情 報 保 護 學 會 誌
第22卷 第8號, 2012. 12

인터넷전화의 해킹 공격과 방어 방안

천 우 성*, 박 대 우 **

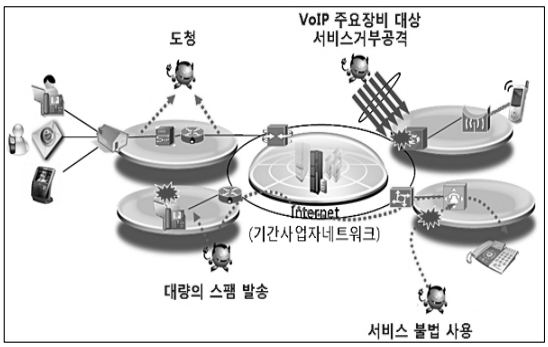
요 약

인터넷전화(VoIP)는 기존 인터넷망을 이용하여 통화내용을 전달한다. 따라서 일반적인 인터넷서비스가 가지고 있는 취약점을 동일하게 가지고 있다. 또한, 기존 유선전화(PSTN)와 달리 물리적인 접근 없이 원격에서 해킹을 통한 도청이 가능하며, 반국가 집단에 의한 사이버테러 감행 시 기관의 업무전산망과 전화망이 동시에 마비될 가능성이 있다. 본 논문에서는 인터넷전화 보안 위협 중에서 호 가로채기, 통화내용 도청, 서비스 오용에 대한 모의해킹을 한다. 또한 모의해킹 시나리오를 작성하고, 인터넷전화 시험센터에서 모의해킹을 통하여 발견된 취약점을 연구한다. 발견된 인터넷전화 취약점에 대한 공격방어 방안을 제시한다.

Ⅰ. 서 론

2010년 11월, SK네트워크의 자회사인 M사가 인터넷전화의 해킹을 당해 사용하지 않은 국제전화 요금 2,000만원이 청구됐다. 방송통신위원회에 따르면 사고의 원인은 이 회사에 인터넷전화 서비스를 제공하는 B사의 인터넷전화 장비가 해킹을 당했기 때문이다. 해커들은 M사의 인터넷전화를 이용해 프랑스에 국제전화를 걸었다. 결국 B사는 해킹 책임을 지고 국제전화 요금을 물어주기로 했다.

또한, 2012년 7월에 국내 한 여행사의 인터넷전화 교환기가 해킹당해 미국, 영국 등의 국제전화에 사용되면서 수천만 원의 손실이 발생하였다. 그림 1은 방송통신위원회에서 인터넷전화 보안 위협에 대한 자료이다[1].



[그림 1] 인터넷전화 보안 위협

이와 같이 인터넷전화에 대한 해킹공격과 서비스오용 공격으로 인한 피해사례가 발생하고 있으며, 특히 개인정보보호법 시행에 따른 개인정보의 보호를 위해서도 호 가로채기, 불법 도청에 대한 연구가 필요하다[2].

본 논문에서는 VoIP 보안 위협 중 호 가로채기, 통화내용 도청, 서비스 오용에 대한 모의해킹을 하기위해, 인터넷전화 시험센터에서 모의해킹 시나리오를 작성한다. 그리고 모의해킹을 통하여 호 가로채기, 통화내용 도청, 서비스 오용에서 발견된 취약점을 연구한다. 또한 취약점을 분석하여 인터넷전화 공격에 대한 공격방어 방안을 연구한다.

Ⅱ. 인터넷전화 공격 시나리오

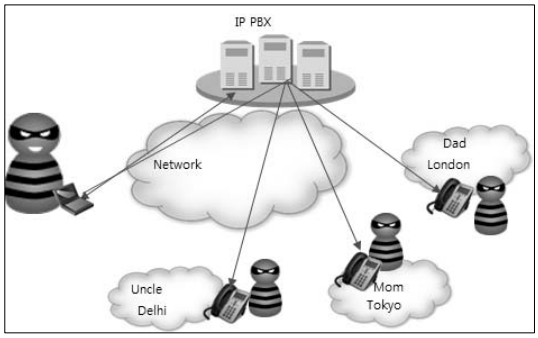
인터넷전화의 보안 위협들 중에서 인터넷 전화전화 공격으로 호 가로채기, 통화내용 도청, 서비스 오용에 대해 연구한다.

즉 인터넷전화 3가지 보안위협에 대해 공격시나리오를 작성하고 다음과 같이 실험하였다.

