情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

IPv6 환경에서 이동성 보안 프로토콜의 제고

권 혁 찬*, 안 개 일*, 나 재 훈*, 장 종 수**

요 약

IT839의 3대 인프라 중 하나인 IPv6 환경에서 단말의 이동성을 지원하기 위한 기술로 IETF(Internet Engineering Task Force) 표준화 기구에서는 Mobile IPv6 기술을 제안하였으며, 현재 RFC3775와 RFC3776으로 기본 스펙이 확정된 상태이다. 상기 표준 문서에 의하면 이동노드의 위치 인증을 위해 RR(Return Routability)을 사용하도록 규정되어 있으며, 이동노드와 홈에이전트 구간의 보호를 위해 IPsec 사용을 제안하고 있다. IETF 기구는 또한 이동 중인 단말이 새로운 네트워크에 접속시 수행하는 Auto-configuraton을 통한 주소 생성 과정을 안전하게 하기 위한 프로토콜로 SEND(SEcure Neighbor Discovery) 라는 프로토콜을 제안하기도 하였다. 최근에 IPv6 단말의 이동성 보안과 관련하여 주요 이슈가 되고 있는 분야는 이동노드의 Bootstrapping 기술이다. 이동노드의 Bootstrapping 시에 AAA와 같은 안전한 인프라를 이용하여 인증, 위치갱신, 홈에이전트 할당, 보안연계 설정 등의 작업을 해주고자 하는 것이 이 기술의 목표이다. 본 고에서는 IPv6 환경에서 이동성 지원을 위해 현재 정의된 그리고 연구 중인 보안 프로토콜들을 살펴보고 ETRI에서 개발한 MIPv6 Bootstrapping 기술을 간단히 소개하도록 한다.

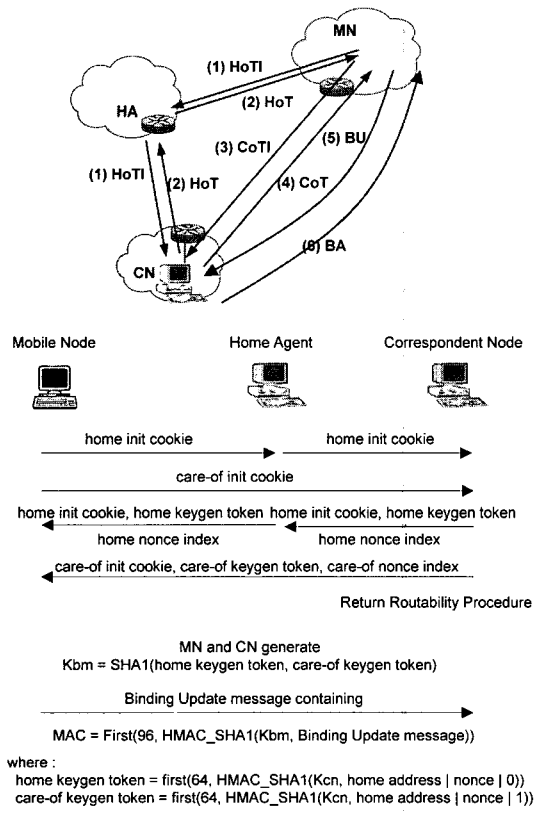
Ⅰ. 서 론

IETF Internet area의 mip6 워킹그룹은 IPv6 네트워크 계층에서의 단말의 이동성을 지원하고자 하는 프로토콜 제정 그룹으로서, IPv6 호스트가 자신의 영구적인 홈 주소를 갖고 인터넷을 움직일 수 있도록 하는 라우팅 기술을 제공하는 것이 목표이다. 이러한 IPv6 환경에서 이동성을 제공하기 위한 기술이 Mobile IPv6기술이다. Mobile IPv6 기술은 네트워크 계층 상위의 프로토콜에 투명하게 동작하며, 활성화된 TCP 연결과 UDP 포트 연결의 끊김 없이 IPv6 호스트의 이동성을 제공하는 기술이다.

이동통신의 양대 표준 기구인 3GPP와 3GPP2의 표준에서는 이동인터넷 환경의 표준으로 Mobile IPv6를 채택하였다. 이는 Mobile IPv6 기술이 갖는 특징들 즉, 이동통신의 최대 약점이라고 할 수 있는 정보보호 기능의 안정적인 제공, 충분한 주소공간의 확보로 인한 각종 전자제품의 효율적인 네트워크화, 플러그&플레이 방식의 자동 네트워킹 방식 지원 그리고 최적화된 라우팅 패스 설정을 통한 효율적인 네트워킹 제공 등의 장점 때문이라 볼 수 있다.

MIPv6 기술을 실제 망에 적용하기 위해 선결되어야 하는 문제가 있는데 그것은 바로 보안 문제이다. 실제로 현재 IETF를 중심으로 Mobile IPv6 관련된 주요 이슈는 바로 보안 문제이다. 현재 도출된 보안 기술로서 IPsec, RR, SEND 등이 있다. IETF RFC 3775[1]와 RFC 3776[2]에서는 이동 단말과 홈에이전트와의 보안을 위해 IPsec을 사용할 것과, 이동 단말이 대응노드로 자신의 위치를 안전하게 인증하기 위한 방법으로 RR(Return Routability)을 정의하고 있다. 또한 이동 단말이 새로이 네트워크에 접속하였을 때 자동주소생성(Auto-configuration) 과정을 통해 자신의 주소를 구성하게 되는데 이 과정에 대한 보안을 보장하기 위한 기술로 SEND[3]라는 프로토콜이 제안되기도 하였다. 또한 현재 주요 이슈가 되고 있는 토픽 중 하나는 바로 Mobile IPv6의 동작을 위한 Bootstrapping 기술이다. Bootstrapping절차는 Mobile IPv6 상용화를 위해 선결되어야 할 중요한 기술로서, 현재 비교적 활발하게 이에 대한 표준화가 진행 중에 있다.

