主題

VoIP를 위한 보안 기술 현황과 전망

고려대학교 이근호, 이송희, 김정범, 한상범, 김태윤

차 례

1. 서론

최근 인터넷 관련기술의 급속한 발전으로 데이터, 음성, 영상, 화상 등의 다양한 멀티미디어 서비스는 통합한 개방형 네트워크로 진화하고 있으며 궁극적으로는 모든 미디어가 인터넷으로 수렴되는 NGN (Next Generation Network)으로 발전할 전망이다. 이러한 개방형 네트워크로의 진화는 경제성과 효율의 증가, 신규 서비스의 창출 등 많은 장점을 가지고 있으나 다양한 유무선 통신망의 융합화에 따른 통신망간의 간섭이 증가하고 네트워크 접속점 중심의 통신망간 접속구조가 확대되어 지금까지의 시스템 보안 위주의 단순한 보안 기술을 적용하기가 어렵다. 따라서 네트워크 노드 간을 효율적으로 보호하는 네트워크 중심의 보안기술이 필요한 시점이다. VoIP (Voice Over Internet Protocol)는 인터넷과 같이 패킷 교환 기술을 기반으로 하는 통신망에서의 음성통신을 통칭하는 것으로 향후 전 세계의 모든 유무선통신이 IP기반으로 통합되는 경우 비단 음성뿐만이 아니라 통신망이 제공하는 모든 서비스에 포함되는 필수적인 기술로 자리매김할 것이다.

논문의 구성은 크게 VoIP 시스템에 대한 소개와 VoIP 시스템에서의 보안기술과 앞으로의 전망을 살펴보겠다. VoIP 시스템에서의 보안 기술은 ITU-T와 IETF, ETSI의 세분야로 나누어진다. ITU-T에서는 H.235를 정의하여 H.323에서 호 신호 채널의 안전성과 사용자 인증을 위해 시그널링 메시지의 무결성 보장과 음성 정보의 암호화를 통한 비밀성을 보장한다. IETF에서는 SIP 기반의 프로토콜이 대표적이다. SIP 프로토콜은 암호화를 통하여 개인의 비밀성을 보장하고, 인증을 통하여 접근 제어와 메시지 무결성을 보장한다. 하지만 사용자의 음성을 보호하는 기능은 정의되어 있지 않지만 현재 연구가 진행되고 있다. SIP에서는 IETF에서 기존에 사용되고 있는 보안 메커니즘을 이용하여 암호화를 권장하고 있으나 이러한 프로토콜은 VoIP만을 위한 보안 프로토콜이 아니므로 여러 가지 문제점들이 노출된다. 앞으로 SIP 관련으로 연구 발표되는 문서에는 보안 관련

분야를 반드시 고려하도록 규정할 정도로 중요한 이슈가 되고 있다[4]. VoIP 프로토콜에서의 보안 문제점과 네트워크 인프라의 요소인 방화벽과 NAT에서는 VoIP 프로토콜이 통과하지 못하는 문제가 있어 이를 해결하기 위한 방법으로 MIDCOM(Middle-box Communication)을 구성하여 문제 해결방안을 모색하고 있다. 본 논문에서는 VoIP 시스템의 전체적인 구성과 네트워크의 보안을 기본으로 하여 현재의 VoIP의 보안 기술에 대해 살펴본 후 앞으로의 발전 방향을 제시하겠다.

2. VoIP 기술

VoIP는 기존의 음성 전화 서비스에 인터넷을 사용하여 인터넷의 IP 계층을 이용할 수 있는 기술이다. VoIP는 응용계층(Application Layer), 신호계층(Signalling Layer), 매체계층(Media Layer)으로 나누어지며, 계층별로 상대방과 같은 프로토콜을 이용하여 통신한다. VoIP 기술은 단순히 값싼 요금의 전화 서비스 제공에 머물지 않고 음성과 데이터를 통합한 부가 서비스 제공에 역점을 두고 연구되어 지고 있다.

2.1 VoIP 프로토콜

VoIP 프로토콜은 그림 1과 같이 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 1은 TCP와 UDP 상의 응용 계층에서 동작하는 프로토콜로 기존의 인터넷 프로토콜들에 비해 대단히 복잡하고 보안상으로도 기존의 네트워크의 인프라와의 통합에 많은 문제점이 발생된다.

VoIP 표준화 단체는 ITU-T(International Telecommunication Standardization Sector)