본 연구는 한국연구재단 연구과제 WiBro 인터넷 금융거래에 대한 공격과 취약점 분석 및 포렌식 수사 기술 연구 (2011-0005784) 지원으로 수행되었습니다)
* 호서대학교 벤처전문대학원(deux8522@daum.net)
** 호서대학교 벤처전문대학원(prof_pdw@naver.com)

2.1. 호 가로채기(Call interception)

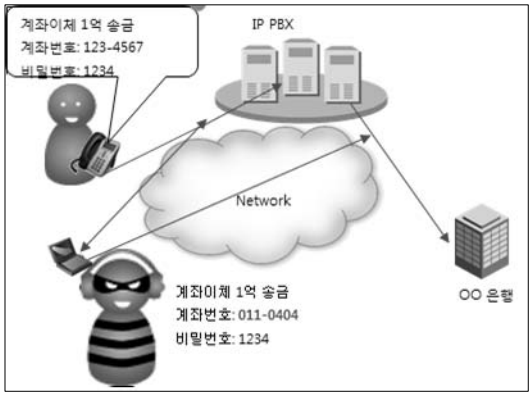
정상 가입자의 등록정보를 획득하여 불법으로 무료 인터넷전화를 사용한다. 그림 2는 인터넷전화의 호 가로채기 시나리오이다[3][4].



〔그림 2〕 인터넷전화 호 가로채기 시나리오

2.2. 통화내용 도청(Eavesdropping)

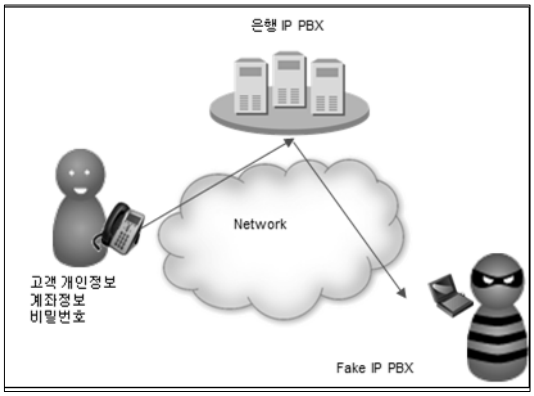
VoIP 통화, 정보 내용을 도청하여 불법적으로 개인의 중요 정보를 취득한다. 그림 3은 인터넷전화의 불법 도청 시나리오이다[5].



[그림 3] 인터넷전화 도청 시나리오

2.3. 서비스 오용(Misuse of Service)

정상적인 인터넷전화를 공격하여 연결을 끊게 한다. VoIP 메시지를 변형시켜 잘못된 정보를 전달하거나 개인정보를 취득한다. 불법 호 처리 서버로 가입자를 유도하여 정보 유출 및 금융 피해를 발생 시킨다[6][7]. 그림

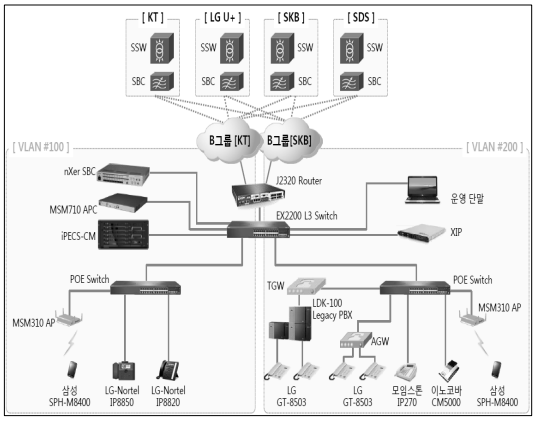


[그림 4] 인터넷전화 서비스오용 시나리오

4는 인터넷전화의 서비스 오용 시나리오이다.

Ⅲ. 인터넷전화 해킹공격

호 가로채기, 통화내용 도청, 서비스 오용에 대한 3가지의 시나리오를 바탕으로 그림 5와 같이 구성되어 있는 테스트베드에서 해킹 실험을 한다.



