주 제

IPv6 기반의 이동인터넷 보안 기술

목포대학교 김현곤

차례

I. 서 론

이동인터넷이란 모바일 장치가 이동하는 중에도 자신이 초기에 할당 받은 영구적인 홈 주소를 유지하면서 인터넷 서비스를 끊김 없이 제공받을 수 있는 기술이다. IPv6 주소체계를 갖는 네트워크에서 이동인터넷을 가능하게 해 주는 대표적인 프로토콜로서 Mobile IPv6 (MIPv6)를 들 수 있다[1]. 유선 환경에서 IPv6 노드가 이동하게 되면 그 노드가 속해있는 서브넷이 바뀌게 되므로 초기에 할당 받은 홈 주소가 바뀌어야 하고, 그 결과로 현재 진행중인 응용 세션이 단절되게 된다. MIPv6 프로토콜은 이러한 주소의 변경을 응용 단으로부터 감추어줌으로써 끊김 없는 응용서비스를 제공하고자 하는 것이다.

MIPv6 프로토콜 및 관련 보안 기술은 IETF에 의해 표준화가 완료된 상태이다[1-2]. 그러나 MIPv6 보안 메커니즘으로 채택된 RR(Return Routability)이 안전한 초기시동을 위한 보안연계 설정의 어려움과 이동노드에 대한 리다이렉트 공격에 취약함이 밝혀졌으며, 이를 해소하기 위한 여러 측면의 보완 기술들이 현재 표준화에서 논의되고 있다. 결과적으로 보안 문제가 MIPv6의 상용화에 걸림돌로 작용하고 있는 것이다.

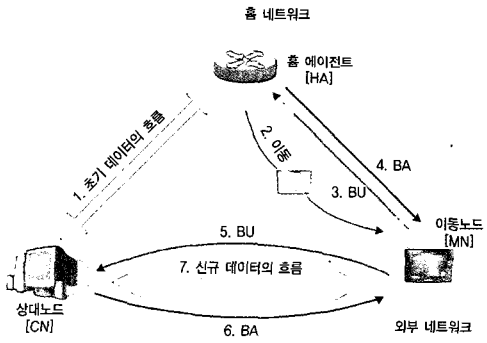
이와 관련하여 최근 RR을 대처할 수 있는 3GPP2 (3rd Generation Partnership Project 2) 네트워크 인증 메커니즘이 이동통신 진영의 시스코, 노텔, Starent 네트워크사에 의해 표준화 되었다[3]. 이 메커니즘은 이동통신과 같은 한정된 네트워크에 적합하며 3GPP2 표준화에도 반영된 상태이다[4]. 기존 Mobile IPv4의 공유키 기반의 인증 메커니즘과 유사하다. IPsec을 적용하지 않음으로 인한 부하 경감, 이동통신 계층 2의 별도 채널(out-of-band)을 통한

보안연계 설정의 용이함, 동적 홈 에이전트와 홈 주소가 설정되는 환경에 적합, 백 엔드 서버와의 보안연계를 통한 인증 등의 장점들을 가진다. 따라서 셀룰러 시스템인 UMTS, cdma2000, WiBro 등에서 RR을 적용하지 않고 3GPP 네트워크 인증 메커니즘을 적용할 가능성이 커졌다.

본 고에서는 IPv6 환경에서 안전한 이동인터넷을 위한 MIPv6의 보안 기술에 대한 최근의 이슈와 연구동향을 살펴보고자 한다. 제 2장에서는 MIPv6의 개요와 프로토콜 도입에 따른 새로운 보안 취약점들을 간략하게 기술한다. 제 3장에서는 기본적인 보안 메커니즘인 RR을 동작 흐름 위주로 기술하고 제 4장에서는 최근에 표준으로 채택된 3GPP2 네트워크 인증 메커니즘을 보다 구체적으로 다룬다. 그리고 제 5장에서는 최근 이슈화 되고 있는 보안 기술과 이와 관련된 표준화 동향을 알아본다.

II. Mobile IPv6 및 보안 위협

MIPv6 동작 흐름을 (그림 1)에 나타내었다. 초기에 홈 서브넷에서 이동노드(MN; Mobile Node)는 홈 주소를 가지고 통신 상대인 상대노드(CN; Correspondent Node)와의 통신을 이룬다. 이 때, 트래픽은 MN과 CN간에 직접 라우팅 된다(1). MN이 새로운 서브넷 영역으로 진입하면(2) MN은 자신의 이동 사실을 인지하고 해당 서브넷의 임시주소(CoA; Care-of Address)를 할당 받거나 또는 IPv6의 주소 자동 설정(auto-configuration) 기능을 이용하여 임시주소를 할당 받는다. 이후 자신의 위치를 등록시키기 위해 BU(Binding Update) 메시지를 홈 에이전트(HA; Home Agent)로 전송하여 자신의 임시주소를 HA에게 등록시킨다(3). BU를 수신한 HA는 MN 인증을 수행하고, 인증이 성공적이면 바인딩 캐쉬 앤트리에 MN을 등록하고 BA (Binding Acknowledgement) 메시지로 응답한다(4). 이 때, CN은 MN의 임시주소를 알 수 없으므로 이전의 홈 주소를 목적지 주소로 하여 트래픽을 전달한다. MN이 이동하였음을 알고 있는 HA는 홈 서브넷에서 트래픽을 가로채어 MN에게 전달한다. 이후에 MN은 CN과 직접 통신을 위해 CN에게 등록을 요청을 하고(5) 이에 대한 응답이 이루어진다(6). 위치 등록이 정상적으로 이루어지면 MN은 HA를 거치지 않고 CN과 직접 통신을 이룬다(7). 상기와 같이 MN의 서브넷간 이동이 발생할 때마다 위치 등록 절차가 정상적으로 수행된다면 MN은 자신의 위치와 무관하게 기존의 응용 세션을 유지하면서 인터넷 서비스를 끊김 없이 제공받을 수 있다.



