IP-PBX에 대한 해킹공격과 포렌식 증거 추출

박대우
호서대학교 벤처전문대학원

Extraction of Forensic Evidence and Hacking Attacks about IP-PBX

Dea-Woo Park
Hoseo Graduate School of Venture
E-mail : prof_pdw@naver.com

요 약

인터넷전화는 기존의 일반전화인 PSTN에 비해 통신비용이 저렴하고 사용이 편리하여 인터넷전화의 사용이 확산되고 있다. 광대역통합망(BCN) 구축 일환으로 인터넷사업자(KT, SKT, LG)가 행정기관에 모든 전화망을 인터넷전화로 전환하고 있다. 또한 일반인들도 사용하는 인터넷전화 서비스를 하고 있다. 본 논문에서는 인터넷전화에서 사용되는 IETF SIP 기반 IP-PBX에 해킹공격에 대한 분석을 하고 연구를 한다. 인터넷전화 시스템과 똑같이 구축되어 있는 테스트베드에서 IP-PBX에 대한 해킹공격을 실시하고 결과를 분석하여 포렌식 증거를 추출하는 연구를 한다. 인터넷전화를 해킹하여 범죄에 사용되었을 때 법적 효력을 가지는 포렌식 증거로 사용할 수 있는 방법을 제시한다.

ABSTRACT

Internet phone, communication cost and easy-to-use low-cost compared to the PSTN is a mobile phone of a conventional, and use of the Internet phone is spreading. Construction as part of the broadband convergence network(BCN), Internet service provider(KT, SKT, LG) has converted to Internet phone telephone network to all government agencies. In addition, members of the public also have an Internet phone service that you are using. In this paper, we analyze the hacking attack on IP-PBX in the IETF SIP-based that are used in Internet telephony, to the study. The test bed is constructed in the same way as the Internet telephone system to perform studies carried hacking attacks on IP-PBX, analyze the results and to extract evidence forensics. When used in crime by hacking the Internet telephone, we propose a method which can be used as evidence in forensic having legal effect.

키워드
IP-PBX, 해킹 공격, 분석, 취약점

Key word
IP-PBX, Hacking Attack, Analysis, Vulnerabilities

Ⅰ. 서 론

인터넷전화는 국내외에 인터넷망으로 연결되어 있으면 사용이 가능하다. 특히 PC, 노트북이나 이동단말을 이용하여 인터넷망을 이용하여 전화 통화를 하기 때문에 기존의 PSTN에 비해 상대적으로 통화료가 싸고, 쉽게 사용이 가능하다.

2012년 6월, 국내 모 여행사의 VoIP가 해킹돼 미국, 영국 등지에서 국제전화가 사용되면서 수천만 원의 피해가 발생했다. 미국에서도 정부, 기업용 교환기 대상 과금 우회 공격으로 피해액만 55억 달러에 달했던 것으로 추정되고 있다. 보안이 취약한 무선랜(Wi-Fi) 접속장치(AP) 등을 해킹해 인터넷전화의 통화내용을 불법적으로 청취하는 도청의 위험성도 끊임없이 제기되고 있다.

디도스 공격에도 인터넷전화가 활용되기도 한다. 악성코드에 감염된 스마트폰이나 인터넷전화를 이용해 인터넷전화 교환기를 공격해 서비스를 마비시키는 방식이다. 지난 2009년에도 국제 해커가 국내의 한 업체 인터넷전화를 해킹해 1억 원이 넘는 국제전화 요금을 유발시키기도 했다.

전문가들은 이들이 인터넷전화 교환기(IPBX)에 설정된 암호를 알아내 교환기에 접속한 뒤 국제전화를 거는 수법을 사용하는 것으로 추정하고 있다[1].

2009년 9월, 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[2].

본 논문에서는 인터넷전화에서 사용되는 IETF SIP 기반 IP-PBX에 대한 해킹공격을 실시하고 분석하여 포렌식 증거를 추출하는 연구이다.

인터넷전화 시스템이 구축되어 있는 인터넷전화 테스트베드에서 IP-PBX에 대한 해킹 공격을 하여 해킹공격에 대한 결과를 분석하고 취약점을 도출하여 안전한 인터넷전화를 위하여 취약점을 개선하는 보안대책을 제시한다.

Ⅱ. 관련연구

2.1 IP-PBX

IP-PBX(Internet Protocol-Private Automatic Branch exchange)는 네트워크에서 데이터망을 이용하여 음성 데이터와 비디오 데이터를 전달할 수 있도록 PSTN(Public Switched Telephone Network)과 연동되는 사설 교환기이다. IP-PBX의 하드웨어는 서버로써 동작하며 일반적으로 사용되는 X86서버에 IP-PBX 소프트웨어를 설치해서 PBX로 동작을 하게 한다. IP-PBX는 RJ-45 커넥터를 통해 스위치에 연결이 되어, 호 처리, 가입자 수용, 부가서비스 등의 PBX와 같은 역할을 한다. 그러나 PBX와 같이 PSTN을 연결하는 기능은 Voice Gateway가 한다. 음성사서함과 같이 리소스가 많이 필요한 부가서비스의 경우에는 별도의 서버를 사용하여 독립적으로 수행한다[3][4].

