情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

MIPv6 보안문제 분석

전 용 수*, 이 종 민**, 권 오 준**

요 약

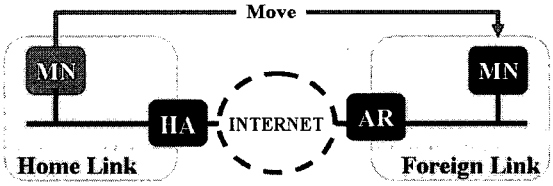
차세대 인터넷 주소체계로 IPv6의 표준화가 마무리단계에 이르러 이동성 지원을 위한 MIPv6(mobile ipv6)의 표준화도 RFC3775[1]로 마무리되었다. 하지만 IPv6를 기반으로 한 MIPv6의 보안 문제점은 완전하게 해결되지 않는 연구과제로 남아있는 상태이다. IPv6의 autoconfiguration 과정에서의 주소중복, DoS공격의 취약점은 IPv6를 기반으로 한 MIPv6에서도 적용되는 보안문제이다. 특히 모바일 단말기의 로밍 환경에서의 HA와 MN간의 보안인증 절차문제, 전원공급으로 인한 bootstrapping 관련 추가적인 보안문제가 있어 보안관련 연구단체에서 연구가 진행 중에 있다.

Ⅰ. 서 론

본 보고서에서는 Mobile IPv6의 보안에 관련된 부분에 대해서 기술한다. MIPv6의 보안과 관련된 사항은 MIPv6 표준문서 RFC3775[1]의 15절에 기술되어 있다. MIPv6상에서 어떤 위협이 존재하는지 분석하고 이러한 위협요소를 표준화 문서에서는 어떤방법으로 보안하는지 기술한다. 먼저 MIPv6의 보안 위협을 분석하기 전에 MIPv6의 기본적인 구동방식을 살펴보고, MN(mobile node - 이동노드)가 홈 망에서 외부 망으로 이동한 즉시 수행하는 MN과 HA (home agent)간의 홈 등록(home registration) 과정과 MN가 이동된 후 CN(correspondent node - 통신노드)와 통신하기 전에 인증절차에 관한 MN과 CN간의 RR(return routability)과정을 기술하고 각각에 대한 보안적인 위협을 기술하고, 표준문서에서 제시한 위협에 대한 대응방안과 HA와 MN간의 인증절차 문제로 대두되고 있는 초기구동[2]을 살펴보고자 한다.

Ⅱ. MIPv6 구동방식

MIPv6의 기본적인 동작을 구분해서 기술하자면 우선은 그림 2.1에 나와 있듯이 홈 망에 있던 MN이 외부 망으로 이동되는 것을 전제로 한다. MN이 외부

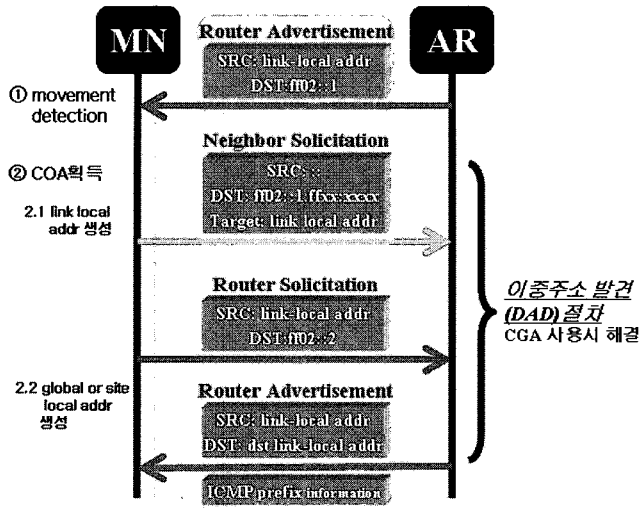


〔그림 2.1〕 MN의 Movement

망으로 이동되기 전에는 Link-local address 주소와 HA의 프리픽스 정보를 가진 site-local 혹은 global address의 홈 주소(home address)가 보유된 상태이다.

