All-IP방식과 Gateway방식에 대한 해킹공격과 보안대책

권세환* · 박대우*· 윤경배**

*호서대학교 벤처전문대학원 · **김포대학교

Hacking Attacks and Security Measures on All-IP Method and Gateway Method

Se-Hwan Kwon* · Dea-Woo Park*· Kyung-Bae Yoon**

*Hoseo Graduate School of Venture· **Kimpo College

E-mail : light@dgu.edu · prof1@paran.com · kbyoon@kimpo.ac.kr

요 약

인터넷전화는 All-IP방식과 Gateway방식 등으로 VoIP 서비스를 제공하고 있다. All-IP방식은 인터넷 환경에서 기기까지 모두 IP를 적용하여 서비스하는 인터넷 전화 방식이고 Gateway방식은 일반 전화기를 이용하여 인터넷 전화를 하는 방식으로 인터넷전화를 사용하고 있다. 본 논문에서는 테스트베드에서 All-IP방식과 Gateway방식의 인터넷전화의 시스템과 네트워크에 대한 스캔을 통해 취약점을 분석한다. 발견된 All-IP방식과 Gateway방식의 인터넷전화 취약점에 대한 해킹 공격을 실시하여 서비스거부 공격, 인터넷전화 스팸 공격을 실시한다. 공격 후 분석을 통하여 보안 대책을 제안한다.

ABSTRACT

Voice over Internet protocol(VoIP) is support a VoIP service as All-IP method and Gateway method etc. All-IP method to the unit in an Internet environment by applying both the IP service is an VoIP system. Gateway method, using a normal phone call in a way that the Internet is using VoIP. In this paper, scanning and analyze the vulnerability for VoIP systems and networks from All-IP method and the Gateway method In the test bed. All-IP method and Gateway method found in the VoIP vulnerabilities, hacking attack, a denial of service attacks and VoIP spam attacks are carried out. Through analysis of post-attack security measures is proposed.

키워드

All-IP, Gateway, Hacking Attack, Attack Analysis

Ⅰ. 서 론

2011년 행정기관의 인터넷전화 이용 유형을 분석하여 보면, 국가정보통신서비스 `C'그룹 4개 사업자 KT, SK브로드밴드, LG유플러스, 삼성SDS가 All-IP방식과 Gateway방식 2가지 방식으로 행정기관의 인터넷전화를 운영하고 있다. 현재 행정기관의 인터넷전화 이용 유형을 분석해 본 결과 All-IP방식은 11개 기관, Gateway방식으로는 16개 기관으로 나타났다.

All-IP방식과 Gateway방식 2가지 방식의 기본 서비스로는 기관간통화, 국내통화, 이동통화, 국제통화가 제공되며, 부가서비스에는 SMS, 통화연결음, 영상통화, 대표번호발신, 번호변경안내, 센트릭스, 레터링, CID가 있다.

각 행정기관의 인터넷전화 이용 방식의 결정은 행정기관의 인터넷전화 사용자의 성격이나 기관의 특성을 고려하여 결정하는 것으로 나타났다.

특히 최근에 해외와 국내 행정기관에 대한 해킹사고가 발생하고 있어, 행정기관의 인터넷전화의 이용 유형인 All-IP방식과 Gateway방식에 대한 해킹공격과 보안대책에 관한 연구가 필요하다[1].

본 논문에서는 All-IP방식과 Gateway방식에 대한 인터넷전화의 시스템과 네트워크에 대한 스캔을 통해 취약점을 분석한다. 발견된 취약점에 대한 해킹 공격을 실시하여 All-IP방식과

Gateway방식에 대한 서비스거부 공격, 인터넷전화 스팸 공격을 실시한다. 공격 후 단계별 보안 대책을 연구하여 제안한다.

Ⅱ. 관련연구

2.1 ALL-IP방식

ALL-IP방식을 이용하는 대상 기관은 ALL-IP방식 시스템 도입 예산을 확보한 경우나 기존 PBX 사용 연한이 얼마 남지 않았거나, UC 등 부가서비스를 제공 받고자 할 경우나, 기관 간 통합 예정인 경우에 이용하게 된다. 그림 1은 All-IP방식 유형 구성도이다.

