情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

IETF IPSEC 관련 그룹 및 MSEC 그룹 표준화 동향

홍 기 훈*, 정 수 환*, 이 계 상**

요 약

본고에서는 IETF IPSEC WG과 IPSEC 프로토콜 관련 표준화 작업을 위해 최근 결성되어 관심을 모으고 활발히 활동을 시작한 MOBIKE WG 및 PKI4IPSEC WG의 표준화 활동을 소개하고 간략히 요약한다. 또한 멀티캐스트 보안 표준화 작업을 수행하는 MSEC WG의 활동을 소개하고 현재 진행 사항과 최근의 표준화 작업의 내용과 기술 동향을 기술한다.

Ⅰ. 서 론

인터넷의 대중화와 고속화로 인터넷을 이용한 서비스가 급속히 다양화되고 많은 매체를 이용하게 되었는데, 특히, 영상이나 음성의 전달이 주류를 이루게 되었으며 이러한 서비스는 많은 트래픽을 발생시켜 네트워크 자원을 소모한다. 따라서 이러한 서비스의 기반 기술로 등장한 프로토콜이 멀티캐스트이며, 멀티캐스트는 일대일 연결을 이용한 유니캐스트와 달리 일 대 다의 통신을 기반으로 하기 때문에 패킷이 복사되어 분산된다. 이렇게 패킷이 분산되는 멀티캐스트 환경은 특히, 보안에 취약하고 공격자의 악의적인 공격이 다수에게 영향을 미칠 수 있다. 그러나 인터넷 방송이나 다자간 회의 시스템과 같이 멀티캐스트 기반의 서비스가 증가하고 있어 보안을 이용한 서비스의 관리가 절실히 요구되고 있다. 몇 년 전까지 멀티캐스트 보안이 주로 학계에서 연구되어 왔지만 표준의 필요성이 대두됨으로서 국제 표준화 단체에서도 표준화를 시작하여 관련 작업을 수행하고 있다.

IPSEC 프로토콜은 대표적인 인터넷 보안 프로토콜로, 널리 잘 알려져 있다. 대부분의 인터넷 보안 프로토콜은 응용 계층에서 동작되므로, 그 응용 데이터에 국한하여 보안 서비스를 제공하는데 비해, IPSEC 프로토콜은 네트워크 계층인 IP 계층에서 동작되는 프로토콜로서, 소스 인증, 무결성, 기밀성과 같은 보안 서비스를 개개의 IP 패킷에 대해 제공함으로, 모든 응용에 트랜스패런트하게 공통으로 적용될 수 있다. IPSEC 프로토콜은 원래 개별 호스트와 호스트간 보안 통신, 클라이언트-서버 간 보안 통신, 및 안전한 VPN (Virtual Private Network)의 구축 등 여러 시나리오에 적용될 목적으로 고안되었으나, 표준화의 지연으로 그 활용 범위가 VPN 구축 정도에 국한되어 왔다. 하지만, 최근 표준화의 진척으로 보안에 민감한 인터넷 정보 교환의 여러 분야 (예, 모바일 IP 보안, 모바일 네트워크 보안, IP 저장 장치 네트워크 보안 등)에서 그 적용이 늘어나고 있다. 또한 IPSEC은 기본적인 보안 구조와 암호알고리즘을 포함하고 있으므로 멀티캐스트 보안 기술의 적용 기술로 논의되고 있다. 따라서 본고에서는 MSEC과 IPSEC 관련 기술의 표준화를 알아 보고자 한다.

본고의 구성은 다음과 같다. II장에서는 IPSEC 워킹 그룹과 IPSEC 관련 그룹인 MOBIKE와 PKI4IPSEC 워킹 그룹의 표준화 동향을 살펴본다. III장에서는 MSEC 워킹 그룹의 표준화 동향을 살펴보고 마지막으로 IV장에서는 IPSEC 관련 그룹과 MSEC 워킹 그룹의 표준화 전망에 대해 언급한다.

Ⅱ. IPSEC 관련 그룹의 표준화 동향

IPSEC 프로토콜은 IETF의 Security Area (보

* 숭실대학교 정보통신전자공학부 ({kihun, souhwanj}@ssu.ac.kr)
** 동의대학교 정보통신공학과 (ksl@dongeui.ac.kr)

안 분야) 중 IPSEC 워킹그룹을 중심으로 그동안 표준화 되어 왔다. 다음 절에서, IPSEC 프로토콜 표준화를 시작한 IPSEC WG과, IPSEC 프로토콜 관련한 부대 표준화 작업을 위해 최근 결성되어 관심을 모으고 활발히 활동을 시작한 MOBIKE WG 및 PKI4IPSEC WG의 표준화 활동을 간략히 요약한다.