* 한국전자통신연구원 정보보호연구단 P2P 보안연구팀 ({hckwon, fogone, jhnah}@etri.re.kr)
** 한국전자통신연구원 정보보호연구단 네트워크보안그룹 (jsjang@etri.re.kr)



〔그림 1〕 RR 프로토콜 동작과정

본 고에서는 IPv6 환경에서 단말의 이동성을 지원하기 위한 보안 기술을 살펴보도록 한다. 먼저 2장에서 이미 표준화가 완료된 IPv6 이동성 지원을 위한 보안 프로토콜인 RR과 IPsec 기술에 대해 간략히 살펴보고, 3장에서 안전한 IPv6 주소 생성기술을 살펴본다. 4장에서 MIPv6의 Bootstrapping 기술에 대해 살펴보고 5장에서 결론을 맺는다.

II. IPv6기반 이동 단말의 위치 인증 기술

2.1 RR (Return Routability)

RR 프로토콜[1]은 이동노드와 대응노드 사이에서 바인딩 갱신 및 바인딩 응답 메시지를 인증하기 위해서 사용되는 보안연계를 생성하는 역할을 담당한다. RR 프로토콜은 이미 RFC로 표준이 확정된 프로토콜이기는 하지만, 좀 더 향상된 보안을 위해서 RR을 대체할 수 있는 새로운 프로토콜이 필요하다는 의견도 제기되고 있고, IETF를 중심으로 RR을 대체하기 위한 프로토콜에 대한 연구도 일부 진행 중에 있다.

대응노드로 바인딩 업데이트 메시지를 전송할 때에

〔표 1〕 RR 시그널링 메시지

순서	메시지	방향	내용
1	HoTI (Home Test Init)	MN->HA->CN	RR 초기화 (src.: HoA)
2	CoTI (Care-of Test Init)	MN->CN	RR초기화 (src.: CoA)
3	Hot (Home Test)	CN->HA->MN	1에 대한 응답
4	CoT (Care-of Test)	CN->MN	2에 대한 응답
5	BU (Binding Update)	MN->CN	바인딩 갱신 정보 알림
6	BA (Binding Acknow-ledgement)	CN->MN	바인딩 응답 정보 알림

는 RR 메커니즘을 사용하여 여러 유형의 공격으로부터 메시지를 보호한다. RR 메커니즘의 기본 동작은 그림 1과 같으며 RR 메커니즘을 수행하기 위해서 새로 정의된 메시지는 표 1과 같다.

각각의 메시지들은 각각 Mobility 헤더의 타입필드의 값에 따라서 데이터 필드에 담겨져 전송된다. 위 절차에 따라서 이동노드의 홈주소 (HoA : Home Address)와 이동노드가 새로 접속한 네트워크에서 재구성한 주소 (CoA : Care-of-Address)에 대해서 각각 Reachability와 Validity를 체크한 후, 바인딩 업데이트를 전송함으로써 바인딩 업데이트 권한을 가진 이동노드를 정확히 인증할 수 있게 되고, 따라서 안전한 바인딩 업데이트가 가능하게 된다.

2.2 IPsec (IP Security)

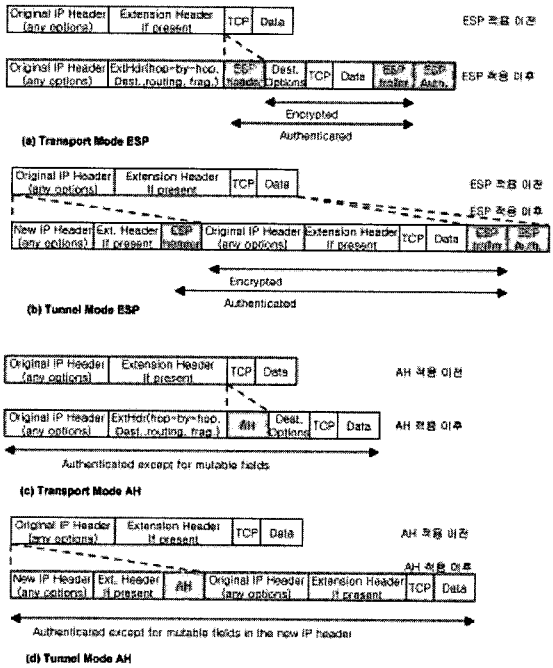
RR 프로토콜과 MIPv6의 BU/BA를 통해 이동노드를 인증한다고 해도, 이동노드와 홈에이전트 사이에 제어 트래픽에 대한 보안 메커니즘이 적용되지 않는다면, 이동노드와 대응노드는 Man-in-the-Middle, Hijacking, Confidentiality, Impersonation, DoS 공격에 취약할 것이다. 이러한 공격을 피하기 위해, RFC 3775와 3776에서는 홈에이전트와 이동노드 사이에 제어 트래픽을 보호하기 위해 IPsec[5]을 사용할 것을 제안한다. IPsec을 통해 보호되는 제어 트래픽은 다음과 같다.

- 이동노드와 홈에이전트 사이에 교환되는 바인딩 갱신과 응답 메시지 (IPsec transport mode)
- 홈에이전트를 통하여 대응노드로 전달되는 HoTI

메시지 (IPsec tunnel mode)
- 홈에이전트를 통하여 이동노드로 전달되는 HoT 메시지 (IPsec tunnel mode)

노드들은 또한 부가적으로 홈에이전트를 통하여 전달되는 페이로드 트래픽을 보호할 수 있다. 멀티캐스트 그룹 멤버쉽 제어 프로토콜 혹은 상태보존형 주소 자동 설정 프로토콜이 지원된다면, 페이로드 데이터의 보호가 요구된다. 이동노드와 홈에이전트 사이에 제어 트래픽은 메시지 인증, 무결성, 올바른 순서화, 그리고 Replay 보호를 요구한다. 이 트래픽을 보호하기 위해 이동노드와 홈에이전트는 보안연계를 가져야만 한다. 더욱이, 이동 IPv6 홈에이전트로 보안연계를 설정하기 위해 IKE를 사용하는 경우 상당한 주의가 요구된다. 올바른 종류의 주소들이 IKE 전송을 위해 사용되어야만 한다. 이것은 Circular Dependency를 피하기 위해 필수적이다. Circular Dependency는 바인딩 갱신을 사용하는 것이 바인딩 갱신 절차가 완결되기 이전에 아직 완료될 수 없는 IKE 교환에 대한 요구를 유발하는 것을 의미한다.

