MIPv6에서의 바인딩 갱신 인증

이광수 • 숙명여대 정보과학부

1. 서론

모바일 IP는 컴퓨터가 위치를 이동하여 인터넷 접속점을 변경하면서도 인터넷상의 다른 노드들과의 통신을 계속할 수 있도록 지원하는 것을 목표로 개발된 프로토콜로서 이에 대한 표준화 작업은 IETF (Internet Engineering Task Force)의 mobileip(IP Routing for Wireless/Mobile Hosts) [1] 작업반에 의해 수행되고 있다. 이러한 이동에 수반되는 모든 접속 환경의 변화와 동적인 연결 유지는 자동적으로 이루어져야 하며, 모바일 IP는 이러한 이동성 지원을 IP 계층에서 제공함으로써 전송계층 이상에서의 연결을 유지한 상태에서 물리적 접속을 변경할 수 있도록 허용한다.

모바일 IP에서는 각 모바일 노드에게 홈 네트워크와, 변하지 않는 IP 주소인 홈 어드레스(Home Address; HoA)를 지정한 후, 홈 네트워크의 라우터인 홈 에이전트(Home Agent; HA)를 통해 이동된 위치로 IP 패킷을 중계해 주는 방법이 사용된다. 이동된 위치에서 모바일 노드가 연결되는 네트워크를 외지 네트워크(foreign network)라고 부르며, 외지 네트워크에서 임시로 IP주소를 부여받게 되는데, 이는 의탁주소(care-of address; CoA)라고 불린다. 모바일 노드는 CoA를 홈 에이전트에 등록하게 되며, 이후 모바일 노드의 HoA를 목적지로 하는 IP패킷들은 HA에 의해 현재의 위치인 CoA로 전달되는 방식이 일반적으로 사용된다.

모바일 노드(Mobile Node; MN)에서 상대 노드(Correspondent Node; CN)로 향하는 패킷은 일반 IP에서와 동일하게 직접 전달되는데, CN에서 MN으로 향하는 패킷은 일단 홈 에이전트를 경유하게 된다. MN이 홈 네트워크에서 멀리 떨어져 있을 경우 홈 네트워크를 우회하는 경로는 상당한 전송지연을 초래하게 되며, 이를 삼각 라우팅(triangle routing) 문제라고 한다. 삼각 라우팅으로 인한 비효율성을 개선하기 위해 모바일 IP에서는 경로 최적화 메커니즘을 도입하여 CN이 MN의 위치정보를 가질 수 있도록 하였고, 이를 위해 MN이 CN에게 위치 정보를 전달하는 것을 바인딩 갱신(Binding Update; BU)이라고 한다. 즉, MN이 자신의 <HoA, CoA, BU 유효기간> 을 CN에게 보내면, CN은 이 내용을 바인딩 캐시라는 곳에 저장해 두었다가 MN에게 보낼 패킷이 있으면, 바인딩 캐시를 조회하여 CoA라는 주소를 사용하여 HA를 경유하지 않고 직접 전달

할 수 있게 된다.

그런데, BU 정보의 전달에 있어 적절한 인증이 이루어지지 않을 경우, 거짓 CoA 주소를 포함하는 잘못된 바인딩 갱신이 발생할 수 있으며, 이를 이용하여 CN이 MN에게 보낼 패킷을 엉뚱한 노드에게 전달하는 경로변경 공격이 가능해진다. 이러한 공격의 결과로 특정 노드가 받게 될 패킷들을 다른 노드에게 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 바인딩 갱신이 도입될 경우 비-모바일 노드들도 원격 공격자에 의한 경로변경에 노출되게 되며, 특히 IPv6에서의 이동성 지원을 규정하고 있는 MIPv6 명세[2]는 모든 IPv6 노드들에 대해 MIPv6 지원을 의무화하고 있으므로 인터넷 상의 모든 노드들을 대상으로 하는 공격이 가능해진다.