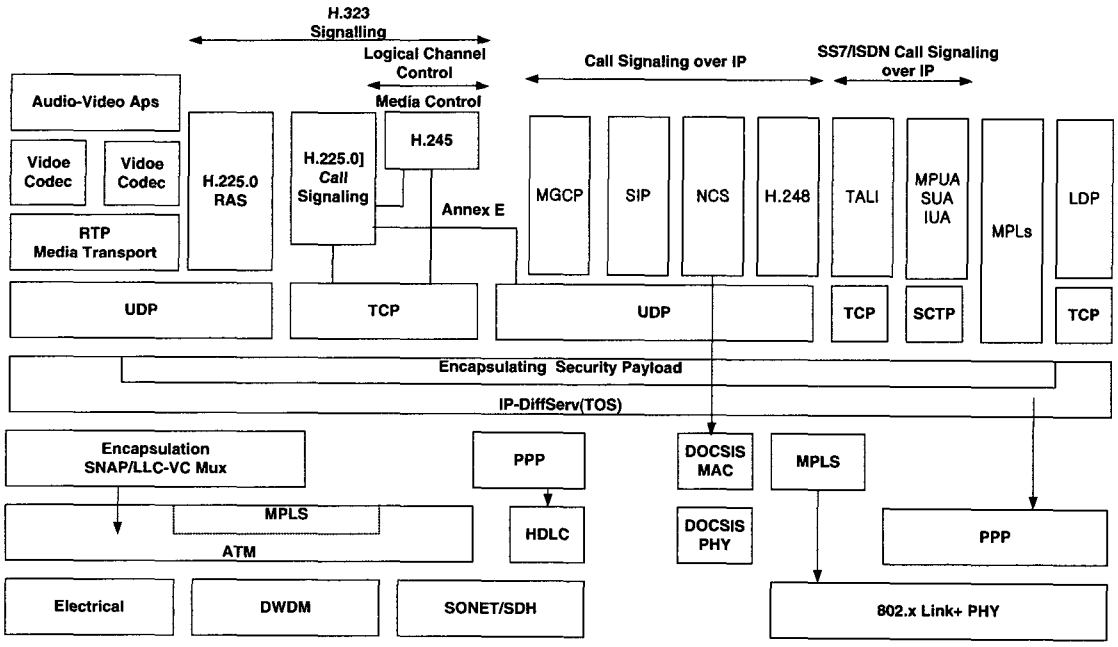


그림 1. VoIP 프로트콜 스택

와 IETF(Internet Engineering Task Force)에서 주로 표준화를 제정하고 있다.

ITU-T는 H.323 시스템을 기반으로 한다. ITU-T는 하부조직으로서 Study Group을 16 Multimedia로 나누어서 표준화를 진행하고 있다[10].

H.323의 구성요소로는 Terminal, GateKeeper, Gateway, MCU등이 있다. H.323은 1996년 인터넷 환경을 위하여 H.323 v1을 표준화하였고, 1997년 9월에는 H.323 v2를 개정하였다. H.323 v2에서는 Fast call setup, overlaping sending, tunneling, user input indication, layered video coders, Security Framework, Base document, Call Transfer, Call Forwarding, Large scale conference등이 추가되었다. 1998년 9월에 H.323 v3을 개정하였다. 개정 내용은 Realtime-Fax, Call connection over UDP, Single Use Audio Devices, Inter-Domain Communication, Hold, Message Waiting, Caller and Called Name, MIBs등이 추가되었다. 2000년 11월에는 H.323 v4를 개정하였고, MEGACO (Media Gateway Control)의 지원을 위한 구조로 변경하였으며, 여러 가지 부가적인 기능을 추가하였다. IETF는 SIP(Session Initiation Protocol)을 중심으로 표준화를 제정해 나가고 있다. IETF는 2002년 2월에 현재의 8개 표준화 영역을 구성하였다. 8개의 영역 중에서 VoIP와 관련된 표준화 영역은 Transport Area이다. Transport 분야는 ENUM(Telephone Number Mapping), IPTEL(IP Telephony), MEGACO(Media Gateway Control), MIDCOM(Middlebox Communication), MMUSIC(Multiparty Multimedia Session Control), PINT(PSTN and Internet Internetworking, SIGTRAN (Signaling Transport), SIP(Session Initiation Protocol), SPIRITS(Service in th PSTN/IN Requesting Internet Service) 워킹 그룹 등이 VoIP 표준화와 관련이 있다[11].

ITU-T와 IETF가 신호와 교환을 분리하는 Softswitch 개념이 도입되어 융통성 있는 서비스를 할 수 있는 MEGACO(Media Gateway Control) 표준을 제정하고 있다.

이밖에도 ETSI(the European Telecommunications Standards Institute)에서 TIPHON(Telecommunication and Internet Protocol Harmonization over Networks)이라는 프로젝트를 수행하고 있다[8]. 1997년 60개 이상의 업체의 참여로 구성되었으며, H.323v2를 기반으로 하고 있으며, PC-PC, PC-SCN, SCN-PC, PC-PC, SCN-SCN의 5가지 시나리오에 대한 표준화가 진행되고 있다[9]. IMTC(The International Multimedia Telecommunications Consortium, Inc)으로 전세계 150 여개 이상의 업체가 참여하는 비영리 단체이다[12]. IMTC의 목적은 개방형 국제 표준에 기반 하여 상호 연동 가능한 원격회의 솔루션을 연구하는 것이다. 주요 활동은 상호 동작 테스트, 기술 교환을 위한 포럼, 제품과 서비스의 상호 호환성과 사용성 향상 등이다.

2.2 VoIP 시스템의 구성 요소

VoIP 시스템의 구성 요소는 응용 계층, 신호 계층, 매체 계층으로 나누어진다. 그림 2는 계층별로 상대방과 같은 프로토콜을 이용하여 통신을 수행한다. 응용계층에서는 서비스의 생성/수행 기능, 지능화된 처리, 서비스관리를 하며, 신호계층에서는 호 처리, 호 변환, 자원 관리, 매체 제어를 한다. 매체 계층에서는 실제 데이터 처리/전달 또는 변형, 품질 보장, 톤 발생 기능을 담당한다. 신호 계층간에는 H.323, SIP등의 프로토콜이 사용되어, 상대방과 통화 연결/종료 신호등을 처리한다. 매체 계층에서는