(그림 1) MIPv6 동작 흐름

MIPv6의 보안 위협을 살펴보면, 주요한 위협은 MN의 위치 등록을 하기위해 주고 받는 BU 메시지로 인해 발생한다. 공격자는 BU 메시지를 위변조하고 이를 이용하면 서비스 거부 공격, 중재자 공격(man-in-the-middle attack), 하이재킹, 플러딩 등의 공격을 쉽게 할 수 있다. <표 1>에 MIPv6 도입에 따라 초래될 수 있는 보안 취약성을 나타내었다[5].

2.1 바인딩 업데이트로 인한 보안 위협

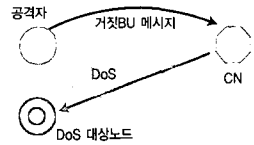
MN은 CN에게 패킷을 전송할 때 패킷의 소스 주소로 자신의 임시주소를 사용하고 홈 주소를 넣어서 전송한다. 이를 수신한 CN은 소스 주소와 HAO (Home Address Option)내의 두 주소를 교체하여 사용한다. 이를 이용해 가능한 공격은 크게 MN이 BU 메시지를 HA로 전송할 때와 CN으로 전송할 때로 구분할 수 있다.

전자의 경우, MN이 HA로 BU 메시지를 전송할 때 공격자가 MN에 대해 현재 위치가 아닌 다른 위치에 있다는 거짓 정보를 주고 HA가 이 정보를 받아들인다면, MN은 패킷을 받지 못하는 반면, 다른 노드는 원하지 않는 패킷을 수신하게 된다. 후자의 경우, MN이 CN으로 BU 메시지를 전송할 때, 공격자가 자신의 홈 주소를 희생자의 홈 주소로 설정하여 거짓 정보를 알릴 경우, CN에서 희생자로 전송되는 패킷은 공격자를 거치게 되므로 가용성과 기밀성이 모두 보장 받기 어렵다. 그리고 공격자가 자신의 임시주소를 거짓으로 알리는 경우, CN이 MN으로 보내는 패킷들은 모두 거짓 임시주소로 전송되므로 서비스 거부 공격을 당할 수 있다.

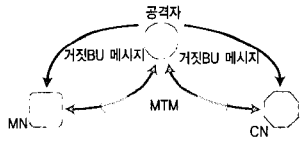
〈표 1〉 MIPv6의 보안 취약성

구 분	보안 취약성
바인딩 업데이트(BU)	• HA로의 BU 메시지에 대한 취약성 • CN과의 루트 최적화에 대한 취약성 • CN이 다른 노드로의 반사 공격의 시발점으로 사용될 수 있는 취약성
홈 어드레스 옵션(HAO)	• 보안 기법들을 위한 고비용의 암호 알고리즘을 불필요하게 실행시키도록 하는 등의 공격을 받을 수 있음
라우팅 헤더	• MIPv6를 사용하는 IPv6 헤더가 FW상의 규칙에 기반한 IP 주소를 우회하거나 타 노드들로부터 트래픽을 반사시키는데 사용될 취약성
터널링(IP 헤더)	• MN과 HA간의 터널에 MN이 트래픽을 보내는 것처럼 보이게 하는 공격으로 인한 취약성

BU 메시지를 이용한 공격에 있어서 공격자의 위치에 따라 가능한 공격들을 살펴본다. 먼저 공격자가 임의의 위치에 있을 때 가능한 공격을 세가지로 분리하여 설명한다. 첫째, 공격자는 MN의 홈 주소와 CN의 주소를 알고 있어 잘못된 임시주소가 담긴 BU 메시지를 CN에게 보내어 해당 임시주소를 가진 노드에게 서비스 거부 공격이 발생하도록 유도할 수 있다. 또한, 공격자가 BU 메시지를 MN과 CN에게 보내어 MN과 CN상에 교환되는 메시지를 중간에 가로채거나 변조할 수 있다.

