유무선 인터넷전화 단말에 대한 해킹 공격 연구

권세환* · 박대우*

*호서대학교 벤처전문대학원

A Study on Hacking Attack of Wire and Wireless Voice over Internet Protocol Terminals

Se-Hwan Kwon* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : light@dgu.edu · prof1@paran.com

요 약

최근 인터넷전화는 IP기반에서 유선과 무선을 이용하여 음성뿐만 아니라 멀티미디어 정보전송을 제공한다. 유무선 인터넷전화는 네트워크상에서 인터넷전화 호 제어 신호 및 통화 내용의 불법 도청이 용이하며, 서비스 오용 공격, 서비스 거부 공격의 대상이 될 수 있는 등 기존 유선전화에 비해 여러가지 보안취약점이 존재한다. 본 논문에서는 인터넷전화 단말에서 IP Phone 정보를 획득하기 위한 스캐닝을 통해 IP Phone의 패스워드를 확인하고, 관리자 페이지를 통해 로그인을 성공한다. 그 후 IP Phone 관리자 페이지를 접속한 후 VoIP 설정 화면으로 전화번호, 포트번호, 인증번호 등을 수정한다. 또한 관리자 페이지에서 등록되어 있는 IP Phone들의 통화기록을 확인하여 개인정보 해킹을 연구한다.

ABSTRACT

Recently, Voice over Internet protocol(VoIP) in IP-based wired and wireless voice, as well as by providing multimedia information transfer. Wired and wireless VoIP is easy on illegal eavesdropping of phone calls and VoIP call control signals on the network. In addition, service misuse attacks, denial of service attacks can be targeted as compared to traditional landline phones, there are several security vulnerabilities. In this paper, VoIP equipment in order to obtain information on the IP Phone is scanning. And check the password of IP Phone, and log in successful from the administrator's page. Then after reaching the page VoIP IP Phone Administrator Settings screen, phone number, port number, certification number, is changed. In addition, IP Phones that are registered in the administrator page of the call records check and personal information is the study of hacking.

키워드

Hacking Attack, Wire VoIP, Wireless VoIP, Eavesdropping, Voice over Internet Protocol

Ⅰ. 서 론

2009년 3월 26일 SIP 단말에서 패스워드 획득 프로그램이 공개되었다. 이 해킹 프로그램을 실제 실험한 결과 Linksys, Grandstream, AVM사의 단말에서 패스워드 획득하는 데, 성공 하였다.

또한 대만 보안업체인 Trend Micro는 인터넷 전화 관련 봇넷인 “Koobface Variant” 발견을 발표 하였다. 내용은 그림 1처럼 “Koobface Variant”는 Skype 소프트폰 설치 후에 PC를 감염시켜 통화내역, 주소록 정보, 위치정보 등 사용자 통화 정보를 탈취하고, 주소록에 있는 전화번호를 대상으로 무작위 SMS 발송을 하는 기능을 가지고 있다는 것이다.

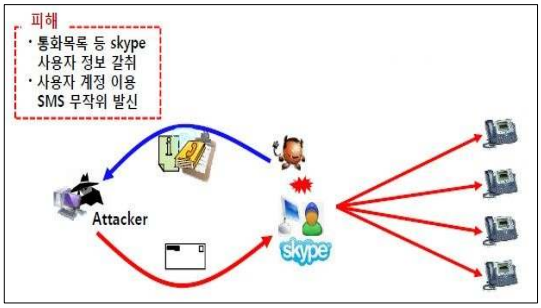

그림 1. Skype 정보 탈취 및 SMS 발송 봇넷

이와 같이 인터넷전화 단말을 이용한 침해사고의 발생과 해킹공격에 대비한 연구가 필요하다 1[][2].

본 논문에서는 인터넷전화 단말에서 IP Phone 정보를 획득하기 위한 스캐닝을 통해 IP Phone의 패스워드를 확인하고, 관리자 페이지를 통해 로그인을 성공한다. 그 후 IP Phone 관리자 페이지를 접속한 후 VoIP 설정 화면으로 전화번호, 포트번호, 인증번호 등을 수정한다. 또한 관리자 페이지에서 등록되어 있는 IP Phone들의 통화기록을 확인해 본다.

