VoIP 보안관련 주요기술에 대한 분석

나성훈* · 신현식**

Analysis of key technologies related to VoIP security

Sung-hun Rha* · Hyun-sik Shin**

요 약

VoIP(Voice over IP)서비스는 기존의 일반전화와 달리 인터넷망을 이용하여 음성 및 영상통화를 제공하는 서비스이다. VoIP의 사용이 보편화되고 발전되면서 보안의 위협도 계속 발전하고 있다. 이에대해 다양한 측면에서 VoIP의 보안에 대한 문제점 및 취약성에 대해 알아보고, 이 취약성을 해결하기 위한 방법인 보안 솔루션의 주요기술에 대해 알아보고자 한다.

ABSTRACT

VoIP Service is provided voice & image call using internetwork unlike traditional call. VoIP usage is becoming generalization & development. As a result, threats of security are steadily increasing. Regarding this situation, we will investigate the security problem of VoIP in various aspects. Also We will investigate main technology of security solution method for solve this problem.

키워드

VoIP. PSTN, RTP, Authentication, Authorization, 보안

제1장. 서 론

VoIP는 데이터망과의 통합과 새로운 부가 서비스의 창출을 가능하게 하며 향후 차세대 통신 서비스로 사용될것이라고 대부분 추측한다. 현재의 발전 추세로 보아도 안정성과 비용에 있어 기존의 PSTN(Public Switched Telephone Network)을 앞지르고 있고, 새로운 부가 서비스가 가능하다는 장점이 부각되고 있다. 하지만, VoIP의 보안성은 아직 성숙단계에 있다고 할 수 없다. VoIP 보안에 대해 알아봄으로써 VoIP 활성화에 기여하고자 한다.

제2장. VoIP 네트워크의 개략적 이해

VoIP는 전화의 호(call)를 제어하는 프로토콜을 기반으로 한다. 양 단말기(User Agent)사이에 호연결을 위한 콜 서버(Call server) 장비가 필요하며. 콜 서버는 각 프로토콜에 따라 다른 명칭을 사용하는데 게이트키퍼, 프락시 서버, 소프트스위치라 부른다. VoIP 네트워크의 기본 구조는 호를 제어하는 콜 서버와 사용자간 인터페이스를 위한 단말로 구성되며, 콜서버와 단말은 정해진 프로토콜(H.323/MGCP/SIP)에 의해 통신한다. 호가 성립되면 단말간 음성데이터는 RTP 프로토콜(Real-time Transport Protocol)에 의해 단말기에 전달된다.

* 전남대학교 전자통신공학과(rsh0321@lguplus.co.kr) ** 교신저자 : 전남대학교 전자통신공학과(shinhs@chonnam.ac.kr)
접수일자 : 2010. 06. 30 심사(수정)일자 : 2010. 07. 08 게재확정일자 : 2010. 08. 05

RTP는 오디오나 비디오 같은 실시간 데이터를 전송하기 위한 인터넷 프로토콜이다.

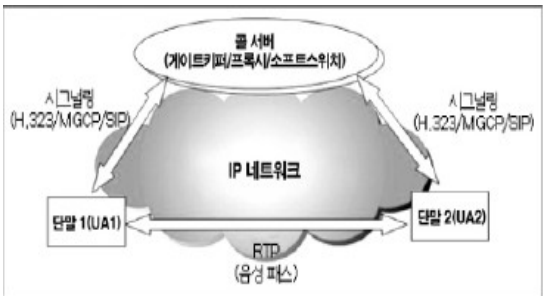

그림 1. VoIP 네트워크의 기본구조
Fig. 1 The basic structure of a VoIP network

VoIP의 중요한 특징은 콜 제어와 미디어 데이터가 분리 운영된다는 점이다. 이 특징은 VoIP가 인터넷 환경에서 매우 빠르게 채용될 수 있는 구조를 제공한다. VoIP에서는 각각의 기능이 범용성을 가지므로 기존의 미디어 트래픽 처리 구조를 그대로 수용할 수 있다. 또한, 미디어 세션 전송 역할을 UA에게 많이 이양함(Intelligent Terminal)으로써 관리가 용이하다.

