특 집

VoIP 시스템에서의 보안기술

임 채 훈*

● 목 차 ●

1. 서 론

인터넷은 이제 데이터 뿐만 아니라 음성이나 동화상 등 멀티미디어 서비스를 위한 통합 네트웍 환경으로 발전되고 있고, 그에 따라 다양한 통신 프로토콜과 응용 서비스들이 활발히 개발 구현되고 있다. 최근 들어 가장 큰 이슈가 되고 있는 것이 아마도 VoIP와 무선 인터넷일 것이다. 결국은 유무선 통신망이 IP 네트웍을 근간으로 상호 연동되고 그 위에서 데이터, 음성, 화상 등의 다양한 멀티미디어 서비스들이 끊임이 없이 제공될 것이다.

인터넷은 원래 trusted community간의 파일 교환을 목적으로 개발된 연구망이었고 따라서 보안을 염두에 두고 설계된 망이 아니다. 그러나 인터넷이 발전되어 기업활동이나 국가 기간망의 근간으로 자리를 잡게 됨에 따라 보안문제가 가장 큰 선결과제의 하나로 부각되고 있다. 특히 기존의 전용선이나 Dial-up modem 뿐만 아니라 DSL이나 Cable modem, 무선, 위성 등의 다양한 광대역 액세스 망들이 속속 인터넷에 접속되고 이들 위에서 VoIP나 P2P 등 다양한 새로운 응용 서비스들이 제공됨에 따라 보안문제는 그 복잡도가 날로 증가하고 있고 실제로 많은 응용에서 아직까지 제대로 된 보안을 하는 것이 불가능한 경우가 많다.

본 논문에서는 VoIP 시스템에서 이슈가 되고 있는 보안문제와 그 표준화 동향 등을 간략히 살펴보고자 한다. VoIP 시스템 자체의 보안 뿐만 아니라 VoIP 프로토콜의 특성상 기존의 네트웍 인프라로 자리잡고 있는 방화벽이나 NAT (Network Address Translator) 등을 통과하는 문제가 오히려 더 큰 선결 과제이므로 이와 관련된 기술동향도 소개하고자 한다.

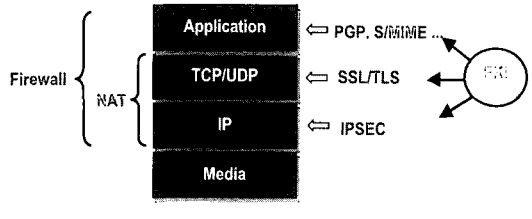
2. 네트웍 보안기술

우선 기존 보안기술 중 VoIP 시스템의 보안과 밀접한 관계가 있는 대표적인 보안기술들을 간략히 살펴본다. 인터넷 보안기술은 크게 식별 가능한 사용자들에게 적용 가능한 암호기술을 이용한 보안과 불특정 다수의 인터넷 사용자로부터 내부의 자원들을 보호하기 위한 모니터링 기반의 보안기술로 나눌 수 있다. 암호기술은 사용자 인증, 데이터의 비밀성이나 무결성 보장 등 다양한 보안 서비스를 가능하게 하는 가장 효과적이고 경제적인 보안

* (주) 퓨처시스템, 암호체계센타 소장

기술이지만 비밀키의 분배 및 사용을 전제로 하는 만큼 적용범위에 제한이 있고, 각종 응용 서비스나 네트웍 자체가 불완전하여 발생되는 대부분의 보안문제를 해결하는 데는 별로 도움이 되지 않는다. 반면 방화벽이나 바이러스/침입탐지 등 인터넷 트래픽의 분석을 통해 불법적인 접근을 차단하거나 악성코드나 공격패턴을 탐지하여 경고해 주는 모니터링 기반의 보안기술들은 암호기술로 해결할 수 없는 많은 보안문제를 해결하는 데 도움을 주는 중요한 보안기술이다. 물론 이 부류의 보안기술들은 근본적으로 불안전할 수 밖에 없고 현실적으로도 모든 공격을 차단하거나 탐지할 수 있는 것은 아니지만 잠재적인 공격자인 불특정 다수의 인터넷 사용자들로부터 내부자원을 보호하는데 사용될 수 있는 최선의 보안기술이라 할 수 있다.