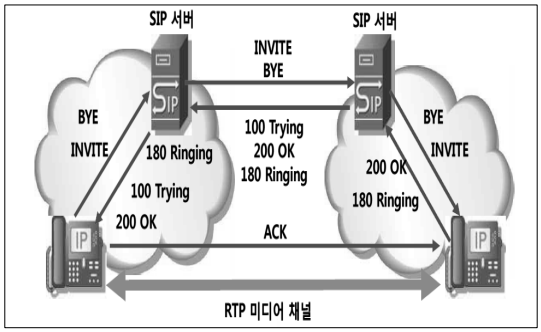
〔그림 5〕 행정기관 인터넷전화 테스트베드

3.1. 호 가로채기 공격

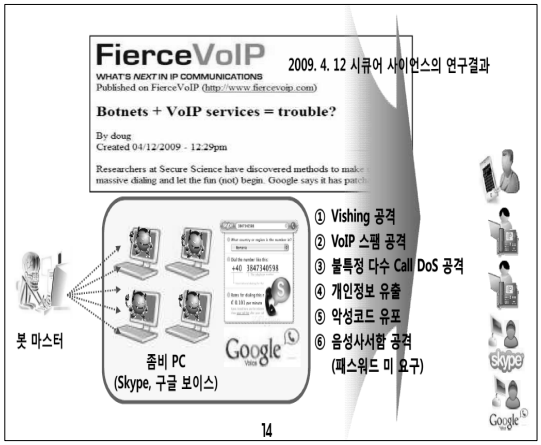
그림 6처럼 호 가로채기 공격을 위해서는 VoIP 서비스 프로토콜을 파악해야 한다.

그림 7처럼 봇넷을 이용하여 VoIP 서비스 어플리케이션을 통해 감염시키고, 감염된 좀비 PC들을 사용하는 개인 정보 유출, 악성코드 유포, 음성사서함 공격, 불특정 다수 Call DoS공격, VoIP 스팸 공격, Vishing공격

을 통해 2, 3차 침해사고가 발생할 수 있다.



〔그림 6〕 호 가로채기 공격을 위한 VoIP 프로토콜 내용 파악



〔그림 7〕 봇넷을 이용한 호 가로채기 연결 공격

3.2. 통화내용 도청 공격

그림 8과 같이 송신자는 암호화된 상황에서 통화가

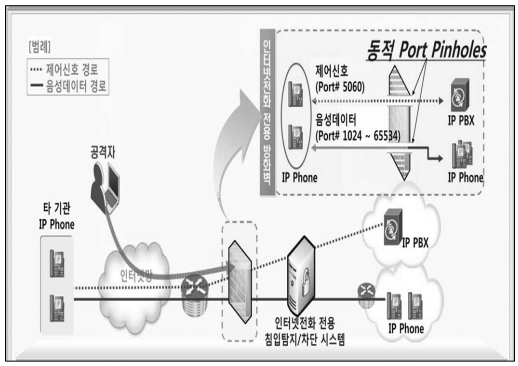
〔그림 8〕 인터넷전화 도청 시연

진행된다고 생각하지만, 해커가 송수신되는 패킷을 가로채 암호통신(sRTP)를 일반통신(RTP)으로 변경시켰기 때문에 조건적인 환경에서 통화 내용은 도청될 수 있다.

Ⅳ. 인터넷전화 해킹공격에 대한 방어 방안

4.1. 인터넷전화 전용 보안장비

국가·공공기관의 인터넷전화 구축 시, CC인증을 획득한 인터넷전화 전용 보안장비(방화벽, IPS 등)를 도입·사용하여야 한다. 그림 9는 인터넷전화 전용보안장비 구축 개념도이다.



〔그림 9〕 인터넷전화 전용 보안장비 구축도

4.2. 인터넷전화망과 데이터망 분리 운영

물리적 분리 또는 논리적 분리로 사용, 경제성 등을 고려할 때 논리적 분리를 권장한다[8].

사설 IP주소를 사용한 분리 방법으로는 음성망의 IP Phone(192.168.x.x)과 데이터망의 PC(172.16.x.x)에 할당되는 사설 IP 대역의 주소를 별도로 주소 대역을 가지는 논리적인 서브넷에 할당한다. VLAN 기법을 적용하여 서브넷을 분리한다.

음성 VLAN 접근 차단은 포트 기반에서는 장비의 MAC 주소 기반으로 차단하고, IEEE 802.1X Port 인증 기반으로 차단한다.

방화벽 및 접근제어 리스트를 이용한 분리(Path 분리)는 데이터와 음성의 트래픽 특성을 접근 제어 리스트에 등록하여, 데이터망과 음성망의 분리를 수행한다.