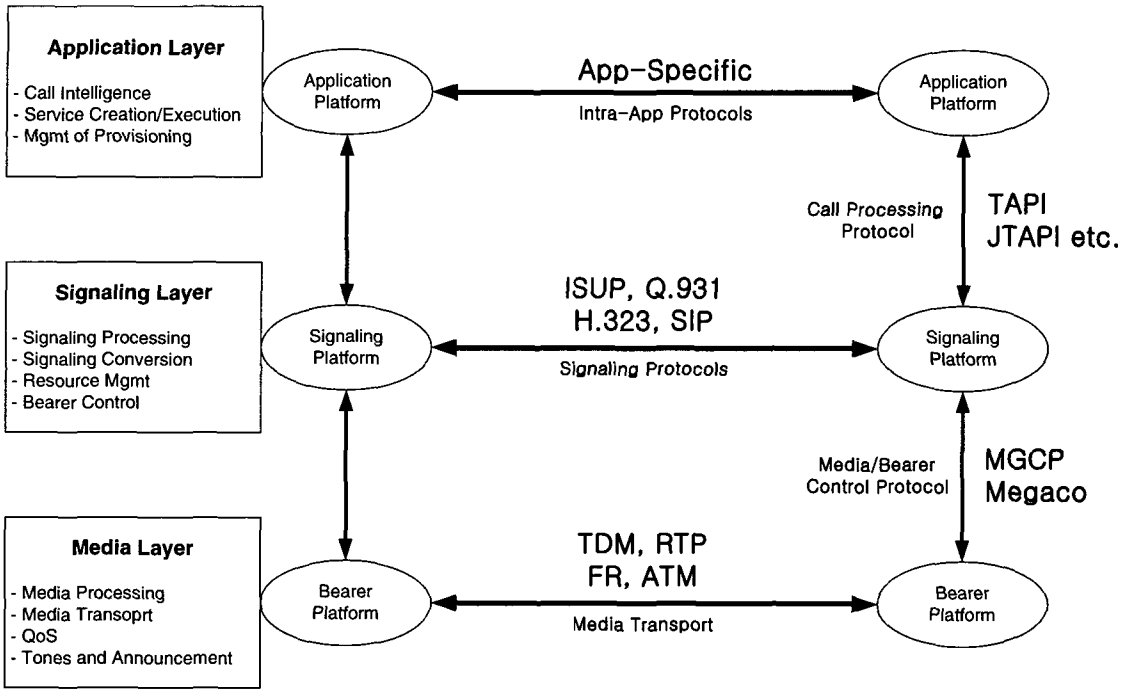


그림 2. VoIP 시스템의 구성 요소

음성 데이터를 RTP 프로토콜을 이용, 패킷으로 만들어 전송한다. 응용 계층과 신호 계층 사이에는 Call Processing Protocol이 사용되며, 응용 계층과 신호 계층 사이에 제어 정보를 전달한다. 신호 계층과 매체 계층은 Media Gateway Control Protocol을 이용하여 제어 정보를 교환하여, 신호 계층에서 실제 데이터의 경로나 매체 특성을 결정하고 수행하도록 할 수 있다[27][28].

3. 네트워크 보안 기술

VoIP와 관련된 보안 기술은 암호 기술을 이용하는 보안과 내부의 자원들을 보호하기 위한 모니터링 기반의 보안 기술로 구분할 수 있다. 암호 기술은 사용자에 대한 인증과 데이터 전송에 필요한 비밀성과 무결성을 보장하지만, 적용 범위에 대한 제한과 응용 서비스나 네트워크 자체의 불완전으로 인하여 보안 문제 해결에 도움이 되지 못한다. 내부의 시스템을 보호하는 방화벽과 침입탐지 시스템 등은 불법적인 시스템 접근을 차단하여 악성 코드나 공격패턴에 대한 사전 경고를 통해 시스템의 안전성을 보장해 준다. 이러한 모니터링 기반의 보안 기술은 암호 기술로 해결할 수 없는 부분에 도움을 주는 보안기술이다[6]. 암호 기술을 이용한 보안 기술은 네트워크의 각 계층에서 사용되어 진다(그림 3참조). IP 계층에서는 IPSec이 정보 보호 서비스를 제공하며, TLS/SSL은 TCP 계층과 응용 계층 사이에 위치한다. PGP나 S/MIMIE 은 E-mail 보안 도구이며 S-HTTP는 응용 계층인 http에 보안 서비스를 제공한다.

IPSec은 네트워크나 네트워크 통신의 패킷 처리 계층에서의 보안을 위한 표준이다. 이전의 보안 기법들에서는 보안이 통신 모델의 응용 계층에 삽입되었지만, IPSec은 가상 사설망과 사설망에 다이얼업 접

속을 통한 원격 사용자 접속의 구현에 사용한다. IPSec의 장점은 개별 사용자 컴퓨터의 변경 없이도 보안에 관한 준비가 처리될 수 있다는 것이다. IPSec은 본질적으로 데이터 송신자의 인증을 허용하는 인증 헤더와, 송신자의 인증 및 데이터 암호화를 함께 지원하는 ESP (Encapsulating Security Payload) 등 두 종류의 보안 서비스를 제공한다. 또한 IPSec은 IPv6에서도 의무적으로 지원하고 있다.

TLS는 두 개의 통신 응용 프로그램 사이에서 개인의 정보 보호와 데이터의 무결성을 제공하기 위해 만들어졌고, TLS Record 프로토콜과 TLS Handshake 프로토콜로 구성되어 있다. TLS Record Protocol은 TCP 계층의 바로 위에 위치하여 호스트 사이의 통신 연결 시 보안을 제공하며, Privacy와 Reliability service를 제공한다. TLS Record 프로토콜은 상위계층 프로토콜의 캡슐화를 위해 사용된다. 이러한 프로토콜중의 하나가 TLS Handshake 프로토콜이다. Handshake 프로토콜은 서버와 클라이언트가 데이터를 전송하기 전에 서로 인증할 수 있도록 해주며, 사용할 암호화 알고리즘과 암호키를 협상하도록 해준다. 이 프로토콜은 통신 연결 시 보안성을 제공한다.

TLS의 장점은 응용 프로토콜과 독립적이라는 것이다. Transport 계층을 기반으로 개발되기 때문에 어떠한 응용 프로그램이라도 TLS를 이용하여 안전한 통신 기반을 구축할 수 있도록 지원하고 있다. 상위 계층의 프로토콜은 TLS 프로토콜 위에서 동작할 수 있으며, TLS 보안 메커니즘을 사용하여 응용 프로그램의 보안성을 향상시킬 수 있다.