그림 1에 VoIP 시스템의 보안에 적용 가능하거나 고려해야 할 대표적인 보안기술을 인터넷 프로토콜 스택상의 각 계층에 표시하여 보았다. 암호기술을 이용한 보안기술로 가장 널리 사용되는 것으로 IP 계층 위에서 동작하는 IPSEC과 TCP상에서 동작하는 SSL/TLS, 그리고 응용계층에서 적용되는 PGP나 S/MIME 등이 있다. 기존의 네트웍 인프라로 널리 깔려 있는 NAT나 Firewall도 VoIP 서비스가 실제로 제공되기 위해 통과해야 할 중요한 고려사항이다.



(그림 1) TCP/IP 계층별 네트웍 보안 프로토콜

IPSEC(IP SECurity)은 IP 패켓에 대한 인증이나 암호화, 접근제어 등의 다양한 보안서비스를 제공해 주는 Peer-to-Peer 기반의 보안 프로토콜로 가상사설망(Virtual Private Network: VPN)의 구현에 가장 널리 사용된다. IP 계층 바로 위에서 동작하는 만큼 TCP나 UDP 등 Transport protocol에 무관하게 적용 가능하며, 특히 VoIP에서 PSTN 시그날링 메시지를 IP 네트웍상으로 전송하기 위해 개발된 전송계층 프로토콜인 SCTP(Stream Control Transmission Protocol)에서도 보안을 위해 IPSEC을 권고하고 있고 IPSEC Working Group에서도 SCTP를 지원하기 위한 확장 작업을 하고 있다. 또한 IPSEC은 IPv6에서 의무적으로 지원하도록 되어 있으며, 3세대 이동통신에서도 네트웍보안을 위해 IPSEC을 고려하고 있다.

TLS(Transport Layer Security)는 웹 트랜잭션 보안용으로 널리 사용되고 있는 SSL(Secure Session Layer)을 IETF에서 표준화시킨 것으로 TCP상의 응용 프로토콜에 대한 암호화나 무결성 등의 보안서비스를 제공해 주는 Client-Server 모델의 보안 프로토콜이다. IPSEC에 비해 좀 더 간단하나 멀티미디어 프로토콜에서 널리 사용되는 UDP상의 응용에는 적용될 수 없으며, 특히 IPSEC과 같은 보안정책 기반의 중앙 집중식 통합 보안 관리 기능은 제공할 수 없다. 한편 WAP Forum에서는 무선 데이타의 보호를 위해 TLS를 무선환경에 최적화시킨 WTLS (Wireless Transport Layer Security)를 제안하였는데, 이는 기본적으로 UDP와 같은 데이타그램 프로토콜상에서 동작하므로 필요하다면 인터넷의 UDP 통신을 보호하는데 사용될 수도 있을 것이다.

PGP(Pretty Good Privacy)나 S/MIME은 주로 E-mail 보안용으로 널리 사용되는 응용 계층 보안 프로토콜로 메시지에 대한 암호화나 인증, 서명 등의 기능을 제공한다. 특히 PGP는 Web of Trust 형의 분산구조 공개키 인증 방식을 택해 별도의 공개키 기반구조 없이도 동작한다는 잇점으로 가장 널리 사용되는 응용 보안 프로토콜이다.

