情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

VoIP서비스 보안 취약성 분석

구 자 현*

요 약

광대역통합망(Broadband Convergence Network, BcN)의 핵심서비스로 자리 잡고 있는 VoIP(Voice over Internet Protocol)는 IP망 경유를 통한 저렴한 통신비용 및 다양한 부가서비스 제공가능성에 따라 서비스 사업자 뿐만 아니라 기업에서도 점차 도입이 증가할 것으로 예상되는 서비스이다. 그러나, 보안솔루션의 인터넷 전화 트래픽 통과 문제 및 IP망에서 발생 가능한 공격뿐만 아니라 VoIP스팸 이나 도청 같은 새로운 보안이슈들이 많이 발생할 것으로 예상됨에 따라 본 논문에서는 VoIP 서비스에 대한 기밀성, 무결성, 가용성적인 측면에서 예측 가능한 취약성을 살펴봄으로서 더 좋은 서비스를 제공하는데 이바지할 수 있을 것이다.

Ⅰ. 서 론

VoIP(Voice over Internet Protocol) 기술은 인터넷의 IP프로토콜을 사용하여 음성을 전송하는 기술을 말하며 VoIP기술을 바탕으로 제공되는 서비스를 인터넷전화 서비스, 인터넷 텔레포니(Internet Telephony) 등으로 혼재하여 부르고 있다. 그러나, 기존의 음성전화서비스(Public Switched Telephone Network, PSTN)에 비해서 열악한 통화품질이나 착신통화의 어려움에 따른 문제점 그리고 일부 통신사업자 등의 비즈니스적인 측면에서 소극적인 투자를 해왔던 것이 사실이다. 그러나 정부의 IT839 정책에 있어서 VoIP기술을 통한 PSTN과 IP망, 무선통신망을 연동하는 음성 및 영상멀티미디어서비스가 광대역 통합망의 핵심기술로 떠오르면서 점차 상용화가 확대되고 있다. VoIP는 경제성뿐만 아니라 IP기술을 기반으로 인터넷 콜센터, 다자간 화상전화서비스, 사용자 위치정보 제공 등 다양한 어플리케이션 개발에 응용력이 크므로 비즈니스 모델이 무한하다고 할 수 있다. 그러나 에러 발생에 민감한 데이터 신호(Data)와 달리 음성(Voice)은 시간에 민감하다는 특성(Time-critical nature)이 있다. 인터넷의 Best-effort전송 속성은 허용 가능한 시간 내에 오류 없이 데이터를 수신하는데 적합하기 때문에 음성을 데이터처럼 패킷화 하여 보내는 경우에는 음성전화망과 유사한 음성품질을 보장하기 위해서 통화품질 기술이 뒷받침되어야 한다. 이러한 통화품질 못지않게 VoIP는 기존의 인터넷망을 그대로 활용함에 따라 인터넷망에서 발생할 수 있는 보안 취약성뿐만 아니라 공중전화망과 유, 무선 인터넷망의 연동에 따른 기존과 다른 새로운 취약점의 발생하게 된다. 따라서 본 논문에서는 VoIP서비스 자체에 대한 취약점을 중점적으로 살펴봄으로서 안정적인 서비스를 제공하기 위한 보호대책을 수립하는데 도움이 되고자 한다.

Ⅱ. VoIP서비스 보안 취약점과 위협

기본적으로 VoIP서비스 환경은 IP기반 망에서 발생할 수 있는 위협을 모두 고려할 수 있지만, 이 장에서는 그러한 IP기반 망에서의 위협은 논외로 하고 현재까지 발표된 VoIP장비 관련 보안취약점을 살펴보고 앞으로 발생가능한 위협을 기밀성, 무결성, 가용성적인 측면으로 구분하여 특정 VoIP사용자의 음성에 대한 도청 가능성, 비과금호 발생(Free Phone Call), 다수의 의사호 발생 공격(War Dialing Attack) 및 잡음삽입 공격(Media Injection Attack) 가능성 및 VoIP서비스를 제공하기 위한 필수적인 각 요소들에 대한 서비스 거부 공격(Denial

* (주)데이콤 (k55k559@chol.com)

of Service, DoS) 가능성에 대해서 주로 논의하고자 한다.

2.1 보안 취약점

기존에 알려진 보안취약점은 주로 VoIP단말기에 대한 기밀성이나 가용성을 침해하는 공격내용이 대부분이며 상세한 내용은 아래 표에 정리한다.