이미 VoIP 기술은 90년대 중반부터 제기돼 다양한 프로토콜이 개발됐다. 이런 프로토콜에는 H.323, MGCP/MEGACO, SIP 등이 대표적이라고 할 수 있다.[1]

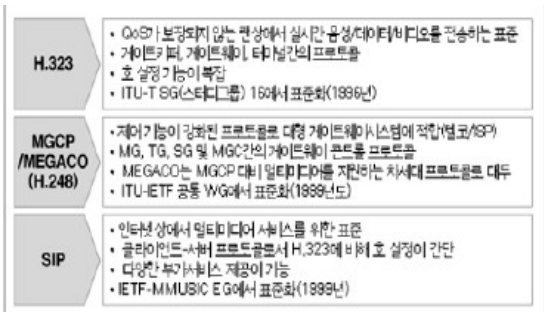

그림 2. VoIP 특징
Fig. 2 VoIP features

2.1. VoIP 보안 규약 현황

각각의 프로토콜의 규약들은 VoIP 보안기능을 강화하기 위해 인증방식, 데이터 암호화, 키관리 방식을 제안하고 있다. 이러한 일련의 이슈들을 정리하면 아래와 같다.

H.323의 보안 규정은 별도로 H.235 보안 프로파일에서 규정하고 있다. H.235v2는 2000년 11월에 승인된 H.235 차기 버전인데 3가지의 프로파일을 아래와 같이 정의하고 있다.

Annex D - 공유 키와 해쉬방식 (기본 프로파일)
Annex E - 모든 메시지의 디지털 서명
Annex F - 공유 키 성립과 디지털 서명[2]

SIP 프로토콜에서도 보안기능을 강화하기 위해 사용자 인증방식, 데이터 암호화, 키관리 방식을 제안하고 있다. 즉, SIP 시그널링에 대한 사용자 인증(Authentication)을 위해 RFC2617의 HTTP 다이제스트 방식을 사용하는 것으로 규정했고, 메시지 콘텐츠의 암호화를 위해 S/MIME 방식으로 메시지를 암호화하기로 RFC3261에 규정했다. 미디어 트래픽의 암호화를 위해서는 RTP 대신 SRTP를 사용하도록 규정했다. UDP 기반의 SIP을 보강하고 신뢰성 있는 보안을 강화하고자 TLS 기반의 전송 프로토콜과 IPSec을 권고하고 있다.[3]

Megaco(RFC3525)는 IPSec과 같은 전송 프로토콜 계층의 보안을 추천하고 있고, H.248은 좀더 구체적인 구현 방법에 대해 정의하고 있으나, H.323/SIP과 비교해 상세한 보안 이슈를 제기하지 않고 있는 실정이다. 마찬가지로, MGCP 역시 보안 규격에 대해 상세한 규약을 제정하지 않고 있다.

2.2. VoIP 보안 특징

VoIP는 인터넷프로토콜에의해 개발된 네트워크 환경하에서 동작한다. 따라서 기존의 유선전화의 보안성 외에도 기존 IP네트워크의 취약성을 더 포함하고 있다. 예를 들어 기존에 전화는 유선 탭핑(wire-tapping)을 통해 도감청을 수행했다면, 기존 IP네트워크에서는 IP 스누핑(ip-spoofing)이나 세션 하이젝킹(session hijacking) 등을 통해 도감청의 방법이 다양해 졌다. 이러한 VoIP 보안의 특징에 대해 알아보고자 한다.[4]