IPsec은 IP계층에서 기밀성과 인증 서비스를 제공하기 위하여 개발된 프로토콜로서 이미 오래전에 표준이 확정된 프로토콜이다. 제공하는 보안 서비스로는 접근제어(Access Control), 기밀성(Confidentiality), 비연결형 무결성(Connectionless Integrity), 재현공격방지(Anti-replay Service), 원적지 인증(Data Origin Authentication) 그리고 제한된 트래픽 흐름 기밀성(Limited Flow Confidentiality)이 있다. 그림 2에서 IPsec 적용 전 후의 IP 패킷의 구조를 볼 수 있다.



〔그림 2〕 IPsec 적용 전후의 IPv6 packet 형태

- RD (Router Discovery) : 호스트가 인접 라우터를 발견하고자 할 때 사용함
- 주소 자동 생성(Address Auto-configuration) : 호스트에게 주소를 자동 할당할 때 사용함
- 프로토콜 주소 변환 : IPv6 주소에 대응하는 링크 계층 주소를 얻고자 할 때 사용함
- NUD (Neighbor Unreachability Detection): 인접 호스트 및 라우터의 도달성 여부를 검사할 때 사용함
- DAD (Duplicate Address Detection) : 호스트가 주소 충돌 시험시 사용함
- Redirection : 라우터가 호스트에게 더 좋은 라우팅 경로가 있다는 것을 알려줄 때 사용함

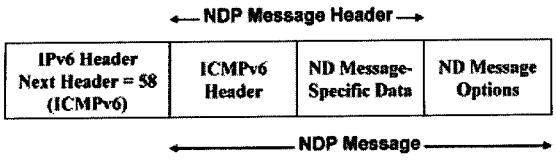
주소 자동 생성 기능은 Stateful 또는 Stateless 메커니즘으로 제공될 수 있다. Stateful인 경우에는 DHCPv6(Dynamic Host Configuration Protocol) 프로토콜을 사용하여 주소를 생성한다. Stateless인 경우에는, 호스트는 RD를 통하여 서브넷 Prefix 정보를 획득하고 또한 자신의 인터페이스 식별자를 생성하여 최종적으로 IPv6 주소를 생성한다. 그리고 마지막으로 DAD 메커니즘을 실행하여, 그 생성된 주소가 다른 호스트에 의해 사용되고 있지 않음을 확인한다.

Ⅲ. 안전한 IPv6 주소 생성 기술

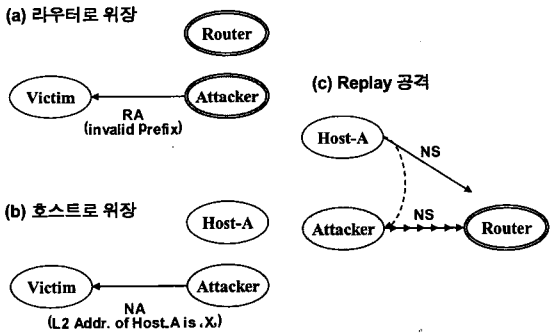
본 절에서는 IPv6 주소의 자동 생성 기능을 제공하는 NDP (Neighbor Discovery Protocol)[4] 프로토콜에 대한 개요와 보안 취약성을 간단히 살펴보고, 안전한 IPv6 주소 생성을 보장하는 SEND (Secure Neighbor Discovery)[3] 프로토콜에 대하여 설명한다.

3.1 NDP 프로토콜의 개요 및 보안 취약성

NDP 프로토콜은 같은 링크상에 있는 호스트들 및 호스트와 라우터사이에서 동작하며 그 주요 기능은 다음과 같다.



〔그림 3〕 NDP 메시지 포맷



〔그림 4〕 NDP 프로토콜에서 보안취약성 예

NDP 프로토콜을 ICMPv6 메시지 포맷을 따른다. NDP 프로토콜의 모든 기능은 RS (Router Solicitation), RA (Router Advertisement), NS (Neighbor Solicitation), NA (Neighbor Advertisement), Redirect 메시지를 통하여 제공된다. 그림 3은 NDP 프로토콜의 메시지 포맷이다.

NDP 프로토콜은 그림 4에서 도시된 바와 같이 악의 있는 사용자가 합법적인 호스트 또는 라우터로 위장함으로써 Redirect 공격과 DoS 공격이 가능하며, 또한 Replay 공격에 매우 취약하다. 그림 4-a는 공격자가 라우터로 위장하여 잘못된 서브넷 Prefix 정보를 호스트에게 전달함으로써 호스트는 다른 외부 호스트와 통신할 수 없게 된다. 그림 4-b는 공격자가 호스트 Hoat-A로 위장하여 잘못된 Host-A의 링크 계층 주소를 전달함으로써 Victim 호스트는 Host-A와 통신할 수 없게 된다. 그림 4-c는 Host-A의 NS 메시지를 복사하여 Router에게 그 메시지를 다시 재현하는 Replay 공격이다.

3.2 SEND 프로토콜

SEND 프로토콜은 NDP 프로토콜을 보호하기 위하여 제안되었다. SEND 프로토콜은 주소 소유권 증명 메커니즘, NDP 메시지 보호 메커니즘, Replay 공격 방지 메커니즘, 그리고 라우터의 권한 인증 메커니즘을 제공한다.

먼저, 주소 소유권 증명 메커니즘은 NDP 메시지의 송신 주소가 바로 그 메시지를 보낸 노드의 주소라는 것을 증명하는 메커니즘이다. 이를 위하여 SEND 프로토콜은 CGA (Cryptographically Generated Address) 옵션을 정의하고 있다. CGA 옵션은 그림 3에 보여진 NDP 메시지 옵션을 사용하여 전달된다. CGA에서 인터페이스 식별자는 공개키와 보조 파라미터를 입력으로 하여 수행한 해쉬 함수의 결과에 의하여 결정된다. 그 인터페이스 식별자와 서브넷 prefix를 합한 주소가 바로 CGA 주소이다. 따라서 CGA는 공격 호스트가 기존의 다른 호스트의 주소를 위조하는 것을 막을 수 있다.