IPSEC이나 SSL/TLS, S/MIME 등 공개키 기반의 키 관리를 사용하는 보안 프로토콜들은 이들이 인

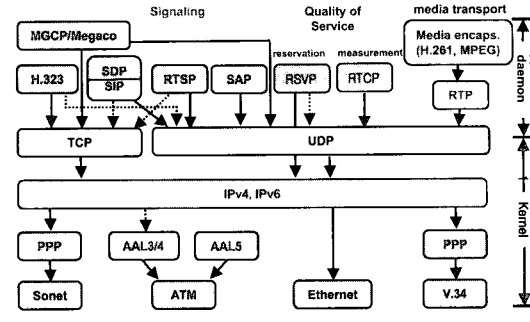
터넷상에서 널리 사용되기 위해서는 공개키 기반구조(Public Key Infrastructure: PKI)를 필요로 한다. 그러나 상호 연동하는 공개키 기반구조의 구축은 아직도 상당한 기간이 흘러야 가능하고, 또한 모든 사용자들이 공개키 인증서를 발행받아야 된다는 것도 이들이 널리 사용되는데 상당한 제한이 되고 있다. IPSEC이나 WTLS에서는 미리 공유된 비밀키(Pre-shared secret)만을 사용하여 키 관리를 할 수 있는 기능도 함께 제공하지만 이들은 scalability 문제로 대규모의 사용자 기반에서는 사용이 거의 불가능하다.

방화벽은 통상 인터넷과 내부망의 경계 부분에 존재하여 기본적으로 IP 주소, TCP/UDP 포트 및 프로토콜 등 TCP/IP 헤더의 정보를 바탕으로 미리 설정된 보안정책에 따라 패킷의 통과여부를 결정한다. 이러한 간단한 패킷 필터링에 더해 대부분의 방화벽들은 응용 프로토콜의 데이터를 해석하거나 Proxy를 구현하여 중요한 프로토콜들(FTP, HTTP, SMTP 등)을 통제한다. NAT는 주로 IP 주소의 부족 문제나 내부망의 구조를 숨길 목적으로 널리 사용되는 네트웍 장비로 주로 라우터나 방화벽 등에 기본적으로 내장되어 있다. 내부의 사설 IP를 인터넷에서 라우팅 가능한 공개 IP로 변환해 주는 역할을 하며, IP 주소뿐만 아니라 TCP/UDP의 포트번호까지를 변환해 주는 NAPT (Network Address Port Translator)가 가장 널리 사용된다.

이상의 각 보안 메커니즘에 대한 표준문서나 참고자료는 참고문헌 [22,24]에 잘 정리되어 있다.

3. VoIP 프로토콜

VoIP 프로토콜은 크게 H.323 (H.225.0, H.245), SIP, SAP, MGCP, Megaco/H.248, RTSP 등 호 설정이나 제어를 담당하는 시그날링 프로토콜과 실제로 미디어 스트림을 전송하는 RTP/RTCP 등의 전송 프로토콜로 구성된다 (그림 2 참조: VoIP의 표준문서나 관련 참고자료는 참고문헌 [20,21,23,24] 참조). 이들은 모두 TCP나 UDP 상의 응용계층에서 동작하는 프로토콜로 기존의 대부분의 인터넷 프로토콜들에 비해 대단히 복잡할 뿐더러 보안상의 관점에서도 기존의 네트웍 인프라에 통합되는데 많은 난제를 안고 있다.



(그림 2) 인터넷 VoIP 프로토콜 스택

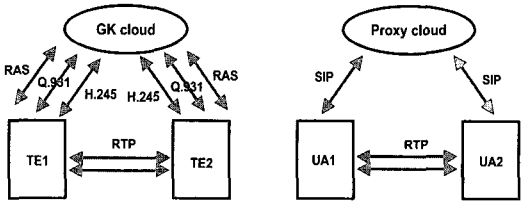
보안측면에서 VoIP 프로토콜의 주요 특성들을 살펴보면 다음과 같다.

◦ Session Bundling: 하나의 미디어 통신에 복수개의 상호연쇄된 채널들을 사용한다. 예를들어 H.323의 경우 H.225.0/Q.931 call signaling channel, H.245 call control channel 및 미디어 스트림을 위한 복수개의 RTP/RTCP logical channel들이 있으며 이전의 채널에서 다음 채널을 여는 형태로 동작한다. SIP의 경우도 SIP에서 RTP/RTCP 채널을 열어준다 (그림 3 참조).