〔표 1〕 2005년 이후 발견된 VoIP 취약점

제 목	내 용	참고 사이트
CVE-2006-0375	ACT P202S IP Phone 에서 NTP를 활용하여 remote attack이 가능	http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041434.html
CVE-2006-0374	ACT P202S IP Phone 에서 UDP17185, TCP 7, TCP 513포트를 이용하여 인증을 우회한 공격이 가능	http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041434.html
CVE-2006-0360	MPM SIP HP-180W Wireless IP Phone 에서 UDP 9090 remote 공격이 가능	http://www.securityfocus.com/bid/16285
CVE-2006-0305	Clipcomm CPW-100E VoIP 802.11b Wireless Handset Phone and CP-100E VoIP 802.11b Wireless Phone TCP 60023로 비인가 접속이 가능	http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041439.html
CVE-2006-0302	ZyXel P2000W VoIP 802.11b Wireless Phone UDP 9090포트를 이용하여 remote 공격이 가능	http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041438.html
CVE-2005-4050	Long INVITE field in a SIP packet를 이용하여 buffer overflow 공격 가능	http://www.securityfocus.com/archive/1/archive/1/418653/100/0/threaded
CVE-2005-3989	Avaya TN2602AP IP Media DoS공격이 가능	http://www.securityfocus.com/bid/15668
CVE-2005-3804	Cisco IP Phone 7920 UDP 17185 remote 공격이 가능	http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml
CVE-2005-3803	Cisco IP Phone 7920 고정된 SNMP community strings 을 통해 정보 유출 가능성	http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml
CVE-2005-3725	Zyxel P2000W VOIP WIFI Phone hardcoded IP addresses 로 인한 취약성 존재	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217443126673&w=2
CVE-2005-3724	Zyxel P2000W VOIP WIFI Phone UDP 9090 remote 공격이 가능	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217443126673&w=2
CVE-2005-3723	Hitachi IP5000 does not allow the user to disable access to (1) SNMP or (2) TCP 3390	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217425618951&w=2
CVE-2005-3722	The SNMP v1/v2c daemon in Hitachi IP5000 remote 공격이 가능	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217425618951&w=2
CVE-2005-3721	Hitachi IP5000 VOIP WIFI Phone 비인가 접속이 가능	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217425618951&w=2
CVE-2005-3720	Hitachi IP5000 VOIP WIFI Phone 웹을 통한 비인가 접속이 가능	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217425618951&w=2
CVE-2005-3719	Hitachi IP5000 VOIP WIFI Phone Administrator password 가 "0000"으로 설정되어 있는 취약점	http://marc.theaimsgroup.com/?l=full-disclosure&m=113217425618951&w=2
CVE-2005-3718	UTStarcom F1000 (1) SNMP or (2) TCP 513 remote 공격이 가능	http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038834.html
CVE-2005-3717	UTStarcom F1000 default username "target" and password "password" 가 존재	http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038834.html
CVE-2005-3716	UTStarcom F1000 VOIP SNMP 취약점 존재	http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038834.html
CVE-2005-3715	Senao SI-680H UDP 17185 인증우회 취약점 존재	http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038836.html
CVE-2005-2182	Grandstream BudgeTone (BT) 100 NOTIFY 메시지에 있는 Call-ID, branch, and tag values을 chech하지 않음으로서 스푸핑 공격 가능	http://marc.theaimsgroup.com/?l=bugtraq&m=112067698624686&w=2
CVE-2005-2181	Cisco 7940/7960 IP phones NOTIFY 메시지에 있는 Call-ID, branch, and tag values을 chech하지 않음으로서 스푸핑 공격 가능	http://marc.theaimsgroup.com/?l=bugtraq&m=112067698624686&w=2
CVE-2005-2081	Asterisk 1.0.7 Buffer overflow 취약점 존재	http://marc.theaimsgroup.com/?l=bugtraq&m=111946399501080&w=2
CVE-2005-0745	UTStarcom iAN-02EX 에서 "*#26845#"누르면 장비 reset 되는 취약점 존재	http://seclists.org/lists/bugtraq/2005/Mar/0168.html

