IP-PBX에 대한 해킹 공격 분석 연구

천우성* · 박대우* · 윤경배**

*호서대학교 벤처전문대학원 · **김포대학교

A Study of Hacking Attack Analysis for IP-PBX

Woo-Sung Chun* · Dea-Woo Park* · Kyung-Bae Yoon**

*Hoseo Graduate School of Venture · **Kimpo College

E-mail : deux8522@gmail.com · prof1@paran.com · kbyoon@kimpo.ac.kr

요 약

인터넷전화는 기존의 PSTN에 비해 통신비용 절감과 사용의 편리성 때문에, 인터넷전화 사용이 확산되고 있다. 광대역통합망(BCN) 구축 일환으로 민간 인터넷사업자와 더불어 2010년 이후 행정기관에 모든 전화망을 인터넷전화로 전환하고 있다. 본 논문에서는 인터넷전화에서 사용되는 IETF SIP 기반 IP-PBX에 대한 해킹 공격 분석 연구이다. 인터넷전화 시스템과 똑같이 구축되어 있는 테스트베드의 IP-PBX에 대한 해킹 공격을 하고 결과를 분석 하여 취약점을 도출한다. 안전한 인터넷전화를 위하여 취약점을 개선한 보안대책을 제시한다.

ABSTRACT

Voice over Internet Protocol(VoIP) compared to the traditional PSTN communications costs and because of the ease of use has been widespread use of VoIP. Broadband Convergence Network (BCN) as part of building with private Internet service provider since 2010, all government agencies are turning to the telephone network and VoIP. In this paper, we used the Internet on your phone in the IETF SIP-based IP-PBX is a hacking attack analysis studies. VoIP systems are built the same way as a test bed for IP-PBX hacking attacks and vulnerabilities by analyzing the results yielded. Proposes measures to improve security vulnerabilities to secure VoIP.

키워드

IP-PBX, Hacking Attack, Analysis, Vulnerabilities

Ⅰ. 서 론

인터넷전화는 국내뿐만 아니라, 해외 인터넷전화까지도 사용이 가능하다. 특히 본인의 노트북이나 이동단말을 이용하여 기존의 PSTN에 비해 상대적으로 값싸고, 쉽게 사용이 가능하다.

하지만 citibank 영국지점과 연동된 SIP-gateway 및 IP-PBX 대상으로 무작위 INVITE 해킹공격이 발생하였다. IP-PBX에 대한 모든 메시지의 Contact 필드 IP는 '217.23.7.47'(포르투갈)로 고정되어 있었다.

이와 같은 IP-PBX에 대한 공격을 통해 Scan을 시도하고 원하는 IP-PBX의 정보를 탈취하여 국내외 인터넷전화에 대한 서비스오용, 불법과금 등 피해를 유발할 수 있다[1][2].

본 논문에서는 인터넷전화에서 사용되는 IETF SIP 기반 IP-PBX에 대한 해킹 공격 분석 연구이다.

인터넷전화 시스템과 똑같이 구축되어 있는 인터넷전화 테스트베드에서 IP-PBX에 대한 해킹 공격을 하고, 해킹 결과를 분석 하여 취약점을 도출한다. 그리고 안전한 인터넷전화를 위하여 취약점을 개선한 보안대책을 제시한다.

Ⅱ. 관련연구

2.1 IP-PBX 개념

IP-PBX(Internet Protocol-Private Automatic Branch exchange)는 데이터 네트워크를 통해 보이스와 비디오를 전달할 수 있도록 PSTN과 연동되는 사설 교환기를 의미한다. IP-PBX의 하드웨어는 서버로써 동작하며 일반적으로 사용되는 X86서버에 IP-PBX 소프트웨어를 설치해서 PBX로 동작을 하게 한다. IP-PBX는 RJ-45 커넥터를 통해서 스위치에 연결이 되고, 호 처리, 가입자 수용, 부가서비스 등 PBX와 똑같은 역할을 한다. 그러나 PBX와 같이 PSTN을 연결하는 기능은 Voice Gateway에 일임을 하고, 음성사서함과 같이 리소스가 많이 필요한 부가서비스도 별도의 서버로 독립적으로 수행한다[3][4].

IP-PBX는 IP 네트워크에서 사용되기 때문에 거리에 제약이 없으며 IP Phone에 부가서비스에 대한 소프트키, 혹은 XML을 통한 그림버튼제공 등으로 직관적이고 사용자에게 편리한 인터페이스를 제공하는 것이 장점이다[5].

2.2 IP-PBX 기능

IP-PBX의 가장 중요한 기능 중 하나는 호처리(Call Processing)이다. 전화를 걸고 받을 때 시그널(Signal)과 미디어(Media) 두 가지 형태의 패킷이 만들어진다. 시그널은 발신자 전화번호, 수신자 전화번호, 코덱, IP Address등, 음성 이외의 모든 전화를 위한 정보를 담고 있다. 반면 미디어는 정해진 코덱으로 인코딩된 음성을 RTP(Real Time Protocol)로 전송하게 된다. 시그널은 SIP, H.323, MGCP, SCCP 등 다양한 종류가 있으며 각 시그널링 프로토콜은 각각 용도나 환경에 맞게 사용된다[6][7]. IP-PBX는 호 처리 이외에도 IP Phone, Voce Gateway 등의 등록 및 Control, Dial Plan을 보유 및 관리, 전화기 부가서비스 제공, 디렉토리 서비스, 프로그래밍 인터페이스 제공 등 다양한 기능을 수행한다[8].