◦ Heavy use of dynamic & embedded IP addresses: 대부분의 채널들이 다이내믹하게 열리고 닫히는데 이러한 채널에 대한 IP address/port들이 응용 프로토콜 메시지로 교환된다. 따라서 대부분의 네트웍에 깔려있는 NAT나 Firewall들에서 Application-Level Gateway(ALG)나 Proxy가 지원되지 않으면 이들을 통과할 수가 없다. 더욱이 이러한 메시지가 암호화되거나 MAC이 걸리는 경우는 필요한 IP address/port 정보를 알거나 바꿀 수 없으

므로 Firewall이나 NAT를 통과하는 것은 불가능하다.

• Heavy use of UDP: 멀티미디어 통신의 실시간 특성상 대부분의 VoIP 프로토콜들이 UDP상에서 동작하도록 설계되는데 보안상의 관점에서 보면 UDP는 stateless한 데이터그램 통신이므로 Firewall 등에서 통제하기가 매우 어려운 프로토콜이다. 따라서 대부분의 Firewall에서는 기본적으로 사용자 레벨의 UDP 통신은 허용하지 않도록 설정한다. 또한 NAT의 경우에도 UDP는 Address binding의 timeout 문제로 관리가 쉽지 않다.



(그림 3) H.323과 SIP의 호 설정 및 미디어 통신 예

4. VoIP 프로토콜의 보안

VoIP 시스템이 실제로 운용되기 위해서는 사용자 인증, 시스날링 메시지나 미디어 스트림의 암호화/무결성 등의 보안은 필수적이다 (VoIP 프로토콜의 보안 요구조건이나 H.323/SIP 등에서의 보안상의 이슈 등은 참고문헌 [1-4] 참조). 이러한 VoIP 시스템의 보안을 위한 접근방법에는 크게 두 가지가 있을 수 있다.

• 첫 번째 방법으로 IPSEC이나 TLS와 같이 잘 정립되어 있고 널리 사용되는 보안 인프라를 재사용하는 것이다. 이는 보안 전문가들에 의해 검증된 기존의 보안 인프라를 재사용함으로써 안전성을 보장받고 개발기간을 단축시킬 수 있으며 중복 투자를 피할 수 있으므로 대부분의 응용 프로토콜에서 추구하는 가장 일반적인 접근방법이다. ITU-T나 IETF에서도 기본적으로는 가능한 기존의 보안 프로토콜을 재사용하는 것을 전제로 하지만, 이러한 보안 인프라가 널리 깔리기 전까지는 과도기적으로 Application-specific한 보안 메커니즘을 제공하기도 한다. IPSEC에는 아직까지 VoIP 서비스에서 필수적인 Multicast 통신용의 키 분배 메커니즘이 표준화되어 있지 않으므로 IPSEC으로 RTP/RTCP 메시지를 보호하는 것은 쉽지 않다.

• 두 번째는 VoIP 프로토콜 자체 내에서 Built-in security mechanism을 제공하는 것이다. 이는 각 프로토콜에 맞는 최적의 암호화/인증 방법을 적용할 수 있으므로 보다 효과적인 보안을 제공할 수는 있으나, 각 프로토콜 마다 자체의 보안 메커니즘을 따로 설계한다는 것은 비효율적이며 또한 충분한 분석을 통해 검증되지 않은 새로운 보안 프로토콜을 사용하는 것에는 상당한 위험부담이 따른다. 그러나 특정한 응용에 대해서는 IPSEC이나 TLS와 같은 일반적인 보안 프로토콜이 적용되기 어렵거나 비효율적인 경우가 있으므로 RTP 등에서는 별도의 Built-in security mechanism을 제공하고 있다.

