Mobile IPv6환경에서 MN과 HA간의 IPsec 적용 방안에 관한 연구

박원주* · 서동일**

*한국전자통신연구원 정보보호연구본부 네트워크보안연구부

The Methods of applying IPsec between MN and HA based on Mobile IPv6

Wonjoo PARK* · Dongil SEO**

*Information Security Technology Division, ETRI

E-mail : [wjpark,bluesea]@etri.re.kr

요 약

최근 IETF mobileip 워킹 그룹은 Mobile IPv6의 보안 문제를 가장 중요하게 다루고 있고, 홈 에이전트와 이동 노드는 IPsec을 적용하여 인터넷 보안을 제공하고, 상대 노드와 이동 노드는 RR과정으로 서로를 인증 할 수 있는 표준안을 제출하였다. 이동 노드는 자신의 홈 주소를 획득하여 인터넷 연결의 이동성을 보장받기 위하여 특정 라우터에게 홈 에이전트를 등록하고 홈 에이전트와 이동 노드는 IPsec 적용을 위한 보안 연계 정보를 교환할 수 있어 IPsec 적용이 가능하다. 반면 상대 노드와 이동 노드와 IPsec을 적용하기 위해서는 이동 단말기의 한계 및 IPsec 프로세싱의 부하로 RR과정을 통하여 상호 인증하는 메커니즘을 채택하였다. 본 고는 Mobile IPv6 환경에서 홈 에이전트와 이동 노드사이에 IPsec 적용 방안을 위한 보안 연계 및 보안 정책 관리 방향을 제시한다.

ABSTRACT

Recently, IETF Mobile IP WG focus on security problem issues in Mobile IPv6 and provide appropriate protocol to solve them. These include the protections of Binding Updates both to home agents and correspondent nodes, prefix discovery messages and transporting data packets.In Mobile IPv6, control traffics between home agents and mobile nodes uses IPsec to avoid that mobile nodes and correspondent nodes may be vulnerable to attacks. It is used, however, Return Routability procedure for correspondent node to assure that the right mobile node is sending the messages. In this paper, we propose method of IPsec processing to protect messages between home agents and mobile nodes.

Keywords

IPsec, Mobile IPv6, MIPv6 Security, Return Routability, Secuirty Association, Security Policy

I. 서 론

모바일 IP는 노드가 위치를 이동하여 인터넷 접속점의 링크 계층이 변경된 후에도 다른 노드와 통신이 가능하고, 기존의 노드들과의 연결을 유지할 수 있도록 지원하는 것을 목표로 개발된 프로토콜이다. 이러한 이동성을 제공하기 위하여 IETF(Internet Engine -ering Task Force)의 mobileip(IP Routing for Wire -less/Mobile Hosts)[1] 워킹 그룹에 의해 표준화 작업이 수행되고 있다.

Mobile ip워킹 그룹은 IPv4 인터넷 환경에서 노드의 이동성을 지원하기 위한 표준화 작업을 완료하였고, 현재 IPv6 인터넷 환경에서 모바일IP 표준화를 위한 활발한 토의가 진행되고 있다. 최근 Mobile IPv6제공을 위한 인터넷 드래프트가 21번째 개정판이 제출되었고 이 문서는 RFC문서로의 승인을 위해 IESG에 제출되었다.

공중망을 사용하는 이동 환경에서 보안은 특히 중요한 요소이다. 초기에 Mobile IPv6는 보안 표준으로서 기존의 IPv6보안의 mandatory 요소인 IPsec을 적용하기로 확정하였으나,[2] IETF 51차 영국 런던 회의 직전부터 이동 단말기의 여러 가지 제한된 요소 등을 고려할 때, 통신 전 구간에 IPsec을 적용하는 것은 무리가 있다는 의견이 제시되었다. PDA나 휴대폰과 같은 이동 단말기는 기존 고정 단말에 비해 하드웨어 성능이 미약하여IPsec 프로세싱에 대한 부담이 크고, IPsec 보안

프로토콜을 위한 키 교환 프로토콜은 프로토콜 자체가 복잡하고 패킷의 길이가 길어 상대적으로 가벼운 프로토콜의 가능성을 제시하였다.