NDP 메시지 보호 메커니즘은 NDP 메시지의 무결성과 송신자의 인증 제공을 목표로 하고 있다. 이를 위하여 SEND 프로토콜에서는 공개키 기반의 디지털서명 기법인 RSA 시그니처 옵션을 정의하고 있다. RSA 옵션은 그림 3에 보여진 NDP 메시지 옵션을 사용하여 전달된다. 송신 호스트에서는 패킷의 송신 IP, 수신 IP, 그리고 NDP 메시지를 개인키로 암호화하여 디지털 시그니처를 생성하며, 수신 호스트에서는 공개키를 사용하여 전달된 디지털 시그니처를 복호함으로써 NDP 메시지의 무결성과 송신자의 인증을 확인한다.

SEND 프로토콜에서는 Replay 공격 방지를 위하여 타임스탬프(Timestamp)와 난스(Nonce) 옵션을 정의하고 있다. 타임스탬프는 Redirect 메시지와 같은 광고형 메시지에 사용되며, 전송 호스트의 현재 시간이 NDP 메시지의 옵션 부분에 포함되어 전달된다. 수신 호스트는 그 메시지에 포함된 타임스탬프의 시간값을 수신 호스트의 현재 시간과 비교함으로써 Replay 공격여부를 결정할 수 있다. 난스는 무작위로 생성된 값으로써 요구/응답형 메시지에 사용된다. 난스를 포함하는 요구/응답 메시지를 받은 호스트는 난스값이 중복되었는지를 조사함으로써 Replay 공격을 탐지할 수 있다.

마지막으로, 라우터의 권한 인증 메커니즘은 라우터가 서브넷 Prefix 등 구성 정보를 호스트들에게 광고할 권한이 있는지를 인증하는 메커니즘이다. 라우터는 자신이 권한이 있음을 증명하기 위해서 신뢰 앵커(Trust Anchor)로부터 권한을 위임 받았음을 증명하는 인증서(Certificate)와 그 신뢰 앵커로부터의 인증 경로(Certification Path) 정보를 호스트들에게 제공해야 한다. 호스트는 자신이 신뢰하는 신뢰 앵커와 라우터로부터 받은 인증서 및 인증 경로를 검사함으로써 라우터의 권한 유무를 확인할 수 있다.

SEND 프로토콜에서는 호스트가 라우터에게 인증 경로를 요구하고 또한 라우터가 그 요구에 대한 응답을 할 수 있도록 CPS (Certification Path Solicitation)와 CPA (Certification Path Advertisement)란 메시지를 정의하고 있다.

Ⅳ. Mobile IPv6 Bootstrapping 기술

본 절에서는 MIPv6와 AAA연동을 통한 안전한 MIPv6 초기 구동 기술에 대해 살펴본다. IETF를 중심으로 이에 대한 표준화 연구가 활발히 진행되어 왔으며, 최근 몇 년 동안 기고된 대표적인 연동 기술에 대해 살펴보도록 한다.

4.1 Diameter Mobile IPv6 Application

Charles E. Perkins가 제안한 "Diameter Mobile IPv6 Application"[6]은 이동노드가 다른 망으로 로밍을 한 후에도 서비스를 지속적으로 제공받을 수 있도록 해주기 위한 기술로서 인증 메시지를 이용한 피기백 방식과 Diameter 프로토콜을 사용하고 있다.

기본 모델을 위한 구성요소는 다음과 같다.

- MN (이동노드) : 로밍시에도 Mobile IPv6 서비스를 지속적으로 받고자 하는 IPv6 단말
- AAA 클라이언트 : 사용자를 검증하고 망 사용에 대한 과금 정보를 생성하며 사용자의 권한을 검증하기 위해 AAA 인프라 구조를 사용해서 로컬망으로 사용자의 ID 및 인증 정보를 제공함으로서 MN이 네트워크 서비스 제공자에게 등록하고 인증 받을 수 있게 해준다.
- AAAv : 방문 망에 존재하는 AAA 서버
- AAAh : MN의 홈 망에 존재하는 AAA 서버
- HA : 이동노드의 홈에이전트

기본 가정은 다음과 같다.

- 이동노드의 식별을 위해 MN-NAI (Network Address Identifier)를 사용한다. (RFC 2784를 따름)
- MN과 AAAh는 long-term key를 공유하고 있다.
- AAAv와 AAAh간의 구간은 안전하다.
- 이동노드는 외부 도메인으로 로밍시 AAA 인프라 구조에 의해 사용자 인증 및 권한 검증을 위해 자신의 홈 주소 대신 NAI를 사용할 수 있다.
- 이동노드가 MN-NAI를 가지고 있지 않은 경우 이동노드 식별을 위해 IPv6 홈 주소를 사용할 수도 있다.

이 문서에서는 다음과 같은 AVP를 도입하였다.

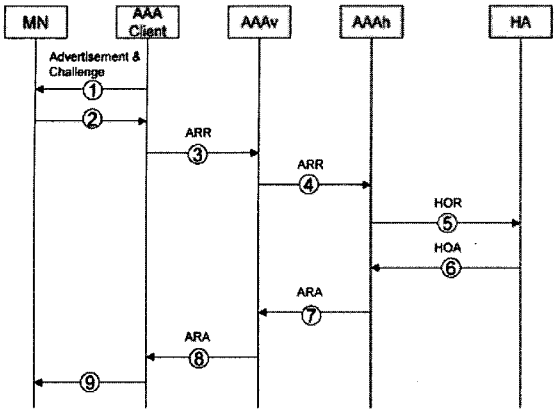
- MIP-Binding-Update AVP : OctetString 형태이고 MIP 바인딩 갱신 메시지를 포함.
- MIP-Binding-acknowledgement AVP : OctetString 형태이고 HA에서 MN으로 전송된 MIP 바인딩 응답 메시지를 포함.
- Mobile-Node-Address AVP : IP 주소 형태이고 MN의 홈 주소를 포함.
- Home-Agent-Address AVP : IP 주소 형태이고 MN의 홈에이전트 주소를 포함.
- MIPv6-Feature-Vector AVP : Unsigned32 형태이고 홈 도메인 내에 동적 홈에이전트 할당을 위해 허용.
- Security Key AVPs : AAA 서버들은 키 분배 역할수 수행할 수 있음. 서버의 특성에 따라 다양한 방법이 사용 가능함.

