모바일 IPv6 보안†

숙명여자대학교 이광수*

1. 서 론

모바일 IP는 IETF(Internet Engineering Task Force)의 mobileip(IP Routing for Wireless/Mobile Hosts) 작업반에 의해 개발된 프로토콜로서, 위치를 이동하여 인터넷 접속점을 변경하는 노드가 인터넷 상의 다른 노드들과의 통신을 계속할 수 있도록 지원하는 것을 목표로 하고 있다. 이러한 이동은 한 장소에서 인터넷에 연결되어 통신을 하다가 모든 접속을 종료한 후 새로운 장소에서 다시 인터넷에 연결되는 일반 노트북 사용자의 경우와는 다르며, 모든 접속 환경의 변화와 동적인 연결 유지가 자동적으로 이루어져야 한다. 모바일 IP는 이러한 이동성 지원을 IP 계층에서 제공함으로써 전송 계층 이상에서의 연결을 투명하게 유지한 상태에서 물리적 접속을 변경할 수 있도록 허용한다. 모바일 IP는 유선 인터넷 환경에서도 가능하긴 하지만 가장 자연스러운 운용 환경은 무선 통신 환경일 것이다.

IP 계층에서의 이동성 지원은 각 모바일 노드에게 홈(home) 네트워크와 변하지 않는 IP 주소인 홈 어드레스를 지정한 후 홈 네트워크의 라우터인 홈 에이전트(home agent)를 통해 이동된 위치로 IP 패킷 라우팅 서비스를 받는 방법이 사용된다. 이동된 위치에서 모바일 노드가 연결되는 네트워크를 외지 네트워크(foreign network)라고 부르며, 외지 네트워크에서 부여받게 되는 임시 IP 주소를 홈 에이전트에 등록하면, 이후 모바일 노드의 홈 어드레스를 목적지로 하는 IP 패킷들은 홈 에이전트에 의해 현재의 위치로 전달되는 방식이 일반적으로 사용된다.

1996년 10월에 발표된 RFC 2002[1]는 IPv4 환경에서 모바일 노드와의 인터넷 통신에 대한 지원을 규정하고 있는데, 2002년 1월에 그 개정판인 RFC 3220[2]이 발표되었으며 홈 에이전트와 외지 에이전트 사이에서 역 터널링의 지원 추가, 외지 에이전트에서의 등록 요청에 대한 검사 기능 강화, 인증을 위한 기본 MAC 함수의 HMAC-MD5로의 변경, 기존 보안 연계를 활용한 등록 요청의 인증 기능 추가 등을 포함하여 많은 내용이 변경되었다. IPv4에서의 이동성 지원을 위한 프로토콜(MIPv4)을 규정한 RFC 2002에 대한 개발 작업이 완료될 시점인 1995년 mobileip 작업반에서는 그 내용을 IPv6에 맞게 수정하여 IPv6에서의 이동성 지원을 위한 프로토콜(MIPv6) 개발 작업에 착수하였다. IPv6에는 비-상태 주소 자동구성[3], 인접 노드 발견[4] 등의 효율적인 이동성 지원에 사용될 수 있는 기능들이 추가되어 있으며, 또한 주소 변경이 크게 단순화되어 있다. 또한 IPv6의 확장 헤더 옵션들과 전면적인 보안 지원 등도 이동성 지원에 유리하며, 무엇보다도 중요한 것은 IPv6가 아직 배치되어 사용되고 있지 않으며 그 표준화도 아직 최종 단계가 아니어서 새로운 아이디어의 반영이 가능하다는 점에서 MIPv6 개발은 단순히 IPv4 버전의 각색이 아니라 그 설계에 있어 많은 새로운 가능성을 갖고 진행되어 오고 있다. MIPv6를 규정하고 있는 인터넷 드래프트[5]에 의하면, 라우팅 최적화의 기본적 지원, 유입점 필터링(ingress filtering)[6] 문제의 해결, IPv6 목적지 옵션을 이용한 MIPv6 제어 트래픽의 피기백(piggybacking) 방식의 전송, 외지 에이전트의 필요성 제거, 라우팅 헤더의 사용으로 부담이 큰 IP-within-IP 캡슐화 사용 필요성 제거 등을 포함하는 많은 개선이 이루어졌다.

2001년 3월 미국 미니애폴리스에서 개최된 제50차 IETF 회의 직전 mobileip 작업반은 MIPv6 드래프트

† 본 연구는 숙명여자대학교 2001년도 교내연구비 지원에 의해 수행되었음

* 종신회원

의 13번째 개정판에 대해 RFC 문서로의 승인을 위해 IESG에 제출하였으나, IESG에 참여하고 있는 보안 영역 의장단에 의해 그 도입이 기존의 인터넷 보안 환경을 크게 저해할 우려가 있다는 지적을 받고 승인이 보류되었다. 주로 문제가 된 부분은 경로 최적화를 위해 모바일 노드가 통신 상대 노드에게 자신의 현재 위치를 알릴 때 사용되는 바인딩 갱신 메시지의 인증에 관한 것이었으며, 이후 mobileip 작업반에서는 이 문제의 해결을 위해 노력해 왔으며, 또한 MIPv6에서의 다른 보안 문제들도 다시 검토하게 되었다. 2001년 12월에 미국 솔트레이크시티에서 개최된 52차 IETF 회의에서는 바인딩 갱신 보안에 관한 여러 제안과 라우팅 헤더와 홈 어드레스 옵션 등으로 인한 보안 문제들이 토의되었다. 이들 제안 중 어느 것이 표준으로 수용되고 이에 따라 MIPv6 문서의 표준화가 진전될 것인지에 대해서는 아직 판단하기 이르지만 현재의 작업 상황에 대해 보안 영역 의장들도 긍정적으로 평가하고 있는 것으로 알려지고 있어 2002년 중 중요 윤곽은 정해질 것으로 전망된다.

