제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

차세대 통신망에서의 보안 기술에 관한 연구

이근호*, 이송희, 김정범, 김태윤
*고려대학교 컴퓨터학과
e-mail:root1004@korea.ac.kr

A Study on Security Technology in Next Generation Network

Keun-Ho Lee*, Song-Hee Yi, Jeong-Beom Kim, Tai-Yun Kim
*Dept of Computer Science and Engineering, Korea University

요 약

최근 인터넷 관련 기술이 급속하게 발전하고 있다. 과거의 단순한 데이터 서비스에서 음성, 화상 등의 다양한 멀티미디어 서비스를 제공하고 있다. 모든 미디어가 인터넷으로 수렴되는 NGN(Next Generation Network)으로 발전되어 가고 있다. 개방형 네트워크는 다양한 유무선 통합망의 융합화에 따른 통신망간의 간섭이 증가하고 네트워크 접속점 중심의 통신망간 접속구조가 확대되어 지금까지의 시스템 보안 위주의 단순한 보안 기술을 적용하기가 어려웠다. 따라서 네트워크 노드간을 효율적으로 보호하는 네트워크 중심의 보안 기술이 필요한 시점이다. 이에 본 논문은 진화망을 중심으로 하는 통신 산업의 유.무선 데이터 서비스 증가로 원래 데이터 서비스를 위하여 설계된 것에 다양한 데이터 응용 서비스의 하나로 전화 서비스를 수용할 수 있는 새로운 통신 인프라를 구축하여 통합하는 차세대 통신망에 대해서 살펴보고 차세대 통신망(NGN)에서의 보안기술을 연구한다..

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 차세대 통신망(NGN : Next Generation Network)으로 발전하고 있다. 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 유·무선 통신이 IP기반으로 통합되는 경우 비단 음성뿐만이 아니라 통신망이 제공하는 모든 서비스에 포함되는 필수적인 기술로 자리매김할 것이다.

데이터 통신을 위한 인프라 구축 비용이 기존의 음성 위주의 통신망의 그것에 비하여 가격이 저렴함에 따라 NGN의 도입이 더욱더 타당성을 갖게 된다.

NGN에서는 차세대 통신망을 위한 진행에 서비스 품질, 망관리, 망의 진화, 보안, 경제성등이 반드시 필요한 사항들이 고려되어야 한다[4].

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.

VoIP 시스템의 구성 요소는 응용 계층, 신호 계층, 매체 계층으로 나누어진다. 그림 2는 계층별로 상대

방과 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 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[6][7].

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[8]. 암호 기술을 이용한 보안 기술은 네트워크의 각 계층에서 사용되어 진다. 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 접속을 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.

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

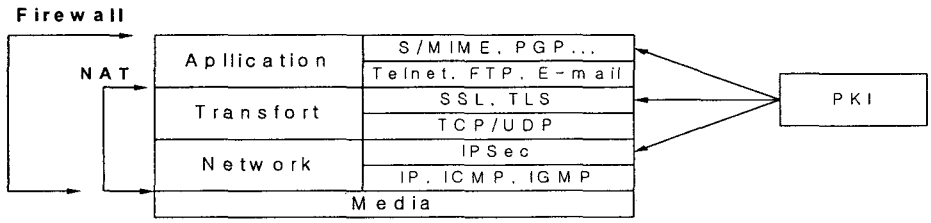

그림 1. 네트워크 계층별 보안 프로토콜

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. 차세대 통신망의 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. 두 번째는 VoIP 프로토콜 자체의 Security 메커니즘을 사용하는 것이다.

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. 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.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. 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 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 제공

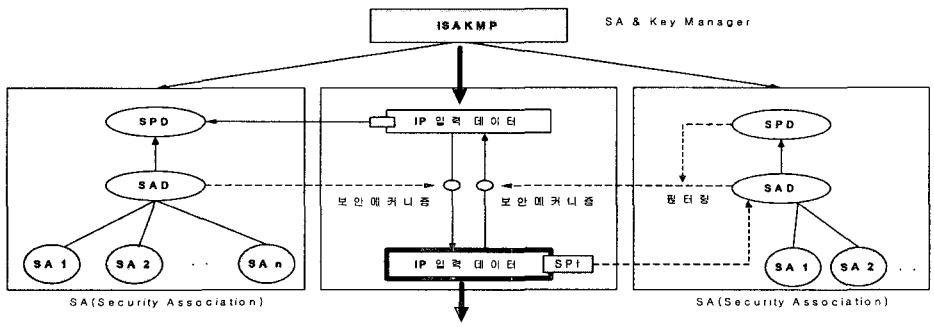

그림 4. IPSec에서의 패킷 처리 과정

자에게 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.

RTP/RTCP는 H.323이나 SIP, RTSP를 사용하는 VoIP 시스템에서 미디어 스트림의 전송을 위해 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 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.

방화벽이나 NAT의 문제를 해결하기 위해 제안된 세 가지 방법을 살펴보겠다.

첫 번째는 응용계층에서 프록시나 게이트웨이를 지원하는 것이다. 두 번째는 방화벽을 Traversal 하는 방법이다. 이 방법은 방화벽과 NAT 자체보다는 VoIP 단말과 VoIP 프록시 쪽에서의 변경을 통해 방화벽을 안전하게 통과하는 방법이다. 세 번째는 외부 방화벽 제어 프로토콜을 사용하는 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.

6. 결론

지금까지 차세대 통신망의 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] Christian Huitema, "Challenges of the Next Generation Networks", Keynote for Internet '99 Conference, Moscow, Oct. pp. 25-28

[2] T. Sweeney, "Next Generation Networks : The Future of Business", http://www.alcatel.com/newslink/0102/cover.htm, Alcatel Newslink 2nd Quarter 2001.

[3] NGN SG, "Conclusion from the NGN-SG", ETSI 38th General Assembly Meeting, Nov. 2001

[4] 장청룡, "NGN 보안", 한국통신학회지 제 19권 제 6호, pp 862-873. 2002. 6.

[5] 이근호, 이송희, 김정범, 김태윤, "VoIP를 위한 보안 기술 현황과 전망", 한국통신학회지 제 19권 제 8호, pp 1217-1229, 2002, 8

[6] 민재홍, 조평동, " VoIP 기술 동향", ITKP 주간 기술 동향, ETRI IT 정보센터, 2001. 11. 07

[7] 김영한, 고석갑, "VoIP 기술 개요 및 표준화 동향", 정보처리학회지 제 8권 제 2호, pp. 10-21, 2001.3

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