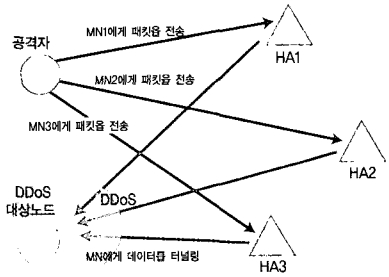


(그림 2) 임의의 위치에서의 보안 위협 1



(그림 3) 임의의 위치에서의 보안 위협 2

둘째, CN으로 의미 없는 BU 메시지를 일시에 대량으로 전송하여 CN의 자원을 고갈시켜 정상적인 패킷 처리를 할 수 없게 한다. 셋째, (그림 4)와 같이 잘못된 임시주소를 가진 BU 메시지를 HA들에게 보냄으로써 HA가 MN의 잘못된 임시주소를 가지도록 한다. 공격자는 각 MN의 HA에게 MN으로 보낼 메시지를 보내고 HA는 자신이 가지고 있는 MN의 거짓



(그림 4) BU 메시지의 임시주소 위조 예

임시주소로 데이터를 터널링 한다. 따라서 공격자는 자신을 숨기면서 실제 임시주소를 가진 노드에게는 분산 서비스 거부 공격을 할 수 있다.

공격자가 MN과 동일 위치에 있을 때 가능한 공격으로서, 공격자가 MN과 같은 서브넷 상에서 MN의 BU 메시지를 관찰하여 CN에게 거짓 BU 메시지를 보낸다. 이를 이용하여 공격자는 거짓 BU 메시지 내에 임시주소로 지정된 노드를 대상으로 서비스 거부 공격을 할 수 있다. 공격자가 HA와 동일 위치에 있을 때 가능한 공격으로서, MN이 HA 영역에 있을 때 공격자는 MN과 같은 서브넷에 존재하기 때문에 CN을 쉽게 알 수 있다. 이를 이용하여 공격자는 거짓의 BU 메시지를 CN에게 보낸다. 따라서 거짓의 임시주소를 가진 노드는 서비스 거부 공격을 당할 수 있다. 마지막으로 공격자가 MN과 CN 사이에 위치에 있을 때 가능한 공격으로서, 공격자가 MN의 BU 메시지를 CN에게 대신 보냄으로써 자신을 MN과 CN 경로상에 위치하도록 하여 중간에서 교환되는 데이터를 도청하거나 변조할 수 있다.

2.2 홈 어드레스 옵션

MIPv6에서는 외부 네트워크에 위치한 MN이 CN에게 패킷을 보낼 때, 패킷의 소스 주소에는 임시주소를 HAO 필드에는 홈 주소를 지정한다. 이를 수신한 CN은 MIP 계층에서 임시주소와 홈 주소를 교환하여 소스 주소가 홈 주소인 것처럼 함으로써 IP 이상의 계층에서는 MN의 현재 위치에 무관하게 통신을 가능하게 해 준다.

이와 같이 MN이 홈 주소를 사용할 경우에 공격자는 HAO를 이용하여 서비스 거부 공격을 할 수 있다. 공격자가 전송 패킷의 HAO 필드에 공격대상 주소를 넣어 전송하면 CN은 그 주소로 응답하게 된다. 따라서 CN을 이용하여 특정 노드를 서비스 거부 공격 할 수 있다. 또한, 암호화 통신을 수행하는 환경에서는 공격대상 노드들에게 불필요한 암호 알고리즘을 수행하게 하여 계산 부하를 가중시킬 수 있다.

2.3 라우팅 헤더

라우팅 헤더는 상위계층 간의 투명한 통신을 위해서 MIPv6 환경에서 CN이 MN으로 패킷을 전송할 때 사용된다. 또한 멀티호밍 환경에서 라우팅 헤더의 소스 라우팅을 이용하여 동적으로 ISP를 선택할 수 있다. 일반적인 타입 0의 라우팅 헤더는 호스트나 라우터에서 모두 처리 가능하며 다수의 주소가 동시에 지정되어 전송될 수 있기 때문에 반사 공격(reflection attack)에 이용될 수 있다.

2.4 터널링

HA와 MN간 터널링을 이용한 공격이 가능하다. 만약 알 수 없는 노드가 터널링된 패킷 내부 헤더의 MN의 목적지 주소에 거짓 주소를 포함시켜 HA에게 보낸다면 HA는 해당 패킷을 거짓 주소를 갖는 MN에게 전달한다. 이를 이용하여 서비스 거부 공격이 가능하다.

III. Return Routablity 인증

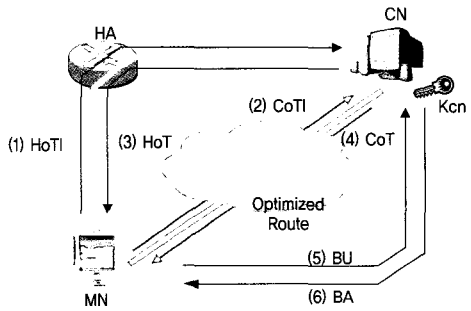
제 2장에서 기술한 보안 취약점들을 해결하기 위해서 MIPv6에서는 MN과 HA간에는 IPsec을 적용하도록 하고 MN과 CN간에는 새롭게 제안한 RR 인증 메커니즘을 적용하도록 권고하고 있다. RR은 동적 보안연계를 설정하며 적합한 MN이 CN에게 BU 메시지를 보내는지 반대로 적합한 CN이 MN에게 BA 메시지를 보내는지를 검증한다. 즉, 홈 주소와 임