이동노드와 AAA 클라이언트 사이의 정보교환을 위해서는 정의된 MIP Feature vector AVP내에 요구된 정보를 포함한 MIP Feature Data, EAP, 관련 Security Data 그리고 Embedded Data를 사용한다. Embedded data는 이동노드가 네트워크에 의해 인증되고 권한 검증되는 시간과 동시에 바인딩 갱신을 전송하는 것을 가능하게 하기 위한 역할을 한다.

그림 5는 Mobile IPv6 서비스를 위한 AAA 인증 과정의 전체 Protocol flow를 보여준다.

그림 5의 인증 절차는 다음과 같다.

(1) 이동노드가 네트워크로 들어가거나 Power-on 했을 때, 라우터 광고 메시지를 수신하고 다음의 정보를 검색한다.
   * Local challenge, 방문망의 Identifier, CoA를 도출하기 위한 정보
(2) 이동노드는 CoA를 계산하고, 소스 IP를 CoA로 하고, 목적지 IP를 AAA client로 하여 다음 정보를 전송한다.
   * 이동노드의 NAI, AAAh와 공유하고 있는 Long-term Security Key, 미리 구성된 이동노드 홈 주소, 홈에이전트의 주소(옵션), 바인딩 갱신 데이터 (옵션)
(3) AAA 클라이언트는 먼저 이동노드로부터 수신한 메시지 검증을 수행하고, DAD를 수행한



[그림 5] Mobile IPv6 서비스를 위한 AAA 인증 과정 (ARR : AAA-Registration-Request, ARA : AAA-Registration-Answer, HOR : Home-Agent-MIPv6-Request, HOA : Home Agent-MIPv6Answer)

후, AAAh로 다음과 같은 정보를 포함하는 Diameter ARR메시지를 생성하여 전달한다.

* 사용자의 NAI를 운반하는 User Name AVP, 인증 데이터를 운반하기 위한 EAP AVP, MIP-Feature-Vector AVP, MIP-Binding Update AVP(이동노드의 메시지에 홈 바인딩 갱신이 포함된 경우), Home Agent의 IP주소, Security Key AVPs(이동노드가 키 요청 데이터를 제공한 경우)

(4) AAAv는 수신한 ARR메시지가 유효한 AAA 클라이언트로부터 온 것인지 검증하고, 이동노드의 홈 AAA 서버로 전송한다.

(5) AAAh는 수신한 ARR메시지가 유효한 AAAv로부터 온 것인지 검증하고, MN에 의해 제공된 NAI를 사용하여 사용자를 인증한다. 다음으로 AAAh는 이동노드를 대신하여 (MIPv6-Home-Agent-Address AVP가 존재하지 않고 MIPv6 Feature Vector AVP가 존재하는 경우) 홈에이전트를 할당하고 새롭게 생성된 홈 바인딩 갱신 메시지와 보안 키 재료를 포함하여 홈에이전트에게 HOR 메시지를 전달한다. 보안 키 재료는 홈에이전트와 이동노드 사이에 보안 연계를 위한 키를 계산하도록 하기 위한 정보이다.

(6) HOR을 수신한 홈에이전트는 먼저 Diameter 메시지를 처리한 후, 바인딩 갱신을 처리하고 수신된 메시지로부터 이동노드와 보안 연계를 위한 키를 계산한다. 또한 이동노드로 전송할 캡슐화된 바인딩 응답메시지를 포함한 HOA 메시지를 AAAh에게 전송한다.

(7) AAAh는 전달된 키 재료와 바인딩 응답 메시지를 포함한 ARA 메시지를 AAAv로 전송한다.

(8) AAAv로부터 ARA 메시지를 수신한 AAA client는 이 메시지를 이동노드로 전달 가능하도록 적당한 프로토콜로 이 메시지를 변환한다. 그리고 다음의 정보를 포함한 메시지를 이동노드로 전달한다.

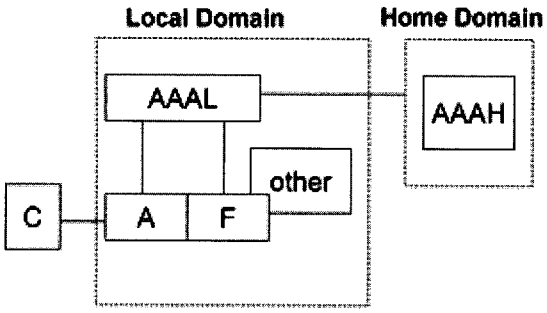
* 인증 데이터, Embedded Data 로서 바인딩 응답(이동노드가 홈 바인딩 갱신을 보냈거나 동적 홈에이전트 할당을 요청한 경우), 키 생성 재료

(9) AAA Client로부터 응답 메시지를 받으면, 이동 노드는 AAA 클라이언트가 보낸 네트워크 인증 데이터를 통해 네트워크를 인증한다. 그리고 이동노드가 홈에이전트를 요청한 경우라면, 홈 바인딩 응답 옵션의 소스 IP로 저장된 홈에이전트 주소를 추출하여 저장한다. 그리고 수신된 키 재료로부터 보안 연계를 생성한다. 만약 이동노드가 처음에 전송한 메시지에 바인딩 갱신 메시지를 Embedding 하였었다면, 수신한 데이터를 통해 바인딩 응답 정보를 추출한다. 만약 그렇지 않은 경우라면, 추가로 이동노드는 생성된 세션 키를 이용하여 보안연계 정보를 생성하고 이를 이용하여 홈에이전트에게 바인딩 갱신 메시지를 보내는 절차가 이어질 것이다.

Charles E. Perkins가 제안한 "Diameter Mobile IPv6 Application" 기술의 특징은 AAA 메시지의 Embedded data를 정의하여 이동노드의 AAA 인증과정에서 BU, Key 정보, Home Address 할당, Home Agent 할당 등의 MIPv6 Configuration의 상당부분을 처리할 수 있도록 한 것이다. 그러나 초기에 이동노드와 AAA 클라이언트간에 세션키가 설정되지 않은 상태에서 AAA 메시지에 BU를 Piggybacking 하는 경우, 이동노드 및 홈에이전트의 정보가 노출될 수 있는 위험성이 있으며, 악의적인 공격자는 노출된 정보를 이용하여 분산서비스 거부 공격을 감행할 수 있는 위험성이 존재하는 문제점이 있다.