Ⅲ. IP-PBX 취약점

3.1 IP-PBX 동작 원리 분석

그림 1은 IP-PBX와 IP Phone간 동작 원리를 나타내었다.

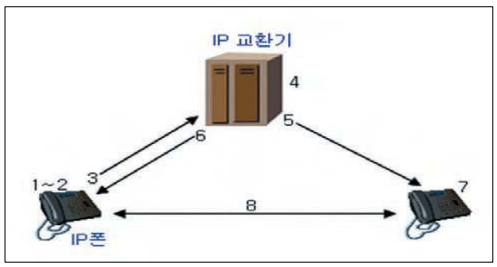

그림 1. IP-PBX와 IP Phone간 동작 원리

호 및 세션 제어시스템으로 각 기관에서 운용중인 사설교환기 역할 수행한다. IP Phone 및 AG(Access Gateway)를 수용 관리하며, 인터넷 전화 서비스사업자의 SSW(Softswitch)와 연동하는 역할 수행한다.

3.2 실험장비

표 1의 CSC Series 장치와 표 2의 iPECS-COM(CM-S2k) 장치를 실험장비로 준비를 하였다.

표 1. CSC Series 장치의 주요 규격

제품명	Size	장비사양
CSC Series	2U	·IBM x3650 (Red hat Enterprise Linux 4.0) ·CPU : 3.0GHz * 2 ·Memory : 8G, HDD : 146GByte*2ea, DVD ·MySQL, 전원이중화
		
주요기능	**내용**	
Protocol	·SIP(RFC3261), SIP-connect	
Security	·sRTP, TLS, Ipsec ·행정안전부 암호화 기술규격 준수	
QoS	·CAC(Call Admission Control)	

표 2. iPECS-COM(CM-S2k) 장치의 주요 규격

제품명	Size	장비사양
iPECS-COM(CM-S2k)	5U	·OS(Linux CentOS 5.1) ·CPU : 1.5~2.0 Ghz ·Memory : 2G, ·HDD : 120GByte SAATA
		
주요기능	**내용**	
Protocol	·SIP(RFC3261), SIP-connect	

Security	·HTTP Digestion, sRTP, TLS, AES, SDES ·행정안전부 암호화 기술규격 준수
QoS	·피무, 802.1p/q, Diffserv 등 지원

3.3 IP-PBX 스캐닝

그림 2는 스캐닝을 통해 IP-PBX의 정보를 검색하였다.

그림 2. 스캐닝을 통한 IP-PBX 정보검색

스캐닝을 통해 IP-PBX의 IP를 알아내어 IP로 접속을 시도한다. 또한 그림 3과 같이 IP-PBX의 IP를 통하여 외부망에서 접속을 시도한다.

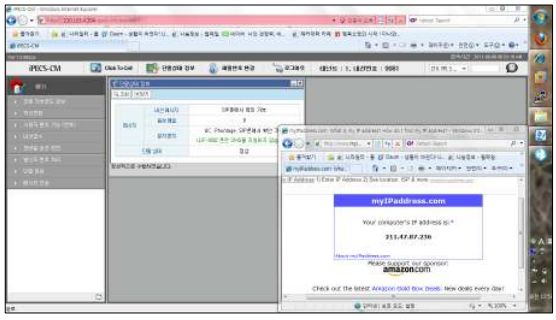

그림 3. IP-PBX의 IP로 외부망에서 접속화면

스캐닝을 통해 알아낸 IP-PBX의 IP로 내부망 및 외부망에서도 접속 가능한것으로 확인하였다.

Ⅳ. IP-PBX에 대한 해킹 공격 분석

4.1 IP-PBX 해킹

Scanning한 자료를 바탕으로 외부망에서 접속 가능한지 확인하였다. 외부망에서 접속이 가능한 것을 확인하였고, XSS 취약점을 이용하여 IP-PBX 공격이 가능하다.

그림 4. 외부망에서 공격 시도

그림 4와 같이 내/외부망에서 모두 접속이 가능하였고, 전체 웹 페이지가 플래시로 구성되어 있으며, 플래시의 경우 디컴파일을 통하여 공격이 가능하다.

4.2 IP-PBX 관리자 페이지 해킹

또한, IP-PBX의 IP를 통하여 관리자 페이지로 접속하여 IP-PBX에 연결되어 있는 모든 시스템을 통제할 수 있다.

그림 5. IP-PBX에 운영자 계정 생성

그림 5와 같이 운영자 계정을 생성하고 등록된 전화번호를 확인한다. 또한, 운영자 계정으로 임의의 번호를 생성하고 외부에서 접속 가능하도록 설정을 하여 등록을 한다.