기타, IPSEC 프로토콜 관련 WG으로 IPSEC 정책 이슈를 다루는 IPSP WG[1]을 들 수 있으나, 이 WG은 그동안 정책 정보 모델과 정책 프로토콜 요구사항 RFC 문서를 발간한 정도이며, 시장 상황에 비해 매우 뒤쳐진 표준화 진척으로 회의를 거의 갖지 않고 있으며 메일 리스팅에서도 그 활동이 매우 저조하다.

1. IPSEC 워킹 그룹

IPSEC WG (IP Security WG)은 1993년 발족되어, 1998년 11월, IPSEC 프로토콜 표준화를 일단락 하였다. 현재, IPSEC 아키텍쳐, AH (Authentication Header) 프로토콜, ESP (Encapsulating Security Payload) 프로토콜, IKE (Internet Key Exchange) 프로토콜 그리고 다양한 암호 알고리즘 등을 규정한 26 여개의 RFC 표준문서가 발간되어 있다[2].

최근에는 이들 프로토콜에 부수되는 확장 문서들과 관리 측면의 문서 작업, 그리고 AES 알고리즘을 수용하기 위한 표준화 작업 등이 진행되어 왔다. 이 중 최근 가장 주목을 받아 왔던 표준화 작업은, 키관리 (IKE) 프로토콜의 버전업 작업이다. IKE 프로토콜은 대규모 IPSEC 시스템의 구축시 그 확장성을 위해 반드시 필요한 IPSEC 핵심 프로토콜의 하나로, 대칭키 암호 알고리즘을 기반으로 한 AH와 ESP 프로토콜의 동작에 필요한 키를 사람의 손을 거치지 않고 자동으로 제공해 주는 기능을 담당한다.

98년 11월 표준화 된 IKE 표준안 (IKEv1)은 너무 복잡하여 그동안 서로 다른 구현 제품간의 상호연동성이 제대로 확보되지 못해 왔다. 이는 멀티벤더 제품을 사용한 VPN의 구축을 방해하여 왔다. 게다가 IKEv1이 표준화 되고 난 후, 인터넷 보안 및 사용환경이 대폭 변화하였다. 서비스 거부 공격 (DoS)의 빈발, 원격 사용자 접속 이용의 증가 및 NAT (Network Address Translation) 장치의 사용 증가 등을 들 수 있다. IKEv1은 설계시 이러한 요구사항이 적절히 고려되지 않았다.

이에 따라, 네트워크 환경의 변화에 대응하고, 프로토콜의 복잡성을 해결하기 위해 IKEv2의 개발이 2001년 8월에 시작되어 최근 까지 진행되어 왔으며, 2003년 11월 IETF 미니애폴리스 회의 직전 마무리되어, 곧 RFC 초안으로 발간될 예정이다. 다음에 IKEv2 프로토콜의 특징을 간략히 살펴 본다[3].

IKEv2 프로토콜은 11월 회의 직전 워킹 그룹 차원의 last call을 통과하여, 현재 IETF의 IESG에 표준 초안으로 상정되어 있다. IKEv2는 기존 RFC 2409 IKEv1 프로토콜의 설계 개념을 계승하고 있지만, 그 기능은 훨씬 축약되어 설계되었다. 즉, 기존 IKE 프로토콜의 페이스 개념을 계승하고 있고 동일한 ISAKMP 메시지 포맷을 사용하고 있지만, 기본적으로 페이스 I에서 교환되어야 하는 기본 메시지 개수가 6개에서 4개로 줄어들었고 인증 방식도 기존의 4가지 방식에서 2 가지 방식 (공개키 방식과 사전공유 비밀키 방식)으로 줄었고, 기존 표준이 여러 문서에 나뉘어 기술되었던 것에 비해 IKEv2는 하나의 문서에 통합 기술되고 있다.

IKEv2는 또한 DoS 공격에 잘 견디도록 설계되었다. DoS 공격은 주로 응답자의 메모리 자원을 고갈시키기 위해 공격자가 IKE SA 요청 메시지를 대량 송신할 때 발생한다. IKEv2는 이 때 응답자로 하여금 상태 정보 저장에 필요한 메모리를 할당하게 하는 대신 쿠키로 응답하게 하고 이 쿠키에 정상적으로 반응할 수 있는 선의의 개시자에 대하여만 자원을 할당하는 방식을 규정하고 있다. DoS 공격은 기존 IKE 프로토콜이 제정된 1998년 이 후 심각하게 대두된 보안 공격으로 기존 IKE 프로토콜에는 이에 대한 대응책이 미비되어 있었다.