2001년 3월 미국 미니애폴리스에서 개최된 제50차 IETF 회의직전 mobileip 작업반은 MIPv6 드래프트의 13번째 개정판에 대해 RFC 문서로의 승인을 위해 IESG에 제출하였으나, IESG에 참여하고 있는 보안영역 의장단에 의해 그 도입이 기존의 인터넷 보안환경을 크게 저해할 우려가 있다는 지적을 받고 승인이 보류되었다. 이 때 주로 문제가 된 부분은 경로 최적화를 위해 모바일 노드가 통신 상대노드에게 자신의 현재 위치를 알릴 때 사용되는 바인딩 갱신 메시지의 인증에 관한 것이었으며, 이후 mobileip 작업반에서 이 문제의 해결을 위한 여러 방안들이 논의되어 왔다. 본 고는 그러한 노력을 살펴본다.

본 고의 나머지 부분의 구성은 다음과 같다. 2절에서는 원래의 MIPv6 드래프트에서 채택되었던 바인딩 갱신 인증 메커니즘과 문제점, 그리고 2001년 동안 mobileip 작업반에서 제안되고 토의되었던 여러 인증 메커니즘을 소개한다. 3절에서는 MIPv6 디자인 팀에서 제안되었던 메커니즘들을 종합 평가한 후 최근의 드래프트에서 채택한 보안 메커니즘에 대해 기술하며, 4절에서 향후 작업에 대한 전망과 결론을 싣는다.

2. MIPv6에서의 바인딩 갱신 인증을 위한 초기 메커니즘과 여러 제안들

2.1 MIPv6에서의 바인딩 갱신 인증을 위한 초기 메커니즘

2001년 3월 IESG에 제출된 MIPv6 드래프트에서는 바인딩 갱신 메시지 BU와 바인딩 갱신 확인 메시지 BA 인증을 위해 IPsec 인증헤더(AH; Authentication Header)[3]의 사용을 제안하였다. IPsec AH는 IP 헤더 부분을 포함하는 전체 IP 패킷에 대해 메시지 인증코드(MAC; Message Authentication Code)를 사용하여 패킷의 송신자와 그 내용에 대한 인증, 그리고 재전송 공격 탐지기능 등을 제공하는 강력한 인증 메커니즘이다.

MIPv6에서의 바인딩 갱신에는 모바일 노드 MN이 외지 네트워크에서 받은 의탁 주소 CoA를 홈 에이전트 HA에게 등록하는 것과 경로 최적화를 위해 통신 상대 노드 CN에게 자신의 CoA를 알리는 두 가지 경우가 있다. 이 때, HA에게 보내는 BU 메시지는 MN과 HA의 사전 약속에 의해 정해진 암호키 등을 사용하여 보호하는 것이 용이하며, 실제로 MIPv6에서 HA와 MN 사이의 통신은 인증, 무결성, 기밀성 등의 보호가 제공되는 것으로 가정된다. 그러나, 임의의 통신 상대노드인 CN과 사전에 미리 암

호키 등을 약속해 둔다는 것은 별로 현실적이지 않다. 사전 약속이 없는 임의의 두 노드 사이에 IPsec AH를 사용하기 위해서는 키 교환이 필요하며, 이 경우 안전한 키 교환을 위해서는 인증된 공개키 방식이 필요한데, 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[4] 프로토콜인데, IKE는 너무 많은 메시지의 교환을 요구한다는 점과 또 진행중인 키 교환 상대방에 대한 상태정보의 저장을 필요로 하는 약점을 갖고 있다. 상태정보 저장은 쉽게 메모리 소모를 통한 서비스 거부 공격에 악용될 수 있으며, IKE에 포함된 많은 지수 계산은 분산 서비스 거부 공격에 대한 취약성을 갖는다.