본 고에서는 먼저 바인딩 갱신과 관련 보안 문제, 그리고 해결 방안으로서의 바인딩 갱신 인증을 위한 제안들을 살펴보고, 다음에 라우팅 헤더와 홈 어드레스 옵션에 관한 보안 문제를 논의한다.

2. MIPv6에서의 바인딩 갱신

2.1 MIPv6에서의 바인딩 갱신 관련 보안 문제

MIPv6로 인한 문제의 근본 원인은 노드의 이동성에 있다. 즉, 특정 모바일 노드의 주소가 자주 변할 수 있다는 점이다. 이를 이용하여 해당 노드의 주소를 다르게 알려줌으로써 해당 노드로의 패킷이 다른 호스트로 전달되게 할 수도 있고, 그 노드를 서비스 거부 상태에 있게 할 수도 있다. 이상의 공격이 가능한 근본 문제로 MIPv6에서의 바인딩 갱신(BU; Binding Update) 문제가 있는데, 이의 설명을 위해 모바일 노드의 통신을 살펴보면 다음과 같다.

모바일 노드를 MN(Mobile Node)이라고 부르며, MN의 통신 상대방을 CN(Correspondent Node)이라 부른다. 모바일 노드는 홈 주소(Home Address; HoA)라고 불리는 고유한 IP 주소를 갖는데, 이 주소는 모바일 노드의 현재 위치와 무관하다. HoA를 포함하는 서브 네트워크를 그 모바일 노드의 홈 네트워크라고 하며, 홈 네트워크 안에 있는 라우터인 홈 에이전트(HA; Home Agent)는 모바일 노드가 홈 네트워크를 떠나 있을 때 모바일 노드에게 보내진 패킷들을 전달하는 역할을 수행한다. 모바일 노드가 홈 네트워크에 위치할 때는 모바일 노드는 일반 노드와 전혀 차이가 없다. 모바일 노드가 홈 네트워크를 떠나 다른 곳에서 인터넷에 연결될 때, 접속 위치의 네트워크를 외지 네트워크, 외지 네트워크의 라우터를 외지 에이전트(FA; Foreign Agent), 외지 네트워크에서 임시로 부여받은 IP 주소를 CoA(Care-of Address; 의탁 주소)라고 부른다. CN이 모바일 노드가 아닐 경우, MN에서 인터넷 상에 위치한 CN에 패킷을 보내는 일은 일반적인 인터넷에서의 통신과 별반 다르지 않다. 그러나, CN에서 MN으로 패킷을 보낼 경우, 단순한 방법은 HoA를 목적지 주소로 해서 MN의 홈 네트워크로 패킷을 전달하는데, 이 때 HA가 그 패킷을 가로채서 이동된 위치의 MN에게 전달하는 방식이 사용된다. 따라서 HA는 MN의 현재 위치를 파악할 수 있어야 하며, 이를 위해 각 MN은 이동 후에 HA에게 자신의 현재 위치 CoA를 알려주게 되어 있다. 이와 같이 MN이 HA에게 현재 위치를 알려주는 것을 홈 등록(Home Registration)이라고 부른다. HA가 MN에게 보내는 패킷은 기존의 IP 패킷 앞에 별도의 IP 헤더가 추가되는 IP-within-IP 터널링 방식을 사용하여 전달하게 되어있으며, HA와 MN 사이의 통신은 사전에 확립된 보안 연계(SA; Security Association)를 이용한 보안 터널링을 사용할 수 있다. SA는 적용될 보안 기능, 사용될 암호 알고리즘, 관련 암호키 등을 포함하며, 보안 터널링을 통해 안전한 방식으로 패킷들을 교환하는 홈 등록은 별다른 보안 문제를 발생시키지 않는다. 그림 1은 모바일 노드와의 일반적인 통신 상황을 나타내고 있는데, 특히 MN에서 CN으로의 통신이 직접 전달 경로를 취하는데 비해 CN에서 MN으로의 통신이 HA를 경유하는 방식을 사용하고 있음을 유의하자.

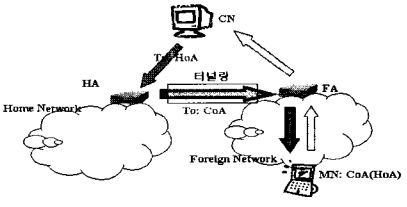

그림 1 MN과 CN 사이의 일반적 통신

그런데, 이렇게 HA 노드를 경유하는 방식을 쓰면 CN으로부터 MN으로 전달되는 패킷은 불필요한 우회 경로로 인해 전달이 지연되게 되며, 이를 삼각 라우팅(triangle routing) 문제라고 한다. 삼각 라우팅으로 인한 비효율성을 개선하기 위해 모바일 IP에서는 경로 최적화 메커니즘을 도입하여 CN이 MN의 위치 정보를 가질 수 있도록 하였고, 이를 위해 MN이 CN에게 전달하는 정보가 바로 BU이다. 즉, MN이 <HoA, CoA>를 포함하는 정보를 CN에게 보내면, CN은 이 내용을 바인딩 캐시라는 곳에 저장해 두었다가 MN에게 보낼 패킷이 있으면, 바인딩 캐시를 조회하여 CoA라는 주소를 사용하여 HA를 경유하지 않고 직접 전달할 수 있게 된다. 경로 최적화와 바인딩 갱신 메커니즘은 MIPv4에도 도입되어 있으나 바인딩 갱신 관련 메시지를 다른 메시지에 실어 보낼 수 없고, 또 CN들 중 MIPv4 지원을 위해 업그레이드된 노드들만이 바인딩 캐시를 지원할 것이므로 IPv4 네트워크 환경에서는 그 전면적 채택을 기대하기는 어렵다. 그림 2는 바인딩 갱신에 의한 경로 최적화를 사용한 모바일 노드와의 통신을 나타낸다.