그림 6과 같이 IP-PBX의 인증서를 쉽게 획득할 수 있다.

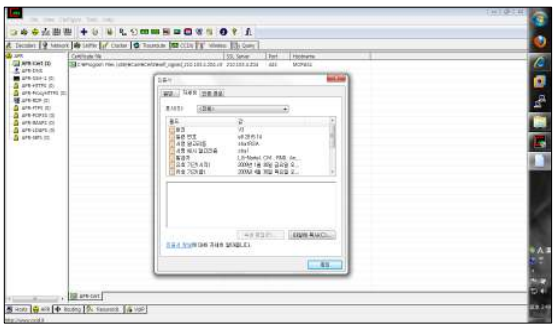

그림 6. PBX 인증서 획득

4.3 IP-PBX에 Invite Flooding 공격

PBX에 대해 BackTrack5를 이용하여 그림 7과 같이 Invite Flood공격을 시도하였다.

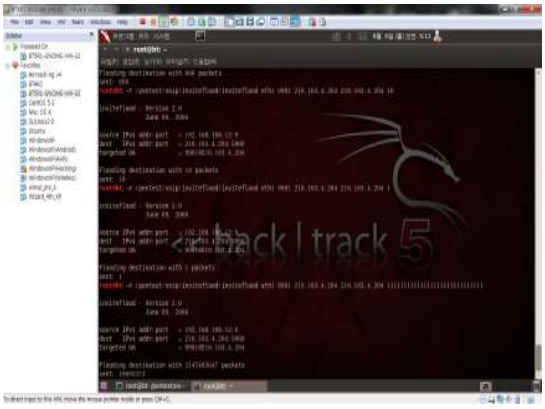

그림 7. PBX에 대한 Invite Flood 공격 시도

IP-PBX는 내부망과 외부망에서 접속이 가능하여 내부망에서는 공격이 이루어지는 것은 어렵게 생각되어 외부망에서 Invite Flood공격을 시도하였다.

4.4 IP-PBX 공격 후 로그기록 삭제

IP-PBX에 관리페이지에 접속하여 IP-PBX에 등록되어 잇는 IP Phone 정보나 여러 가지 정보 등을 확인하고 일의의 IP-Phone 정보를 설정하는 등 여러 가지 정보들을 알아내고 수정하였다.

정보를 알아내고 수정한 것을 관리자가 알아낼 수 없게 접속하여 행해진 여러 가지 작업들에 대해 로그기록을 삭제한다. 로그 기록을 삭제하게 되면 어디서 무슨 정보를 수정하였는지 관리자는 알 수 없게 하는 것이다.

V. 결 론

인터넷전화에서 교환기 역할을 하고 있는 IP-PBX에 대한 공격을 하기위해 Scan을 시도하고 원하는 IP-PBX의 정보를 탈취하여 인터넷전화에 대한 서비스오용, 불법과금 등과 같은 해킹 공격을 통해 인터넷전화 시스템과 똑같이 구축되어 있는 인터넷전화 테스트베드에서 IP-PBX에 대한 해킹 공격을 하고, 외부망 접속이나 사용자 계정 생성 등의 해킹 결과를 분석 하여 취약점을 도출하여 피해를 유발할 수 있는 공격이 가능한 것을 확인하였다.

향후 연구에서는 인터넷전화의 취약점을 바탕으로 해킹 공격이 가능하지 않고 안전한 인터넷전화를 위하여 취약점을 개선하고 보안대책을 제시하여야 하겠다.

참고문헌

[1] 정윤수, 김용태, 박길철, "저가형 IP-PBX 미디어 서비스 플랫폼 설계," 한국정보기술학회 논문지, 제9권, 제6호, pp.197-207, 2011년 6월.

[2] 최재원, "B-ISDN 프로토콜 내장의 멀티미디어통신용 IP-PBX 시스템 구현," 한국해양정보통신학회논문지, Vol.11, No.12, pp.2256-2264, 2007년 12월.

[3] Q. F. Liu, H. H. Zhou, and Y. J. Qin, "Design and Implementation of SIP Phone Based on SCTP and DCCP", Telecommunication Engineering, pp.32-36, Jan. 2008.

[4] B. C. Zhang, Q. L. He, and K. Qu, "The Design and Realization of Distance Teaching System Based on SIP Protocol", Microelectronics & Computer, pp. 150-153, March 2007.

[5] A. Johnston, R. Sparks, C. Cunningham, S.Donovan, and K. Summers, "Session Initiation Protocol Service Examples", draft-ietf-sip-pingservice-examples-07, pp. 1-168, July 2004.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, and A. Johnston, "SIP: Session Initiation Protocol", RFC 3261, pp. 1-269, June 2002.

[7] A. B. Roach, "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, pp. 1-38, June 2002.

[8] W. Lu, W. Zeng, " The Research of Asterisk-An Open Source PBX", Computer Systems Applications, pp. 80-83, Feb. 2007.