그리고 두 노드 사이에, IPsec 메커니즘의 적용여부는 사전에 설정된 IPsec의 보안정책 데이터베이스에 의해 표현되며, 이 정책항목은 자주 변경되지 않는다. 따라서 두 노드 사이에 AH 메커니즘의 사용이 일단 선택되면, 두 노드 사이의 모든 패킷은 AH 계산 및 확인절차를 거쳐야 하는데, 실제 인증이 필요한 부분은 발생빈도가 극히 낮은 BU/BA 패킷뿐이므로 많은 시간과 대역폭이 낭비되는 결과를 초래한다. 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 보안문제들을 야기할 것으로 우려되며, 바로 이와같은 이유로 MIPv6 문서가 IESG에 참여하는 보안영역 의장단에 의해 거부된 것이다.

2.2 MIPv6에서의 바인딩 갱신 인증을 위한 여러 제안들

바인딩 갱신에 대한 보안의 이상적인 목표는 홈 어드레스가 HoA이고 의탁주소가 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 보안영역 의장단이 제시하고 있는 MIPv6에 대한 최소한의 보안 요구사항도 완벽한 보안성이라기보다는 MIPv6의 도입이 현재의 IPv4의 보안수준을 더 이상 악화시켜서는 안 된다는 것이다. 그리고, 현재까지의 현실성이 있어 보이는 모든 BU 인증 제안들에서 드러나고 있는 정상통신 경로상의 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.

이상과 같은 BU 인증에 대한 요구사항을 충족하는 여러 메커니즘들이 제안되어 2001년 12월 솔트레이크시티에서의 제52차 IETF 총회의 mobileip 회의에서 토의가 진행되었으며, 이러한 작업들을 기초로 MIPv6 바인딩 갱신 보호 메커니즘이 설계되게 된다. 2001년 동안 제안된 8개의 BU 보안 메커니즘은 표 1에서와 같이 크게 3 종류로 구분될 수 있으며, 아래에서 이들을 차례대로 살펴본다.

표 1. BU 인증을 위한 제안들

분류	이름	관련 문서
RR(Return Routability) 사용	BAKE	[5]
	BUSEC	[6]
	BU3WAY	[7]
공개키와 연계된 ID 사용	PBK	[8]
	SUCV	[9]
	CAM-DH	[10]
Diffie-Hellman 키 교환 사용	DHMIPv6	[11]
	SAP	[12]

2.2.1 RR 방식의 BU 보안 메커니즘

BU 보호를 위해 제안된 첫 번째 종류의 인증 메커니즘으로는 CN에서 HA를 경유하여 MN에게 보낸 패킷의 수신여부를 확인하는 RR 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 전송된 값이 제대로 전달되었는지 확인한다. 전달되는 메시지는 암호화되지 않는다. 이 방식은 물론 완벽한 보안을 제공하지는 않는데, 이것은 CN과 HA 사이의 전송경로 상의 임의의 노드 또는 HA와 MN 사이의 전송이 암호화되지 않을 경우 해당 경로상의 임의의 노드가 CN이 MN에게 보낸 메시지들을 볼 수 있기 때문이며, 따라서 이들 노드들은 MN을 위장하는 것이 가능해지기 때문이다.

RR 방식의 메커니즘 중의 하나인 BAKE(Binding Authentication Key Establishment)는 그림 1과 같은 3개의 메시지를 이용하여 BU 인증에 사용될 암호키를 확립하는데, HA와 MN 사이에 보안을 위한 SA가 확립되어 있다고 가정하며 이를 활용한다.

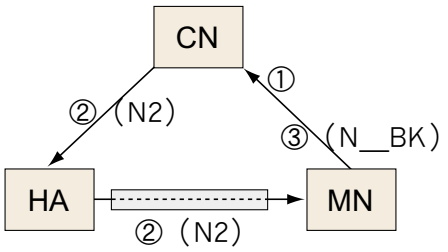

그림 1. BAKE 암호키 확립 모델

그림 1에서 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 받게되는 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 경유해 MN에게 보낸 N2와 MN이 생성하여 CN에게 직접 보낸 N_BK를 이용해 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 확립없이 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 경로상에 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 시험이다. 물론 BU는 바인딩 갱신 메시지이다. N1은 CN만이 알고있는 비밀인 secret을 사용하여 다음과 같이 계산된 인증 토큰이다.