4.3. 호 가로채기에 대한 보안대책

Call Hijacking 공격은 통화 시도 시 위/변조된 301/302 메시지로 수신자의 통화를 공격자로 돌린다. 지속적으로 301/302 메시지를 테스트 하고 SIP서버에서 Call Hijacking이 차단되었는지 로그를 확인한다. 메시지 digest 공격은 등록된 단말을 통화 통화를 시도하여 단말 로그를 통해 Authentication 과정이 MD5 알고리즘으로 동작하는지 확인하고 있다.

4.4. 도청에 대한 보안대책

국가정보원 공공/행정기관 보안가이드라인에 근거하여 신호는 TLS, 미디어는 sRTP로 암호화하고 있다. TLS는 단말기와 VoIP Server 간 통신 시 암호화된 SIP 패킷에 대한 탐지를 위해 인터넷전화 전용 방화벽에서 복호화 기능 지원한다. 또, 패킷 자체에 대한 암호화는 단말기와 VoIP Server 에서 지원한다.

단말기와 VoIP Server 간 통신 시 암호화된 SIP 패킷에(TLS) 에 대한 탐지를 위해 VoIP전용 방화벽에서 복호화 기능 지원하고, 패킷 자체에 대한 암호화는 단말기와 VoIP Server에서 지원한다.

국가정보원과 행정안전부의 국가공공기관 인터넷전화 보안가이드라인에 따라, 공개키 기반의 기기인증서를 통한 VoIP장비(SBC)/VoIP단말(IP PBX, IP Phone) 간의 유효성 인증 및 시그널신호(SIP)에 대하여 TLS 암호화 프로토콜기반의 AES/ARIA 암호화 알고리즘 적용과 미디어트래픽(RTP)에 대하여 sRTP 암호화 프로토콜기반의 AES/ARIA 암호화 알고리즘 적용하고 있다.

호 교환시에는 TLS의 버전을 v1.0 또는 v1.2를 사용하고, 비대칭 키교환 방식인 RSA를 사용한다. AES_128_CBC_SHA(0x2F) 암호화 알고리즘을 지원한다. 또한 Root, 중계기관, 단말 등 기기인증서를 확인한다. 음성 통화에는 암호화 알고리즘으로 ARIA_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_80을 사용하고, 통화내용이 재생가능한지 확인하고 있다.

LAN 구간 도청(내부사용자), LAN 구간 도청(외부해커), WAN 구간 도청에 대해 인터넷전화 트래픽 암호화 적용하여 제어신호는 TLS, 미디어는 sRTP로 행정기관으로부터 당사 SBC까지 전구간 보안(AES or ARIA)을 적용하고 있다. TLS로 제어신호를 암호화 하는 경우 PKI 기반, 공인인증서를 이용한 인증 메커니즘이 적용되어 현재 공인 인증기관에 인증서 검증시스템이 구축되어 있지 않으므로, 현재 TTA의 Test 방식인 장비내 자체 검증 수행 방식으로 인증을 하고 있으며, 향후 공인인증기관에 검증시스템 구축시 검증 시스템과 연동할 예정이다.

4.5. 서비스 오용 공격에 대한 보안대책

접속 라우터 홉 카운터 개수 제한 및 고객사별 국제전화 통화 패턴을 관리하여 임계치를 관리하고 있다.

SIP 서버 우회 공격은 보안장비에 등록되지 않은 SIP Server를 경유하여 SIP 메시지를 전송하고, 내부사용자 위장 공격은 보안장비에 등록되지 않은 IP, URI로 Outbound SIP 메시지를 전송한다. 공격자 PC에서 스크립트를 실행했을 때, SIP 서버의 로그를 확인한다.

SIP SQL injection 공격에 대해서는 REGISTER URL에 SQL Injection 공격을 시도한 후 SIP 서버의 로그를 확인한다. Topology Hiding 공격은 등록된 단말을 통해 통화를 시도하고, SBC로부터 응답 메시지의 SIP헤더에 SBC 서비스 IP 주소 외의 인프라 IP 주소가 기록되어 있는지 여부를 확인하고 있다.

근본적으로 공개키 기반의 기기인증서를 통해 상호 기기인증이 이루어지고 있으며(기기 무결성, 부인봉쇄), HTTP Digest방식의 사용자인증이 SBC를 통하여 실제 가입자와 단말의 서비스인증이 이루어지므로 등록되지 않은 단말의 서비스오용은 불가능하다.

비인증 단말 통화 시 차단을 위해 4XX Status 메시지 응답 여부를 확인하고, 소프트스위치의 로그를 확인하여 트래픽이 인입되지 않았음을 확인하고 있다.

