·IPS 및 SBC의 Call Gapping

V. 결 론

국가정보통신 인프라 및 행정기관 인터넷전화를 이용할 때, 행정기관 인터넷전화망에서 발생할 수 있는 이용 유형과 보안 대응 대책을 알아보고 분석을 바탕으로 보안 침해 모델과 보안 침해 시나리오를 도출하고, 보안 위협별 보호 기술 분석과 개발과 보안 침해 단계별 대응 체계와 방안을 마련하여 국가행정의 행정기관 인터넷전화에 대해 보안성을 강화하고, 안전성을 강화하여 국가정보통신 발전에 기여 할 수 있을 것이다.

참고문헌

[1] 이문길(TTA), 행정기관 인터넷전화 보안규격 시험인증 기술동향, 2011.03.04.
[2] 행정안전부, 국가정보통신서비스 이용지침서, 2011.04.
[3] 한국정보통신기술협회(TTA), 행정기관 인터넷전화 적용 표준 및 인증, 2010.08.20.
[4] 국가정보원(NIS), 국가 공공기관 인터넷 전화 보안 가이드라인, 2009.05.
[5] 한국인터넷진흥원(KISA) – 인터넷전화 보안위협 및 보안정책, 2010.08.
[6] 정현철(KISA), 안전한 인터넷전화 서비스제공을 위한 보안대책, 2009.06.11.
[7] 정재훈(방송통신위원회), 인터넷전화(VoIP) 보안위협 및 대책, 2009.
[8] 권성수, 김태완, 양종한, “행정기관 인터넷 전화 : 규격 및 보안 방향성 대한 연구,” 정보와 사회, 2008.
[9] 법제처, 행정정보통신망운영관리규정, 2008.07.18.
[10] 한국과학기술한림원(KAST), 국가전산망의 네트워크 및 시스템 보안에 관한 연구, 2009.
[11] 천우성, 박대우, 양종한, "Smart Phone VoIP 서비스에 대한 공격과 도청 연구," 한국해양정보통신학회논문지, 제15권, 제6호, pp.1313-1319, 2011.6.