VoIP 시스템의 보안은 또한 보안이 적용되는 구간에 따라 Hop-by-hop security와 End-to-end security로 구분할 수 있다.

• Hop-by-hop security는 IP 패켓이 전송되는 각 링크 (예를들어 Endpoint-Proxy, Proxy-Proxy 등) 상의 모든 트래픽을 통째로 암호화시키거나 MAC을 걸어 주는 방법으로, 비록 End-to-end path의 중간 매게 장비들에서 복호화 후 다시 암호화가 일어나므로 보안상 취약점이 될 수 있으나 헤더를 포함한 전체 패켓을 보호할 수가 있다는 장점이 있다. 이 목적으로 IPSEC이나 TLS 등이 사용될 수 있다. 그러나 TLS는 TCP 위에서만 동작하므로 적용에 제한이 있으므로 IPSEC이 가장 일반적인 솔루션이 될 것이다. 실제로 대부분의 프로토콜에서 Hop-by-hop security를 위해서는 IPSEC을 권고하고 있다. 그러나 IPSEC은 키 관리 프로토콜인 ISAKMP/IKE가 지나치게 무거워 무선 단말과 같은 제한된 환경

에서는 구현이 어렵다는 문제가 있다. 대신 키 관리 목적으로 Kerberos 같은 기존의 인증 서버를 사용할 수도 있을 것이다.

• End-to-end security는 말 그대로 통신 당사자들 간의 단대단 보안을 제공하는 것으로 중간의 각종 서버나 프락시들의 동작에 필요한 정보들은 암호화하거나 MAC을 걸 수 없으므로 평문으로 남아 있어야 한다. 따라서 IP 주소나 사용자 ID 등 프라이버시상 중요한 정보들이 노출될 수 있으므로 이들을 보호하기 위해 Hop-by-hop security와 병행해서 사용할 수 있다. 단대단 보안은 사용자들이나 서비스 제공자 측에서 보았을 때 진정한 보안을 줄 수 있으므로 가능한 이를 추구하려고 하지만 이로 인한 많은 문제점들 때문에 실제로 구현되기는 매우 어려워 보인다. 그러나 End-to-end로 사용자 인증 기능을 제공하는 것은 가능하며 실제로 H.235는 이에 대한 절차가 포함되어 있다.

ITU-T에서는 H.235라는 별도의 표준문서에서 H.245 logical channel signaling procedure를 사용하는 모든 H-series protocol (e.g., H.310, H.323, H.324)에서 사용 가능한 전반적인 보안에 관한 프레임웍을 규정하고 또한 호환성을 위한 프로파일을 제공하고 있다. 반면 IETF VoIP 표준들은 프로토콜 스택의 개념없이 각 프로토콜들이 독립적으로 설계되었으며 따라서 보안관련 사항도 각 프로토콜 문서에서 개별적으로 다루고 있다.

SIP나 RTSP는 기본적으로 HTTP와 매우 유사한 프로토콜로 보안 역시 HTTP의 보안 메커니즘을 주로 사용한다. 기본적으로 패스워드 기반의 Basic Authentication과 Digest Authentication을 지원하며, End-to-end 보안을 위해 PGP 기반의 강한 인증 및 암호화 기능을 사용하도록 권고하고 있다. SAP의 경우는 Multicast의 특성상 응용계층의 보안 프로토콜인 PGP나 S/MIME을 권장하고 있다.

RTP/RTCP는 H.323이나 SIP, RTSP 등 대부분의 VoIP 시스템에서 미디어 스트림의 전송을 위해 공통적으로 사용하는 프로토콜이다. IETF의 RTP/RTCP 표준문서에서는 기본적으로 보안을 위해 IPSEC과 같은 하위계층의 보안 인프라를 사용하는 것을 전제로 하고 이러한 보안 인프라가 일반화되기 전에 사용될 목적으로 자체 프로토콜에서 PEM 방식의 변형으로 DES CBC로 암호화하는 방법을 제시하고 있다. 그러나 현재의 IPSEC은 키 관리나 multicast 지원문제, CBC 모드 암호화의 에러 확산 문제나 Random access property 등 다양한 환경에서 적용되기에는 무리가 있으므로 최근 IETF의 AVT WG에서는 미디어 스트림의 보안을 위한 다양한 요구조건을 바탕으로 secure RTP라는 RTP/RTCP의 보안 프로파일을 표준화 중에 있다 [5,6].