Topology Hiding에는 SBC로부터 응답 메시지의 SIP 헤더에 SBC 서비스 IP 주소 외의 인프라 IP 주소가 기록되어있는지 여부를 확인하고 있다.

관리상 오류 공격, SIP SQL 삽입(SIP SQL Injection)에 대해 네트워크/OS 레벨의 접근제어와 Topology Hiding을 제공하며 주기적인 취약점 분석을 통해 보안성 강화하고 있다. Access List 및 방화벽 룰셋으로 제어 목적의 트래픽에 대해 인가된 네트워크 대역 이외의 접근을 원천적으로 차단하고 SBC에서 제공되는 Topology Hiding으로 내부 인프라에 대한 IP,

Domain 등의 정보 유출을 차단하고 있다. 내/외부 전문 인력에 의해 연 1회 이상 주기적인 취약점 분석을 수행하여 보안성을 유지 및 강화하고 있다.

Ⅴ. 결 론

인터넷전화에 대한 해킹공격 피해사례가 발생하고 있고, 개인정보보호법 시행에 따른 개인정보의 보호를 위해서 VoIP 보안 위협 중 호 가로채기, 통화내용 도청, 서비스 오용 에 대한 모의해킹을 하기위해, 인터넷전화 시험센터에서 모의해킹 시나리오를 작성하였다. 그리고 모의해킹을 통하여 호 가로채기, 통화내용 도청, 서비스 오용에서 발견된 취약점에 대해 분석하여 인터넷전화 공격에 대한 공격방어 방안을 연구하였다.

향후 연구에서는 공격방어 방안을 적용하여 검증이 필요할 것이다.

참고문헌

[1] 도형래 기자, "방통위, 해킹·요금폭탄 인터넷전화 보안대책 마련," 미디어스, http://www.mediaus.co.kr/news/articleView.html?idxno=29639, 2012년 11월

[2] VoIP 기술 동향, 정보통신연구진흥원 학술정보, 주간기술동향 1021호, 2008년 09월.

[3] 윤상준, 김기천, “SIP을 이용한 VoIP 서비스에서의 Invite Flooding 공격 탐지 및 방어 기법 설계,” 한국정보과학회 학술발표논문집, 제38권 제1호, pp.215-218, 2011년 6월.

[4] 천재홍, 박대우, "VoIP의 DoS공격 차단을 위한 IPS의 동적 업데이트엔진,” 한국컴퓨터정보학회논문지, 2006년 12월.

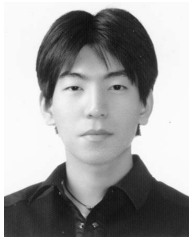
[5] 박대우, 윤석현, "VOIP 서비스의 도청공격과 보안에 관한 연구,” 한국컴퓨터정보학회논문지, 2006년 9월.

[6] 이인희, 박대우, "VoIP 서비스의 스팸 공격에 대한 차단 연구,” 한국컴퓨터정보학회논문지, 2006년 9월.

[7] 장유정, 정수환, 문형권, 최재덕, 원유재, 조영덕, “SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법,” 한국통신학회논문지, 제 32권 제 8호(네트워크 및 서비스), 2007년 08월.

[8] 김병호, "인터넷전화 서비스의 향후 패러다임 제안 ,” 한국해양정보통신학회논문지, Vol.13, No.1, pp.127-133, 2009년 1월.

〈著者紹介〉



천 우 성 (Woo-Sung Chun)
정회원

2006년 2월 : 숭실대학교 전산원 졸업
2006년 8월 : 한국교육개발원 멀티미디어학 전공 (공학사)
2009년 2월 : 호서대학교 벤처전문대학원 IT응용기술학과 (공학석사(정보보호전공))
2010년 3월 ~ 현재 : 호서대학교 벤처전문대학원 IT응용기술학과 박사과정
<관심분야> 정보보호, 추적기법, Hacking, Forensic

박 대 우 (Dea-Woo Park)
종신회원

1998년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
2004년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
2004년 2월 : 숭실대학교 겸임교수
2006년 2월 : 정보보호진흥원(KISA) 선임연구원
2007년 3월 ~ 현재 : 호서대학교 벤처전문대학원 교수
관심분야 : Hacking, CERT/CC, 침해사고대응, e-Discovery, Forensic, 사이버국방, 정보보호, 유비쿼터스 네트워크 보안, WiBro 보안, VoIP보안, 스마트폰 및 이동단말 보안