N1 = hash(secret, HoA, CoA, CNA, 타임스탬프, 유효기간)

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 보

안성에 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 비용측면에서는 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 기간동안 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 접속시에는 사전 신뢰를 확보하는 방법이 명시되어 있지 않으며, MN과 HA 사이에 사전 확립된 SA를 활용하지 않는다는 단점도 있다. 그리고, MN과 CN 사이의 통신경로 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 전달방식에 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 비밀키로 Diffie-Hellman 키 교환방식을 사용해서 생성하며, CN이 Diffie-Hellman 키 교환상대에 대한 인증을 위해 MN이 만들어 보낸 공개키 서명을 확인하는 방식을 사용하며, 또한 CN이 MN에게 보내는 Diffie-Hellman 공개 값은 HA를 경유하게 함으로써 부분적인 경로검증까지 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 주소구성에 사용하지 않는다. CAM-DH는 Diffie-Hellman 키 교환방식을 사용하는 점에 있어서는

SUCV와 유사하지만, Diffie-Hellman 키 교환 메시지의 인증을 위해 MN의 개인키에 의한 서명도 사용하고 또 CN이 MN에게 HA 경유여부에 따라 달라지는 두 개의 서로 다른 경로를 통해 전달한 값을 이용하여 생성된 키를 이용한 인증도 사용함으로써 좀 더 철저한 경로검증을 거친다.

SUCV나 CAM-DH는 보안성에 있어서 다른 메커니즘들보다 우수한 것으로 평가받고 있지만 공개키 서명과 Diffie-Hellman이라는 두 가지의 공개키 연산을 포함하고 있어 계산비용이 가장 높은 방식이라는 단점을 갖는다.

2.2.3 Diffie-Hellman 키 교환방식의 BU 보안 메커니즘

세 번째 유형의 BU 보안 메커니즘에서는 BU 보호를 위해 Diffie-Hellman 키 교환방식을 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 주소지정 등을 제외하면 앞 절의 SUCV와 유사하다. Diffie-Hellman 키 교환방식에서도 중개인 공격이 가능하지만, 이를 위해서는 두 가지 전달경로 모두에서 능동적 공격을 요한다. DHMIPv6에서는 HA와 MN 사이에 사전 확립된 SA는 활용되지 않는다. 대신에, AAA(Authentication, Authorization, Accounting) 기반 구조가 제공될 경우 이를 이용한 강한 인증방식이 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 교환방식의 사용은 공개키 연산시간이 좀 많이 걸리기는 하지만 능동적 공격능력이 없는 공격자들로부터의 효과적인 방어를 제공한다는 점에서 RR 방식보다는 대체로 더 안전하다고 볼 수 있다. 그렇지만 공개키 서명이 추가되어 있는 SUCV나 CAM-DH 만큼의 보안성을 제공하지는 않는다.

3. MIPv6 디자인 팀의 바인딩 갱신 인증 메커니즘

MIPv6 디자인 팀에서는 2절에서 소개된 여러 제안들을 비교평가한 후 공개키 암호에 의존하는 방식들이 무선장비 등에서 연산부담이 너무 크고 특히 CGA 방식의 경우 특허문제가 걸려 있어 일단 표준화 대상에서 제외하고, RR 방식을 필수 구현사항으로 권고하기로 결정하였다. 또한 RR 시험을 기존에 제안된 방법들에 비해 다소 강화하는 방향으로 수정하였다. 이 절에서는 먼저 최근의 MIPv6 드래프트[2]에서 채택하고 있는 RR 절차를 먼저 소개한 후, 관련된 보안특성을 기술한다.

3.1 RR 절차

RR 시험과 관련 BU/BA 메시지들이 전달되는 순서는 아래와 같으며, 이 중 메시지 ①과 ②는 동시에 전송될 수 있으며, 메시지 ③과 ④도 동시에 전송될 수 있다. 메시지 ⑤가 BU 메시지이며, 메시지 ⑥이 BA 메시지이다.