〈표 2〉 RR의 신호 메시지 및 파라미터

순서	신호 메시지	파라미터	방 향	내 용
(1)	HoTI (Home Test Init)	- Home Init Cookie	MN→HA→CN	RR 초기화(HoA)
(2)	CoTI (Care-of Test Init)	- Care-of Init Cookie	MN→CN	RR 초기화(CoA)
(3)	HoT (Home Test)	- Home Init Cookie - Home Keygen Token - Home Nonce Index	CN→HA→MN	(1)에 대한 응답
(4)	CoT (Care-of Test)	- Care-of Init Cookie - Care-of Keygen Token - Care-of Nonce Index	CN→MN	(2)에 대한 응답
(5)	BU	- Nonce indices - MAC, Sequence #, CoA	MN→CN	바인딩 정보 알림
(6)	BA	- Type2 Routing Header - MAC, Sequence #, status	CN→MN	바인딩 응답 알림

시주소에 대해서 각각 Reachability와 Validity를 체크 한 후, BU 메시지를 전송함으로써 BU 권한을 가진 MN을 인증할 수 있고 이를 통해 안전하게 위치 등록 과정을 수행한다.

RR에 정의된 신호 메시지와 파라미터를 <표 2>에 나타내었다. RR의 동작 흐름을 (그림 5)에 나타내었으며 다음과 같이 동작한다.



(그림 5) RR 의 동작 흐름

(1) MN은 메시지 구별자로 사용되는 64비트 쿠키 즉, Home Init Cookie와 Care-of Init Cookie를 생성한다. 이 쿠키는 전송한 HoTI/CoTI 메시지와 수신한 HoT/CoT 메시지가 같은 쌍인지 확인하는데 사용된다. 즉 HoTI/HoTI 메시지를 수신하지 않는 노드가 응답하는 것을 방지한다.

(2) 이를 수신한 CN은 두개의 토큰 즉, Home Keygen 토큰과 Care-of Keygen 토큰을 생성한다. Kcn은 CN이 MN에게 보내는 Keygen 토큰을 생성하기 위한 20비트 비밀 키이며, CN에 의해서 생성된다. 넌스 인덱스는 Keygen 토큰을 생성하기 위한 seed로서 재생공격을 방지하기 위해 사용된다. 넌스 인덱스가 MN에게 전해지고, MN은 BU 전송 시 넌스 인덱스를 CN에게 전달하여 CN이 다시 Keygen 토큰을 생성한 후 Kbm을 만들 수 있도록 한다. 유효기간이 만료된 넌스는 파기하며 MN으로부터 파기된 넌스를 가진 메시지를 수신하면 해당 메시지는 무시한다. Kbm은 추후 BU 메시지의 인증을 위해 사용되며 아래와 같이 계산한다. 한편, CN은 인증이 완성되기 전까지 바인딩 캐시를 할당하지 않는다.

Home Keygen Token = *First (64, HMAC_SHA1 (Kcn, (Home Address, HoA nonce, 0)))*
Care-of Keygen Token = *First (64, HMAC_SHA1 (Kcn, (Care-of Address, CoA nonce, 0)))*
Kbm = *SHA1(Home Keygen Token, Care-of Keygen Token))*

(3) BU가 완료되면 CN은 메시지를 HA 를 거치지 않고 직접 MN으로 보내기 때문에 MN이 정당한 노드인지를 검증하는 것이 필요하다. 이 메시지를 통해 CN은 두 경로로 동시에 보낸 패킷들 즉, Keygen 토큰을 생성하기 위한 seed들을 MN이 잘 수신했는지 판단할 수 있다.

(4) MN은 수신된 Keygen 토큰들을 가지고 Kbm을 생성한다. 생성된 Kbm은 BU 메시지의 MAC을 계산하는데 입력으로 사용된다.

BU MAC = *First(96, HMAC-SHA1(Kbm, Sequence Number, Home Address Nonce Index, Care-of Nonce Index))*

(5) 계산된 BU MAC은 아래와 같이 BU 메시지의

파라미터로 포함되어 CN으로 전달되며 CN은 BU MAC을 계산하여 메시지 인증을 수행한다.

BU 메시지 = *(Home Address Option, BU MAC, Sequence Number, Home Address Nonce Index, Care-of Nonce Index)*

(6) CN은 정당한 MN에 의한 BU 메시지를 인증한 후에 BA 메시지로 응답한다. 이 때 2.3절에 기술된 라우팅 헤더에 의한 위협을 제거하기 위해서 새롭게 정의한 Type 2 라우팅 헤더를 적용한다. 상기의 RR 절차가 정상적으로 완료되면 트래픽은 HA를 거치지 않고 최적화 루틴인 MN과 CN 간에 직접 전송된다.