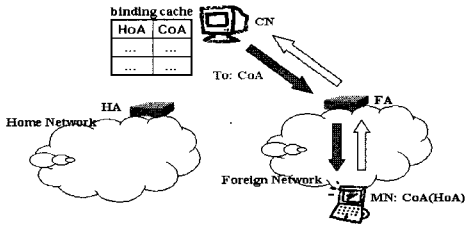

그림 2 경로 최적화를 사용하는 MN과 CN 사이의 통신

그런데, BU 전달에 있어 적절한 인증이 이루어지지 않을 경우, 거짓 BU의 전달이 가능해지는데, 이를 이용하여 CN이 MN에게 보낼 패킷을 엉뚱한 노드에게 전달하게 된다. 이것은 특히 CN과 MN 사이의 통신 경로 상에 있지 않은 공격자도 바인딩 갱신 메시지를 위조하여 보낼 수 있으며, 그 결과 임의의 노드 사이의 메시지를 다른 노드에게로 향하게 할 수 있게 되는데, 이와 같은 공격을 원격 경로 변경(remote redirection)이라고 한다. 원격 경로 변경은 특정 노드가 받게 될 패킷들을 다른 노드에게로 보냄으로써 원래의 수신 노드를 서비스 거부 상태에 이르게 할 수도 있고, 또 그 노드가 받게 될 메시지의 내용을 다른 노드에 노출시키게 되는 기밀성 공격을 초래할 수도 있다. 그리고, 이러한 공격은 비-모바일 노드를 대상으로 이루어질 수도 있는데, 이것은 CoA로 지칭되는 주소 자체만으로는 해당 노드가 모바일 노드인지 여부를 판단할 수 없기 때문이다. 따라서, 적절하고도 충분한 인증이 보장되지 않는 BU가 도입될 경우 비-모바일 노드들도 원격 경로 변경에 노출되게 되며, 특히 MIPv6 명세는 모든 IPv6 노드들에 대해 MIPv6 지원을 의무화하고 있으므로 인터넷 상의 모든 노드들을 대상으로 하는 공격이 가능해진다.

BU를 전달받은 CN은 응답 메시지인 바인딩 확인(BA; Binding Acknowledgement) 메시지를 보내게 된다. BA에 대한 인증도 필요한데, 이것은 MN이 BU를 보냈을 때 공격 행위 또는 네트워크 장애 현상 등으로 인해 바인딩 갱신이 이루어지지 않았는데, 공격자가 거짓 BA 메시지를 위조해 보냄으로써 BU의 재시도를 방해하는 것을 막기 위함이다.

IESG에 제출된 MIPv6 문서에서는 BU와 BA 인증을 위해 IPsec[7]의 인증 헤더(AH; Authentication Header)의 사용을 제안하였다. IPsec AH는 IP 헤더 부분을 포함하는 전체 IP 패킷에 대해 메시지 인증 코드(MAC; Message Authentication Code)를 사용하여 패킷의 송신자와 그 내용에 대한 인증, 그리고 재전송 공격 탐지 기능 등을 제공하는 강력한 인증 메커니즘이다. 그런데 두 노드 사이에 IPsec 메커니즘의 적용 여부는 사전에 설정된 IPsec의 보안정책 데이터베이스에 의해 표현되며, 이 정책 항목은 자주 변경되지 않는다. 따라서 두 노드 사이에 AH 메커니즘의 사용이 일단 선택되면, 두 노드 사이의 모든 패킷은 AH 계산 및 확인 절차를 거쳐야 하는데, 실제 인증이 필요한 부분은 발생 빈도가 극히 낮은 BU/BA 패킷뿐이므로 많은 시간과 대역폭이 낭비되는 결과를 초래한다. 또한 사전 약속이 없는 임의의 두 노드 사이에 AH를 사용하기 위해서는 키 교환이 필요하며 이 경우 안전한 키 교환을 위해서는 인증된 공개키 방식이 필요하며, 임의의 노드의 공개키에 대한 신뢰성 있는 인증을 위해서는 모든 인터넷 노드를 대상으로 하는 전면적 PKI(공개키 기반구조)가 필수적이지만 그 누구도 가까운 장래에 전면적 PKI의 실현을 예상하지는 않고 있다. 그리고, IPsec에서 사용할 수 있는 키 교환 메커니즘은 IKE 프로토콜인데, IKE는 너무 많은 메시지의 교환을 요구한다는 점과 또 진행 중인 키 교환 상대방에 대한 상태 정보의 저

장을 필요로 하는 약점을 갖고 있다. 상태 정보 저장은 쉽게 메모리 소모를 통한 서비스 거부 공격에 악용될 수 있으며, IKE에 포함된 많은 지수 계산은 분산 서비스 거부 공격에 대한 취약성을 갖는다. 이러한 여러 가지 문제들로 인해 제안된 IPsec AH 메커니즘은 BU/BA 인증에 사용되지 않을 가능성이 높으며, 이는 곧 인증되지 않은 BU/BA의 횡행으로 인해 앞에서 언급된 보안 문제들을 야기할 것으로 우려되고 있다.

2.2 바인딩 갱신 보안을 위한 제안들

바인딩 갱신에 대한 보안의 이상적인 목표는 홈 어드레스가 HoA이고 의탁 주소가 CoA인 모바일 노드만이 <HoA, CoA>를 포함하는 바인딩 갱신 메시지를 보낼 수 있도록 보장하는 것일 것이다. 그러나, 전면적 PKI나 유사한 사전 인증 메커니즘을 채택할 수 없는 현재의 환경에서는 이런 정도의 강한 인증을 실현할 수는 없는 것으로 평가되고 있으며, MIPv6의 표준화 진행을 위해 IETF 보안 영역 의장단이 제시하고 있는 MIPv6에 대한 최소한의 보안 요구사항도 완벽한 보안성이라기보다는 MIPv6의 도입이 현재의 IPv4의 보안 수준을 더 이상 악화시켜서는 안 된다는 것이다. 그리고, 현재까지의 현실성이 있어 보이는 모든 BU 인증 제안들에서 드러나고 있는 정상 통신 경로 상의 공격자에 의한 중개인(MITM; Man-in-the-middle) 공격에 대해서는 궁극적으로는 해결되어야 할 문제이지만 현재의 인터넷 환경에서는 대비하기 어려우므로 당장 해결하지 않아도 좋다고 양보하고 있다. mobileip 작업반에서는 이러한 최소 보안 요구사항을 반영하고, 가능하면 보다 높은 수준의 보안을 제공할 수 있는 메커니즘을 개발하는데 대체적인 동의가 이루어진 바 있다.