또한, IKEv2는 원격 접속의 경우 (예, VPN 클라이언트가 자사 VPN에 원격 접속하는 경우), 사용자 인증과 원격 호스트 설정을 위한 메커니즘을 포함하고 있다. 원격 접속 또한 기존 IKE 프로토콜이 제정된 이 후 급증하게 된 요구사항으로 기존 IKE 프로토콜에서는 고려되지 않았던 이슈였다. 특히, 원격 사용자 인증에 있어서는 공개키 방식이 아닌 현재 널리 사용되고 있는 여러 기존 인증 방식도 사용될 수 있도록 IKEv2의 메시지 교환이 확장될 수 있다. 아울러, 원격지의 클라이언트를 VPN 내부에 존재하는 것 처럼 보이도록 하여 보안을 강화할 수 있도록, 원격 호스트의 네트워크 변수 (IP 주소, 마스크 등)를 VPN 내부 서브넷의 환경으로 설정해 주는 메커니즘도 IKEv2에 포함되어 있다.

IKEv2는 또한 최근 많이 사용되고 있는 NAT 장비와도 잘 호환하여 동작하도록 고려되어 설계되었다. 즉, IKE 통신 양단 간에 NAT이 존재하는 경우 이를 트랜스패런트하게 통과하여 IPSEC 통신이 일어나도록, 모든 IKE 메시지와 IPSEC 패킷을 UDP 캡슐화하는 메커니즘이 포함되어 있다. NAT 장비는 주로 IPSEC 호스트와 호스트 간 통신에서나, 위에서 언급한 원격 접속의 경우 원격 호스트 쪽에 위치할 수 있다.

IKEv2 표준 작업이 마무리 되면서, 2003년 11월 미니애폴리스 회의에서는 나머지 작은 보완 작업들을 논의하였고, 2004년 서울에서는 회의를 갖지 않았다.

IPSEC WG은 IKEv2 표준안 발간과 그에 관련된 아키텍쳐 (RFC 2401 bis) 및 AH/ ESP 표준 문서의 보완 작업이 곧 마무리되는 대로 소기의 목적을 달성하고 종료될 전망이다.

2. MOBIKE 워킹 그룹

IP 단말기의 이동성 (mobility)을 향상시키기 위해 로우밍 (roaming) 기능이 추가되는 경우, 통신 도중 IP 주소의 변경이 허용된다. 이는, 좀 더 범위를 좁혀, IPSEC 통신의 경우, 하나의 IKE (또는 IPSEC) SA 통신 중, 로우밍으로 인한 주소 변경이 새로운 SA의 생성이나 rekeying을 유발시키지 않고 SA 통신이 지속될 수 있어야 함을 의미한다.

한편, 두 개 이상의 네트워크 인터페이스를 갖는 라우터의 경우, 하나의 IKE 또는 IPSEC SA가 각 인터페이스에 부여되는 IP 주소를 모두 수용해야할 필요가 있다. 이 점은 무선 LAN 인터페이스와 GPRS 인터페이스를 모두 갖고 있는 IP 이동 단말기의 경우에서도 마찬가지이다.

최근 IPSEC WG의 IKEv2 논의 과정 중, 위와 같은 통신 중 IP 주소의 변경이나 복수 IP 주소의 지원이 IKEv2의 기능으로 추가되어야 한다는 주장이 제기되어 왔다. IPSEC WG에서는 일단 기본 IKEv2 표준의 조기 발간을 최우선 목표로 하였기 때문에, 이 논의를 별도의 새로운 WG에서 다루기로 하여, MOBIKE WG이 탄생되었다.

MOBIKE WG (IKEv2 Mobility and Multihoming WG)[4]은 2003년 11월 미니애폴리스 회의에서 워킹그룹 발족을 위한 첫 BOF 모임을 갖고 2004년 2월 정식 WG으로 발족하였다.

2003년 11월 BOF 회의에서는, 향후 생성될 워킹그룹의 목표와 임무가 논의 되었다. 주소가 변경되는 구체적인 시나리오로, 느린 속도와 사용자 상호작용이 요구되어 기존 SA들을 다시 생성하기가 어려운 로우밍 시나리오가 제시되었다. 한편, 가용도를 높이기 위해 여러 개의 인터페이스를 갖는 라우터의 경우와, GPRS와 무선 LAN 인터페이스를 동시에 갖는 PDA의 경우와 같은 멀티플 인터페이스 시나리오도 제시되었다. 아울러, 현 IKEv2와 MobileIP 프로토콜간의 비호환성 해결 방법도 이 워킹그룹의 임무로 포함되었다.