IV. 3GPP2 네트워크 인증

MIPv6 기본 규격에서는 MN과 HA간에 신호메시지를 보호하기 위한 수단으로 IPsec을 적용한다. 그러나 3GPP2의 인증 메커니즘은 MN과 HA간 IPsec 보안연계 설정과는 무관하게 적용할 수 있다[4]. 따라서 MN은 IPsec 모듈을 접목시키지 않고도 MIPv6를 구현할 수 있다. 이 메커니즘에서는 MN과 HA간에 BU와 BA 메시지에 새로운 이동성 메시지 인증 옵션(mobility message authentication option)을 추가하여 두 메시지를 보호한다. 한편, 이 옵션이 HA가 MN을 인증하기 위해 사용될 경우에는 RR 메시지의 기밀성과 모바일 프리픽스 발견 메시지의 인증 및 무결성 보호는 제공되지 않는다.

4.1 적용 가능한 네트워크

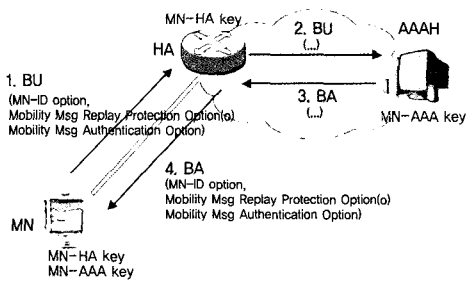
3GPP 네트워크 인증은 아래와 같은 특성을 갖는 네트워크에 적용할 수 있다. 적합한 네트워크의 한가지 예로서 3GPP2의 CDMA 네트워크를 들 수 있다[4].

- 네트워크 엑세스를 위한 MN의 인증이 HA와 연결된 홈 네트워크의 인증 서버에 의해 수행되는 네트워크에 적합하다. MN과 백 엔드 서버 즉, 홈 AAA 서버(AAAH; Home Authentication, Authorization, and Accounting) 사이의 보안연계는 네트워크 운영자에 의해 사전 설정된다. HA의 할당이 동적이고, 보안연계가 정적이거나 long-term 일 경우에 적용 가능하다.
- MN이 동적 HA 할당이나 홈 주소 할당을 필요로 하는 네트워크에 적합하다. 할당은 세션별로 또는 MN의 파워 업 별로 될 수 있다. 이 경우 MN은 NAI(Network Access Identifier) [6]와 같은 식별자를 사용한다. 따라서 초기 시동 정보를 얻기 위해서는 AAA 서버[7]와 보안연계가 필요하며 이 때, 보안연계는 별도의 채널(out-of-band)에 의해 지정될 수 있다. CDMA 환경에서, 이러한 정보는 AAA exten-sion과 액세스 링크상에서 PPP 또는 DHCPv6 extension을 통해 네트워크 액세스 인증 동안에 이루어질 수 있다.
- 일부의 MN과 HA들만이 IKEv2 기능을 가진 상태에서 벡엔드 AAA 인프라와 IKEv2를 접목시킬 수 있는 네트워크에 적합하다. 그러나 IKEv2가 기술적으로 미완성된 상태이고 대규모 스케일의 상업적인 설치를 필요로 하고 있지 않기 때문에 운영자의 입장에서는 IKEv2가 접목된 MIPv6를 설치하기에는 부담스러울 수 있다.
- MIPv6 서비스를 위한 사용자의 식별과 인증/권한 검증을 전적으로 백엔드 AAA 인프라에 의존하는 네트워크에 적합하다.
- MN과 홈 AAA 서버 사이에 별도의 채널을 통해 보안연계가 설정되며 키 교환 프로토콜을 사용하지 않는 네트워크에 적합하다.
- 셀룰러 네트워크와 같이 대역이 한정되고 무선 인터페이스상에 교환되는 신호 메시지의 수를 최소

화해야 하는 네트워크에 적합하다. MN과 HA간 보안연계를 설정하기 위해 IKE를 이용하는 경우에는 MIPv6 시그널링의 신호 메시지의 수가 많아진다. 그러나 이와 비교해서 3GPP2 네트워크 인증 메커니즘은 상대적으로 그 수를 최소화 시킬 수 있다.

4.2 동작 흐름

3GPP2 네트워크 인증 절차를 (그림 6)에 나타내었다. HA가 MN을 인증하기 위해서는 MN은 자신의 식별자로서 MN-NAI *mobility option*[6]의 이동 노드 식별자 옵션을 지정해야 한다. MN은 인증 데이터를 전송하기 위해 4.3절에 기술된 이동성 메시지 인증 옵션을 사용한다. 이 때 MN과 HA는 다수의 mobility 보안연계들을 인덱스 하기 위해 Mobility SPI를 지정한다. 그리고 MN은 BU 메시지에 추가적인 재생공격을 막기 위해서 4.5절에 정의된 이동성 메시지 재생공격 방지 옵션을 포함시킬 수 있다. 한편, HA와 AAAH간에 인터페이스는 현재까지 정의되지 않은 상태이다.

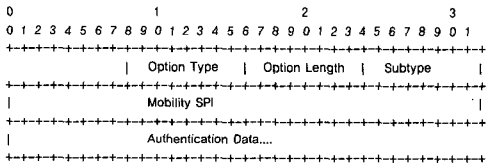


(그림 6) 3GPP2 네트워크 인증 메커니즘

4.3 이동성 메시지 인증 옵션

이 절에서는 BU와 BA 메시지를 보호하기 위해 사용될 이동성 메시지 인증 옵션을 정의한다. 이 옵션은 IPsec과 동시에 사용될 수도 있으며 또한, IPsec이 없는 환경에서도 BU 및 BA 메시지를 인증하기 위한 또 다른 메커니즘으로 사용될 수 있다.