① MN(HoA) -> CN: HoTI(HoA, MC1)
② MN(CoA) -> CN: CoTI(CoA, MC2)
③ CN -> MN(HoA): HoT(MC1, K0, j)

④ CN –> MN(CoA) : CoT(MC2, K1, i)
⑤ MN(CoA) –> CN: BU(HoA, MAC, j, i, seq)
⑥ CN –> MN(CoA) : BA(seq)

HoTI(Home Test Init) 메시지는 MN이 HA를 경유하여 CN에서 RR 확인절차의 시작을 알리는 메시지이며 MN의 홈 주소 HoA와 모바일 쿠키 MC1을 전달한다. CoTI(Care-of Test Init) 메시지는 HA를 경유하지 않고 MN에서 CN으로 직접 전달되는 RR 확인절차 시작 메시지이며 MN의 의탁주소 CoA와 모바일 쿠키 MC2를 전달한다.

HoT(Home Test) 메시지와 CoT(Care-of Test) 메시지는 각기 HoTI와 CoTI에 대한 응답으로 해당 메시지에 대한 경로를 따라 역으로 전달되며, K0와 K1은 각각 메시지 인증코드 MAC_{Kcn}(HoA ‖ Nj), MAC_{Kcn}(CoA ‖ Ni)로 계산된다. Kcn은 CN만이 알고 있는 비밀키이며, Ni와 Nj는 CN이 발생시키는 비표이며, CN은 일정 시간동안 동일한 비표 값을 사용하므로 색인 i와 j는 동일한 값일 가능성이 높다. K0와 K1은 메시지 ⑤의 BU 보호를 위한 인증 키 유도에 사용되며, 이는 모바일 노드가 HoT와 CoT를 모두 받을 수 있는 위치에 있음을 증명한다.

메시지 ⑤의 BU 보호를 위한 인증 키 Kbu는 해쉬 값 H(K0 ‖ K1)으로 정의되며, 메시지 ⑤의 MAC은 MAC_{Kbu}(CoA ‖ CNA ‖ BU)로 계산되는데, 여기서 CNA는 CN의 주소를 나타낸다. 그리고, 메시지 ⑤의 seq는 메시지 ⑥의 BA에 대한 약한 인증을 위해 사용될 일련번호를 나타낸다. 메시지 ⑥은 메시지 ⑤의 일련번호 seq를 갖고 돌아가는 것 이외의 다른 인증은 사용하지 않는다.

3.2 RR 절차방법의 보안특성

3.1절의 RR 절차는 2절에서의 RR 절차들에 비해 보안성이 강화되어 있는데, 중요한 특성들을 살펴보면 다음과 같다.

우선 HA와 MN 사이의 중요 정보인 MC1이나 K0 등은 IPsec ESP[13]에 의해 보호된다. 이것은 공격자가 MN 주위의 네트워크에 위치하더라도 ESP가 보호하는 정보를 볼 수 없으므로 공격을 불가능하게 만든다. 그러나, ESP의 보호를 받지 못하는 HA-CN 구간에 위치하는 공격자에 대한 방어는 제공하지 못한다. 이러한 경로상의 공격자에 대한 완전한 방어는 기존의 IPv4나 IPv6에서도 제공하지 못하므로 여기서 문제 삼지는 않는다. 그러나, MIPv6에서의 공격은 공격자가 공격가능 위치를 떠난 후에도 지속된다는 점이 일반 IPv4나 IPv6에서의 공격과의 차이이며, MIPv6 바인딩 갱신 보호의 중요한 지침인 “현재 인터넷 보안상황을 더 악화시켜서는 안 된다”라는 원칙[14]에 반하게 된다. 이러한 이유로 MIPv6 드래프트[2]에서는 RR 절차를 통해 이루어진 BU 정보의 유효기간을 짧게 두고 이 기간이 지나면 다시 RR 절차를 수행하게끔 요구하고 있으며, 유효기간으로는 5분 정도를 제안하고 있다.