2004년 3월 서울서 가진 첫 WG 회의에서는 MOBIKE 프로토콜 안이 논의되었다. Dupont (ENST Bretagne)[5]과 Kivinen (SafeNet, WG 공동의장)[6]의 두개 안이 제안되어 발표 되었으며, 프로토콜 설계시 고려 사항[7]이 발표 되었고 이들에 대한 참석자들의 반응이 조사되었다. 이 문서들은 아직 개인 문서로 향후 조정을 거쳐 WG 문서로 발전될 전망이다. MOBIKE 프로토콜은 새로운 IKE SA의 생성이나 rekeying을 하지 않고, SA내의 IP 주소의 변경이나 추가를 담당하는 프로토콜로, 변경 추가된 주소에 대한 인증, 갱신 기능을 담당하여 IKEv2를 보조할 것이다.

3. PKI4IPSEC 워킹 그룹

IPSEC 프로토콜 표준안이 1998년 11월 제정된지 5년이 넘게 경과되었지만, 아직도 IPSEC 표준에서 규정된 X.509 인증서의 사용이 IPSEC 시스템에서 거의 구축되지 않고 있다. 이는 두 가지 요인에 기인한다. 하나는 X.509 인증서가 IPSEC 시스템에서 사용될 경우, 그 사용법에 대한 명확한 표준 규격이 없는 것이고, 또 다른 요인은 IPSEC 시스템과 공개키 기반 (PKI) 시스템과의 연동에 대한 명확하고 간결하며 확장성 있는 연동 표준 규격이 결여되어 있는 것이다.

PKI4IPSEC WG (Profiling Use of PKI in IPSEC WG)[8]은 이러한 규격 표준의 결여를 메꾸기 위해 2003년 11월 미니애폴리스 회의에서 첫 BOF 회의를 갖고 2004년 1월 정식 워킹그룹으로 발족되어 2004년 3월 서울에서 첫 워킹그룹 회의를 갖게 되었다.

이 WG은 두 가지 문서의 조속한 발간을 단기 목표로 하고 있다. 하나는 표준 문서로 발간을 목표로 하는데, IPSEC 시스템에서 X.509 인증서가 사용될

때 인증서의 각 필드의 사용 값들을 IPSEC 시스템에 맞게 결정 (프로파일링)하는 것이다. 표준화될 인증서 프로파일은 IKEv1과 IKEv2에서의 사용이 모두 고려될 것이다. 또 하나의 문서는 표준 트랙을 밟지 않을 정보 문서로 발간될 예정으로, IPSEC 시스템이 PKI 시스템과 연동시 인증서 요청과 추출, 및 인증서 관리에 필요한 프로토콜 프로파일 작성을 위한 요구사항을 담게 될 것이다. 이 문서가 완성되고 나면, CMS (RFC 2797) 프로토콜의 인증서 관리 메시지의 내용에 대한 프로파일 표준 문서 작업이 계속될 계획이다.

이 WG의 이러한 인증서 및 인증서 관리 메시지의 프로파일링 표준화 작업은 대규모로 구축되는 IPSEC 시스템에서의 사용을 전제로 하고 있다. 예를 들어, 대기업에 구축된 IPSEC 시스템에서, 게이트웨이와 게이트웨이 간 IPSEC 통신과, 원격 IPSEC 단말기와 게이트웨이 간 IPSEC 통신이 우선적으로 고려될 것이다.

2004년 서울 회의에서는 위에서 언급한 WG의 단기 목표 달성을 위한 요구사항 문서가 발표되어 논의되었다. Chris Bonatti는 인증서 관리 프로파일링을 위한 요구사항 문서[9]를 발표하였고, Paul Hoffman은 IPSEC 워킹그룹에서 기고되었던 요구사항 문서[10]을 소개하였으며, 이어서 이들 문서에 대한 WG 문서로의 승격이 논의되었다.

Ⅲ. MSEC 워킹 그룹의 표준화 동향

멀티캐스트는 송신자가 많은 수신자에게 동일한 패킷을 전송하는 서비스를 지원하기 위한 프로토콜로서 네트워크의 과부하를 고려하여 송신측에서 하나의 패킷을 전송하면 가입한 수신자에게로 패킷이 복사되어 전달된다. 그러나 이러한 정보가 보안이 요구되는 중요한 정보일 경우, 엄격한 보안 관리가 요구되며 이를 충족하기 위해서는 멀티캐스트 보안이 필요하다. 그러나 멀티캐스트에서의 보안은 많은 사용자들의 키를 관리하고 사용자의 가입과 탈퇴 시에 키의 분배와 키의 업데이트 과정이 수행되어야 하므로 보안 구조와 키 관리 메커니즘에 따라 많은 계산 과정이 수행되어야 한다. 또한 패킷 및 송신자의 인증은 허가되지 않은 사용자가 패킷을 생성하여 그룹 구성원들에게 보내거나 혹은 패킷을 변조하여 멀티캐스트 환경에서 오류를 발생하도록 하는 문제를 막기 위한 방법으로 이는 안전한 서비스를 제공하며 오류 없는 지속적인 서비스를 보장한다. 이러한 연구는 IRTF(Internet Research Task Force)의 GSEC(Group Security)에서 먼저 연구가 시작되었으며 그룹 통신 환경에서 보안 요구 사항과 보안 기반에 관한 연구가 수행되었다. 이 연구를 기반으로 2000년에 IETF에서 MSEC (Multicast Security) WG을 구성하여 멀티캐스트 환경에서 그룹 통신 데이터의 기밀성과 메시지 인증, 송신자 인증 등에 대한 프로토콜 정의와 같이 실제적인 표준화 작업을 수행하고 있다[11].