PGP나 S/MIME는 주로 E-mail 보안용으로 널리 사용되는 응용 계층 보안프로토콜이다. PGP는 송신자의 신원을 확인함으로써 그 메시지가 전달 도중에 변경되지 않았음을 확신할 수 있도록 해주는 암호화된 전자 서명에도 사용한다. 다른 사용자들이나 침입자들이 읽지 못하도록, 파일들을 암호화한다. PGP는 메시지를 암호화하기 위해 더 빠른 암호화 알고리즘을 사용하며, 그 다음에 전체 메시지를 암호화하는데 사용되었던 짧은 키를 암호화하기 위해 RSA와 Diffie-Hellman 등 두 가지 공개키를 사용한다. RSA 버전에서는 전체 메시지를 암호화하는데 사용되는 짧은 키의 생성을 위해 IDEA 알고리즘을 사용하며, 짧은 키를 암호화하기 위해 RSA를 사용한다. Diffie-Hellman 버전은 전체 메시지를 암호화하기 위한 짧은 키의 생성에 CAST 알고리즘을 사용하며, 짧은 키의 암호화에는 Diffie-Hellman 알고리즘을 사용한다. 전자서명을 보내기 위해 PGP는 사용자의 이름과 기타 서명 정보로부터 해시코드

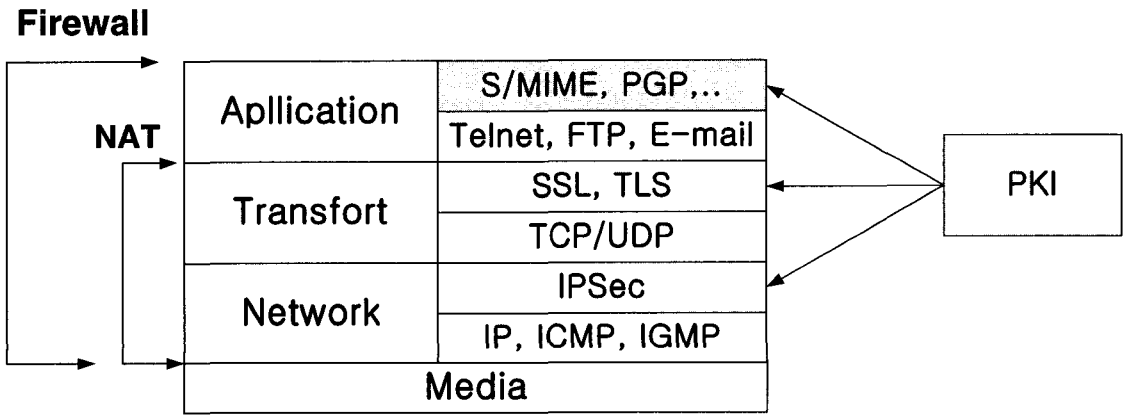


그림 3. 네트워크 계층별 보안 프로토콜

를 생성하는 효율적인 알고리즘을 사용한다. PGP의 RSA 버전은 해시코드를 생성하기 위해 MD5 알고리즘을 사용하며 Diffie-Hellman 버전은 SHA-1 알고리즘을 사용한다.

방화벽은 네트워크 게이트웨이 서버에 위치하고 있는 일련의 연관된 프로그램들로서, 다른 네트워크의 사용자들로부터 사설 네트워크의 자원들을 보호해 준다. 방화벽은 외부인이 자신의 공개되지 않은 자원에 접근하는 것을 막고, 자기회사의 직원들이 접속해야할 외부의 자원들을 통제하기 위해 기업의 인트라넷과 인터넷 사이에 설치된다. 기본적으로 방화벽은 라우터 프로그램과 밀접하게 동작함으로써 모든 네트워크 패킷들을 그들의 수신처로 전달할 것인지를 결정하기 위해 검사하고 여과한다. 또한 방화벽은 워크스테이션 사용자 대신 네트워크에 요청을 해주는 프락시 서버의 기능을 포함하거나 또는 함께 상호 협력하여 동작한다. 방화벽은 네트워크의 다른 부분들과는 별개로 특별히 지정된 컴퓨터에 설치되는 경우가 많은데 이는 들어오는 요구가 사설 네트워크 자원으로 곧바로 전달되지 않도록 하기 위한 것이다. 방화벽의 차폐방법에는 몇 가지가 있다. 단순한 방법 중 하나는 들어오는 요구가 받아들일만한 도메인 이름이나 IP 주소로부터 오는 것인지를 확인하는 것이다. 이동중인 사용자들을 위해서는 보안 접속 절차나 인증 확인 등을 통해 사설 네트워크에 원격 접속 할 수 있도록 허용한다.

NAT는 주로 IP 주소의 부족 문제나 내부망의 구조를 숨길 목적으로 널리 사용되는 네트워크 장비로 주로 라우터나 방화벽 등에 기본적으로 내장되어 있다. NAT 방식은 공개된 인터넷의 IP를 이용하여 외부로부터 공격이 들어오는 것을 막아주는 방화벽의 용도로도 사용될 수 있다. 공개된 외부의 통신망인 인터넷에서 내부의 사설망으로 들어오기 위해서는 공개되지 않은 사설망 내부의 IP까지 알아야 가능하다. 공인 IP를 가지고 있는 컴퓨터보다 공격이 어렵다.

4. VoIP 프로토콜의 보안 기술

VoIP 프로토콜은 TCP/UDP/IP 상에서 Call Signalling Part, Gateway or Device Control Part, Media Transmission Part의 세 가지 기능적인 측면으로 구별된다. Security와 관련된 기능도 어느 정보의 보호에 관점을 두는가에 따라 VoIP 프로토콜에 포함되느냐 아니면 응용 계층 혹은 네트워크 계층에 포함시키는가가 결정된다.

VoIP 시스템의 보안 접근 방법은 두 가지로 나누어 볼 수 있다.

첫째는 MGCP와 같이 네트워크 계층 프로토콜인 IPSec 처럼 널리 이용되는 보안 인프라를 사용하는 방법이다. 보안 전문가로부터 검증된 보안 인프라를 사용함으로써 안전성 보장과 개발기간의 단축, 중복 투자의 비용을 절감할 수 있다. 이러한 방법은 대부분 응용 프로토콜에서 가장 일반적인 접근 방법으로 이용하고 있다. ITU-T나 IETF에서도 기본적으로는 기존의 보안 프로토콜을 재사용하는 것을 전제로 하고 있다. IPSec에는 VoIP 서비스에서 필수적인 Multicast 통신용 키 분배 메커니즘이 표준화되어 있지 않으므로 RTP/RTCP 메시지를 보호하기가 쉽지 않다.