그림 1. ALL-IP 방식

2.2 Gateway방식

Gateway방식 유형을 이용하는 대상 기관은 기존 PBX 사용 연한이 많이 남았을 경우나 예산 확보 및 내부 정책 등을 고려하여 점진적인 인터넷 전화 도입을 원할 경우에 이용하게 된다. 그림 2는 Gateway방식 유형 구성도이다.

그림 2. Gateway 방식

2.3 혼합형방식

혼합형방식을 이용하는 대상 기관은 기존 시스템 사용 연한이 많이 남았을 경우나 UC 등 부가서비스를 제공 받고자 하지만 예산이 확보되지 않았을 경우, 모든 단말이 인터넷전화 부가서비스를 제공할 필요가 없는 경우에 이용하게 된다. 그림 3은 혼합형방식 유형 구성도이다.

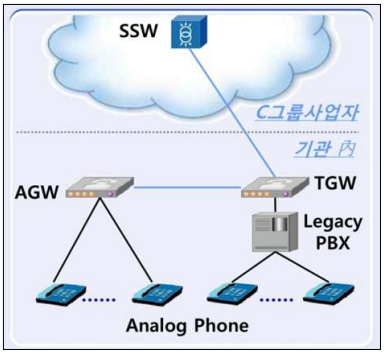

그림 3. 혼합형방식

2.4 IP-Centrex방식

IP-Centrex방식 유형을 이용하는 대상 기관은 도입 기관이 소규모이거나 예산 확보 및 내부 정책 등을 고려하여 기관 내 IP-PBX방식 도입이 불필요한 경우에 이용하게 된다. IP-Centrex 유형의 특징은 인터넷 전화기만 도입하면 되므로 가장 저렴하고, IP기반 단말을 사용하므로, 다양한 인터넷전화 부가서비스 가능하다. 또한, IP-PBX를 기관에서 관리하지 않으므로 호처리 및 통신 제어 권한이 적다. 그림 4는 IP-Centrex방식 유형 구성도이다.

그림 4. IP-Centrex 방식

Ⅲ. All-IP방식과 Gateway방식에 대한 공격

3.1 공격 실험 환경

All-IP방식과 Gateway방식에서 공격에 대한 실험을 하기 위해 두 가지 방식이 모두 구축되어 잇는 테스트베드에서 공격을 실험하였다. 그림 5는 테스트베드의 시험 환경 구성도이다.

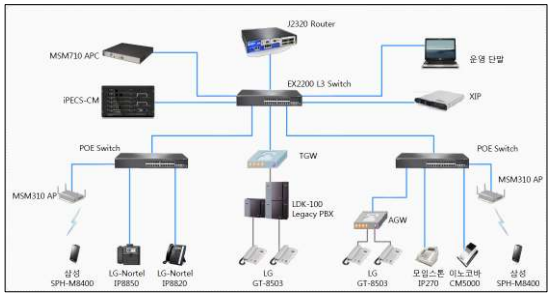

그림 5. 행정기관 인터넷전화 기본기능 시험 환경 구성도

3.2 All-IP방식과 Gateway방식에 대한 공격

기본적으로 Scan을 통해 행정기관 인터넷전화 네트워크의 구성과 시스템의 정보를 알아낸다.

기본 네트워크 정보 → GW : 210.103.4.193

네트워크 접속만으로 식별된 정보

210.103.4.204 00:40:5A:2B:E5:8E GOLDSTAR INFORMATION & COMM

210.103.4.233 E8:11:32:4C:B0:FD Samsung Electronics Co.,LTD

125.61.89.2 2C:6B:F5:67:D7:81 Juniper networks

현재 네트워크는 MAC Address로 통제하고 있다. MAC 변조를 통하여 네트워크에 접속이 가능하다. MAC 변조로 네트워크에 접속 후 네트워크의 정보가 확인된다. Cain & Abel을 이용하여 Sniffer공격을 통해 IP Address와 MAC Address를 알아낸다.