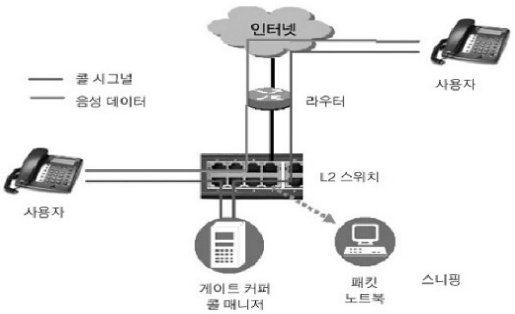

그림 3. 도청의 예
Fig. 3 example of tapping

2.2.1. VoIP의 동작원리

VoIP는 지능적인(Intelligent) 플랫폼위에서 동작한다. 고전적인 PSTN 전화기는 더미폰(Dummy Phone)이라고 부른다. 전화를 걸고 받는 기능만이 있기 때문이다. 따라서 복잡한 동작을 수행하지 않는다. 하지만, VoIP 폰은 PSTN의 전화기에 비해 엄청나게 복잡한 기능을 수행하고 있다. 이러한 기능은, 하드웨어 폰의 경우 임베디드 OS의 응용프로그램으로 동작하고, 소프트폰의 경우 개인용 컴퓨터 OS상의 응용프로그램으로 동작한다. 설정해야 할 사항이 많아서 오류 및 관리할 부분도 덩달아 많아진다. 그리고 기존 OS의 취약성을 더 추가적으로 내포한다. 이러한 취약성의 종류로 버퍼오버플로우(buffer overflow) 공격이나 트로이목마(Trojan virus) 공격이 그것이다.[5]

2.2.2. VoIP의 대중화 및 공개화.

VoIP 프로토콜은 국제 표준기구의 표준프로토콜에 기반하고 있다. 따라서 컴퓨터 지식이 있는 사람은 누구나 이해할 수 있고, 프로그래머는 그 프로토콜을 구현하거나 이용할 수 있다. 컴퓨터의 대중화에 따라, 구현기술도 용이해졌으며 배포도 자유롭다. 따라서 하나의 취약성에 의한 공격은 매우 빠른 속도로 전파돼 전국적 혹은 전세계적인 통신 마비를 가져올 수도 있다.[6]

제3장. VoIP 보안 문제의 분류

VoIP 보안의 문제는 크게 개인의 정보보호(Privacy), 시스템 및 서비스 보호규제로 분류할수 있다. 각각의 분류에 대한 보안 문제들을 정리하면 아래와 같다.

3.1. 개인의 정보 보호

개인의 정보보호는 개인의 정보를 다른 사람에게 노출하지 않고, 사생활을 보장받는 것을 의미한다. 인터넷 전화에서 전화중의 도청이 명확한 개인 정보의 침해이다. 인터넷 전화는 일반 데이터 회선을 공유하는 것이 일반적이다. PSTN상에서는 물리적인 탭핑을 이용해 도청을 시도했다면, 인터넷 전화는 일반 네트워크회선상에서 보다 다양한 방법으로 개인 인터넷 전화의 도감청이 가능하다. 일반적인 데이터 통신의 노출과 같이 전송 경로상의 네트워크 장비를 해킹하거나, 설정을 변경해, 소프트웨어적인 스푸핑 방식으로 도감청이 훨씬 용이해졌다. 이외에도 수집된 패킷을 사용해 재생하는 방법이 많이 범용화됐다. 세션 하이재킹(Session Hijacking)과 같은 사용자 및 단말기 위조도 중요한 공격의 유형이다.

3.2. 시스템 및 서비스의 보호

시스템 및 서비스의 보호는 VoIP사업자가 고민할 부분이다. 인터넷의 대중화의 나쁜 단면은 취약성을 이용해 악의적인 해킹, 정보유출, 웜/바이러스, DoS 공격 등이 일상화됐다는 것이다. VoIP 네트워크 및 서비스도 신중한 고려 및 방어를 세우지 않는다면 다양한 취약성으로 악의적인 공격자에게 노출되기 쉬운 구조다. 이러한 공격에는 아래와 같은 것들이 대표적이라고 할 수 있다.

- 불법적인 사용자의 액세스 제한
- 사용자별 서비스의 액세스 제한
- 방화벽의 호환성 및 NAT 트라버설(Traversal)의 문제
- VoIP 게이트웨이/콜 서버의 해킹, 정보 유출
- DoS/DDoS 공격
- 바이러스와 인터넷 전화 스팸(SPIT)[7]