미니애폴리스에서의 제50차 IETF 회의에서는 보안 영역 의장인 Jeffrey Schiller 등이 제안한 PBK (Purpose Built Keys) 프로토콜[8]과 hipsec(Host Identity Payload Security) BOF에서 제안된 보다 광범위한 문제의 해결을 위한 HIP(Host Identity Payload)[9] 등이 검토되었으나 충분한 호응을 얻지 못하였으며, 보다 근본적으로 MIPv6의 보안 문제에 대한 분석과 해결 방법을 모색하자는 방향으로 합의되었다. 런던에서 개최된 2001년 8월의 제51차 IETF 회의에서는 BU 보안을 위해 3개 정도의 추가 문서가 준비되었으나 토의가 진행되지는 못하였는데, 솔트레이크시티에서의 제52차 총회의 mobileip 회의에서는 토의 시간의 거의 대부분이 MIPv6 보안에 관한 토의로 진행될 정도로 많은 진전이 있었다.

BU/BA 보호를 위해 제안된 보안 메커니즘은 기본적으로 BU를 보내기에 앞서 BU를 보호하기 위한 키 또는 SA를 확립하는 절차를 두고, MN과 CN 사이에 확립된 공유 비밀키를 사용하여 BU를 보호하는 방식을 사용한다. 보호의 내용은 송신자 인증, 데이터 무결성, 재전송 방지 등이며 기밀성 제공도 가능하지만 현재 기밀성 추가의 이점은 명확하게 밝혀져 있지 않다. 그리고, 이들 제안들은 BU 메시지를 송신하는 MN에 대한 실체 인증은 하지 않고 있다. 현재 제안되어 있는 8개의 BU 보안 메커니즘은 표 1에서와 같이 크게 3 종류로 구분될 수 있으며, 이들을 차례대로 살펴보자.

표 1 BU 인증을 위한 제안들

분류	이름	관련 문서
RR(Return Routability) 사용	BAKE	[10]
	BUSEC	[11]
	BU3WAY	[12]
공개키와 연계된 ID 사용	PBK	[8]
	SUCV	[13]
	CAM-DH	[14]
Diffie-Hellman 키 교환 사용	DHMIPv6	[15]
	SAP	[16]

2.2.1 RR 방식의 BU 보안 메커니즘

BU 보호를 위해 제안된 첫 번째 종류의 인증 메커니즘으로는 CN에서 HA를 경유하여 MN에게 보낸 패킷의 수신 여부를 확인하는 RR(Return Routability) 방식이다. 이것은 HA는 홈 등록을 통해 MN의 정확한 위치를 알고 있을 것으로 가정하여 MN에게 정확히 전달할 수 있을 것으로 기대하고 암호키 구성에 사용되는 값, 메시지의 인증 및 재전송 방지를 위한 비표(nonce)나 토큰 등을 보내며, MN으로부터의 응답을 통해 전송한 값이 제대로 전달되었는지 확인한다. 전달되는 메시지는 암호화되지 않는다. 이 방식은 물론 완벽한 보안을 제공하지는 않는데, 이것은 CN과 HA 사이의 전송 경로 상의 임의의 노드 또는 HA와 MN 사이의 전송이 암호화되지 않을 경우 해당 경로 상의 임의의 노드가 CN이 MN에게 보낸 메시지들을 볼 수 있기 때문이며, 따라서 이들 노드들

은 MN을 위장하는 것이 가능해지기 때문이다.

RR 방식의 메커니즘 중의 하나인 BAKE(Binding Authentication Key Establishment)는 그림 3과 같은 3개의 메시지를 이용하여 BU 인증에 사용될 암호키를 확립하는데, HA와 MN 사이에 보안을 위한 SA가 확립되어 있다고 가정하며 이를 활용한다.

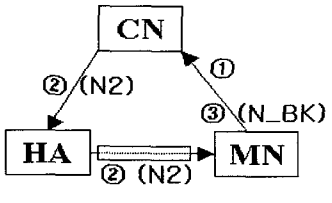

그림 3 BAKE 암호키 확립 모델

그림 3에서 전달되는 메시지는 다음과 같다.

① MN→CN : <CoA, CNA, HoA, N1, T1>

② CN→MN (HA 경유) : <CNA, HoA, N1, T1, N2, T2>

③ MN→CN : <CoA, CNA, HoA, T0, T2, N_BK>

여기서, CNA는 CN의 주소를 나타내며, N1, N2, N_BK 등은 난수이다. K_CN은 CN만이 알고있는 비밀키이며, K_MN-HA는 MN과 HA가 공유하는 비밀키이다. T0, T1, T2는 아래와 같이 계산되며, 인증용 토큰으로 사용된다.

T0=HMAC-SHA1-128 (K_MN-HA, N1 ‖ CNA ‖ CoA ‖ HoA)

T1=SHA1-128 (T0 ‖ 32개의 공백문자)

T2=HMAC-SHA1-128 (K_CN, T1 ‖ CoA ‖ CNA ‖ HoA)

Ti의 계산에서 "‖"는 연접을 나타내는 기호이며, SHA1-128은 해쉬 알고리즘 SHA-1을 적용한 결과에서 오른쪽 128비트만을 취하는 함수이며, HMAC-SHA1-128은 인증 알고리즘 HMAC-SHA1을 적용한 결과에서 오른쪽 128비트만을 취하는 함수이다.