그리고, 메시지 ①, ②에 대한 응답 메시지 ③, ④가 원래 메시지 출발지 주소로 돌아가는 대칭적 메시지 교환을 사용하는 것에는 CN이 서비스 거부 공격의 경유지로 사용되는 반사 공격(reflection attack)을 방지하기 위한 목적도 있다. 그리고, CN은 BU가 이루어질 때까지 각 요청에 따른 어떠한 상태정보도 기억할 필요가 없는 방식으로 작동함으로써 상태 저장공간의 소모를 이용하는 서비스 거부 공격을 방지한다. 그리고, 복잡한 연산을 요하는 공개키 암호를 사용하지 않음으로 해서 CPU 소모를 통한 서비스 거부 공격도 방지하고 있다.

BU 메시지에 대한 재전송 공격은 BU에 포함된 인증된 일련번호를 통해 방지될 수 있는데, 만일 CN에서 BU를 삭제한 후에는 일련번호에 의한 재전송

탐지가 불가능하다. 그러나, CN에서 비표를 충분히 자주 변경한다면 비표가 재전송 탐지에 사용될 수 있다.

4. 결론

모바일 노드가 자신의 현재 위치를 알리는 바인딩 갱신은 홈 에이전트에 대한 것과 임의의 통신 상대 노드에 대한 것이 있으며, 이 중 홈 에이전트에 대한 것은 IPsec ESP에 의해 충분히 보호되고 있다. 다만, 홈 에이전트가 재부팅되면서 재전송 방지를 위해 사용되는 일련번호를 잃어버리는 경우 재전송이 가능하지만 이 경우에도 IPsec 관련 키 관리 메커니즘의 사용으로 재전송 공격을 방지할 수 있다.

임의의 통신 상대노드에 대한 바인딩 갱신은 RR 절차를 사용하는 인증방법을 사용한다. 이 방법은 홈 에이전트와 상대노드 사이의 경로상에 위치하는 공격자는 막을 수 없지만 그 이외의 위치에 있는 공격자는 막을 수 있다. 그리고, 공격자가 떠난 후 공격효과의 지속을 막기 위해 바인딩 갱신의 유효기간을 짧게 주는 방법이 채택되어 있다. 그러나, RR 절차보다 보안성이 우수한 실용적인 방법이 개발될 경우 RR 절차와 새로운 방식 중에서 선택할 수 있는 장치가 필요하다.

그리고, PKI나 AAA 등의 기반구조가 제공되는 환경에서 이들을 활용하는 강한 바인딩 갱신 인증방식, 특히 IPsec의 사용에 의한 인증 등에 대한 작업도 필요할 것으로 전망된다.

참고문헌

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

[2] David B. Johnson et al., "Mobility Support in IPv6," IETF Internet Draft, draft-ietf-mobileip-ipv6-17.txt, May 2002 (work in progress)

[3] Stephen Kent and Randall Atkinson, "IP Authentication Header," IETF RFC 2402, November 1998

[4] D. Carrel and D. Harkins, "The Internet Key Exchange (IKE)," IETF RFC 2409, November 1998

[5] 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)

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

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

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

[10] 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)

[11] 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)

[12] 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)

[13] Stephen Kent and Randall Atkinson, "IP Encapsulating Security Payload (ESP)," IETF RFC 2406, November 1998

[14] Allison Mankin et al., "Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6," IETF Internet Draft, draft-ietf-mobileip-mipv6-scrty-reqts-02.txt, November 2001 (work in progress)

저자 약력

1981년	서울대학교 계산통계학과 이학사
1986년	와싱톤대학교(세인트루이스) 컴퓨터과학과 이학석사
1990년	와싱톤대학교(세이트루이스) 컴퓨터과학과 이학박사
1990년 ~ 현재	숙명여대 정보과학부 교수
2000년 ~ 현재	OSIA 보안 TG 의장

▶ 관심분야 : 네트워크 보안, 암호학, 인터넷 보안기술 표준