3.3. VoIP 보안 기술 분류

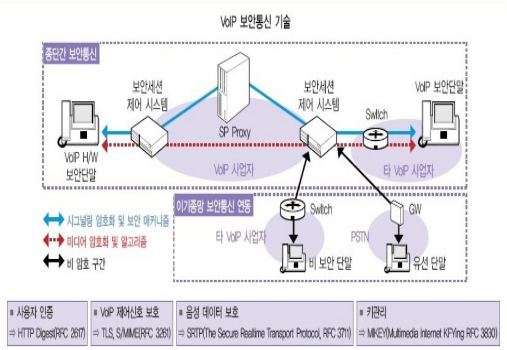

그림 4. VoIP 보안통신 기술
Fig. 4 VoIP security and communication technology

3.3.1. 사용자 측면

VoIP 사용자의 범위를 규정해 보면, 사용자는 일반 개인 혹은 가정(Home)의 사용자와 기업단위의 사용자(기업고객군)로 나눌 수 있다. 부인봉쇄(Non-Repudiation)란 정보의 발신자가 정보를 보냈다는 사실 혹은 수신자가 정보를 받았다는 사실을 부인하지 못하도록 하는 것을 말한다.

VoIP의 특성은 'Availability/Convenience' 측면에서 데이터 보안과 차이를 나타내고 있다. 'Availability'는 가용성으로 자원이 사용 가능하도록 유지하는 특성이다. 사용자의 UA 혹은 네트워크를 직간접적으로 공격해 실질적인 통화를 방해하는 모든 경우의 공격이 여기에 해당한다.[8]

또한 'Convenience' 보안모델은 사용자의 불편 및 감정적 피해를 미치는 요소들이다. 사용자의 원치 않는 스팸성 전화들, 품질에 저하를 미치는 각종 공격들이 여기에 해당한다.

이러한 Availability/Convenience 모델은 그 취약성이 타 데이터 보안에 비해 취약하며, 사용자에게 큰 영향을 미칠 수 있다.

3.3.2. 물리적 보안

사용자의 단말기(Endpoints, 혹은 Terminals)는 다양한 종류가 존재할 수 있다. 크게 하드웨어와 소프트웨어형태로 구별할 수 있다. 일반적으로 말을 할 때, 'VoIP 폰(Phone)'혹은 IP폰을 지칭할 경우 일반 전화기 형태의 전용의 하드웨어 형태의 전화기를 말한다.

소프트웨어 형태의 전화기는 일반 PC에 설치해 PC와 동일 인터넷 라인을 이용해 사용하는 프로그램으로 '소프트폰'이라고 불린다. 엔드포인트는 프로토콜의 종류, 혹은 기능에 따른 구분도 가능하다. 예를 들어 기존에 많이 사용하던 VoIP 전화기는 H.323 프로토콜에 기반했다. 최근에, SIP프로토콜이 많이 사용되면서, 'SIP-폰'이 언급되기도 한다. 현재의 IP폰 추세는 단일한 프로토콜만을 지원하는 것이 아니라, 2~3개의 프로토콜을 선택적으로 사용할 수 있는 경향이 많다. 또한 단순 호연결의 기능에서, 영상전화 등 멀티미디어 및 IM(Instant Message)와 같은 부가서비스가 가능한 전화기 등 지능이 높은 단말기가 증가하는 추세다.

3.3.3. ISP 측면에서의 VoIP 보안 기술

VoIP 보안기술의 핵심요소는 아래와 같다.

- VoIP 네트워크 망의 물리적 혹은 논리적인 분리
- 중간 경로의 장비 혹은 엔드 포인트 장비의 접근 권한 제한
- 사용자 인증(Authentication), 권한부여(Authorization)
- 엑세스 제어 : 사용자 액세스 컨트롤, 파이어월, 침입방지(Intru sion Prevention)[9]

3.4.SIP 프로토콜의 보안 기술

SIP 표준은 IETF에서 가장 활발하고 광범위한 워킹그룹으로 성장했고, 그 응용은 나날이 새로워지고 있다.SIP프로토콜이 텍스트 기반이며 기존의 HTTP의 메커니즘을 많이 따르고 있는 것도 대중화의 큰 요소다. RFC 3261는 SIP의 표준 문서이면서 동시에 보안에 대해 다양한 기능을 정의하고 있다.