5. VoIP 프로토콜과 Firewall/NAT

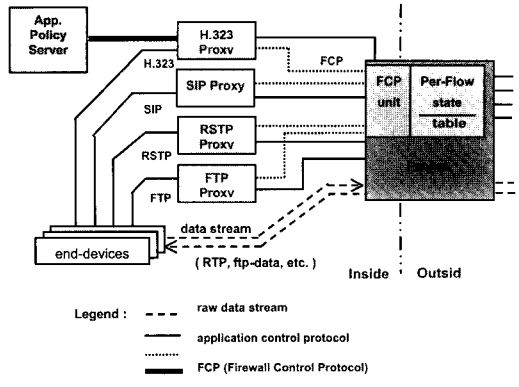
3절에서 살펴보았듯이 VoIP 프로토콜의 특성상 기존의 Firewall이나 NAT를 통과하는 것은 VoIP 시스템 자체나 Firewall/NAT에서의 변경없이는 거의 불가능하다 [7-11]. 그러나 이 문제는 VoIP 시스템의 실제 사용을 위해서는 반드시 해결되어야 할 중요한 과제이므로 IETF에서는 다양한 제안들이 논의되고 있다. Firewall/NAT 문제를 해결하고자 하는 접근방법은 크게 다음의 세 가지로 나눌 수 있다.

◦ 가장 쉽게 생각할 수 있는 것이 Firewall이나 NAT에서 Application-level proxy나 Gateway를 지원하는 것이다[10-12]. 그러나 VoIP 프로토콜 자체의 복잡성과 다양한 응용 시나리오로 인해 Transparent한 Proxy/Gateway를 지원하는 것은 결코 쉬운 일이 아니며, Firewall/NAT에서의 지나친 과부하로 인해 병목현상을 유발할 수 있다. 또한 다양한 VoIP 프로토콜별로 Proxy나 Gateway를 지원하는 것은 이들 프로토콜의 발전에 따라 끈임없이 upgrade시켜 주어야 하므로 개발이나 관리 측면에서도 scalable한 접근방법은 되지 못한다. 그러나 Proxy나

Gateway가 과도기적으로 가장 빨리 Firewall/NAT 문제를 해결할 수 있는 방법이기도 하므로 현재의 주요 Firewall 업체들은 이 방법을 주로 사용하고 있다. 그러나 이들 상용 제품이 지원하는 프로토콜은 아주 단순한 시나리오일 뿐이고 문제를 완전히 해결해 주지는 못한다[13].

• 다음으로 생각할 수 있는 것은 Firewall traversal 방법이다[14-16]. 이는 Firewall이나 NAT 자체보다 VoIP 단말과 VoIP proxy쪽에서의 변경을 통해 Firewall을 안전하게 통과하고자 하는 것이다. SOCKS V5를 이용하거나 이와 유사한 Firewall traversal protocol을 이용할 수 있다. SOCKS V5는 Generic session-level proxy로 거의 대부분의 응용 프로토콜을 중계해 줄 수 있으나, UDP 통신의 제어를 위해 별도의 TCP control channel을 이용하므로 UDP를 주로 사용하는 멀티미디어 통신의 경우 scalability면에서 문제가 될 수 있다.