Ⅱ. 유무선 인터넷전화 단말기에 대한 취약점 분석

3.1 유무선 인터넷전화 단말기, Router, Switch 분석

유무선 인터넷전화 단말기에 대한 취약점 분석을 위하여 다음과 같은 주요 인터넷전화의 단말기를 사용하여 취약점 분석을 실시한다[3].

표 1은 CM-5000 인터넷전화의 주요 규격을 나타낸 것이고 표 2는 J2320 장치의 주요 규격이고 표 3은 EX2200 장치의 주요 규격이다.

표 1. CM-5000 인터넷전화의 주요 규격

제품명	프로토콜
CM-5000	SIP 표준 프로토콜
	
주요기능	주요내용
Signaling 프로토콜	·표준 SIP지원 (RFC3261, RFC3264, RFC3515, RFC3842)
하드웨어	프로세서	·RISC CPU with 32MB
---	---	---
	Memory	·NOR Flash 16MB, SDRAM 32MB
	Key Pad	·최대 24개 이상의 단축키 지원, 중역비서기능 버튼
	LCD	·3.5 Inch 컬러 TFT LCD
Codec		·G.711, G.723.1, G.729(default), G.722, G.726, G.728(optional)
QoS		·DiffServ(DSCP marking) ·IEEE 802.1p/Q ·TOS support ·Port-based hub priority ·Packet Loss concealment
Network 인터페이스		·RJ-45 I/F와의 10/100 Base-T ethenet 연결
PoE		·IEEE 802.3af 표준기반 UTP 회선 전원 공급
Network protocol		·IPv4, IPv6 ·DHCP client, DHCP server, NAT, SNMP, DNS ·NTP/SNTP, ICMP/ICMPv6, LDAP, XML/SOAP, PPPoE
암호모듈 연동기술 규격		·암호화 지원 : AES & ARIA 암호화 알고리즘 지원 ·sRTP, TLS 행안부 표준 암호화 규격 지원
(기능) ·Multi-line key definition (web base key definition among External, Speed Dial, Park, Hold and None) ·3way conference call support ·Transfer, Forward, DND(Do Not Disturb)/Mute, Auto Answering, Pick-up features ·Phonebook, Wake-up call, Schedule, Alarm, Memo, Calculator, World Time, Weight & Measures ·SMS 및 XML 메시지 기능		

표 2. J2320 장치의 주요 규격

제품명	Size	프로토콜	장비사양
J2320	1U	NAT(Network Address Translation) 기능지원, L3 Routing Protocol(Static, OSPF, IS-IS, BGP, RIP v1/v2), IEEE 802.1Q 지원	Memory : 512MB DRAM Flash disk : 512MB

주요기능	내용
Protocol	·BGP, OSPF, RIP, Static, ECMP ·IEEE 802.1Q ·NAT(Network Address Translation)
(특징) ·Support for T1, E1, Synchronous Serial, ISDN BRI, ADSL/2/2+, G.SHDSL, and Gigabit Ethernet interfaces ·Support for application acceleration using the Juniper Networks ISM200 Integrated Services Module ·4 fixed Gigabit Ethernet LAN ports, and 5 PIM slots ·512MB DRAM default, expandable to 1GB DRAM ·512MB compact flash default, upgradeable to 1GB ·Full UTM : antivirus, antispam, Web filtering, intrusion prevention system(with high memory version) ·Unified Access Control(UAC) and content filtering ·BGP, OSPF, RIP, Static, ECMP ·PPP, FR, MLPP, MLFR, HDLC ·Maximum Number of Virtual Routers	

표 3. EX2200 장치의 주요 규격

제품명	Size	프로토콜	장비사양
EX2200	1U	L3 Routing Protocol 지원(Static, RIP v1/v2), IEEE 802.1Q 지원, Dynamic VLAN 할당/Voice VLAN 기능 지원	24-10/100/1000BASE-T Port Densities