2.2 보안 위협

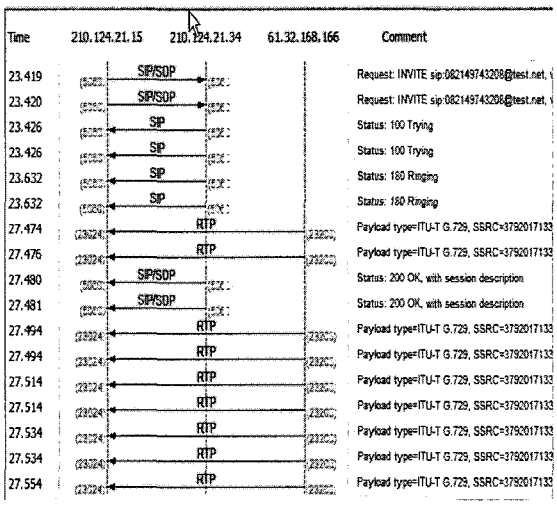
미국 상무국산하 표준기술연구소인 NIST에서는 2005년 2월, VoIP기술 도입에 신중할 것을 경고하였다. 인터넷 전화 서비스는 패킷 형태로 인터넷에 노출되므로 기존 전화서비스보다 보안이 취약하고 공격가능성이 높으며 2005년 5월과 7월 시스코는 자사의 IP전화기의 DNS 쿼리문제와 콜매니저 소프트웨어의 결함이 있음을 밝혔고 국내 VoIP서비스 업체에서는 VoIP관련 게이트웨이의 해킹으로 인한 불법적인 국제전화 피해사례가 보고 되는 등 점차 보안위협이 증대되고 있는 사항이라고 할 수 있다.

2.3 기밀성 침해 공격

VoIP 인프라에 대한 기밀성 침해 공격으로는 음성호나 음성호를 위한 신호의 가로채기 등이 있다. 이러한 정보가 공격자에게 유출되면 음성통화자의 Privacy가 침해될 수 있다.

2.3.1 동일 네트워크상에서의 음성호 도청

스위치 타입의 허브에서 이루어 질 수 있는 가장 일반적인 형태의 공격으로 일반적으로 스위치 타입의 허브는 더미 허브와는 달리 모든 데이터를 브로드캐스팅 하는 것이 아니라 특정 포트 단위로 트래픽을 운반 하므로 공격자에 의해 직접적인 Network sniffing은 불가한 것으로 알려져 있다. 그러나 ARP스푸핑 (Address Resolution Protocol Spoofing)으로 공격자는 공격대상의 MAC(Media Access Control) 어드레스를 가장하여 공격을 취할 수 있다. 공격자는 조작된 MAC 어드레스를 스위치 상에 브로드 캐스팅 하는 것으로 원래는 다른 곳으로 전달되어야 할 데이터 패킷을 수신할 수 있다. 이와 같은 방법으로 공격자는 조작된 ARP 응답을 사용하여 해당 단말장비가 게이트웨이와 통신하는 것을 가정하여 네트워크 공격이 가능하며 공격자는 게이트웨이를 가장하여 음성호의 셋업 단계부터 관여하면 단말장비가 SIP(Session Initiation Protocol) 서버로 보내는 모든 정보를 얻을 수 있다.



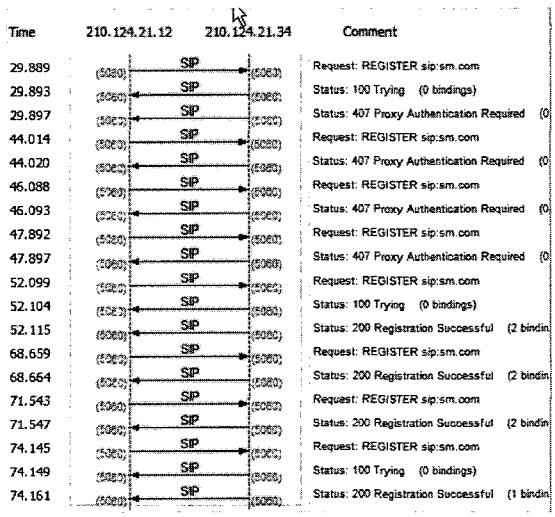
〔그림 1〕 ARP Spoofing 공격

두개의 유사한 패킷이 210.124.21.15 에서 210.124.21.34로 보내지는 것을 볼 수 있다. 그러나 두번째 패킷의 source MAC 어드레스를 공격자의 MAC 어드레스와 동일하게 설정함으로서 공격자는 효과적으로 ARP 스푸핑 공격을 수행할 수 있고 공격자는 의도한 대상 가입자들의 패킷을 받아서 상호 전달해 주는 방식으로 모든 통신 내용을 가로챌 수 있다.

그림 1로 부터, 공격자의 IP 어드레스는 나타나 있지 않지만, 공격자는 대상 가입자들을 가장하고 있고 한쪽 대상 가입자로 부터의 모든 패킷을 다른 대상 가입자로 전달하고 있다. 위의 흐름 분석은 모든 패킷이 두번씩 전달되는 것을 보여주고 있다. 한번은 패킷 송출자가 공격자로 보내는 패킷이고, 다른 하나는 공격자가 실제 수신자로 보내는 패킷이다.