그림 1은 IP-PBX와 IP Phone사이에 동작 원리를 나타낸 것이다.

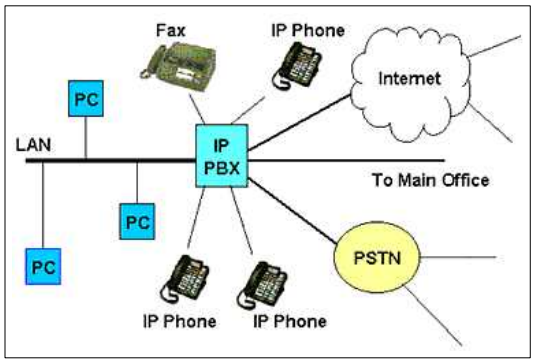

그림 1. IP-PBX와 IP Phone간 동작 원리

호 제어 시스템 및 세션 제어시스템으로 운용중인 사설교환기의 역할 수행한다. IP Phone 및 AG(Access Gateway)를 수용하여 관리하며, 인터넷전화 서비스사업자의 SSW(Softswitch)와 연동하는 역할을 수행한다.

IP-PBX는 인터넷 네트워크에서 사용하기 때문에 거리에 제약이 없으며 IP Phone에 부가서비스에 대한 소프트키나 XML을 통한 그림버튼제공 등으로 사용자에게 편리한 인터페이스를 제공한다.

2.2 IP-PBX 기능

IP-PBX 기능 중 하나는 호 처리(Call Processing)이다. 전화를 걸고 받을 때, 시그널(Signal)과 미디어(Media)로 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(Session Initiation Protocol), H.323, MGCP(Media Gateway Control Protocol), SCCP(Signalling Connection Control Part) 등의 다양한 종류가 있으며, 각 시그널링 프로토콜은 각각 용도나 환경에 맞게 사용된다[5][6]. IP-PBX는 호 처리 이외에도 IP Phone, Voice Gateway 등의 등록 및 Control, Dial Plan을 보유 및 관리, 전화기 부가서비스 제공, 디렉토리 서비스, 프로그래밍 인터페이스 제공 등 다양한 기능을 수행한다[7].

Ⅲ. IP-PBX 해킹 공격

3.1 IP-PBX 스캐닝 공격

IP-PBX의 정보를 알아내기 위해 스캐닝을 통해 그림 2와 같이 실시하여 IP-PBX의 정보를 검색한다.

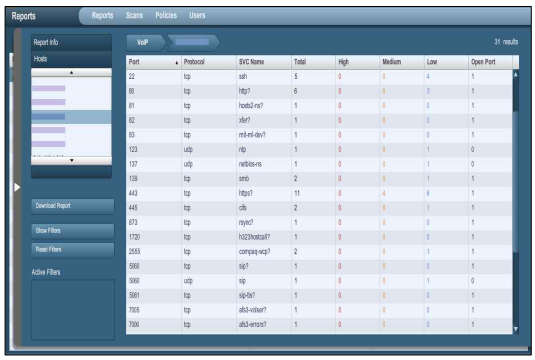

그림 2. 스캐닝을 통한 IP-PBX 정보검색

스캐닝을 통해 IP-PBX의 IP를 알아내고 해당 IP로 접속을 시도한다. 또한 외부망에서 해당 IP-PBX의 IP를 통하여 접속이 가능한지 확인한다.

3.2 IP-PBX 해킹

해당 IP-PBX의 IP로 외부망에서 접속이 가능한 것을 확인하였고, 접속한 IP-PBX의 관리자 웹 페

이지에서 XSS 취약점을 이용하여 IP-PBX의 공격이 가능하다.

그림 3. 외부망에서 공격 시도

그림 3과 같이 내부망 및 외부망에서 모두 접속이 가능한 것을 확인하였고, 전체 웹 페이지가 플래시로 구성되어 있으며, 플래시의 경우에느 디컴파일을 통하여 공격이 가능하다.

3.3 IP-PBX에 Invite Flooding 공격

해당 IP-PBX에 BackTrack5를 이용하여 Invite Flood공격을 그림 4와 같이 시도한다.