주요기능	내용
Protocol	·RIPv1/v2, EIGRP, OSPF, IS-IS, and BGPv4 ·IEEE 802.1Q ·Dynamic VLAN /Voice VLAN 기능 지원
(특징) ·24-10/100/1000BASE-T Port Densities ·4 per switch (fixed ports, SFP required)-100BASE-FX/1000BASE-X(SFP) port Densities ·Throughput : 42Mbps(wire speed) ·MAC Address : 8,000 ·Jumbo Frames : 9216Bytes ·IPv4 Unicast / Multicast Routes : 6,500 / 0 ·Number of VLANs : 1,024 ·ARP Entries : 2,000 ·QoS Queues / Port 8	

Ⅲ. 유무선 인터넷전화 단말기에 대한 해킹 공격 위협 연구

인터넷전화 테스트베드에서 보안 침해 시나리오를 구성하고 해킹 시험을 하기위해 그림 2와 같이 테스트베드를 구성한다.

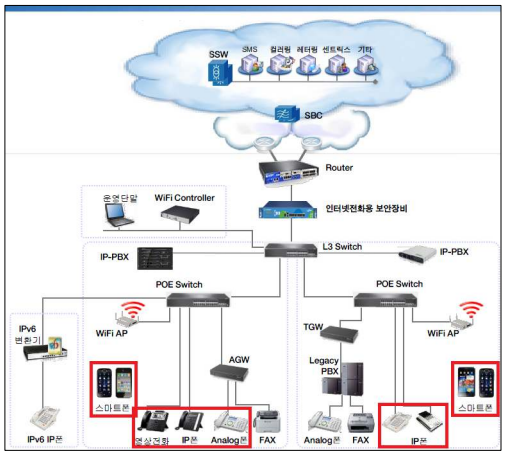

그림 2. 행정기관 인터넷전화 테스트베드

4.1 유무선 인터넷전화 단말기 스캔

그림 3. 스캐닝을 통한 인터넷전화 단말기 정보 획득

그림 4. IP Phone 관리자 페이지 내용

그림 3과 같이 스캐닝을 통해 인터넷전화 단말기의 정보를 획득하여 단말기 관리자 페이지에 접속하고 그림 4와 같이 관리자 페이지를 통해 로그인을 성공하여 인터넷전화 단말기의 설정 정보를 확인하였다.

4.2 유무선 인터넷전화 단말기 공격

그림 5. IP Phone VoIP 설정 화면

그림 5와 같이 IP Phone 관리자 페이지를 접속한 후 VoIP 설정 화면으로 전화번호, 포트번호, 인증번호 등을 수정할 수 있다.

그림 6. IP Phone 통화 기록

그림 6과 같이 관리자 페이지에서 등록되어 있는 IP Phone들의 통화기록을 확인할 수 있다.

Ⅳ. 결 론

인터넷전화 단말기를 이용한 침해사고의 발생과 해킹공격을 실시하였다. 인터넷전화 단말기에서 IP Phone 정보를 획득하기 위한 스캐닝을 통해 IP Phone의 패스워드를 확인하고, 관리자 페이지를 통해 로그인을 성공하였다. 그 후 IP Phone 관리자 페이지를 접속하여 VoIP 설정 화면에서 전화번호, 포트번호, 인증번호 등의 정보를 수정하였다. 또한 관리자 페이지에서 등록되어 있는 IP Phone들의 통화기록을 확인하였다. 이와 같이 단말기를 통해 해킹이 가능한 것을 확인하였다.

향후 연구에서는 인터넷전화 망의 보안 뿐만 아니라 단말기의 보안까지 인터넷전화의 모든 부분에서의 보안이 유기적으로 이루어질 수 있는 보안방안과 기술이 연구되어야 할 것이다.

참고문헌

[1] 송성환, 홍순기, 권성훈, "우리나라 유무선 인터넷전화 수요구조 분석에 관한 연구," 한국기술혁신학회 학술지, pp.47-53, 2009년 5월.

[2] 안영두, 이순흠, “SIP 기반 유무선 통합 컨퍼런스 시스템 개발,” 한국정보기술학회논문지, 제 5권, 제 3호, 2007년 09월.

[3] 이혜정, 정석태, "모바일 단말기를 이용한 실시간 B2B 시스템 구현," 한국해양정보통신학회논문지, Vol.10, No.1, pp.1-6, 2006년 1월.