2.3.2 SIP서버의 Registration 도용에 의한 음성호 도청

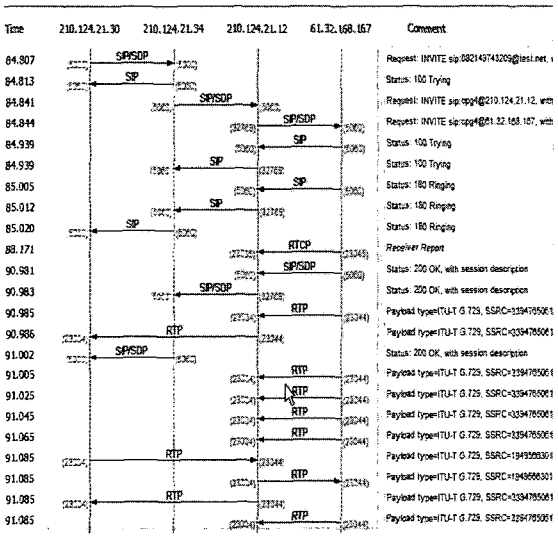
침입탐지 등으로 검출될 수도 있는ARP 스푸핑과는 달리, 또 다른 형태의 음성호 도청 기법으로 임의의 네트워크상에서 도청 대상가입자를 가장하는 방법이 있다. 이러한 방법을 사용하기 위해, 공격자는 공격대상 가입자 단말장비의 접근 권한을 획득하여 SIP 서버로부터 해당 가입자의 권한을 획득할 수 있다.



〔그림 2〕 SIP Proxy서버를 이용한 도청

그림 2에서 보이는 바와 같이, 210.124.21.12에 위치한 공격자는 공격 대상 가입자 단말의 접근 권한을 획득하여 SIP 서버의 가입자 인증을 받아낸다. 공격자는 SIP 서버로 인증요구를 시도하여 공격 대상 가입자 번호로 인증을 성공적으로 획득하였다. 인증 획득 후에 공격자는 SIPproxy 및 rtp를 연결해주는 방법을 사용하여 음성호를 가로챌 수 있다.

그림 3에 보이는 바와 같이, 발신가입자 (210.124.21.30)가 공격대상 가입자 번호를 다이얼 하면 SIP 서버는 SIP 메세지를 공격자에게 보낸다. 공격자는 SIPproxy 소프트웨어를 이용하여 SIP 서버로 부터 받은 메세지를 공격 대상 가입자에게 전달 한다. 공격 대상 가입자는 공격자 장비를 경유하여 발신가입자와 호 셋업을 진행하게 된다. 호 셋업이 이루어진 후 음성 트래픽을 위해 RTP 패킷이 전달되고 공격자는 RTP 연결을 이용하여 RTP를 전달하고 중간에서 RTP 패킷을 획득한다. 이 공격의 성공 여부는 단말장비 설정의 취약점을 이용하여 가입자 정보를 획득하는 것에 달려 있다.



〔그림 3〕 단말장비간 트래픽 Intercepting

2.4 무결성 침해 공격

VoIP 인프라에 대한 무결성을 훼손하는 공격을 통하여 VoIP스팸공격이나 위조된 통화시도(Spoofing Call), 변조된 RTP삽입을 통한 음성통화 방해공격 등이 가능하다.

2.4.1 위조된 통화시도 (Spoofing Call) 공격

다량의 위조된 INVITE SIP 메세지를 보냄으로서 전화벨은 울리고, 수화기를 들었을 때 실제로 아무도 전화를 걸지 않았음을 인식한다. 만약 공격자가 짧은 주기로 이런 공격을 반복한다면 정상적인 업무가 불가능할 것이다. 이런 공격을 위해 공격자는 우선 그림 4 처럼 단말장비에 보낼 SIP 메세지를 준비한다. 다음으로 공격자는 SIP 메세지를 사용해 네트워크로 위조된 UDP 패킷을 삽입시킴으로서 1분에 수 천개의 위조된 호를 보낼 수도 있다. 특히 음성 메일서비스는 일반전화보다 대량의 메시지를 다수의 사용자에게 손쉽게 전송이 가능하다. 특히 IP주소를 이용한 멀티캐스트가 가능하기 때문에 VoIP음성 메일을 통한 스팸공격은 손쉽게 발생할 수 있으며 VoIP 스팸으로 인한 음성 저장 용량의 고갈 문제도 쉽게 예측할 수 있다.