네트워크 해킹을 통하여 획득한 정보는 다음과 같다.

210.xxx.4.94 Linux release 2.6.18-164.el5

인터넷전화망을 Scan을 통하여 네트워크 구성과 시스템에 대한 정보(IP-PBX, FMC, IP-Phone, Port 등)를 알아낼 수 있다. 다음은 Nessus를 이용하여 Scanning을 통해 알아낸 정보는 그림 6과 같다.

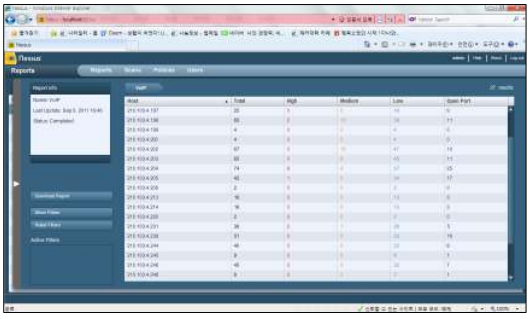

그림 6. 네트워크 대역 스캔 결과

Nessus를 이용하여 Scanning을 통해 PBX의 정보를 알아냈다. Nessus를 이용하여 Scanning을 통해 나온 정보에 대해 공격 대상을 선정하여 공격을 한다.

그림 7. Invite Flood 공격 시도

그림 7은 스캐닝을 통해 알아낸 IP-PBX의 정보를 통해 내부망에 접속하여 Invite Flood공격을 실시하였다.

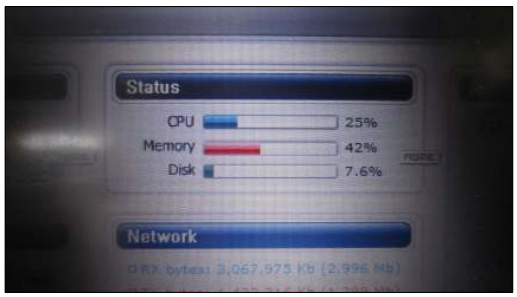

그림 8. DDoS 공격

그림 8은 DDoS공격의 하나인 Invite Flood공격으로 IP-Phone의 상태를 모니터링한 화면이다. 이와 같이 평소엔 메모리가 10%미만인데 노트북 한 대로 Invite Flood공격을 했는데 42%까지 메모리를 차지하여 통화가 일시적으로 안되는 것을 확인하였다.

Ⅳ. All-IP방식과 Gateway방식 해킹공격에 대한 보안대책

4.1 All-IP방식 보안대책

행정기관 인터넷전화를 ALL-IP방식이용하고 있는 S청사에 2009년 ALL-IP방식의 인터넷전화시스템을 구축하여 서비스를 하고 있다. 2011년에 `C' 그룹 서비스로 전환을 하였고, 국가정보원의 “국가사이버안전매뉴얼”과 “국가공공기관 VoIP정보보호가이드라인”의 지침사항을 준용하여 국내

최초로 구축을 하였다.

S청사에 직접 방문하여 행정기관 인터넷전화 담당자와 S청사 인터넷전화 보안 대응 대책에 대한 상담을 통하여 보안 대응 대책 자료를 구하고 상담을 하였다.

·서비스 거부 공격에 대한 보안대책

DDoS전용 방어장비는 구축되어 있지는 않지만, 국가정보원의 "국가사이버안전매뉴얼"과 "국가공공기관 VoIP정보보호가이드라인"을 준용하여 내부 네트워크망을 분리하여 운영하고 있으며, VoIP전용보안장비를 통하여 기본적인 DoS공격을 차단하고 있으며, 사용자 영역에서는 POE스위치의 DoS공격 차단 기능을 이용하고 있다.

·도청에 대한 보안대책

인터넷전화의 모든 신호(TLS)와 미디어(sRTP)에 대해 암호화(AES, ARIA)를 적용하고 있다.

·서비스 오용 공격에 대한 보안대책

VoIP전용보안장비를 통하여 서비스 오용, 공격 탐지, 인증실패/우회탐지 등을 수행하고 있다.