메시지 ①에서 보낸 T1이 메시지 ②를 통해 HA에게 전달되면, HA는 T1의 사전 이미지 계산에서 K_MN-HA라는 MN과 HA가 공유하는 비밀키가 사용된 것을 확인할 수 있으며, 따라서 메시지 ①의 송신자가 진정한 MN임이 확인된다. 메시지 ③을 받게 되는 CN은 자신이 HA를 통해 MN에게 전달한 메시지가 무사히 MN에게 전달된 것을 확인함으로써 HA가 인정하는 MN이 맞는 것으로 판단한다. 또한, 메시지 ③에 포함된 토큰 T0는 이 메시지를 보내는 MN이 메시지 ①을 보낸 MN과 동일한 노드라는 사실을 확인시켜 준다. 이를 요약하면, 위의 프로토콜을 통해 CN은 HA가 그 정체를 보장하는 MN과 통신하고 있음을 확인할 수 있다는 것이다. BU 보호에 사용될 암호키 BK(BU Key)는 해쉬 알고리즘 MD5를 사용하여 다음과 같이 계산된다.

BK = MD5 (N2 ‖ N_BK)

BK는 CN이 생성하여 HA를 경유하여 MN에게 보낸 N2와 MN이 생성하여 CN에게 직접 보낸 N_BK를 이용하여 계산된다. 이 값들은 암호화되지 않고 평문 상태로 전달되므로 제3자가 가로채어 BK를 계산할 수 있는데, 이를 위해서는 이 값들이 전달되는 두 개의 서로 다른 경로 모두에 접근할 수 있어야 한다.

BAKE가 BU 보호에 사용될 수 있는 암호키를 먼저 확립한 후 BU 메시지를 전달하는데 비해 BUSEC(BU Security)와 BU3WAY(BU three way)는 암호키 확립 없이 전송된 비표가 돌아오는지를 검사하는 방식으로 MN의 신분을 확인한다. 먼저 BUSEC에서 교환되는 메시지들은 다음과 같다.

① MN→CN:<BU, Nm>

② CN→MN (HA 경유):<BR, Nc, Nm>

③ MN→CN:<BU, Nc, Nm>

④ CN→MN (HA 경유 않음)<BA, Nc, Nm>

여기서 BU, BR, BA는 각각 바인딩 갱신, 바인딩 요청, 바인딩 확인을 나타내며, Nm과 Nc는 각각 MN과 CN이 생성한 난수이며 비표로 사용된다. MN과 CN은 각각 자신이 생성하여 보낸 비표가 다시 돌아오는 것으로 상대방이 통신 경로 상에 존재하는 노드임을 확인할 수 있다. 그러나, 이 경우 HA와 MN 사이에 존재하는 능동적 공격자는 이 사이의 경로가 적절히 보호되지 않을 경우 가짜 BU를 만들어 보내는 것이 가능하다.

BU3WAY는 BUSEC이 4개의 메시지를 사용하는데 비해 3개의 메시지만을 사용하는데, 교환되는 메시지들은 다음과 같다.

① MN→CN:BUR(HoA, CoA)

② CN→MN (HA 경유):BUC(N1, 타임스탬프)

③ MN→CN:BU(N1, 타임스탬프)

여기서, BUR은 HoA와 CoA를 포함하는 BU 요청이며, BUC는 N1과 타임스탬프를 포함하는 BU 시험

이다. 물론 BU는 바인딩 갱신 메시지이다. N1은 CN만이 알고있는 비밀인 secret을 사용하여 다음과 같이 계산된 인증 토큰이다.

N1=hash(secret, HoA, CoA, CNA, 타임스탬프, 유효 기간)

N1과 타임스탬프를 사용함으로써 CN은 메시지 ②를 보낸 후 아무런 상태도 저장할 필요가 없으며, 따라서 BU 관련 메모리 소모가 원인이 되는 서비스 거부 공격을 방지할 수 있다. 이 점을 제외하고는 보안성에 관한 한 BUSEC과 큰 차이는 없는 것으로 평가된다.

RR 방식의 메커니즘들은 다음 절들에 나타나는 다른 메커니즘들이 높은 비용의 공개키 연산을 사용하는데 비해 난수 생성이나 해쉬 함수 정도의 암호 기술만을 사용함으로써 계산 비용 측면에서는 가장 효율적이지만, 수동적 공격만으로도 공격이 가능하다는 취약점을 갖는다.

2.2.2 공개키 관련 ID 방식의 BU 보안 메커니즘

두 번째 유형의 BU 보안 메커니즘에서는 BU 보호를 위해 공개키 서명을 사용한다. 그런데, 이 공개키의 소유주에 대한 인증을 PKI에 의존할 수 없기 때문에 공개키 소유주에 대한 신뢰를 확보하기 위한 몇 가지 방법이 제안되어 있다.

가장 먼저 발표된 PBK(Purpose Built Keys)에서는 서명에 사용될 임시 공개키/개인키 쌍을 먼저 생성하는데, 일반적인 공개키가 일정 기간 동안 반복해서 사용되는데 비해 여기서는 특별한 목적을 위해 만들어져 한 번만 쓰고 버린다는 의미에서 PBK라는 이름을 갖게 되었다. 공개키 부분에 대한 해쉬 결과를 EID(Endpoint ID)라고 부르며, MN이 현재의 접속지에서 CN과의 세션이 시작될 때 여러 번 EID를 보내고, 현재의 접속지에 있는 동안 적절한 시점에 해당 공개키도 CN에게 보내둔다. MN이 다음 접속지로 이동한 후 <EID, BU, (개인키로) BU에 대한 서명> 등을 보내면, CN은 EID에 해당하는 공개키를 사용하여 서명을 확인할 수 있으며, 따라서 BU 메시지를 보낸 노드가 이전에 EID를 보냈던 그 노드임을 확인할 수 있다. PBK는 BU 메시지를 보낸 노드의 실체에 대해서는 전혀 확인할 수 없지만, 이전에 HoA라는 홈 어드레스를 갖는 것으로 알고 있던 노드에서 메시지가 왔다고 믿는다는 것이 그 원리이다. 그리고, EID를 여러 번 보냄으로써 EID의 손실이나 EID 조작 공격을 막는 효과를 기대한다. 그러나, PBK는 현재 접속지에서 CN과 MN 사이의 신뢰를 가정하는데, 최초의 접속 시에는 사전 신뢰를 확보하는 방법이 명시되어 있지 않으며, MN과 HA 사이에 사전 확립된 SA를 활용하지 않는다는 단점도 있다. 그리고, MN과 CN 사이의 통신 경로 상에 존재하는 능동적 공격자라면, EID와 공개키 등을 변경하여 보내는 것도 가능하다는 취약점도 갖고 있다.