1. MSEC 기술 개요

IETF MSEC WG에서는 IRTF GSEC 연구 그룹에서 연구된 문서를 기반으로 표준화를 진행하고 있으며 초기에는 기본적인 보안 요구 사항과 관련 분야에 관한 범위, 그룹 키 관리 프로토콜 등을 정의하였으나 최근에는 멀티캐스트 프로토콜과 IPSEC, SRTP 등 보안 및 전송 프로토콜 등에 멀티캐스트 보안을 위한 필드의 제안 등 적용 방안이 연구되고 있다.

개발되고 있는 표준은 각각의 그룹이 하나의 신뢰하는 개체(Group Controller)를 가지고 그 개체가 그룹 구성원의 보안 정책과 보안 관리를 담당하도록 구성되어 있다. MSEC의 표준은 적어도 다음과 같은 보안 사항을 지원하도록 하고 있다.

- 그룹 구성원만이 현재의 그룹 통신에 참여할 수 있으며 이 그룹은 가변적인 구성원을 가진다.
- 그룹 구성원은 송신자와 송신자가 보내는 데이터를 인증할 수 있다.
- 추가적으로 DoS(Denial of Service) 공격에 대한 방어가 가능하다.

MSEC WG는 기능별 개발 블록을 구성하고 있으며 이 개발 블록은 하나 혹은 여러 개의 프로토콜로 표현될 수 있다. 이러한 기능별 개발 블록과 프로토콜들은 IRTF의 SMUG (Secure Multicast) Research 그룹에 의해 개발되어져 왔으며 IETF MSEC 워킹 그룹에서는 이를 기반으로 표준을 제정하고 있다. 다음의 기능적 개발 블록들은 표준의 기반으로 사용될 것이다.

- 개발 블록 1 : 데이터 보안

그룹과 소스의 인증 그리고 그룹내의 보안 등을 제공하며 참여하고 있는 구성원들은 필요한 암호 키를

모두 가지고 있어야 한다. IP 계층과 트랜스포트 그리고 어플리케이션 계층의 보안 서비스를 모두 지원해야 한다.

- 개발 블록 2 : 그룹 키 관리 및 그룹 보안 협상

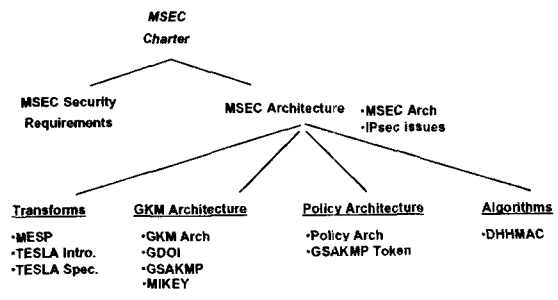
그룹 멤버는 개발 블록 1에서 필요한 보안키를 모두 가지고 있어야 하며 이러한 키의 안전한 생성과 분배 그리고 안전한 업데이트가 필요하다.

- 개발 블록 3 : 그룹 보안 정책 관리

그룹 보안 정책을 결정하고 개발 블록 1과 2를 관리한다.

2. MSEC 표준화 현황

MSEC은 IRTF의 GSEC과 Reliable Multicast(RMRG), Multicast Transport (RMT), IP Security(IPSEC), Policy 등 많은 IETF의 워킹 그룹과 함께 표준화를 진행하고 있다. 다음 그림 1은 MSEC의 구성도로서 데이터의 암호화와 그룹 키 관리, 보안 정책 그리고 암호 알고리즘 등으로 구성되어 있다. MSEC은 우선 보안 고려 사항을 정의하고 이에 적합한 보안 구조를 모색하여 그림과 같이 데이터의 변환과 그룹 키 관리 구조, 정책 구조 그리고 인증을 위한 알고리즘 등으로 세분화하고 각각의 연구를 수행하고 있다. 데이터 변환은 MESP(Multicast Framework for the IPSEC ESP)와 TESLA를 통한 멀티캐스트 패킷의 암호화나 인증 데이터의 생성을 의미한다. GKM (Group Key Management)은 RFC 3547 GDOI(Group DOI)에 정의되어 있으며 GKM Arch(Group Key Management Architecture)와 GSAKMP (Group Secure Association Key Management Protocol) 그리고 MIKEY(Multimedia Internet KEYing)로 구성되어 논의되고 있다. 정책 구조의 토



〔그림 1〕 MSEC 워킹 그룹의 표준화 구성과 현황

큰은 접근 토큰(Access token)에 대하여 정의하고 있고 인증이나 키 관리를 위해 DHHMAC(HMAC-authenticated Diffie-Hellman for MIKEY)가 논의되고 있다.