두 번째는 VoIP 프로토콜 자체의 Security 메커니즘을 사용하는 것이다. 프로토콜들이 최적의 암호화나 인증 방법을 적용 할 수 있으므로 보다 효과적인 보안을 제공한다. 각 프로토콜 마다 자체의 보안 메커니즘을 따로 설계하는 것은 비효율적이고, 충분한 분석을 통한 검증이 이루어지지 않았으므로 위험부담이 따르고 있다. 특정한 응용에 대해서는 IPSec 같은 일반적인 보안 프로토콜이 적용되기 어렵거나 비효율적인 경우가 있으므로 RTP 등에서는 별도의 Built-in 보안 메커니즘을 제공한다[5].

H.323은 복잡하고 다양한 프로토콜로 구성되어 있다. 이에 비하여 SIP과 MGCP는 단순하면서도 확장성을 가지고 있다. 보안 기술도 각 프로토콜의

역할에 따라 차이가 있다. ITU-T에서는 H.235라는 별도의 표준문서에서 전반적인 보안에 관한 프레임워크를 규정하고 호환성을 위한 프로파일을 제공하고 있다.(표 1 참조). H.235의 보안 서비스 구성은 RAS(Registration, Admission and Status), H.225(호 시그날링), H.245(미디어 제어 프로토콜), RTP(실시간 전송 프로토콜 RFC 1889)로 구성되어 진다. RAS 보안은 메시지에 대한 인증과 무결성을 보장하는 기능을 제공하며, 가입자 정보 기반의 패스워드 할당을 위한 키 관리를 한다. H.225 보안은 메시지에 대한 인증과 무결성을 보장하며, Diffie-Hellman의 키 생성을 이용하여 음성 채널 암호화에 이용되어질 키를 암호화하기 위해 키 관리를 한다. H.245에서는 음성 데이터의 암호화에 사용될 암호화 알고리즘의 단말 지원 여부(capability)를 교환한다.

H.323프로토콜은 Call Connection Channel, Call Control Channel 과 Media Channel의 세 가지 경우의 Channel개념을 생각해 볼 수 있다.

H.235에서의 Security 개념은 Call Connection Channel에서는 SSL/TLS이나 IPSec에 의해 Security를 보장받았다. Call Connection 상태에서 H.245 Call Control Channel에 의해 인증을 받는다. RTP와 관련된 security parameter 정보도 교환한다. 인증시 사용되는 방법으로는 대칭형 암호화 기반의 절차와 Subscription 기반의 (password, signature) 대칭, 비대칭 암호화 기술이 사용되며 Diffe-Hellman의 Key Exchange 기법이 제안되고 있다(표 1 참조). 물론 이외의 IPSec나 TLS를 이용한 방법도 가능하다. Media Channel에 대해서는 DES나 Triple DES, RC2를 이용하여 Security를 지원한다.

SIP에서 Authentication과 관련되어서는 Basic authentication, Digest authentication, Proxy authentication, PGP authentication 을 선택적으로 결정한다. 특히 IPSec을 이용한 End-to-End와 Hop-by-Hop Encryption을 모두 제공할 수 있다.

VoIP 프로토콜 보안은 보안의 적용 구간에 따라서 End-to-End 보안과 Hop-by-Hop 보안으로

표 1. H.235 Baseline Security profile

Security Services	Call Functions			
	RAS	H.225.0	H.245	RTP
Authentication and Integrity				
Confidentiality				56-bit DES / 56-bit RC2 / 168-bit Triple-DES
Key Management		authenticated Diffie-Hellman key-exchange	Integrated H.235 session key management (key distribution, key update using 56-bit DES/56-bit RC2-compatible/168-bit Triple-DES)	Voice Encryption Security Profile

구분한다.

- End-to-End 보안은 통신 사용자간의 단대단 보안을 제공하여 중간의 서버나 프락시의 동작에 필요한 정보들을 암호화하거나 MAC을 걸 수 없으므로 평문으로 남아 있다. IP주소나 사용자 ID 등 사적인 중요한 정보가 누출되므로 Hop-by-Hop 보안과 병행하여 사용한다. 단대단 보안은 사용자나 서비스 제공자에게 안전한 보안을 제공하므로 이를 추구하려고 하지만 이로 인한 많은 문제가 발생하여 구현이 매우 어렵다. 그러나 End-to-End로 사용자 인증 기능을 제공하는 것은 가능하며 실제로 H.235는 이에 대한 절차가 포함되어 있다.

- Hop-by-Hop 보안은 IP 패킷 전송시 각 링크상의 모든 트래픽을 통째로 암호화시켜준다. End-to-End path의 중간 매개 장비들에서 복호화 후 다시 암호화가 일어나므로 보안상 취약점이 될 수 있으나 헤더를 포함한 전체 패킷을 보호한다는 장점이 있다. IPSec이나 TLS가 사용되고 있지만, TLS는 TCP상에서만 동작하므로 제한사항이 있어 대부분 IPSec을 일반적인 솔루션으로 사용한다. Hop-by-Hop 보안에서도 IPSec의 사용을 권고하고 있다. IPSec은 키 관리 프로토콜인 ISAKMP/IKE가 지나치게 무거워 무선 단말과 같은 제한된 환경에서는 구현이 어렵다는 문제가 있으므로 키 관리 목적의 Kerberos 같은 기존의 인증 서버를 사용할 수 있다[6].

RTP/RTCP는 H.323이나 SIP, RTSP를 사용하는 VoIP 시스템에서 미디어 스트림의 전송을 위해 사용하는 프로토콜이다. IETF의 RTP/RTCP 표준 문서에서는 기본적으로 보안을 위해 IPSec과 같은 하위계층의 보안 인프라를 사용하는 것을 전제로 하고 이러한 보안 인프라가 일반화되기 전에 사용될 목적으로 자체 프로토콜에서 PEM방식의 변형으로 DES CBC로 암호화하는 방법을 제시하고 있다. 그러나 현재의 IPSec은 키관리나 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[13][14].