4.2 AAA for Mobile IPv6

Francis Dupont가 제안한 "AAA for Mobile



〔그림 6〕 AAA 시스템의 구성 (C : Client, A : Attendant, F : Packet Filter, other : other AAA clients, AAAL : Local Authority, AAAH : Home Authority)

IPv6"[7]에서는 AAA를 이용하여 IPsec SA설정 시간을 단축시키는데 초점을 맞추고 기술을 정의하였다. 이동 환경에서는 IKE(Internet Key Exchange)의 성능이 이동환경에서 문제점으로 지적되고 있다. 본 기고서 에서는 이러한 문제점을 AAA인프라와의 결합을 통해 해결하고자 하며, AAA 메시지 교환 중에 이동노드와 홈에이전트 사이에 동적으로 SA(Security Association)를 설정하도록 하는 메커니즘이 제안되었다. 엔티티 관점에서의 AAA 시스템의 구성은 그림 6과 같다.

각 구성요소는 다음과 같다.

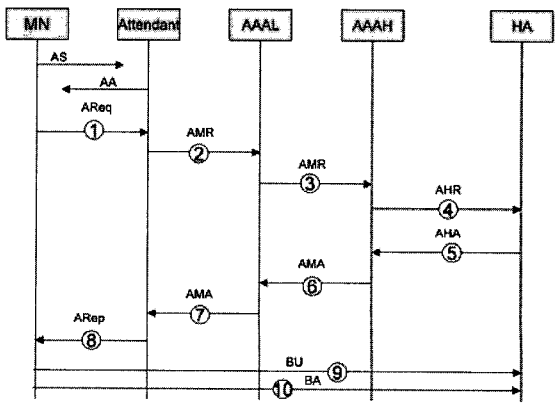
- Attendant : 방문망에 존재하며 이동노드에게 방문망에서의 인터넷 엑세스를 위한 접점을 제공한다. 로컬 AAA서버인 AAAL을 통해 이동노드를 인증하고 세션 키를 공유한다. 관련 구성 요소로서 패킷 포워딩 룰 및 네이버 캐시를 가지고 패킷의 포워딩 여부를 결정한다. 새로이 인증을 필요로 하는 이동노드로부터 AAA 인증 요청 관련 메시지를 수신하여, AAAL로 전달하고 리턴된 결과를 이동노드에게 전달한다.
- Client : Attendant에게 로컬망의 자원 사용을 요청하고 인증에 필요한 정보를 제시한다. 자원 사용 요청이 승인 되면 Attendant와 세션키를 공유한다. Client를 이동노드로 보면 된다.
- AAAL (AAA Local Server) : 방문망의 관리 도메인에 속하는 로컬 AAA 서버로서, 클라이언트의 인증정보를 받아서 클라이언트의 홈 도메인에 있는 AAAH(AAA Home Server)로 메시지를 전달하고 그에 대한 응답을 Attendant에게 전달하는 역할을 수행한다.
- AAAH(AAA Home Server) : client의 홈 도메인에 속하는 인증서버로서 외부망의 이동노드를 인증하고 Attendant로 전송하기 위한 세션키를 생성하며, 그 키를 생성하는데 필요한 키 생성재료를 이동노드에서 전달한다.
- 패킷 필터 : 클라이언트의 인증 여부에 따라 패킷의 전달을 제어한다. 인증되지 않은 이동노드로부터의 패킷의 경우, AAA 인증 요청을 위한 패킷을 제외한 일반 패킷의 경우 외부로 라우팅되는 것을 막는다. 수신되는 패킷 역시 이동노드에게 전달하지 않는다. 인종 요청 패킷은 Attendant로 전달한다.
- 네이버 캐시 : Attendant는 Neighbor Discovery 과정을 통해 자신의 로컬 망에 속한 노드에 대한 정보를 유지하고 이 정보를 기반으로 패킷 필터링 규칙이 동작하는데, 만일 로컬 망 내의 이동노드가 인증에 실패했거나, 세션키의 라이프타임이 만료되면 그 노드에 대해 네이버 캐쉬에 저장된 항목이 삭제되고 이후의 패킷은 패킷 필터에 의해서 폐기되어 진다.

프토토콜의 동작과정은 그림 7과 같다.

그림 7의 인증 절차는 다음과 같다. 메시지 표현 중 〔XX〕로 표기한 것은 Optional Element XX를 의미하며, {YY}zzz 로 표기한 것은 zzz_key Keying Material로 보호된 YY Element를 의미한다.

(1) 이동노드는 자신의 IPv6 주소를 설정하고 AS (Attendant Solicitation)와 AA(Attendant Advertisement)메시지를 통해 Attendamt를 발견 한 후, 다음과 같은 정보를 포함한 인증을 요청메시지를 전송한다.

* Local Challenge, NAI, RPI(AAA Replay



〔그림 7〕 AAA인증 프로토콜 동작 과정

Protection Indicator), [H@](Home Address), [HA@](Home Agent Address) , {aaa_key}pub(keying material for protection of AAA message), {attendant_key}aaa, {SecuParam_I}aaa(Security Association establishment elements for HA), CR(MN authenticator - signature of the AVP set)

(2) Attendant는 이동노드로부터 수신한 인증 정보를 자신의 로컬 AAA 서버로 전달한다. (AMR : Authentication MN-Request)

(3) AAAL은 수신한 요청 메시지를 AAA프로토콜로 변환하여 AAAH로 전달한다.

(4) AAAH는 홈에이전트로 메시지를 전달한다. (AHR : Authentication HA-Request)

(5) 홈에이전트는 이동노드로부터 온 메시지임을 인증하고 이동노드와 홈에이전트간에 미리 구성된 키를 바탕으로 이동노드와 Attendant간에 사용될 세션 키를 생성한 후 키 및 키 생성 재료를 반환한다. (AHA : Authentication HA-Ack)

(6) AAAH는 AAAL로 HA로부터 수신한 응답 메시지를 전달한다. (AMA : Authentication MN-Ack)

(7) AAAL은 AAAH로 부터의 응답 메시지 Attendant에게 전달한다. 전달하는 AMA(AA-MN-Answer)메시지는 다음의 정보를 포함한다.