• 마지막으로 IETF의 MIDCOM WG에서 주력으로 개발 중인 것이 External firewall control protocol이다 [17,18] (그림 4 참조). 이 역시 첫 번째 방법과 유사하게 Firewall이나 NAT에서의 변경을 전제로 한다. 그러나 첫 번째 방법의 문제점을 해결하기 위해 Application proxy/Gateway를 Firewall/NAT로부터 분리시켜 이들이 필요시 마다 Firewall Control Protocol을 이용해 Firewall/NAT를 조절하여 필요한 포트를 열고 닫거나 Address binding을 생성, 소멸시켜 주고자 하는 것이다. 이는 기존의 각종 VoIP Proxy들을 그대로 이용하여 Firewall/NAT를 외부에서 조절할 수 있으므로 장기적으로 가장 바람직한 접근방법이라 할 수 있다. 그러나 이를 위해서는 Firewall/NAT, Proxy들을 upgrade시켜야 하고 구체적인 Firewall Control Protocol(FCP)이 아직 표준화되지 않은 만큼 실제로 적용 가능하기까지는 상당한 시일이 흘러야 할 것으로 보인다. FCP의 대안으로 기존의 SOCKS V5나 RSVP를 확장시켜 사용하는 방법을 고려할 수 있다 [19].



(그림 4) MIDCOM 프로토콜의 동작 원리

위와 같은 Firewall/NAT 통과 방법들은 그 자체로서는 하나의 솔루션이 될 수 있으나 문제는 패킷이 인증이나 암호화를 통해 그 본체가 보호되는 경우 제 기능을 할 수 없다는 것이다. 예를들어 SIP에서는 일부 헤더 필드들과 메시지 body 부분을 PGP로 End-to-end로 보호하는 방법을 권장하고 있으나 메시지 body 부분에 미디어 채널을 열기 위한 SDP가 들어 있는 경우 Firewall이나 NAT에서 그 어드레스/포트 정보를 알 수 없으므로 제 기능을 할 수 없다. 그러나 만일 기업망의 내부 네트웍이 안전하다는 가정하에 End-to-end의 한 종단이 네트웍 경계의 Firewall이나 Proxy가 된다면 무리없이 동작 가능할 것이다.

6. 결 론

IP 네트웍 상에서의 멀티미디어 통신은 인터넷에 새로운 지평을 열어주는 차세대 인터넷 기술로 우리의 일상 생활에 획기적인 변화를 주게 될 것이다. 그러나 아직까지 멀티미디어의 초기단계인 VoIP에서 조차 해결해야 할 과제들이 산적해 있다. 대표적인 것이 인터넷 인프라의 상대적으로 취약한 서비스 품질이나 네트웍 신뢰성을 확보하는 것이고, 다음으로 중요한 것이 서비스 제공자의 사용자 관리/과금문제나 사용자의 프라이버시 보호 등

에 필요한 사용자 인증이나 메시지의 보호 등의 각종 보안 서비스를 지원하는 것이다. VoIP 프로토콜의 복잡성과 기존 네트웍 장비와의 호환성 문제 등으로 VoIP 시스템에서 제대로 된 보안기능을 제공하는 것은 실제로 대단히 어려운 일이다. 현재 이런 문제점들을 해결하기 위한 다양한 제안들이 표준화 단체들에서 논의되고 있으나 실제 구현 가능한 상세 스펙이 나오기까지는 상당한 시일이 걸릴 것으로 예상된다.

참고문헌

[1] D.Kroeselberg, "SIP security requirements from 3G wireless networks," Internet Draft, IETF, Jan. 2001. Work in progress.

[2] M.Marjalaakso, "Security requirements and constraints of VoIP," HUT. http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/marjalaakso/voip.html.

[3] J.maeng, "Firewalls, network address translators (NATs) and H.323," VTEL Presentation, Oct. 2000: http://www.packetizer.com/iptel/h323/papers (our local copy: http://cnscenter.future.co.kr/resource/rsc-center/presentation/packetizer/firewall_nat_vtel.ppt).