MSEC Architecture에서는 대규모의 멀티캐스트 그룹에서 안전한 데이터 전송을 위한 MSEC 구조에 대한 연구와 IP 보안 전송 기반으로 고려되는 IPSEC 멀티캐스트 지원에 관한 고려 사항들이 IPSEC 워킹 그룹간에 논의되고 있다[12].

그룹 키 관리 구조는 멀티캐스트 보안에서 핵심 부분으로 송신자와 수신자간의 키를 분배하고 보안 협상과 보안 정책에 따라 그룹의 키를 관리하게 된다[13~15]. 송신자와 수신자들 간의 일 대 다 혹은 다 대 다 보안 통신을 위해 키를 분배하며 설계 구조에 따라 집중형과 분산형으로 나뉠 수 있다. 집중형의 GKM (Group Key Management)은 보안 정책에 따라 하나의 GKM이 송신자와 수신자들의 키를 관리하지만 분산형의 경우 다른 여러 보안 정책과 다른 GKM에 의해 송신자와 수신자들간의 보안 협상과 키 분배가 이루어진다. 멀티캐스트 키 관리 요구 사항은 아래와 같다.

- 그룹 멤버는 암호키와 인증 및 무결성을 위한 키 그리고 보안 정책을 포함하는 보안 협상(SA)을 수신하여야 한다.
- 키는 미리 결정된 사용 기간을 가져야 하며 주기적으로 업데이트 되어야 한다.
- 키는 안전하게 그룹의 멤버들에게 전달되어야 한다.
- 키 관리 프로토콜은 공격에 대해 안전하여야 하며 그룹 멤버의 가입과 탈퇴시 가입한 멤버는 가입이전의 내용을 알 수 없어야 하며 탈퇴 후에는 이후의 내용을 알 수 없어야 한다.
- 프로토콜은 그룹 멤버와 그룹 제어자간에 유니캐스트 연결 없이 전체 그룹의 키 업데이트 작업을 수행하여야 한다.
- 프로토콜은 IPSEC 이나 어플리케이션 보안과 같은 데이터 보안 프로토콜 구조와 호환이 가능하여야 한다.
- 키 관리 프로토콜은 인증 시스템과 권한 제어 등의 전체 구조를 제공하여야 한다.

그룹 보안의 전체 형태는 중간에 그룹 키 관리(GKM)부분이 위치하고 있으며 그룹 보안 협상은 크

게 세 가지로 구분된다. 우선, 송신자와 수신자간의 데이터를 보호하기 위한 데이터 보안 프로토콜(Data Security Protocol)의 보안 협상(Security Protocol SA)이 있다. 두 번째 SA는 Re-key 보안 협상(Re-key SA)으로 선택적이며 키 관리 프로토콜에 의해 생성된다. KEK (Key-encrypting Key)와 TEK (Traffic -encrypting Key)를 포함한 모든 키는 Registration 프로토콜에 의해 교환될 수 있으며 키의 업데이트가 반드시 필요하지는 않으므로 Re-key 메시지는 선택적이다. 그룹 멤버들과 GCKS (Group Controller/Key Server)의 사이의 Registration 프로토콜은 제 3의 인증기관에 의해 보호되며 이 것을 Registration 프로토콜 보안 협상(SA)라 한다. De-Registration 프로토콜은 선택 사항이며 명시적인 연결 해제나 전화 혹은 컨퍼런스의 호 해제 등에 사용된다. 이렇게 세 개의 SA들이 그룹 Security Association을 구성한다. MIKEY는 실시간 멀티미디어 응용을 위하여 그룹 통신에서의 안전한 키 관리를 제안하고 있다[16].

MESP에서는 ESP를 사용하여 메시지의 송신자 인증을 위한 프레임워크를 정의하고 그룹 인증과 소스 인증 변환형태가 정의되어 있으며 MESP는 소스 인증을 위해 전자 서명과 TESLA 및 기타 소스 인증 방법들을 수용할 수 있도록 하고 있다. TESLA는 멀티캐스트를 위한 데이터 인증 메커니즘으로 하나의 소스에서 많은 수신자에게 보내는 데이터를 송신자와 함께 인증한다. TESLA는 지연 키 노출 인증 방법으로 패킷의 손실에 영향을 받지 않으며 각각의 데이터 패킷을 인증하고 송신자와 수신자 모두 낮은 오버헤드를 가진다.