3.4.1. 유저 에이전트 인증

SIP에서는 호(call)의 성립시 사용자의 인증을 위해 HTTP 요약 권환관리(Digest Authentication)을 사용한다. HTTP 요약 방식이란 사용자의 등록시에 registrar 서버측에서 주어진 key(nonce) value를 알려주고 사용자 이름, 패스워드 등의 값들을 MD5 체크섬으로 전송하게 하는 방식이다. 이렇게 함으로서 개인의 암호값이 플레인 텍스트(plain text)로 노출되는 것을 방지한다. 현재 인터넷 서비스에서 많이 사용하고 있는 방식으로 간단하면서도 효율적인 방식이다. 하지만, 인증의 강도가 높지 않아서, 현재의 RFC3261

에서는 추천하지 않고 있으나, 뚜렷한 대안은 없는 상태다.

3.4.2. 메시지의 보호 : SMIME

SIP 프로토콜을 통하여 전송되는 SIP 메시지는 MIME 포맷으로 전송된다.

MIME는 자체적으로 MIME 데이터 통합, 암호화(confidentiality) 기능을 제공하고 있다. 즉 S/MIME을 활용하여 공개키 분배, 인증, 무결성, 콜 데이터의 기밀성등을 제공할 수 있다. S/MIME의 사용시에 문제점은 메시지의 양이 크기 때문에 UDP보다 TCP상에서 전송을 권장하고 있다.[10]

3.4.3. 미디어의 기밀성

SIP자체는 미디어 데이터의 암호화를 제공하지 않지만 RTP의 보안성을 높인 SRTP의 사용을 권장하고 있다 SRTP는 AES(Advanced Ecryption Standrad)와 같은 대칭키를 기반으로 하고 대칭키의 분배를 위해서는 SDP (RFC 2327)를 이용해 키 관리를 할 수 있다. 하지만 SDP는 SIP 메시지의 일부이므로 SDP의 암호화가 선행돼야 한다. SDP의 암호화를 위해서 SMIME이나 IPSEC/TLS등이 사용된다.

3.4.4. TLS/IPSEC의 이용

표준에서는 SIP 호제어의 보호를 위해서 프록시, 레지스터서버들간 혹은 UA간에 TLS를 사용하도록 권장하고 있다. TLS는 SIP 메시지의 무결성, 기밀성, 재생(replay)공격을 방어하는데 유용하다. 하지만, TLS의 문제점은 여러가지가 있다. 그 중 첫번째는 UDP기반에서는 사용할 수 없다는 것이다. SIP의 장점중의 하나는 UDP는 손쉽게 구현가능하며, 빠르다는 장점이 있는데 이를 활용하지 못한다는 것이다.

둘째로, TLS를 음성 데이터의 보호에는 적용하지 않는다. 셋째로는 홉 바이 홉(Hop-by-Hop)으로만 전송한다는 것이다. SIP의 확장에 따라 여러 프락시나, 서버를 경유해야 할 경우 경로 및 사용자의 처리를 위해서는 암호화된 TLS 패킷을 재차 복호화해야한다. 이는 엔드투엔드의 보안에도 위반될 뿐더러, 성능에 심각한 영향을 미친다.

IPSec은 네트워크 레이어(L3)의 IP 패킷 단위의 암호화를 담당한다. 따라서, UDP/TCP에 모두 적용가능하며, 메시지와 음성데이터의 암호화에 모두 적용가능한 장점이 있다. 따라서 VPN의 적용에서와 같이 SIP VPN 서비스를 수행하거나 기업내망의 서비스를 구축하는 데 매우 유용하다.

IPSec은 인증, 무결성, 기밀성 등을 모두 만족할 수 있다. 또한, 홉 바이 홉, 엔드 투 엔드를 모두 수용할 수 있는 장점이 있다. IPSec의 키 관리를 위해서는 일반적으로 IPSec의 키관리 방식을 그대로 수용한다. 이러한 키관리에는 IKE (Internet Key Exchange), ISAKMP, Oakley, SKEME 등이 있다. 이 중에서 IKE가 많이 사용 중이다.

제4장. VoIP 보안과 QoS의 상관관계

VoIP 시스템의 보안성보다 더 중요한 요구사항중의 하나는 서비스의 품질(QoS)이다. 하지만 두가지의 요구사항(보안성, 품질)을 상당한 어려움이 존재한다. VoIP는 사람과 사람간의 실시간 통신이고, 통신데이터는 작은 패킷들로 쪼개어져 전송된다. 보안성을 높이려는 목적으로 방화벽을 통과시키거나 암호화/복호화를 수행하는 것은 패킷의 지연시간(delay, latency), 지연 편차(Jitter), 패킷손실(loss) 등을 야기시켜서 서비스의 품질에 치명적인 영향을 준다. 보안성을 높이고자 하는 방화벽, 침입차단, VPN 등 모든 보안장치들이 영향을 준다.