SUCV(Statistic Uniqueness and Cryptographic Verifiability)에서는 MN이 갖는 공개키 해쉬 값의 64비트를 MN의 HoA와 CoA 모두에 대해 IPv6 주소의 마지막 64비트로 사용한다. 이것은 PBK의 EID 전달 방식에 비교할 때, MN이 해당 공개키의 소유주임을 MN과의 모든 메시지 교환에서 확인할 수 있다는 점과 또 그 값이 주소에 포함되어 있어 별도의 대역폭을 차지하지 않는다는 장점을 제공한다. SUCV는 BU 보호를 위한 비밀키는 Diffie-Hellman 키 교환 방식을 사용해서 생성하며, CN이 Diffie-Hellman 키 교환 상대에 대한 인증을 위해 MN이 만들어 보낸 공개키 서명을 확인하는 방식을 사용하며, 또한 CN이 MN에게 보내는 Diffie-Hellman 공개 값은 HA를 경유하게 함으로써 부분적인 경로 검증까지 사용한다. 그리고, BU 보호는 IPsec ESP(Encapsulating Security Payload) 방식을 사용한다.

CAM-DH(Child-proof Authentication for MIPv6 with Diffie-Hellman)에서는 공개키 해쉬 값의 64비트를 MN의 HoA의 마지막 64비트로 사용한다. CoA의 경우에는 외지 네트워크에서 주소를 얻는 프로토콜에 따라 MN에게 주소 선택권이 없는 네트워크 환경도 존재하기 때문에 공개키 해쉬 값을 주소 구성에 사용하지 않는다. CAM-DH는 Diffie-Hellman 키 교환 방식을 사용하는 점에 있어서는 SUCV와 유사하지만, Diffie-Hellman 키 교환 메시지의 인증을 위해 MN의 개인키에 의한 서명도 사용하고 또 CN이 MN에게 HA 경유 여부에 따라 달라지는 두 개의 서로 다른 경로를 통해 전달한 값을 이용하여 생성된 키를 이용한 인증도 사용함으로써 좀 더 철저한 경로 검증을 거친다.

SUCV나 CAM-DH는 보안성에 있어서 다른 메커니즘들보다 우수한 것으로 평가받고 있지만 공개키 서명과 Diffie-Hellman이라는 두 가지의 공개키 연산을 포함하고 있어 계산 비용이 가장 높은 방식이라

는 단점을 갖는다.

2.2.3 Diffie-Hellman 키 교환 방식의 BU 보안 메커니즘

세 번째 유형의 BU 보안 메커니즘에서는 BU 보호를 위해 Diffie-Hellman 키 교환 방식을 통해 확립된 암호키를 사용한다. DHMIPv6(Diffie-Hellman based key distribution for MIPv6)에서는 MN과 CN이 각각 Diffie-Hellman 공개 값을 상대방에게 전달하는데, MN에게 보내는 메시지는 HA를 경유하여 전달된다. 이 방식은 공개키 서명과 공개키 해쉬 값을 이용한 MN의 주소 지정 등을 제외하면 앞 절의 SUCV와 유사하다. Diffie-Hellman 키 교환 방식에서도 중개인 공격이 가능하지만, 이를 위해서는 두 가지 전달 경로 모두에서 능동적 공격을 요한다. DHMIPv6에서는 HA와 MN 사이에 사전 확립된 SA는 활용되지 않는다. 대신에, AAA(Authentication, Authorization, Accounting) 기반구조가 제공될 경우 이를 이용한 강한 인증 방식이 기술되어 있다.

SAP(Security Association establishment Protocol for MIPv6)는 DHMIPv6와 유사하지만 MN에게 보내는 메시지가 HA를 경유하지 않고 직접 전달되는 방식이 사용된다. 그 이유는 HA가 통신의 병목이 되는 것을 피하기 위함이다.

Diffie-Hellman 키 교환 방식의 사용은 공개키 연산 시간이 좀 많이 걸리기는 하지만 능동적 공격 능력이 없는 공격자들로부터의 효과적인 방어를 제공한다는 점에서 RR 방식보다는 대체로 더 안전하다고 볼 수 있지만, 공개키 서명이 추가되어 있는 SUCV나 CAM-DH 만큼의 보안성을 제공하지는 않는다.

3. MIPv6에서의 기타 보안 문제

IPv6에서의 라우팅 헤더 옵션(RHOpt; Routing Header Option)과 MIPv6를 위한 홈 어드레스 옵션(HAOpt; Home Address Option)은 MIPv6의 지원에 있어 중요한 기능들인데, 이들의 사용이 제약되지 않을 경우 방화벽의 보안 기능을 우회하거나 공격 행위에 대한 패킷 역추적을 방해하는 등의 보안 문제를 발생시킬 수 있다. 이 절에서는 Savola가 제출한 인터넷 드래프트[17]의 내용을 중심으로 관련 보안 문제들과 해결 방안을 살펴본다.