·호 가로채기에 대한 보안대책

VoIP전용보안장비를 통한 스팸 차단은 전용장비는 없으나 기능적으로 콜 스팸, 메시지 스팸, Call Bombing 등을 차단하고 있다.

·인터넷전화 스팸에 대한 보안대책

VoIP전용보안장비를 통한 스팸 차단은 전용장비는 없으나 기능적으로 콜 스팸, 메시지 스팸, Call Bombing 등을 차단하고 있다.

4.2 Gateway방식 보안대책

행정기관 인터넷전화를 Gateway방식을 이용하고 있는 K구청에서는 부분적으로 행정기관 인터넷전화시스템을 사용하고 있으며, 발신서비스만을 사용하고 있다.

K구청을 직접 방문하여 인터넷전화 담당자와 행정기관 인터넷전화 보안 대응 대책에 대한 상담을 통하여 보안 대응 대책을 어떻게 하고 있는지 상담하고 자료를 구하였다. 그림 9는 K구청의 행정기관 인터넷전화 장비이다.

그림 9. K구청 행정기관 인터넷전화 Gateway

K구청은 C그룹 사업자 KT의 국가정보통신서비스를 이용하고 있으며, KT에서 VoIP패킷만을 보내기 때문에 구청 내 행정기관 인터넷전화의 보안에 대한 시스템이나 장비는 구축하고 있지 않으며, 아직 시험테스트 중이어서 구청 내 몇몇 부서만 부분적으로 사용하고 있다. 안정화를 위하여 시내통화 발신만 G/W방식으로 하고 외부에서 걸려오는 전화는 PSTN으로 받고 있다. <그림 21>은 K구청의 행정기관 인터넷전화 Gateway장비이다.

·서비스 거부 공격에 대한 보안대책

네트워크 전용 IPS는 인터넷 기반의 DDoS 공격 방어용으로 VoIP 전용 IPS는 SIP 기반의 Register, Invite 메시지 공격 방어용으로 구축된 KT 사업자의 보안대책만을 적용하고 있다.

·도청에 대한 보안대책

국가정보원 공공/행정기관 보안가이드라인에 근거하여 신호는 TLS, 미디어는 sRTP로 암호화하여 서비스하고 있는 KT 사업자의 보안대책만을 적용하고 있다.

·서비스 오용 공격에 대한 보안대책

접속 라우터 홉의 카운터 개수를 제한하여 통화 패턴을 관리하고, 임계 치를 관리하는 KT 사업자의 보안 대책만을 적용하고 있다.

·호 가로채기에 대한 보안대책

VoIP전용보안장비를 통해 콜 하이재킹을 탐지하고 메시지 Digest를 확인 등 KT 사업자의 보안대책만 적용하고 있다.

·인터넷전화 스팸에 대한 보안대책

VoIP 전용 IPS의 스팸 차단 기능 적용을 적용하고 있는 KT사업자의 보안 대책만을 적용하고 있다.

V. 결 론

All-IP방식과 Gateway방식에 대한 인터넷전화의 시스템과 네트워크에 대한 스캔을 통해 취약점을 분석하였다. 발견된 취약점에 대한 해킹 공격을 실시하여 All-IP방식과 Gateway방식에 대한 서비스거부 공격, 인터넷전화 스팸 공격을 실시하였다. 공격 후 단계별 보안 대책을 연구하여 제안하였다. All-IP방식과 Gateway방식의 차이점은 크게 없는 것으로 나타났고 점차 Gateway방식에서 All-IP방식으로 바뀌어 나갈 것이다.

향후 연구에서는 All-IP방식에 대한 취약점을 보안하여야 하고 해킹사고가 있을 때 빠른 대처 방안이 필요하겠다.

참고문헌

[1] 윤상준, 김기천, "SIP을 이용한 VoIP 서비스에서의 Invite Flooding 공격 탐지 및 방어기법 설계," 한국정보과학회 학술발표논문집, 제38권 제1호, pp.215-218, 2011.6.