VoIP 시스템에서 단방향으로 음성 패킷의 전송시 음성 품질에 영향을 미치지 않는 최대 지연시간은 약 150m/s로 알려져 있다. 음성데이터를 디지털화하는 인코딩 시간은 약 1~30m/s가 필요하다. 그리고, 음성데이터를 인터넷을 통하여 전송하는 시간은 지역마다 다르다. 이때, 실제의 물리적인 거리도 중요하지만 몇개의 라우터 홉을 경유하느냐가 중요한 요소다.

VoIP보안장비에서는 패킷의 지연시간을 30~ 50m/s 이하로 줄이고, 패킷의 손실을 최소하는 것이 필수사항이다. 만약, 네트워크에서 VoIP 트래픽을 통과하는 VoIP 보안장비나 네트워크 보안 장비가 있다면, VoIP 패킷에 대한 품질에 대한 영향을 중요하게 고려해야 한다.

표 1. VoIP 통화품질 기준
Table 1. VoIP toll quality standard

품질지표		품질기준
통화품질	R 값	70 이상
	종단간 지연	150 ms 이하
접속품질	호 성공률	95% 이상

제5장. 결 론

본 논문에서는 VoIP에서 발생할 수 있는 보안관련 문제를 방지하기 위해 보안관련 주요기술 및 이슈에 대해 분석해 보았다. 기존의 전화시스템은 지난 수십년간 발전하면서, 매우 안정적이며 저렴한 서비스를 제공했고, 많은 보안문제를 해결했다. 인터넷의 보급과 더불어 VoIP서비스라는 새로운 패러다임의 등장으로 보다 저렴하고 다양한 부가서비스를 이용할 수 있으나 본 논문에서 언급한 여러 가지 보안관련 문제의 선해결이 필요하다고 하겠다.

이러한 보안관련 주요기술에 대한 연구를 통해 보다 안정적인 보안기능을 구현할 수 있으리라 예상된다. 따라서 이에 대한 지속적이고 활발한 연구가 요구된다.

참고 문헌

[1] Journal of information security and cryptology the seventeen chapter issue 5 (October 2007)
[2] Korea entertainers Entertainment Industry Institute the third chapter issue 3 pp. 78~83 (September 2009)
[3] VoIP security vulnerabilities to attacks of corr-espondence analysis of the existing security equipment, Korea information security agency (January 1 2007)
[4] Jo yeoung-cheol
[5] Information security and cryptology the nineteen chapter issue 3 (June 2009) pp. 57~65
[6] Networktimes the second chapter On August pp. 20~25
[7] Broadcast and technical the consecutive number of volumes the one hundred sixty three (July 2009) pp. 122~127
[8] Korea Society of Computer and Information the ten chapter issue 5 the consecutive number of volumes issue 37 (November 2005) pp. 237~243
[9] Monthly publication 'information protection 21c' the consecutive number of volumes the ninty eight chapter (November 2007)
[10] Yun hyeong deuk sin hyeon sik Korea Electronics and Telecommunications Institute the four chapter issue 2 pp. 143~147

저자 소개

나성훈(Sung-hun Na)

2002년 한밭대학교 전자공학과 졸업(공학사)
2009년 전남대학교 대학원 전자통신공학과 석사과정
※ 주 관심분야 : VoIP, BcN, 해저광통신

신현식(Hyun-sik Shin)

1969년 광운대학교 무선통신 공학과 졸업(공학사)
1980년 건국대학교 행정대학원 졸업(행정학석사)
1995년 경남대학교 대학원 졸업(행정학박사)
현재 전남대학교 전자통신공학과 교수
전남대학교 산학협력대학원장
(사)한국해양정보통신학회 회장, 명예회장
(사)한국전자통신학회 회장
교육과학기술부 교육과정 심의의원
※ 주 관심분야 : 전파통신법, 데이터통신, 해상재해 및 통신재난, 무선통신, 정보통신