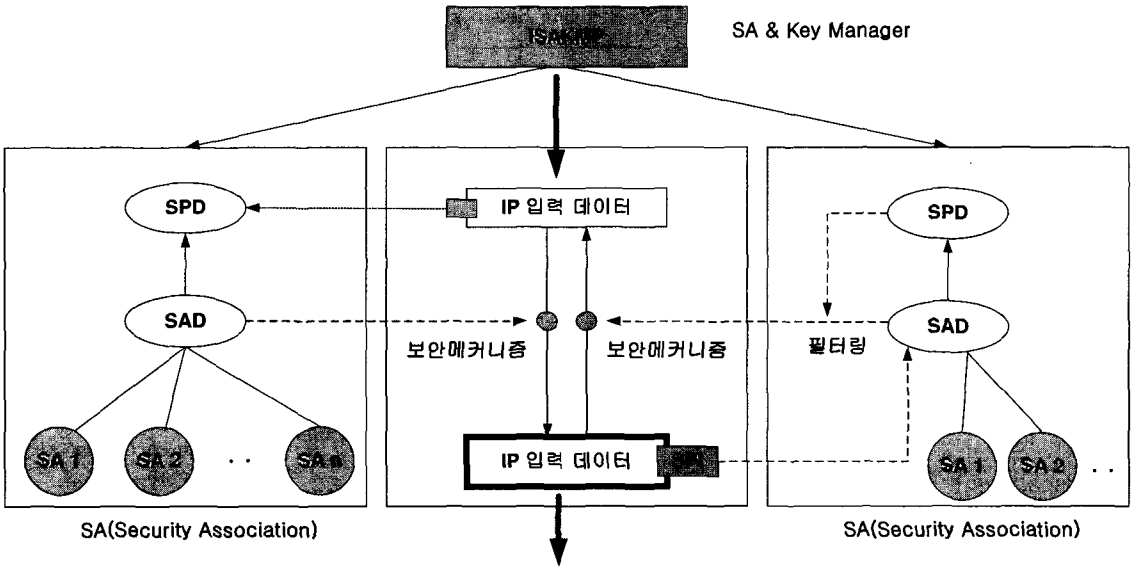


그림 4. IPSec에서의 패킷 처리 과정

표 2. H.235 : Signature security profile

Security Services	Call Functions			
	RAS	H.225.0	H.245	RTP
Authentication	SHA1 / MD5	SHA1 / MD5	SHA1 / MD5	
	digital signature (Procedure II)	digital signature (Procedure II)	digital signature (Procedure II)	
Non-Repudiation	SHA1 / MD5	SHA1 / MD5	SHA1 / MD5	
	digital signature (Procedure II)	digital signature (Procedure II)	digital signature (Procedure II)	
Integrity				
Confidentiality				
Key Management	certificate allocation	certificate allocation		

앞서 살펴 본 VoIP 프로토콜에서는 Firewall과 NAT를 통과하는 것은 VoIP 시스템 자체나 Firewall/NAT에서의 변경이 없이는 작동이 불가능하다[19]. 이러한 문제는 반드시 해결해야할 문제이므로 제 49차 IETF 회의에서 다양한 제안과 연구를 위해서 MIDCOM(Middlebox Communication)이라는 워킹그룹을 구성하였다(그림 5참조). MIDCOM에서는 네트워크에 방화벽이나 NAT등의 보안 장비가 설치되어 전달하는 패킷의 IP 주소나 포트가 변경될 때 통신이 원활히 수행되지 못하는 것을 해결하는 워킹 그룹이다. 실제 음성이 전달 될 때 주소나 포트를 사용하는 경우 NAT나 방화벽을 지나지 못하는 문제는 대단히 심각하다. 지금까지 방화벽이나 NAT의 문제를 해결하기 위해 제안된 세 가지 방법을 살펴보겠다.

첫 번째는 응용계층에서 프록시나 게이트웨이를 지원하는 것이다. 이러한 경우는 지나친 과부화로 인한 병목 현상이 발생할 수 있다. 프토토콜의 발전에 따라 끊임없이 업그레이드 시켜주어야 하므로 개발이나 관리적인 측면에서 Scalable한 접근 방법이 되지 못하는 단점이 있다. 두 번째는 방화벽을 Traversal하는 방법이다. 이 방법은 방화벽과 NAT 자체보다는 VoIP 단말과 VoIP 프록시 쪽에서의 변경을 통해 방화벽을 안전하게 통과하는 방법이다. 이 경우에는 SOCKS V5를 이용한다. SOCKS V5는 세션 계층의 프록시로 응용 프로토콜을 중계해 주고, UDP 통신의 제어를 위하여 별도의 TCP control channel을 이용한다. 이러한 멀티미디어 통신의 경우 scalability면에서 문제를 일으킬 수 있다.