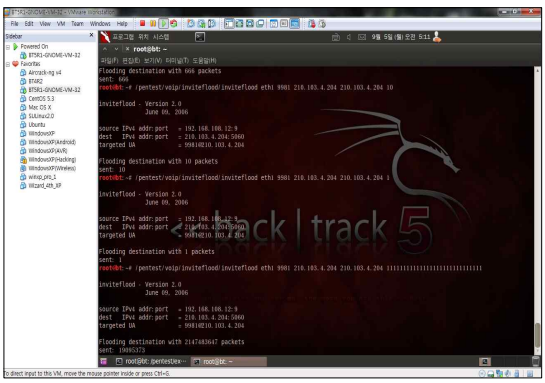

그림 4. PBX에 대한 Invite Flood 공격 시도

해당 IP-PBX는 내부망과 외부망에서 접속이 가능하여 외부망에서 Invite Flood공격을 시도하였다.

Ⅳ. IP-PBX 해킹에 대한 포렌식 증거 추출

4.1 IP-PBX 해킹 자료 분석

기본적으로 외부에서 모든 공격 시나리오가 실시되었다. 그림 5는 외부에서 접속할 수 있는 기본 IP를 통해 스캐닝을 하였고 취약점을 분석하였다.

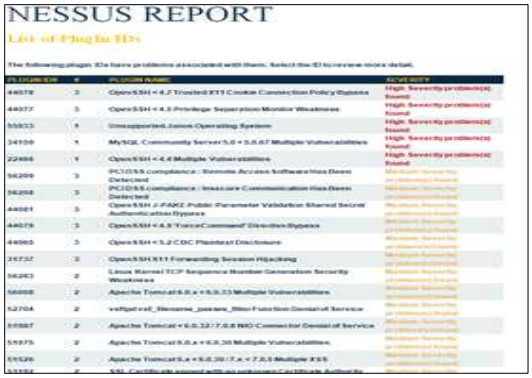

그림 5. 스캐닝을 통한 VoIP 보안장비와 NAT장비 취약점 분석

스캐닝을 통해 알아낸 VoIP 보안장비와 NAT장비의 IP주소를 파악하여 취약점에 대한 공격을 실시하였다.

4.2 IP-PBX 포렌식 증거 추출

그림 6은 테스트베드 네트워크 모니터링 상에서 ARP 현황을 보여주는 것으로 미사용 IP가 발견되었다.

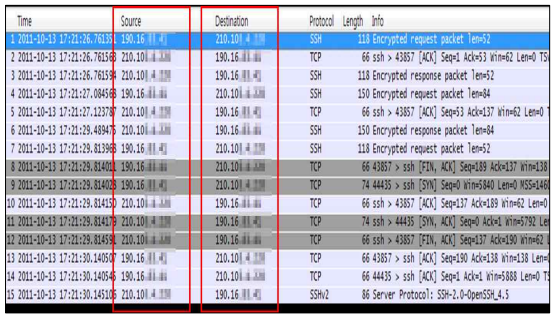

그림 6. 여러 Source IP로 부터 접근시도

그림 7은 L3 스위치에서 모니터 된 것으로 190.16.xxx.xxx는 테스트베드에서 사용하지 않는 IP대역으로 확인 되었고, 210.103.xxx.xxx는 단말이나 서버에서 사용하지 않고 있는 IP로 모니터링 되었다.

그림 7. 불특정 Source IP에 대한 경로 추적

4.3 IP-PBX 포렌식 보고서

인터넷전화에서 포렌식 증거 자료는 법정에서 인정하는 수사관이 인증된 포렌식 툴과 포렌식 기술과 포렌

식 증거 자료를 생성하고, 백업 프로그램을 통해 추출할 수 있는 증거 자료의 원본성과 무결성을 입증하기 위해 Hash 함수 값을 비교하여, 무결성을 입증한 자료를 보고서에 같이 제출한다.

V. 결 론

인터넷전화에서 교환기 역할을 하고 있는 IP-PBX에 대한 해킹 공격을 위해 스캐닝을 시도하고 원하는 IP-PBX의 IP 정보와 관리자 권한을 탈취하여 인터넷전화에 대한 서비스오용, 불법과금 등의 해킹 공격을 하고, 외부망에서 접속을 하여 사용자 계정 생성 등의 해킹 결과를 분석 하여 취약점을 도출하였다.

서비스오용, 불법과금 등의 해킹 공격에 대한 법정에 증거자료로 사용하기 위해 해당 IP-PBX의 공격 증거 자료를 포렌식을 통해 자료를 추출하고 포렌식 자료를 생성하여 포렌식 보고서를 작성한다. 포렌식 보고서는 법적 증거자료로 사용하여 해킹 공격자에게 법적인 책임을 줄 수 있는 연구를 하였고 해킹 공격에 대한 보안 방안을 제시하였다.

참고문헌

[1] 박태우 기자, “한달 전화료 5천300만 원? 인터넷 국제전화 해킹 '주의보',” 부산일보, http://news20.busan.com/controller/newsController.jsp?newsId=20120628000162, 2012년 6월.

[2] 천우성, 박대우, 윤경배, “IP-PBX에 대한 해킹 공격 분석 연구,” 한국해양정보통신학회 종합학술대회논문집, Vol.15, No.2, p.273-276, 2011년 10월.

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

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