[4] J.Rosenberg, "SIP security," presentation at SIP 2000, May 2000: http://www.dynamicsoft.com/resources/presentation.html(our local copy: http://cnscenter.future.co.kr/resource/rsc-center/presentation/dynamic/SIP2000-Security.pdf).

[5] R.Blom, E.Carrara and M.Naslund, "Conversational multimedia security in 3G networks," Internet Draft, IETF, Nov. 2000. Work in progress.

[6] R.Blom, E.Carrara, D.McGrew, M.Naslund, K.Norrman and D.Oran, "The secure real time transport protocol," Internet Draft, IETF, Feb. 2001. Work in progress.

[7] M. Holdrege and P. Srisuresh, "Protocol complications with the IP network address translator (NAT)," RFC 3027, IETF, Jan. 2001.

[8] P. Srisuresh and M. Holdrege, "IP network address translator (NAT) terminology and considerations," RFC 2663, IETF, Aug. 1999.

[9] S. Shieh, F.Ho, Y.Huang and J.Luo, "Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP Stack," IEEE Internet Computing, Vol.4, No. 6, November/December 2000, pp.42-49.

[10] Intel, "The problems and pitfalls of getting H.323 safely through firewalls," http://support.intel.com/support/videophone/trial21/H323_WPR.HTM.

[11] Cisco, "Deploying H.323 applications in Cisco networks," http://www.cisco.com/warp/public/cc/pd/iosw/ioft/mmcm/tech/h323_wp.htm

[12] C.Martin and A.Johnston, "SIP through NAT enabled firewall call flows," Internet Draft, IETF, Feb. 2001. Work in progress.

[13] U.Roedig, R.Ackermann and R.Steinmetz, "Evaluating and improving firewalls for IP-telephony environments," Proc. of the 1st IP-Telephony Workshop (IPTel2000), April 2000.

[14] J.Rosenberg and H.Schulzrinne, "SIP Traversal through residential and enterprise NATs and firewalls," Internet Draft, IETF, Mar. 2001. Work in progress.

[15] S.Davies, S.Read and P.Cordell, "Traversal of non-protocol aware firewalls & NATs," Internet Draft, IETF, Mar. 2001. Work in progress.

[16] K.P.Fung and R.K.C.Chang, "A transport-level

proxy for secure multimedia streams," IEE Internet Computing, Vol.4, No. 6, November/ December 2000, pp.57-67.

[17] R.P.Swale, P.A.Mart and P.Sijben, "Require - ments for the MIDCOM architecture and control language," Internet Draft, IETF, Feb. 2001. Work in progress.

[18] P.Srisuresh, J.Kuthan and J.Rosenberg, "Middlebox Communication Architecture and framework," Internet Draft, IETF, Feb. 2001. Work in progress.

[19] U.Roedig, M.Gortz, M.Karsten, and R.Steinmetz, "RSVP as firewall signalling protocol," Proc. of the 6th IEEE Symposium on Computers and Communications, July 2001. To appear.

[20] Session Initiation Protocol (SIP): http://www. cs.columbia.edu/~hgs/sip/

[21] H.323 Information Site: http://www.packetizer. com/iptel/h323/

[22] 인터넷 보안: http://cnscenter.future.co.kr/menu/ security.html

[23] Hot Topics: http://cnscenter.future.co.kr/menu/ hot-topic.html

[24] IETF 보안 관련 표준 문서: http://cnscenter. future.co.kr/menu/ietf.html

저자약력

임 채 훈

1989년 서울대학교 전자공학과 학사
1989-1990년 ㈜ 데이콤 기술본부
1992년 포항공과대학교 전자전기공학과 석사
1996년 포항공과대학교 전자전기공학과 박사
1996년 백두정보기술/포항공과대학교 정보통신연구소
1997-현재 ㈜퓨쳐시스템 암호체계센타
관심분야 : 암호이론, 암호 프로토콜 설계 및 분석, 인터넷 보안, 멀티미디어 보안 등
e-mail : chlim@future.co.kr