3.1 라우팅 헤더 관련 보안 문제

IPv4에서 이동성 지원을 위해 소스 노드에서 라우팅 경유지들을 미리 지정하는 소스 라우팅의 사용이 고려되었으나, IPv4 소스 라우팅은 응답 역시 역순의 경로를 따르도록 요구되어 위장 공격에 대한 취약성을 증가시킨다는 점과 그 비효율성으로 인해 배제되었다. RH 옵션은 IPv4에서의 소스 라우팅을 발전시킨 IPv6 메커니즘인데, 패킷의 소스 노드에서 경유지 라우터를 표현하는 RH 목록을 만들어 RHOpt 필드에 포함시켜두면, 각 경유지 라우터에서는 RH 목록에서 RH를 하나씩 벗겨내고 IP 헤더의 목적지를 변경하여 다음 행선지로 전달한다. 이 옵션의 주된 용도는 서비스에 따라 다른 ISP를 경유하게 하는 등의 트래픽 엔지니어링과 MIPv6이다.

MIPv6에서 CN에서 MN에게 패킷을 보낼 때 RH 옵션은 HoA가 최종 목적지이고, CoA를 경유지임을 나타낸다. 경유지인 CoA 위치에 MN이 존재할 때는 MN에서 RH 옵션을 처리하는데, RH 옵션이 가리키는 최종 목적지는 HoA이며, MN은 바로 자신을 가리키고 있음을 알고 있어 자신에게 전달함으로써 라우팅이 완료된다. CoA 위치에 MN이 존재하지 않을 때는 FA에서 RH 옵션을 처리하게 되는데, HoA가 가리키는 곳은 MN의 홈 네트워크이며 그 안의 홈 에이전트가 HoA라는 주소를 갖는 MN의 위치를 알고있을 것이므로 적절한 라우팅이 이루어질 것이다.

MIPv6에서는 라우터가 아닌 경우를 포함하여 모든 노드에 대해 RH 옵션 처리 기능을 요구하고 있다. RH 옵션은 패킷의 목적지 주소를 경로 중에 변경하게 되므로 그림 4에서와 같이 목적지 주소 기반 방화벽 필터링을 우회하는 방법으로 사용될 수 있다.

그림 4 목적지 주소 기반 방화벽 필터링 우회

그림 4에서 방화벽은 외부 네트워크에서 웹 서버로 접근하는 것은 허용하지만 DB 서버로 접근하는 것은 차단하고 있다. 그러나, 공격자가 웹 서버를 경유하여 DB 서버에 도착하도록 RH 옵션을 사용하여 패킷을 보낼 경우, 방화벽이 보는 목적지 주소는 웹 서버이므로 통과시키며, 웹 서버는 RH 옵션을 처리

하여 패킷을 최종 목적지인 DB 서버로 전달하게 함으로써 방화벽의 필터링 기능을 무력화시킨다.

RH 옵션은 또한 DoS 공격에 반사기(reflector)로 작용하여 근원 추적을 방해하거나 ITRACE나 IPPT와 같은 패킷 역추적 기법을 방해한다.

제안된 대책은 RH 옵션 처리 기능을 제한적으로 사용하는 것인데, 트래픽 엔지니어링을 위한 RH 옵션 처리 기능은 라우터만이 필요로 한다. 그런데, MIPv6는 모든 노드에 RH 옵션 처리 기능을 요구하는 것이 문제이지만, MIPv6의 경우 경유지 노드는 1개만이 필요하므로 경유지 목록 크기가 1보다 큰 경우 패킷을 폐기하는 방법이 적용될 수 있다.

3.2 홈 어드레스 옵션 관련 보안 문제

MIPv4에서는 모바일 노드 MN이 CN에게 패킷을 보낼 때 IP 헤더의 출발지 주소 자리에 CoA를 쓰지 않고 HoA를 사용하였다. 이것은 IPv4의 관점에서 보면 IP 주소 위장에 해당되며, 특히 인터넷 유입점에서 출발지 주소를 엄격히 검사하여 IP 주소 위장 공격을 방지하자는 유입점 필터링[6] 규칙에 위배된다. 이러한 문제를 해소하기 위해 MIPv6에서는 홈 어드레스 옵션을 두어 외지 네트워크에 위치한 MN이 CN에게 보낼 패킷에서 출발지 주소에는 CoA, HAOpt 필드에는 HoA를 표시하며, CN에서의 MobileIP 계층에서 CoA와 HoA를 교환하여 출발지 주소가 HoA인 것처럼 만들고, IP 이상의 계층에서는 MN의 현재 위치에 무관하게 통신을 제공하기 위한 메커니즘이다.

홈 어드레스 옵션은 최종 목적지 노드의 IP 이상의 계층에서 보게되는 출발지 주소와 그 이전의 중간 경유지 노드가 보게되는 출발지 주소가 일치하지 않게되는 문제를 파생시키며, 이는 출발지 주소 기반 방화벽 필터링의 우회에 악용될 수 있다. 그리고, RH 옵션과 결합되어 반사기 공격을 심화시키고, 반사기 공격 방식의 DDoS 공격을 가능하게 만들기도 한다. ITRACE나 IPPT와 같은 패킷 역추적 기법을 방해하며, 특히 반사기 공격에서 출발지 주소 쪽으로 ICMP 역추적 메시지를 보내는 역 ITRACE와 같은 패킷 역추적 기술도 무력화시키는데, 이 때 공격자는 출발지 주소는 자신으로 하되 HAOpt에 공격 대상 노드 주소를 표시함으로써 반사기 노드의 응답은 공격 대상 노드로 향하게 하고 공격 대상 노드에게 전달되어 역추적에 사용되어야 할 역 ITRACE 메시지는 자신이 받아서 폐기하게 된다.

제안된 대책은 홈 어드레스 옵션을 포함하여 패킷이 인증되어 있는 경우와 (CoA, HoA)에 대한 인증된 바인딩이 존재하는 노드에서만 홈 어드레스 옵션을 처리하도록 제한하여 조작된 홈 어드레스 옵션의 사용을 방지하는 방법이다.