현재 Mobile IP 워킹 그룹에서는 MIPv6의 보안 문제가 가장 핫 이슈이며, 현재 제출된 21 개 정판에서는 이동 노드(MN)과 홈에이전트(HA)는 IPsec을 적용하나 이동 노드와 상대 노드(CN)는 Return Routability Procedure 과정으로 이동 노드와 상대 노드가 키를 교환하여 인증하는 방법을 채택하였다.[3]

본 고는 Mobile IPv6환경에서 홈 에이전트와 이동 노드 사이의 시그널링 및 패킷을 보호하기 위하여 IPsec 을 적용할 때IPsec 보안 프로토콜을 위한 보안 연계 및 보안 정책 관리 방향을 제시한다

II. Mobile IPv6와 Security

Mobile IPv6환경에서 이동 노드는 현재 자신이 홈 링크에 접속하여 있든, 외부 링크에 접속하여 있든 Home Address(HoA)이용하여 통신이 가능해야 한다. HoA는 홈 링크 상에서 홈 서브넷 프리픽스 내에 이동 노드에게 할당된 주소이고, 이동 노드의 유니캐스트 주소로서 영구 주소로 사용된다. 반면 이동 노드가 외부 링크에 접속되어져 있는 경우에는 외부 링크의 프리픽스 내에 할당된 임시 주소로서 Care-of address(CoA)를 할당 받는다. 이 때, 상대 노드에서 이동 노드로 향하는 패킷은 일단 홈 에이전트를 통하여 패킷을 전달하므로 경로 최적화를 위해 이동 노드가 홈 에이전트 및 상대 노드에게 자신의 CoA와 HoA 정보를 묶어서 바인딩 갱신(Binding Update)를 전달한다. 바인딩 갱신을 수신한 홈 에이전트와 상대 노드는 자신의 바인딩 캐시에 바인딩 정보를 저장하여 이동 노드에게 패킷을 보낼 때에 CoA를 사용하여 홈 에이전트를 거치지 않고 패킷을 송신할 수 있다.[3]

또한, Mobile IPv6환경에서 홈 네트워크의 정보가 변경되면 "prefix discovery" 메커니즘을 통하여 이동 노드가 변경된 홈 네트워크 정보를 획득할 수 있다. 이때 홈 에이전트와 이동 노드사이의 바인딩 갱신 및 prefix discovery와 같은 제어 패킷이 보호 받지 못하면 상대 노드와 통신시 취약성을 유발 할 수 있다. [4]

이와 같은 취약성을 극복하기 위하여 홈 에이전트와 이동 노드간의 제어 패킷은 IPsec 보안 프로토콜을 이용하여 보호한다. 이동 노드와 홈 에이전트간의 제어 패킷은 바인딩 갱신을 위한 Binding Update(BU), Binding Acknowledgemnet (BA)메시지, 상대 노드가 이동 노드의 상호 인증을 위한 Return Routabiliy(RR)과정에서 주고받는 Home Test Init(HoTI), Home Test(HoT) 메시지와 이동 노드와 홈 에이전트간에 프리픽스 정보를 주고받기 위한 ICMPv6메시지를 포함한다. IPv6는 Mobile IPv6의 패킷 처리를 위해 기존의 확장헤더에 Mobiley Header를 추가적으로 정의하고 있다.[3]

III. HA와 MN사이의 IPsec

이동 노드와 홈 에이전트는 제어 패킷에 IPsec을 적용하여 보호하기 위하여 보안 연계, Security Association을 가져야만 한다. 또한 IPsec 적용과 적당한 SA를 협상하기 위하여 보안 정책을 가져야만 한다. Binding Update와 Binding Acknowledgeme -nt 메시지는 이동 노드와 홈 에이전트간에 이미 협상된 non-null authentication 알고리즘의 ESP 확장 헤더를 포함해야 한다. [3]