인증 모드와 메시지를 인증하는 상대 엔티티를 구분하기 위해 두개의 서브 타입이 정의된다. 서브 타입 1은 MN-HA 이동성 메시지 인증 옵션이고 서브 타입 2는 MN-AAA 이동성 메시지 인증 옵션이다. 추가적인 서브 타입들이 추후에 정의될 수 있다. 메시지 내에 하나의 이동성 메시지 인증 옵션 인스턴스는 동일한 서브 타입 을 가질 수 없다. 즉, 하나의 메시지는 각기 다른 서브 타입 번호들을 갖는 다수의 이동성 메시지 인증 옵션 인스턴스를 포함한다. 만약 MN-HA와 MN-AAA 인증 옵션이 동시에 존재한다면 MN-AAA 인증 옵션 이전에 MN-HA 인증 옵션이 반드시 존재해야 한다. 그렇지 않으면 HA는 이 메시지를 무시해야 한다. 엔티티가 이동성 메시지 인증 옵션을 사용하는 것으로 설정되었거나 또는 이 옵션을 위해 공유키 기반의 보안연계가 설정된 상태에서 이 옵션이 지정되지 않은 BU와 BA 메시지를 수신하면 수신된 메시지는 무시한다.



(그림 7) 이동성 메시지 인증 옵션

4.3.1 MN-HA 이동성 메시지 인증 옵션

이 옵션은 MN과 HA간에 사전에 설정된 shared-key-based 보안연계를 기반으로 BA 및 BU 메시지를 인증하기 위해 사용되며 포맷은 (그림 7)과 같다. 이 규격에서 정의된 MN과 HA간 shared-key-based mobility 보안연계는 Mobility SPI, 키, 인증 알고리즘, 재생공격 방지 메커니즘으로 구성된다. 키

는 임의의 값으로 구성되며 길이는 16 옥텟이다. 인증 알고리즘은 HMAC-SHA1을 사용한다. 재생 공격 방지를 위한 메커니즘은 MIPv6 기본 규격[8]에 정의된 시퀀스 번호를 사용하거나 4.5절에 정의된 타임 스탬프 옵션을 사용한다. 타임 스탬프 옵션을 사용할 경우에 mobility 보안연계는 클럭 변화를 계산하기 위해 'close enough' 필드를 포함한다. 디폴트 값은 7초가 지정되어야 하며 최소한 3초보다 커야 한다. 인증 데이터(Authentication Data)는 메시지내 이동성 헤더(Mobility Header)부터 시작해서 이 옵션의 Mobility SPI까지 즉, 이 옵션의 인증 데이터 전까지 계산된다.

Authentication Data = *First(96, HMAC_SHA1(MN-HA Shared key, Mobility Data))*
Mobility Data = *(care-of address | home address | Mobility Header (MH) Data)*

MH Data는 이동성 헤더부터 이 옵션의 Mobility SPI 필드까지의 내용이다. 이동성 헤더의 체크섬 필드는 상기의 Mobility Data를 계산하기 위해 반드시 0으로 지정되어야 한다. MAC 결과로부터 도출된 첫 번째 96 비트는 인증 데이터 필드로서 사용된다.

프로세싱 고려사항은 다음과 같다. MN과 HA는 사전에 shared-key-based 보안연계를 가지고 있다고 가정한다. MN이 만약 HA와 shared-key-based mobility 보안연계가 설정되어 있다면 BU에 이 옵션을 반드시 포함시켜야 한다. HA는 수신한 BU 메시지에 이 옵션이 포함되어 있고, 자신이 MN과 shared-key-based mobility 보안연계가 설정되어 있다면 이 옵션을 반드시 포함시켜야 한다. 이 옵션을 수신한 MN 또는 HA는 인증 데이터를 반드시 검증해야 한다. 만약 인증이 실패하면 HA는 상태 코드가 MIPv6-AUTH-FAIL을 갖는 BA 메시지를 응답해야 한다. 만약 HA가 shared-key-based mobility 보안연계를 갖고 있지 않다면 HA는 BU를 무시해야 한다. HA는 이 경우 실패 이벤트를 로깅한다.

4.3.2 MN-AAA 이동성 메시지 인증 옵션

이 옵션은 홈 망에 있는 AAA 서버와 MN간에 shared mobility 보안연계를 기반으로 BU 메시지를 인증하기 위해 사용되며 포멧은 (그림 7)과 같다. 이 옵션을 갖는 BU는 홈 망의 AAAH 서버에 의해 인증된다. 이의 응답인 BA 메시지는 MN-HA 이동성 메시지 인증 옵션을 이용하여 인증되어야 한다. 이 옵션은 반드시 이동성 헤더를 갖는 메시지의 마지막 옵션이 되어야 한다. 이에 대한 응답은 MN-HA 이동성 메시지 인증 옵션을 포함해야 하며 MN-AA 이동성 메시지 인증 옵션은 포함되지 않아야 한다. MN은 HA가 AAA 인프라를 사용할 수 있도록 하기 위해서 RFC 4283에 정의된 NAI를 사용한다.