4. 결 론

현재 IETF mobileip 작업반에서 토의되고 있는 공식 작업반 인터넷 드래프트에는 18개 문서가 있으며, 이들 외에도 개인적으로 제안된 8개 문서가 있다. 이들 중 가장 핵심적인 문서가 "Mobility Support in IPv6(draft-ietf-mobileip-ipv6-15.txt)"이며, 바로 보안 문제로 인해 IESG에 의해 거부된 문서이다. 3GPP 쪽에서도 이 문서가 표준으로 채택되기를 오래도록 기다리고 있지만, 관련된 보안 문제의 해결 없이는 RFC로 승인하지 않는다는 것이 IESG의 확고한 방침이다. mobileip 작업반에서도 이 점을 인식하고 디자인 팀을 구성하여 신속하게 추진하자는 제안이 있었지만, 현재는 보안 문제에 대해 좀 더 근본적인 접근을 하고 있고 여러 제안들을 두고 검토하는 단계에 있어 최종적 해결 방안의 선정에 이르기까지에는 다소 시간이 걸릴 것으로 예상된다.

BU 보안을 위한 제안들은 가장 강력한 보안 기능을 제공하는 방법이 각 모바일 노드에 지정된 공개키의 해쉬 값의 일부를 주소에 반영하고 Diffie-Hellman 키 교환 방식으로 확립된 키를 사용하여 BU 메시지를 보호하는 SUCV와 CAM-DH 등이다. 반면 보안성은 좀 약하지만 관련 노드들 사이의 통신 경로 밖의 공격자로부터의 보호는 충분히 제공하며 대신 공개키 연산을 전혀 사용하지 않아 가장 적은 계산 비용을 요하는 RR 방식의 보안 메커니즘 BAKE, BUSEC, BU3WAY가 있으며, 이 중간쯤에 Diffie-Hellman 키 교환 방식에 의존하는 DHMIPv6와 SAP 등이 있다. 다양한 방식들에 대한 주요 평가 기준으로는 수동적 공격을 용인할 것인지, 그리고 메커니즘들 사이의 계산 비용 차이가 중요한지, 그리고 SUCV나 CAM-DH 수준의 강한 보안성이 꼭 필요한지 등이었는데, 아직 이들 문제에 대해 뚜렷한 결론이 있었던 것은 아니다.

그리고, 라우팅 헤더 옵션과 홈 어드레스 옵션 등

이 초래하는 보안 문제에 대해서도 여러 다른 대책이 검토되고 있으며, 다른 파생 문제들이 더 나타날지는 좀 더 시간을 두고 분석되어야 할 것으로 평가된다. 무엇보다도 MIPv6는 아직 본격적으로 배치되어 검증된 것이 아니어서 또 다른 형태의 결정적인 보안 취약점이 새로 나타날 가능성을 배제할 수 없다.

참고문헌

[1] Charles E. Perkins, "IP Mobility Support," IETF RFC 2002, October 1996.

[2] Charles E. Perkins, "IP Mobility Support for IPv4," IETF RFC 3220, January 2002.

[3] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," IETF RFC 1971, August 1996.

[4] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," IETF RFC 1970, August 1996.

[5] David B. Johnson and Charles Perkins, "Mobility Support in IPv6," IETF Internet Draft, draft-ietf-mobileip-ipv6-15.txt, July 2001 (work in progress).

[6] Paul Ferguson and Daniel Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," IETF RFC 2267, January 1998.

[7] Stephen Kent and Randall Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 2401, November 1998.

[8] Scott Bradner, *et al.*, "A Framework for Purpose Built Keys (PBK)," IETF Internet Draft, draft-bradner-pbk-frame-00.txt, February 2001 (work in progress).

[9] R. Moskowitz, "Host Identity Payload And Protocol," IETF Internet Draft, draft-moskowitz-hip-05.txt, November 2001 (work in progress).

[10] Pekka Nikander and Charles Perkins, "Binding Authentication Key Establishment Protocol for Mobile IPv6," IETF Internet Draft, draft-perkins-bake-01.txt, July 2001 (work in progress).

[11] Michael Thomas, "Binding Updates Security," IETF Internet Draft, draft-thomas-mobileip-bu-sec-00.txt, November 2001(work in progress).

[12] Erik Nordmark, "Securing MIPv6 BUs using return routability (BU3WAY)," IETF Internet Draft, draft-nordmark-mobileip-bu3way-00.txt, November 2001 (work in progress).

[13] G. Montenegro and C. Castelluccia, "SUCV Identifiers and Addresses," IETF Internet Draft, draft-montenegro-sucv-02.txt, July 2001 (work in progress).

[14] M. Roe *et al.*, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments," IETF Internet Draft, draft-roe-mobileip-updateauth-01.txt, November 2001 (work in progress).

[15] Franck Le and Stefano M. Faccin, "Dynamic Diffie Hellman based Key Distribution for Mobile IPv6," IETF Internet Draft, draft-le-mobileip-dh-00.txt, October 2001 (work in progress).

[16] Mohamed Khalil *et al.*, "Dynamic Security Association Establishment Protocol For IPv6," IETF Internet Draft, draft-mkhalil-mobileip-ipv6-sap-02.txt, October 2001 (work in progress).

[17] P. Savola, "Security of IPv6 Routing Header and Home Address Options," IETF Internet Draft, draft-savola-ipv6-rh-ha-security-01.txt, November 2001 (work in progress).

이 광 수

1981 서울대학교 계산통계학과 졸업
1986 워싱톤대학교 컴퓨터과학과 석사
1990 워싱톤대학교 컴퓨터과학과 박사
1990~현재 숙명여자대학교 정보과학부 교수
관심분야:네트워크 보안, 암호학, 알고리즘
E-mail: rhee@sookmyung.ac.kr