DHHMAC은 MIKEY를 위한 일대일 키 관리 프로토콜을 정의하고 있는데 특히 Diffie-Hellman 키 공유 프로토콜과 상호 인증과 메시지 무결성을 위해 키를 이용한 해시 방법을 사용하고 있다[17].

최근에 새롭게 인터넷 드래프트로 올라온 송신자 인증에 관한 2개의 문서가 있다. 이 문서들은 멀티캐스트 환경에서 보내진 패킷의 송신자를 확인하여 인증하는 송신자 인증에 관한 문서로서 송신측에서 보내진 패킷이 복사되어 수 많은 수신자에게 전달되는 멀티캐스트의 특성을 이용하여 변조된 공격 패킷을 이용하여 거짓 정보를 많은 멀티캐스트 사용자들에게 보내는 공격을 막기 위한 것이다.

패킷의 송신자를 인증하기 위해 제안된 방법중에 하나는 전자 서명과 수정된 IPSEC ESP, AH를 이용하는 방법으로 패킷들이 전자 서명에 의해 송신자를 인증 받으며 ESP와 AH에 의해 전달된다[18]. 전자서명 알고리즘은 RSA를 사용하며 공개키는 그룹키 관리시스템의 키 다운로드 정책의 일부로서 전달될 수 있다. 이 방법은 각 패킷 수신후 전자 서명 확인 과정의 과부하에 의해 DoS(Denial of Service) 공격에 대한 취약성을 가지게 되는데 이 경우, ESP나 AH의 MAC과 패킷 순서 번호 확인 과정을 통해 확인된 패킷만 서명 확인을 하게 되므로 취약성을 줄일 수 있다. 그러나 이러한 방법은 가능하지만 수신측 시스템의 성능에 따라 사용에 어려움이 있을 수 있다.

제안된 또 다른 송신자 인증 방법은 TESLA (Timed Efficient Stream Loss-tolerant Authentication)를 이용한 방법으로 TESLA는 기존 인터넷 드래프트에 의해 패킷의 송신자 인증 방법으로 제안되었으며 멀티캐스트 네트워크가 주로 멀티미디어 패킷 전송에 사용되는 점을 감안하여 RTP 패킷에 암호화를 통해 페이로드를 보호하는 RFC 3711 SRTP(Secure Real-time Transport Protocol)에 TESLA를 포함하여 제안하고 있다[19]. 이 드래프트에서는 SRTP와 SRTCP (Secure RTP Control Protocol) 패킷 헤더에 Key ID, Disclosed Key, TESLA MAC 등의 필드를 정의하고 있다. TESLA는 지연 인증 방법을 사용하고 있기 때문에 수신측에서 버퍼링이 요구되며 많은 패킷을 동원한 DoS 공격에 취약점을 가질 수 있다. 따라서 여기에서는 DoS 공격에 대한 방어책으로 작은 크기의 SRTP MAC 사용을 언급하고 있다.

Ⅳ. 전 망

IPSEC 프로토콜 표준화 작업이 마무리 됨으로써, 그동안 10여년에 걸친 IPSEC 워킹그룹의 임무가 성취되고, 그 결과물인 IPSEC 프로토콜의 사용이 확산될 전망이다. 또한, IPSEC의 적용을 여러 분야에 확산시키기 위한 새로운 워킹그룹들이 결성되었으며, 특히, 모바일 분야 등에 IPSEC 프로토콜의 적용이 확산될 전망이다.

우선, IPSEC 프로토콜의 핵심 프로토콜인 IKEv2 표준이 완성됨에 따라, IPSEC 프로토콜을 사용한 VPN의 상호연동성이 크게 개선될 전망이다. 게다가, IPSEC4PKI 워킹그룹의 결성과 이 그룹의 향후 관련 표준 제정으로 IPSEC 시스템과 PKI 시스템의 연동 구축과 그 상호연동성도 크게 개선될 것으로 보

인다. IETF의 이러한 표준화 노력으로 대규모 기업 VPN의 멀티벤더 구축이 용이해 질 것으로 보인다.

한편, MOBIKE WG 결성과 NEMO WG 등 관련 그룹들의 활동으로, IPSEC 프로토콜의 모바일 네트워크 분야에의 적용이 활발해 질 전망이다. 즉, MOBIKE 워킹그룹의 결성은 IPSEC 프로토콜의 모바일 IP 분야의 적용을 촉진시킬 것이며, NEMO 워킹그룹은 ad hoc 모바일 네트워크의 구축을 앞당길 것으로 보인다.