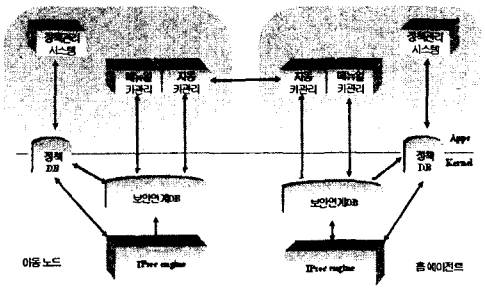

그림 1. MN과 HA의 IPsec 적용시스템

이동 노드의 한 응용 프로그램이 IPsec 엔진을 통하여 패킷을 보내고자 할때, 엔진은 IPsec 적용 여부를 알기위해 정책 DB를 먼저 참조한다. 목적지가 홈 에이전트인 제어 패킷은 IPsec 네트워크 보안 서비스를 제공해야 하므로, SA가 있는지 보안 연계 DB에서 적당한 SA를 찾는다. 이때, 홈 에이전트와 협상된 보안 연계가 없으면 자동 키 관리 응용이나, 매뉴얼 키 관리 응용에게 요청하여 non-null authentication 알고리즘을 가진 트랜스포트 모드의 ESP를 협상하게 한다.[5]

본 시스템은 기본적으로 제공해야하는 매뉴얼 키관리엔진(MKE, Manual Key management Engine)과 IKE를 기초로 구현된 자동 키관리 엔진(DKE, Dynamic Key Management Engine)을 모두 제공한다. MKE 또는 DKE로 협상된 SA는 단방향으로 적용되고, 한 연결이라 할지라도 outbound와 inbound 프로세싱에 따라 다른 보안 연계를 적용해야한다. 이러한 SA는 SPI(Secuirty Parameter Index), 목적지 주소, 보안 프로토콜로 식별되고 추가적으로 IPsec적용 방식이 터널모드인지, 트랜스포트 모드인지 구별될 수 있다.

이동 노드와 홈 에이전트간의 제어 패킷은 이동노드의 HoA와 CoA의 바인딩 정보를 홈 에이전트에게 등록하기 위한 BU, BA메시지가 있다.

이 메시지에 IPsec 처리를 위하여 이동 노드는 다음과 같은 SAs를 갖고, 각 SA의 튜플 정보는 (SPI, 목적지 주소, 보안 프로토콜, 모드)로 구성된다.

이때, HoA는 이동 노드의 홈 주소이고, HA_addr는 홈 에이전트의 주소를 말한다. 또한 상대노드가 이동노드의 상호 인증을 위해 RR과정이 수행될때 이동 노드와 홈 에이전트간의 HoT와 HoTI 메시지의 IPsec 적용을 위한 SA가 필요하다.

이때, 이동노드와 홈 에이전트는 터널링을 통하여 연결이 설정되므로 IPsec 모드도 터널 모드여야만 한다. 이외에 Prefix Discovery 메시지 보안을 위한 inbound, outbound의 두 SA가 필요하

이동노드
SAout = (a, HA_addr, ESP, Transport) - SA1 SAin = (b, HoA, ESP, Transport) - SA2
홈에이전트
SAout = (b, HoA, ESP, Transport) - SA2 SAin = (a, HA_addr, ESP, Transport) - SA1

며, 두 노드간에 주고 받는 데이터 패킷을 위한 터널 모드의 SAin, SAout의 보안 연계가 더 필요하다. 따라서 홈 에이전트와 이동 노드의 IPsec적용을 위하여서는 이동 노드와 홈 에이전트는 각각 최소한 8개의 SA를 가져야만 한다.

이동노드
SAout = (c, HA_addr, ESP, Tunnel) - SA3 SAin = (d, HoA, ESP, Tunnel) - SA4
홈에이전트
SAout = (d, HoA, ESP, Tunnel) - SA4 SAin = (c, HA_addr, ESP, Tunnel) - SA3