* RC (result code), attandant_key(Local Secret between the MN and the Attendant), RPI(New Replay Protection Indicator), [H@](Home Address, if not in AMR, [HA@](Home Agent Address, if not in AMR), {SecuParam_R}(Aaa copied from AHA)

(8) Attendant는 네이버 캐쉬에 이동노드에 관한 항목을 추가하고 패킷 필터의 내용을 변경해서 이동노드로부터의 패킷이 attendant를 통해 외부로 라우팅 될 수 있도록 망 자원의 사용을 허용한다. 그리고 이동노드에게 다음의 정보를 포함한 ARep 메시지를 전송한다.

* [Co@](Care-of Address, Allocated/Registered by the Attendant), RPI copied from AMA, [H@] copied from AMA, [HA@] copied from AMA, {SecuParam_R}aaa copied from AMA

(9,10) 이동노드는 홈에이전트로 홈 등록을 요청하고 응답을 받는다.

Dupont의 기법은 Perkins가 제안한 모델의 많은 옵션들을 최적화하고 보안성을 더 높이고자 하는 측면에서 접근을 시도한 것이다. Dupont의 기법은 인증을 위해 각 이동노드 당 총 10단계의 인증과정을 거치게 되지만 전반적인 처리부하는 Perkins의 기법에 비해 적게 든다.

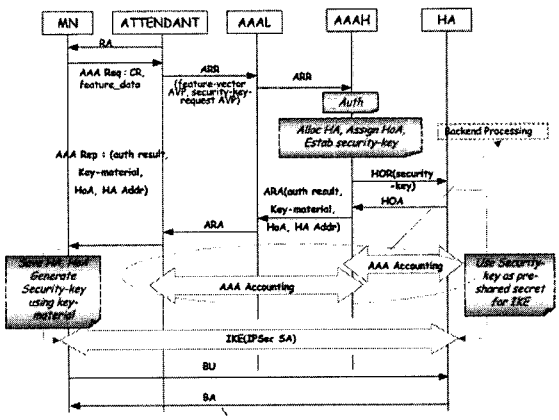
4.3 6Msec(Mobile IPv6 Security) 연동기술

본 절에서는 ETRI에서 Mobile IPv6 보안을 위해 개발한 6Msec 시스템 중 AAA 인프라를 이용한 Mobile IPv6 Bootstrapping 기술에 대해 설명한다. AAA인프라는 Diameter를 기반으로 구축하였다. 그림 8은 6Msec 시스템의 Bootstrapping시의 연동 시나리오를 보여준다.

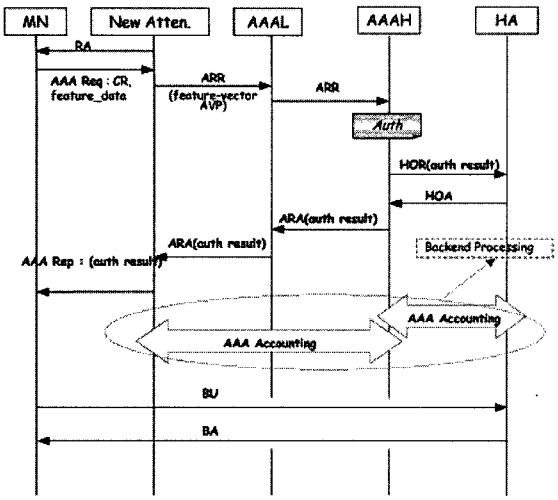
그림 8에서 볼 수 있듯이, 이동노드의 Bootstrapping 시 AAA 인증 과정에서 다음과 같은 작업이 동시에 수행된다.

- 이동노드의 홈에이전트 할당
- 이동노드의 홈 주소 할당
- 이동노드와 홈에이전트로 IKE 협상을 위한 Pre-shared-key 분배. 이동노드에게는 Preshared-key를 도출하기 위한 Key-material 전달

이동노드는 인증 결과를 수신한 후에 수신한 메시



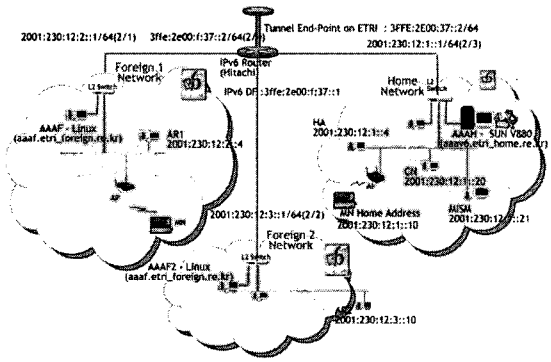
[그림 8] 6Msec Bootstrapping 연동 시나리오 (ARR: AAA-Registration-Request, ARA:AAA-Registration-Answer, HOR:Home-Agent-MIPv6-Request, HOA:Home-Agent-MIPv6-Answer)



〔그림 9〕 6Msec 핸드오프/재인증 연동 시나리오

지의 정보를 참조하여, 자신의 홈 주소와 홈에이전트를 설정하고, 수신한 Key-material을 기반으로 IKE 협상을 위한 Preshared-key를 계산하여 저장한다. 이 작업이 끝나면, 홈에이전트와 IPsec 통신을 위한 SA설정을 위해 IKE를 구동한다. IKE 협상이 끝나면, 생성된 SA를 갖고 IPsec 통신을 통해 BU/BA를 홈에이전트와 교환하게 되면 이동노드의 위치인증을 완료하게 된다. 그림 9는 이동노드의 핸드오프 발생시 또는 재인증시의 연동 시나리오를 보여준다. 이 경우에는 이미 홈에이전트, 홈 주소 그리고 SA가 이미 설정된 상태이므로, AAA 인증 과정에서 별도로 이러한 데이터를 할당할 필요가 없다.

살펴본 바와 같이 6Msec에서는 IPsec SA를 직접 분배하지 않고 IKE 협상을 위한 Preshared-key를 분배하는 구조를 갖는다. AAA 구조로 IPsec SA를 분배할 경우 이동노드와 Attendant 사이의 보안성이 없는 채널로 인해 IPsec SA가 암호화 되지 않은 상태로 분배되게 되고, 그로인해 IPsec 프로토콜에서 중요한 정보인 암호 알고리즘, 키 사이즈, Replay Window Size등이 노출되어 보안에 심각한 위협이 될 수 있다. 따라서 IETF RFC2401에 규정된 대로 IPsec SA분배는 IKE 프로토콜의 안전한 암호화된 채널에 의해 분배하도록 하였다. 또한 BU를 Piggybacking 하지 않은 이유도 보안문제 때문인데, BU를 Piggybacking 하는 경우 발생할 수 있는 보안 위험성은 4.1절에 기술되어 있다. ETRI에서 개발한 6Msec 시스템을 위한 테스트베드 형상은 그림 10과 같다.