인증 데이터는 메시지내 이동성 헤더부터 시작해서 이 옵션의 Mobility SPI까지 즉, 이 옵션의 인증 데이터 전까지 계산된다. 인증 데이터는 아래와 같이 계산한다.

Authentication Data = *hash_fn(MN-AAA Shared key, MAC_Mobility Data)*
SPI = *HMAC_SHA1_SPI*
Mobility Data = *SHA1(care-of address | home address | MH Data)*

해쉬 함수는 MN-AAA 이동성 메시지 인증 옵션 내에 지정된 Mobility SPI 값에 의해 결정된다. 만약 Mobility SPI가 HMAC_SHA1_SPI를 갖는다면 해쉬 함수는 HMAC_SHA1이다. HMAC_SHA1_SPI가 사용되는 경우 AAA는 HMAC_SHA를 이용하여 BU를 인증한다. 마찬가지로 MH Data는 이동성 헤더부터 이 옵션의 Mobility SPI 필드까지의 내용이다. 프로세싱 고려사항으로서 홈 망에 있는 AAAH와 HA간에는 안전한 채널을 통해 통신이 이루어진다고 가정한다.

4.4 MN에서 인증 실패 검출

MN과 HA간에 인증을 위해 shared-key-based mobility 보안연계가 설정된 상태에서 인증이 실패하면 HA는 반드시 상태코드 MIPv6-AUTH-FAIL을 갖는 BA 메시지를 MN에게 송신해야 한다. 만약 shared-key-based mobility 보안연계가 없다면 HA는 BU를 포기한다. 이 경우 HA는 실패 이벤트를 로깅한다. MN은 상태코드 MIPv6-AUTH-FAIL을 갖는 BA 메시지를 수신하면 새로운 BU 메시지를 HA에게 송신하는 것을 정지한다.

4.5 이동성 메시지 재생공격 방지 옵션

이 옵션은 이동성 메시지 인증 옵션을 사용하여 인증이 이루어질 경우에 BU 및 BA 메시지에 적용된다. 목적은 BU가 MN에 의해 적시(freshness)에 생성되었으며 공격자에 의해 이전 BU들로부터 재생되지 않았음을 검증하기 위해 사용된다. HA에서 바인딩 엔트리가 삭제된 후에 MN에 대한 상태 정보가 없는 경우에 유용하다.

HA는 BU 인증이 성공하면 이후에 재생공격 여부를 체크하지 않는다. 이 옵션을 사용하면 MN은 BU에 대응하는 BA를 매칭시킬 수 있으며 shared-key-based mobility 보안연계의 일부분으로 활용할 수 있다. 그리고 이 옵션이 사용되면 BU내에 시퀀스 번호 필드는 사용되지 않아야 한다. HA의 정책이 이 옵션을 사용하여 재생공격 방지를 강제하고 MN이 이 옵션을 포함하지 않는 BU를 보내오면, HA는 BU를 무시하고 BA에 MIPv6-MESG-ID-REQD를 상태코드로 지정하여 응답한다. HA가 이 옵션이 지정된 BU를 수신하면 HA는 BA 메시지에 이 옵션을 반드시 지정해야 한다.

V. 최근 이슈 및 표준화 동향

최근 주로 논의되고 있는 MIPv6 보안 이슈로는 HA와 AAAH간 인터페이스 정의 문제, MN과 HA간 IPsec를 적용하는데 있어서 IKEv2를 적용하는 문제, 초기 시동(bootstrapping) 문제, 주소 위치 프라이버시 문제 등을 들 수 있다[8].

5.1 AAAH와 HA 인터페이스

AAAH와 HA 인터페이스는 현재까지 명시적으로 규격화되지 않고 있는 상태이다. MIPv6에서는 MN이 홈 주소와 HA 주소를 알고 있고 MN과 HA간에 보안 신임정보(security credential)를 공유하고 있다는 가정 하에 운용된다. 이러한 정보는 사전에 미리 설정하거나 초기 시동 과정에서 획득할 수 있다. 사전 설정이 불가능한 경우에는 시동과정에서 AAAH 서버에 저장된 정보를 활용할 수 있다. 이를 위해서 HA는 AAAH와 연결되어야 하므로 AAAH-HA 인터페이스가 필요하다[9]. 이 인터페이스는 중요한 키와 관련된 정보가 전송되므로 기밀성과 무결성이 기본적으로 제공되어야 한다. 참고로 이 인터페이스는 Mobile IPv4에서 정의한 AAAH-HA 인터페이스와 유사하게 정의될 것으로 예측된다.

5.2 IKEv2를 갖는 경량형 IPsec 적용

MIPv6에서는 MN과 HA간 IKEv1을 갖는 IPsec을 적용하여 왔다. 그러나 최근에 개정된 IPsec이 나왔고 IKE 프로토콜도 많은 부분이 개정되고 단순화된 IKEv2가 등장하였다. IKEv2를 포함한 경량형 IPsec을 수용하기 위한 논의가 진행되고 있다[10].