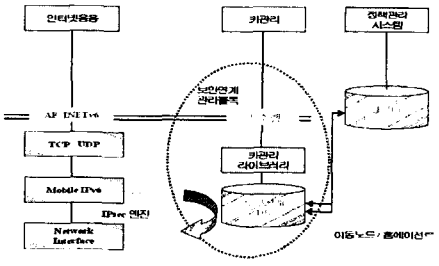

그림 2. SADB와 SPDB와의 관계

키관리 시스템에 의해 협상되면 키 소켓 통신을 통하여 커널의 보안연계DB에 저장하고, IPsec 엔진은 AF_INET6 소켓을 통하여 인터넷 응용이 주고 받는 inbound, outbound 패킷에 IPsec 처리 과정에 필요한 SA를 참조하여 보안 서비스를 제공한다. 필요한 SA의 협상이 끝나면 IPsec 엔진은 이동 노드의 HoA와 CoA를 구분하고, 보안 정책과 연계 DB를 참조하여 ESP 헤더를 추가하여 IPsec처리를 한다.

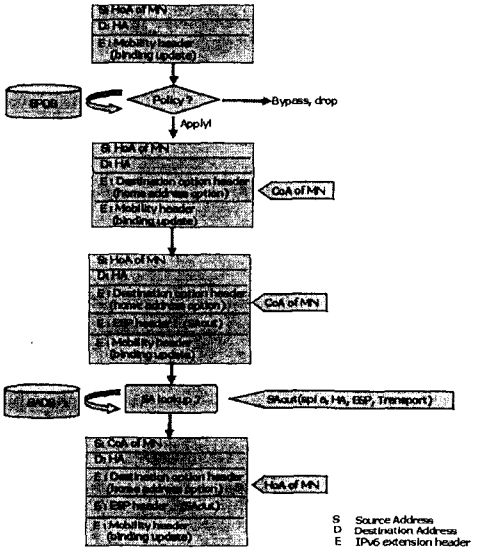

그림 3. 이동노드에서의 BU 메시지 전송 예

위의 그림 3은 이동 노드에서 Binding Update 메시지를 보낼때, SAout을 처리하기위한 IPv6패킷의 생성 순서이다.. 이동 노드는 원래 HoA를 송신지 주소로 패킷을 생성하고, 보안 정책에 따라서 홈 에이전트와 IPsec처리를 하는 경우, IPv6의 목적지 옵션 헤더로 CoA 주소를 삽입한 후, SADB를 lookup하여 ESP 헤더를 추가한다. 그리고 실제로 패킷이 전송될 때에는 송신지 주소를 현재의 자신의 CoA를 삽입하고, HoA는 홈 주소 옵션에 추가하여 전송한다.

IV. 결론 및 고찰

본 고는 Mobile IPv6 환경에서 이동 노드와 홈 에이전트간에 IPsec 적용을 위한 구조 및 보안 연계에 대하여 설명하였다. 기존의 IPv6는 네트워크 보안의 표준으로 IPsec을 필수요구사항으로 정의하였으나, Mobile IPv6는 IPsec의 복잡성과 패킷 처리의 성능의 이유로 이동 노드와 홈 에이전트 사이에만 IPsec을 적용하기로 하였다. 또한 상대 노드와 이동 노드는 Return Routability Procedure 과정으로 이동 노드와 상대 노드가 키를 교환하여 상호 인증한 후에 통신을 설정하여 패킷 보안 서비스는 제공하지 못하고 있다.

본 고는 이동 노드와 홈 에이전트간의 IPsec

시스템을 설계하였고, 두 노드간에 최소한으로 필요한 보안 연계 정보를 구분하였다. 또한 두 노드가 IPsec 처리를 위해 필요한 블록과 처리 과정을 살펴보았다.

최근에 Mobile IPv6워킹 그룹에서 발표한 인터넷 드래프트는 proposed standard로 제출되어 RFC로 심사 중이며, 본 시스템은 표준화에 따라 설계에 따라서 구현될 예정이다.

참고문헌

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

[2] Deering, Hinden "Internet Protocol, Version6(IPv6) Specification", IETF RFC 2460, Dec 1998

[3] Jonhson, Perkins, Arkko, " Mobility Support in IPv6", internet-draft-mobileip-ipv6-21.txt, Feb 2003

[4] Gilligan, Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", IETF RFC 2893, Aug, 2000

[5] Kent, Atkinson, "Security Architecture for IP", IETF RFC 2401, Nov 1998