No.	Time	Source	Destination	Protocol	Info
1	10:59:16	210.124.21.3	61.32.168.166	SIP	Request: INVITE sip:3
2	10:59:16	210.124.21.3	61.32.168.167	SIP	Request: INVITE sip:3
3	10:59:27	61.32.168.167	210.124.21.30	SIP	Request: BYE sip:3397
4	10:59:27	210.124.21.30	61.32.168.167	SIP	Status: 481 Call Leg/
5	10:59:28	61.32.168.166	210.124.21.30	SIP	Request: BYE sip:3397
6	10:59:28	210.124.21.30	61.32.168.166	SIP	Status: 481 Call Leg/
7	10:59:31	210.124.21.3	61.32.168.166	SIP	Request: INVITE sip:3
8	10:59:32	210.124.21.3	61.32.168.167	SIP	Request: INVITE sip:3

〔그림 4〕 faked SIP INVITE message

2.4.2 RTP 삽입을 통한 음성통화 방해 공격

공격대상의 통화를 어렵게 하거나 단절시키기 위하여 유효하지 않은 RTP 패킷을 다량으로 보냄으로서 실제 통화에 문제점을 야기 시킬 수 있다. 이 때 공격자는 사전에 대상가입자로 호를 발생시켜 RTP신호를 모니터링하여 대상자가 사용하는 UDP 포트번호를 확인한다. 실제 UDP포트는 대부분의 경우 2씩 증가하도록 되어 있어 향후 호에 사용될 포트번호 추측이 용이하게 된다. 실제 공격할 경우에는 공격에 사용할 SSRC (Synchronization Source) 번호 및 Sequence 번호를 임의로 설정하여 Incremental하게 증가하면서 공격한다.

2.5 가용성 침해 공격

VoIP 망에 대한 가용성 침해 공격은 VoIP 서비스 망이 정상적으로 동작하지 못하도록 한다. UDP, ICMP, Echo, TCP Syn 패킷 등을 조작하여 발생할 수 있으며, 불필요한 패킷들을 공격대상 시스템에 집중적으로 보냄으로서 시스템 자원을 고갈시킨다. 예를 들어 통화중 임의의 공격자가 TCP RST Brute force 공격을 할 경우 reset명령에 의해 VoIP서비스가 중단된다. 이처럼 초기에 호를 설정하는 과정과 호를 끊는 과정을 반복함으로서 시스템 자원을 고갈시키거나 소프트스위치에 비정상적인 요구를 과도하게 함으로서 정상적인 서비스에 방해를 유발시키는 공격방법이 다양하게 존재한다.

III. 결 론

향후 BcN등의 핵심서비스로 예측되는 VoIP서비스에 대한 보안취약성에 관해서 분석하였다.

본 논문에서는 VoIP서비스를 함에 따라 발생하는 취약성을 기밀성, 무결성, 가용성 적인 측면으로 나누어 분석했다. 이는 IP망을 사용하기 때문에 발생하는 IP망 자체의 보안 취약점이 VoIP서비스에는 존재하지 않는 다는 것이 아니고 기본적으로 모두 존재한다는 전제에서 추가적으로 예측되는 문제점을 주로 분석하였다.

지금의 분석이 향후 VoIP서비스가 대중화 될 경우 더욱 좋은 서비스의 제공을 기대할 수 있을 것이다.

참 고 문 헌

[1] 한국정보보호진흥원, "VoIP 정보보호 가이드", Dec 2005

[2] http://www.voip-forum.or.kr

[3] 구자현, "VoIP구현에서의 보안 고려사항", 한국인터넷기반진흥협회, Dec 2005

[4] NIST Draft, Security Consideration for Voice over IP systems, April 2004

[5] DISA, IP Telephony & Voice over IP - Security Technical Implementation Guide ver2, Dec 2004

[6] Department of communications, Information Technology and the Arts, Examination of policy and Reguration replating voice over Internet protocol(VOIP) Services, Nov 2005

[7] http://www.voipsa.org/

[8] http://www.vocal.org/

[9] 임채훈, "VoIP시스템에서의 보안기술", Netsec-kr2005

〈著 者 紹 介〉

구 자 현 (Ja-Hyun Koo)

정회원

1998년 2월 : 한양대학교 전자공학과 졸업

1998년 1월~현재 : (주) 데이콤 NW보안팀 선임연구원

〈관심분야〉 정보보호, 네트워크 보안, 통합보안, 조기경보, BcN, VoIP