세 번째는 외부 방화벽 제어 프로토콜을 사용하는

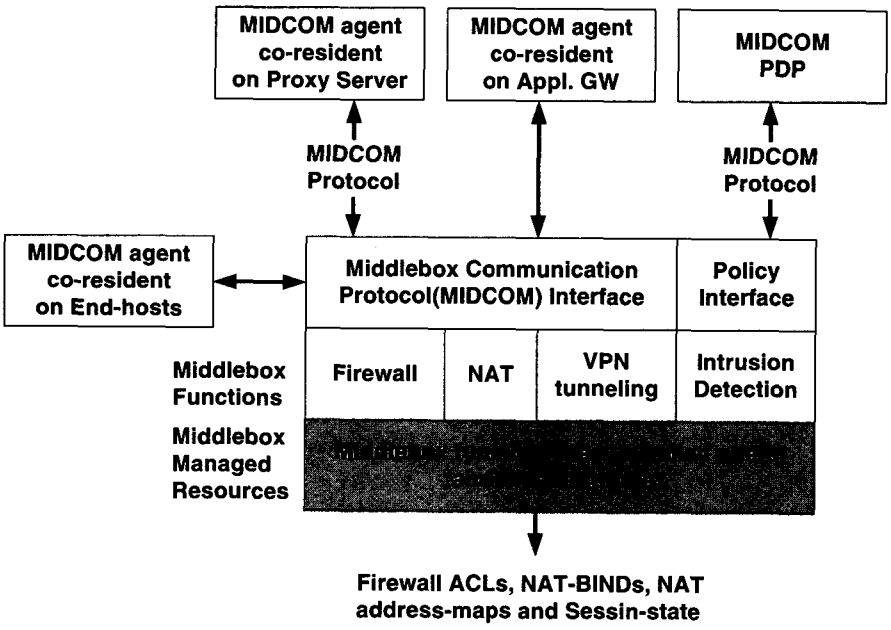


그림 5. MIDCOM Architecture

방법이다. 첫 번째의 방법의 문제점을 해결하기 위하여 응용 프록시/게이트웨이를 방화벽/NAT로부터 독립적으로 분리시킨다. 그리고 필요할 때마다 방화벽 제어 프로토콜을 사용하여 방화벽/NAT를 조정하여 필요한 포트를 열거나 닫도록 주소 바인딩을 생성, 소멸시켜 주어야 한다. 이는 외부에서 조절하므로 장기적으로 바람직한 방법이다. 이러한 시스템을 적용하기까지는 약간의 시간이 흘러야 할 것이다. 이를 좀더 확장시키거나 보완하기 위해 SOCKS v5나 RSVP(Resource Reservation Protocol)를 고려할 수 있다[6].

MIDCOM 워킹 그룹에서는 신뢰하는 제 3자로써 Middlebox를 통해 복잡한 응용을 가능하게 하는 구조를 제안하였다. 이 제안에서는 여러 가지 응용이 필요로 하는 기능과 그 기능들을 만족시키기 위한 NAT나 방화벽의 요구사항 등 기본적인 내용을 다루고 있으며 Middlebox 프로토콜이 사용되는 시나리오를 기술하였다. 최근에는 MIDCOM 이전이라도 신속히 NAT, 방화벽 등을 통과하여 VoIP 등의 peer-to-peer 응용이 가능한 pre-MIDCOM에 관한 연구가 활발히 이루어지고 있다[9].

5. VoIP 보안기술의 전망

H.235는 현재 VoIP을 위한 보안 요소들에 대하여 많은 부분들이 잘 정의 되어 있으며 인증서를 사용한 전자 서명으로 사용자의 인증과 부인 방지 기능 등을 제공한다. 또한 기존에 정의된 암호 알고리즘과 운영모드에 새로운 운영 모드와 알고리즘이 추가될 것으로 예상된다. 반면에 SIP에서는 현재 보안을 위한 추가적인 작업이 한창 진행 중으로 주로 시그널링 메시지의 암호화에 중점을 두어 연구하고 있으며 아직까지 음성 채널의 암호화를 위한 보안은 제공하지 못하고 있다. 물론 기존의 범용 보안 프로토콜을 이용하는 방안이 있지만 VoIP 프로그램과 범용 보안 프로토콜과의 인터페이스가 정의되어 있지 않아 접목이 그리 간단히 진행되지는 않을 것으로 예상된다. MIDCOM 워킹 그룹이 구성됨으로써 방화벽 및

NAT통과 문제 해결을 위한 근본적인 노력이 시작되었지만 VoIP 입장에서는 몇 년 후의 해결책 보다는 현재 빠르게 문제를 해결할 수 있는 방안이 필요한 형편이다. 따라서 현재 이런 문제들을 해결하기 위해 사용되는 방법을 정리하고 드래프트로 제안하여 토론함으로써 해결책을 찾는 작업이 진행 중이다. SIP에서 End-to-End와 Hop-by-Hop방식에 대한 논의는 Hop-by-Hop 방식으로 결론이 날 가능성이 높다. 왜냐하면 아직도 NGN의 구조가 명확하지 않을 뿐만 아니라 계속하여 진화가 진행되는 상황에서 End-to-End 방식은 그리 효율적이지 못하기 때문이다. 또한 어느 날 갑자기 모든 음성서비스가 패킷으로 전환되는 일은 일어나지 않을 것이다. 따라서 상당 기간 종래의 회선교환방식의 음성서비스와 패킷교환방식의 VoIP 서비스가 Access gateway나 Soft switch를 사용하여 상호 연동되어야 하므로 Hop-by-Hop방식의 보안체계가 유리하다고 할 수 있다.

VoIP는 NGN에서 음성서비스를 제공하는 기반기술이므로 NGN의 보안 메커니즘과 밀접하게 연관되어야 한다. NGN의 보안체계는 지금까지의 서비스별 개별적으로 운영하는 보안시스템이 아니라 통합적 상호운용방식으로 진화할 것이 명확하므로 이에 보조를 맞추어야할 필요가 있다.

6. 결론

지금까지 VoIP 의 보안에 관련된 사항들에 대하여 알아보았다. 차세대 VoIP 망을 설계하는데 있어 기존의 PSTN이 가지는 안정성에 맞추기 위해 점점 더 보안에 대한 요구는 증가하고 있다. 이에 따라 표준화 측면에서는 H.323, SIP, MGCP/MEGACO/H.248등 VoIP 관련된 프로토콜안에 보안 관련 내용을 제안하게 되었다. 하지만 구현 측면에서는 아직 IPSec과 같이 대중화되지 않은 부분도 있고 Public Key Certification을 위한 경제성 등도 논란이 될 수 있다. 또한 기존의 방화벽이나 NAT와 같은 네트워크 구성요소와의 부정합성도 문제가 되고 있지만, 많은 솔루션이 등장함으로써 곧 실용화되리라고 생각한다. 특히 VoIP는 NGN의 기반 기술이라는 점에서 NGN의 보안 체계와 밀접하게 연관될 것이다. NGN에서의 정보 보호 기술은 현재의 통신망 접속점에 위치한 시스템에 집중되는 보안 기술에서 노드와 노드간의 안전한 전송을 보장하는 통합적 상호 운용 방식으로 발전할 것이므로 VoIP의 보안문제도 이에 발맞추어 연구하고 발전시켜야 할 것이다.