5.3 초기 시동

초기 시동은 MN이 MIPv6 서비스를 시작할 수 있도록 하기 위해 필요한 HA 주소, 홈 주소 등과 같은 정보를 안전하게 획득하는 과정을 의미한다. 현재 논의되고 있는 시동 시나리오는 분리 시나리오와 통합 시나리오를 대상으로 하고 있다. 이 두 시나리오는 ASA(Access Service Authorizer)와 MSA(Mobility Service Authorizer)가 운용되는 형태에 따라 구분되는데 분리 시나리오는 MIPv6 서비스에 대한 권한 부여가 ASA가 아닌 제 3의 MSA에 의해 제공되며, 통합 시나리오는 ASA가 MIPv6 서비스 권한도 함께 관리하는 형태이다[11-13].

5.4 주소 위치 프라이버시 문제

IP 주소와 관련된 두 가지의 위치 프라이버시 문제가 논의되고 있다[14]. 하나는 MN이 CN에게 자신의 임시주소를 노출시키는 문제이고 또 다른 하나는 자신의 홈 주소가 공격자에게 노출될 수 있다는 문제이다.

5.5 기타 이슈

이 외에도 MN과 CN간에 신호 메시지를 보호하기 위한 방안으로 IPsec을 사용하자는 의견[15]과 제한된 환경에서 경로 최적화 과정에서 신호 메시지를 보호하기 위한 또 다른 메커니즘 등이 논의되고 있다.

VI. 결 론

본 고에서는 IPv6 기반의 이동인터넷 기술에 대해 소개하고 MIPv6 보안을 위해 제안된 RR 인증 메커니즘과 이동통신 시스템을 위해 제안된 3GPP 네트워크 인증 메커니즘을 살펴보았다. 그리고 표준화에서 논의되고 있는 기술적 이슈들을 조사해 보았다. 최근에 완성된 3GPP 네트워크 인증 기법은 IPsec을 적용하지 않음으로 인한 부하 경감, 이동통신 계층 2의 별도 채널을 통한 보안연계 설정의 용이, 동적 홈 에이전트와 홈 주소가 설정되는 환경에 적합, 백 엔드 서버와의 보안연계를 통한 인증 등의 장점들로 인해 이동통신 시스템인 UMTS, cdma2000, WiBro 등에 적용될 가능성이 높아졌다.

국내의 경우 IPv6 기술과 관련하여 정통부 및 관련 포럼을 주축으로 IPv6 시장확대 정책과 저변확대를 기해왔고 또한, IPv6 기술의 연구개발에 많은 노력이 이루어져 왔으나 시장 확대는 더디게 진행되고 있는 상태이다. IPv6의 요소기술인 Mobile IPv6 또한 궤를 같이 하고 있으며 특히, 본 고에서 기술한 MIPv6 보안기술은 상용화 가능한 수준의 표준규격 완성을 위해서 좀 더 많은 노력과 시간이 요구되고 있다.

[참 고 문 헌]

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC3775, July 2003.

[2] J. Arkko, V. Devarapali, and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", RFC3776, July 2003.

[3] A. Patel et. al., "Authentication Protocol for Mobile IPv6", RFC4285, January 2006.

[4] 3GPP2, "cdma2000 Wireless IP Network Standard", 3GPP2 X.S0011-D, September 2005.

[5] 한국정보보호진흥원, "IPv6 보안 기술 해설서", 2005. 10.

[6] A. Patel, K. Leung et. al., "Mobile Node Identifier Option for Mobile IPv6

(MIPv6)", RFC4283, November 2005.

[7] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "mobile IP Authentication, Authorization, and Accounting Requirements", RFC2977, October 2000.

[8] 나재훈, 구재범, "IETF MIPv6 보안 표준화 동향", 정보호호기술 표준화 동향, 한국정보보호진흥원, 2006. 6.

[9] G. Giaretta, I. Guardini, et. al., "Goals for AAA-HA interface", draft-ietf-mip6-aaa-ha-goals-02.txt, June 2006.

[10] V. Devarapalli, F. Dupont, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ike2-ipsec-06.txt, April 2006.

[11] A. Patel, G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-05.txt, May 2006.

[12] G. Giaretta, J. Kempf, V. Devarapalli, "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-02.txt, March 2006.

[13] K. Chowdhury, A. Yegin, " MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-01.txt, June 2006.

[14] Rajeev Koodli, "IP Address Location Privacy and Mobile IPv6: Problem Statement", draft-ietf-mip6-location-privacy-ps-02.txt, June 2006.

[15] F. Dupont, J-M. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes", draft-ietf-mip6-cn-ipsec-03.txt, August 2006.

김현곤

1992년 금오공과대학교 전자공학과 졸업(학사)
1994년 금오공과대학교 대학원 전자공학과 졸업(석사)
2003년 충남대학교 대학원 전자공학과 졸업(박사)
1994년 ~ 2005년 한국전자통신연구원 정보보호연구단 팀장
2005년 ~ 현재 목포대학교 정보공학과 교수
관심분야 : RFID/USN 정보보호, 개인 프라이버시 보호