MSEC WG에서는 현재 하나의 RFC가 존재하며 멀티캐스트 보안 구조 및 그룹 키 관리에 대한 여러 개의 인터넷 드래프트들이 RFC 표준화 단계에 있으며 멀티캐스트 보안이 현실화될 수 있도록 기존 보안 프로토콜에 멀티캐스트 보안 구조를 포함하는 연구가 더욱 강화될 것이다. 이를 위해 MSEC은 보안 관련된 WG들과 협력을 통해 멀티캐스트 지원을 고려하고 있으며 공동 표준화 작업이 진행중이다.

참 고 문 헌

[1] http://www.ietf.org/html.charters/ipsp-charter.html

[2] http://www.ietf.org/html.charters/ipsec-charter.html

[3] Charlie Kaufman, "Internet Key Exchange (IKEv2) Protocol," draft-ietf-ipsec-ikev2-11.txt Oct. 2003.

[4] http://www.ietf.org/html.charters/mobike-charter.html.

[5] Francis Dupont, "Address Management for IKE version 2", draft-dupont-ikev2-addrmgmt-04 .txt, Feb 2004.

[6] T. Kivinen, "MOBIKE protocol," draft-kivinen-mobike-protocol-00.txt, Feb 2004.

[7] T. Kivinen, "Design of the MOBIKE protocol", draft-kivinen-mobike-design-00.txt, Feb 2004.

[8] http://www.ietf.org/html.charters/pki4ipsec-charter.html

[9] Chris Bonatti, "Requirements for an IPsec Certificate Management Profile," draft-bonatti-pki4ipsec-profile-reqts-00.txt, Feb. 2004.

[10] Brian Korver, Eric Rescorla, "The Internet IP Security PKI Profile of ISAKMP and PKIX," draft-ietf-ipsec-pki-profile-04.txt, Feb. 2004.

[11] Http://www.ietf.org/html.charters/msec-charter.html.

[12] Thomas Hardjono, Brian Weis, "The Multicast Group Security Architecture," draft-ietf-msec-arch-05 .txt, Ja. 2004.

[13] Mark Baugher, Thomas Hardjono, Hugh Harney, Brian Weis, "The Group Domain of Interpretation," RFC 3547, July 2003.

[14] Hugh Harney, Uri Meth, Andrea Colegrove, George Gross, "GSAKMP," draft-ietf-msec-gsakmp-sec-05.txt, Feb. 2004.

[15] Mark Baugher, Ran Canetti, Lakshminath Dondeti, Fredrik Lindholm, "MSEC Group Key Management Architecture," draft-ietf-msec-gkmarch-07.txt, Jan. 2003.

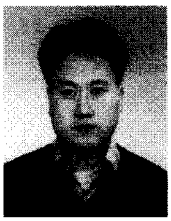
[16] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman, "MIKEY: Multimedia Internet KEYing," draft-ietf-msec-mikey-08.txt, Dec. 2003.

[17] Martin Euchner, "HMAC-authenticated Diffie-Hellman for MIKEY," draft-ietf-msec-mikey-dhhmac-05.txt, Dec. 2003.

[18] Brian Weis, "The Use of RSA Signatures within ESP and AH," draft-ietf-msec-ipsec-signatures-00.txt, Dec. 2003.

[19] Mark Baugher, Elisabetta Carrara, "The Use of TESLA in SRTP," draft-ietf-msec-srtp-tesla-00.txt, Feb. 2004.

〈著 者 紹 介〉



홍 기 훈 (Kihun Hong)
학생회원

2000년 2월 : 숭실대학교 정보통신공학과 공학사
2002년 2월 : 숭실대학교 정보통신공학과 공학석사
2002년 3월~현재 : 숭실대학교 정보통신공학과 박사과정
〈관심분야〉 모바일 보안, 멀티캐스트 보안, IPSEC

정 수 환 (Souhwan Jung)
정회원

1985년 2월 : 서울대학교 전자공학과 졸업
1987년 2월 : 서울대학교 전자공학과 석사
1988년~1991년 : 한국통신 전임연구원
1996년: 미 워싱턴 주립대(시애틀) 박사
1996년~1997년 : Stellar One SW Engineer
1997년~현재 : 숭실대학교 정보통신전자공학부 부교수
〈관심분야〉 모바일 인터넷 보안, NEMO Security, Security Protocol.

이 계 상 (Kye Sang Lee)
정회원

1979년 2월 : 서울대학교 공학사
1981년 2월 : 서울대학교 전자공학과 석사
1981년 10월~1997년 8월 : 한국전자통신연구원 재직
1997년 9월~현재 : 동의대학교 정보통신공학과 재직 중
〈관심분야〉 인터넷 프로토콜, 표준, 인터넷 보안, IPSEC