〔그림 10〕 6Msec 시험환경

V. 결 론

본 고에서는 Mobile IPv6의 보안 프로토콜로서 이미 표준이 확정된 RR, IPsec, SEND 기술에 대해 살펴보았고, 현재 비교적 활발하게 연구가 진행되고 있는 MIPv6 Bootstrapping 기술을 소개하였다.

MIPv6 Bootstrapping에 대한 연구는 현재까지 표준이 확정되지 않은 채 많은 논의가 진행되고 있는 분야이다. Jee[8]는 PANA를 이용한 MIPv6 Bootstrapping을 제안 하였다. 그 밖에 Mun[9]은 지역 이동성을 고려한 MIPv6 계층적 인증 방법에 대한 기술로서, HMIPv6(Hierarchical MIPv6)와 AAA을 연계한 인증 방법을 제안하기도 하였다. Patel[10]은 홈에이전트에 등록하는 BU의 인증을 AAA에게 위임하는 방식을 제안하였다. Mobie IPv6의 Bootstrapping을 위한 Problem Statement[11]문서도 최근까지 계속 올라오고 있으며, 많은 논의가 진행 중에 있다.

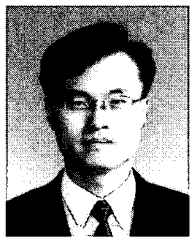
현재 다양한 형태의 Bootstrapping 방식들이 제안되고 연구 되고 있지만, 보안성 측면 그리고 손쉬운 적용 가능성을 고려해 볼 때, AAA 기반의 접근 방법이 유리하다고 볼 수 있다. MIPv6 Bootstrapping 기술은 Mobile IPv6를 실제 망에 적용하고, 상용화하기 위한 필수적인 기술이라고 볼 수 있으며, 이에 공감하는 다수의 연구자들이 현재 이에 대한 표준화 작업에 적극적으로 참여하고 있는 실정이다.

참 고 문 헌

〔1〕 Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", *IETF RFC 3775*, July 2003.

[2] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", *IETF RFC 3776*, July 2003.
[3] J. Arkko, J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)," *IETF RFC 3971*, March 2005
[4] Narten, E. Nordmark and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," *IETF RFC 2461*, Dec. 1998
[5] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", *IETF RFC 2401*, 1998
[6] F. Le, B. Patil, C. Perkins, S. Faccin, "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-04.txt, *Internet Draft*, IETF, 2004
[7] F.Dupont, J.Bournelle, "AAA for Mobile IPv6", draft-dupont-mipv6-aaa-01.txt, *Internet Draft*, IETF, 2001
[8] J.Jee, J.Nah, K.Chung, "Diameter Mobile IPv6 Bootstrapping Application using PANA", draft-jee-mip6-bootstrap-pana-00.txt, *Internet Draft*, IETF, 2004
[9] M.Kim, Y.Mun, J.Nah, S.Sohn, "An Authentication Scheme using AAA in Hierarchical MIPv6", draft-mun-mip6-authhmip-mobileipv6-00.txt, *Internet Draft*, IETF, 2005
[10] A.Patel, K.Leung, M.Khalil, H.Akhtar, K.Chowdhury, "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-auth-protocol-04.txt, *Internet Draft*, IETF, 2005
[11] A.Patel, "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-02.txt, *Internet Draft*, IETF, 2005
[12] 권혁찬, 나재훈, 정교일, "Mobile IPv6 표준화 및 기술동향", *주간기술동향*, 제1146호, pp.1-15, 2004.5.
[13] 문영성, "Mobile IPv6에서의 초기구동(bootstrapping) 표준화 동향", *IT Standard Weekly*, 2004-41호, 2004.10.
[14] 문영성 외, *Mobile IPv6 IPv6sec 서비스 구조에 관한 연구*, ETRI 위탁과제 최종연구보고서, 2002.12.
[15] 나재훈 외, *6Msec 접속 규격서*, ETRI 기술문서, 2004.

〈著 者 紹 介〉



권 혁 찬 (Hyeok Chan Kwon)

1994년 2월 : 서원대학교 전자계산학과 졸업
1996년 2월 : 충남대학교 전산학과 석사
2001년 2월 : 충남대학교 컴퓨터과학과 박사
2001년 1월~현재 : 한국전자통신연구원 P2P보안연구팀 선임연구원
〈관심분야〉 네트워크 보안, Mobile IPv6 보안, P2P 보안

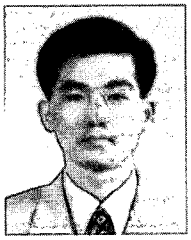
안 개 일 (Gae Il An)

1993년 2월 : 충남대학교 컴퓨터공학과 졸업
1995년 2월 : 충남대학교 컴퓨터공학과 석사
2001년 8월 : 충남대학교 컴퓨터공학과 박사
2001년 8월~현재 : 한국전자통신연구원 P2P보안연구팀 선임연구원
〈관심분야〉 컴퓨터 네트워크, 네트워크 보안, 네트워크 시뮬레이션, P2P 보안

나 재 훈 (Jae Hoon Nah) 정회원

1985년 : 중앙대학교 컴퓨터공학과 졸업
1987년 : 중앙대학교 컴퓨터공학과 석사
2005년 : 한국외국어대학교 전자정보공학과 박사

1987년~현재 : 한국전자통신연구원 P2P보안연구팀 팀장
〈관심분야〉 IPv6/MIPv6 보안, P2P 보안



장 종 수 (Jong Soo Jang)
정회원

1984년 : 경북대학교 전자공학과 공학사
1986년 : 경북대학교 전자공학과 공학석사
2000년 : 충북대학교 컴퓨터공학과 공학박사
1989년~현재 : 한국전자통신연구원 정보보호연구단 네트워크보안그룹 그룹장
〈관심분야〉 네트워크보안, 웹서비스보안, Secure OS, IDS/IPS, Traffic Management