참고문헌

[1] 정수환, "VoIP 시험 및 응용, VoIP 보안 기술", VoIP Forum, 2001.5.

[2] 정수환, "SIP Advanced Protocols, SIP Security", SIP 기반 차세대 VoIP 기술 워크샵 자료, 2001. 7

[3] 임채훈, "VoIP 시스템에서의 보안 기술", VoIP 네트워크솔루션 세미나 및 전시회 자료2000. 8

[4] 정수환, 홍기훈, 박성준, "VoIP 보안 기술", 한국통신학회지, 제 19권 제 2호, pp. 193-203, 2002. 2.

[5] 조원상, 김용건, " 차세대 VoIP망에 있어서의 Security 기술 고찰" 정보처리학회지 제 8권 제 2호, pp. 34-38, 2001. 3

[6] 임채훈, "VoIP 시스템에서의 보안 기술", 정보처리학회지 제 8권 제 2호, pp. 61-68, 2001. 3

[7] 장청룡, "NGN보안", 한국통신학회지 제 19권 제 6호, pp. 862-873, 2002, 6

[8] ETSI TIPHON. http://www.etsi.org/tiphon

[9] 김영한, "VoIP 표준화 동향", 한국통신학회지 제 19권 제 2호 pp. 123- 139, 2002, 2

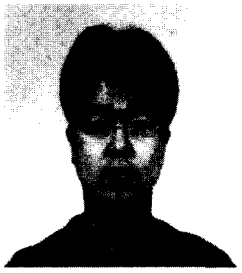
[10] ITU-T Standard Group 16 : H.323, http://www.itu.int/ITU-T/
[11] IETF Transport Area, http://www.ietf.org/
[12] IMTC, http://www.imtc.org
[13] R.Blom, E.Carrara and M.Naslund, "Conversational multimedia security in 3G networks", Internet Draft, IETF, Nov.2000. Work in progress.
[14] R.Blom, E.Carrara, D.McGrew, M.Naslund, K.Norrman and D.Oran, "The secure real time transport protocol", Internet Draft, IETF, Feb.2001. Work in progress.
[15] ITU-T, "Security and encryption for H-Series(H.323 and other H.245-based) multimedia terminals", H.235 v2, Nov. 2000.
[16] Internet Draft, "STUN-Simple Traversal fo UDP Through NATs" IETF MIDCOM WG., Oct. 2001.
[17] Internet Draft, "Traversal of Nonprotocol Aware Firewalls & NATs", IETF/ Firewall Traversal", IETF MIDCOM WG., Sept. 2001.
[18] Internet Draft, "Midcom-unaware NAT/Firewall Traversal", IETF MIDCOM WG, Sept. 2001.
[19] M. Holdrege and P. Srisuresh, "Protocol complications with the IP network address translator(NAT)", RFC 3027, IETF, Jan.2001.
[20] U.Roedig, R.Ackermann and R.Steinmetz, "Evaluating and improving firewalls for IP-telephony enviroments", Proc. of the 1st IP-Telephony Workshop(IPTel2000), April. 2000.
[21] J.Rosenberg and H.Schulzrinne, "SIP Traversal through residential and enterprise NATs and fireswalls", internet Draft, IETF, Mar. 2001.
[22] R.P.Swale, P.A.Mart and P.Sijben, "Requirements for the MIDCOM architecture and control language", Internet Draft, IETF, Feb. 2001.
[23] 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.
[24] ITU-T, "Call signaling protocols and media stream packetization for packet-base multimedia communication systems", H.225.0, 2000.
[25] ITU-T, "Control Protocol for Multimedia Communication", H.245, 2000.
[26] RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication", IETF, 1999
[27] 민재홍, 조평동, " VoIP 기술 동향", ITKP 주간 기술 동향, ETRI IT 정보센터, 2001. 11.07
[28] 김영한, 고석갑, "VoIP 기술 개요 및 표준화 동향", 정보처리학회지 제 8권 제 2호, pp. 10-21, 2001.3
[29] 인터넷 보안 : http://cnscenter.future.co.kr/menu/security.html
[30] Hot Topics : http://cnscenter.future.co.kr/menu/hot-topic.html
[31] IETF 보안 표준 관련 표준 문서 : http://cnscenter.future.co.kr/menu/ietf.html

이 근 호

1998년 2월 순천향대학교 전산학과(학사), 2001년 8월 순천향대학교 전자상거래학과(석사), 2001년~현재 고려대학교 컴퓨터학과 박사과정 〈관심분야〉 Network Security, VoIP, WLAN, NGN, Ad-Hoc

이 송 희

1998년 2월 순천향대학교 전산학과(학사), 2002년 2월 순천향대학교 전자상거래학과(석사), 2002년~현재 고려대학교 컴퓨터학과 박사과정 〈관심분야〉 VoIP, QoS, NGN, Ad-Hoc



김 정 범

2000년 2월 고려대학교 정보공학과(학사), 2002년 2월 고려대학교 컴퓨터학과(석사), 2002년~현재 고려대학교 컴퓨터학과 박사 과정 〈관심분야〉 IPSec, Ad-Hoc Network, WLAN

한 상 범

1997년 2월 서울산업대학교 전자계산학과(학사), 1999년 8월 고려대학교 컴퓨터학과(석사), 2001년~현재 고려대학교 컴퓨터학과 박사 과정 1981년~현재 KT 수도권강남본부 〈관심분야〉 VoIP, NGN, 차세대인터넷

김 태 윤

1981년 고려대학교 산업공학과 학사, 1983년 미국 Wayne State University 전산과학과 석사, 1987년 미국 Auburn University 전산과학과 박사, 1988년~현재 고려대학교 컴퓨터학과 교수 〈관심분야〉 전자상거래, 컴퓨터 네트워크, EDI, 이동통신, 멀티미디어 등