그림 2.1에 나와 있듯이 MN이 홈 망에서 외부 망으로 옮겨졌으면 이동감지를 하게 된다. 이 부분을 그림 2.2에서 홈 망에서 외부 망으로 옮겼을 때 외부 망에서의 CoA를 획득하는 과정을 간략하게 동작절차를 보이고 있다. MN이 이동한 후에는 RA(router advertisement)[3] 메시지의 프리픽스 정보와 NUD (neighbor unreachable detection)메커니즘을 사용하여 이동하였음을 감지할 수 있다. MN는 필요에 따라 RS(router solicitation) 메시지를 사용하여 RA(router advertisement) 메시지를 유도한다. 이동이 감지된 후에는 주소 자동설정(address auto-configuration)[4] 방법으로 CoA(caare of address - 임시주소)를 획득한다. 이 과정에서 MN이 이동 되었을 때를 제외하고는 기본적인 주소 자동설정

* 동의대학교 대학원 컴퓨터소프트웨어공학과 석사과정 (ysjeon@deu.ac.kr)
** 동의대학교 공과대학 컴퓨터 · 소프트웨어공학부 소프트웨어공학전공 조교수 (jongmin@deu.ac.kr, ojkwon@deu.ac.kr)

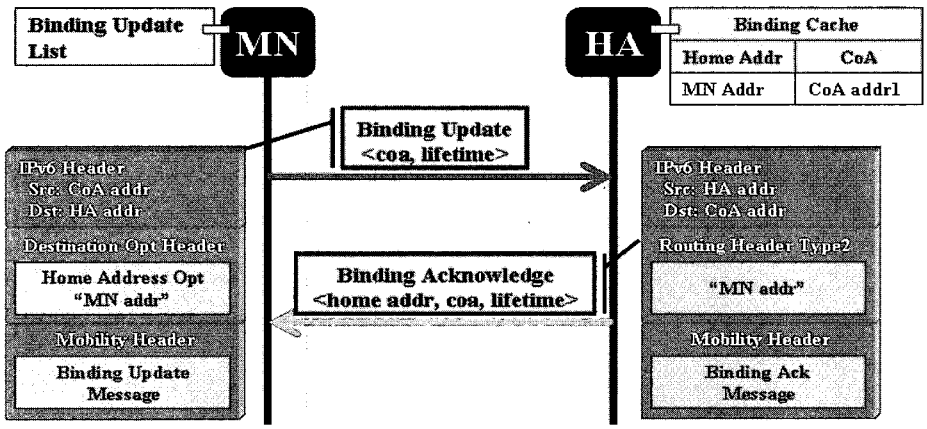


〔그림 2.2〕 MN의 Auto-configuration과정

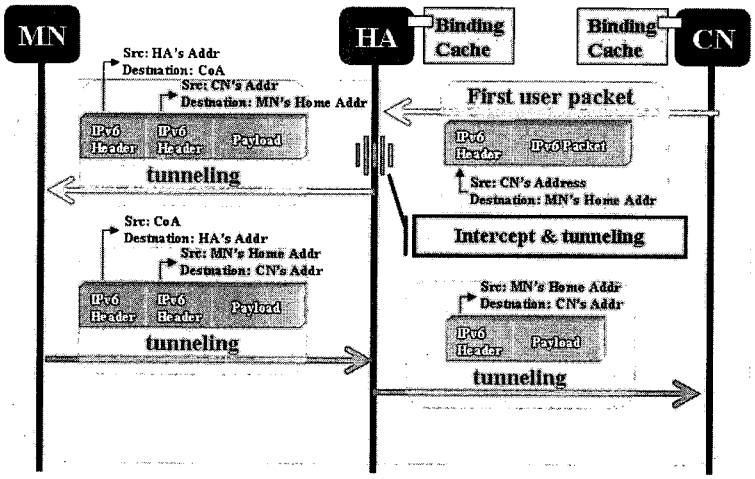
방법은 IPv6를 기반으로 하고 있다. 주소 자동설정 과정은 앞에서도 언급되었듯이 많은 위협에 노출되고 있고, 이에 대한 방안으로 SEND[5] 워킹 그룹에서 제공하는 방안 CGA(cryptographically generated addresses)[6] 등을 이용하여 위협에 대한 대응방안을 연구 중에 있다.

이렇게 하여 외부 망에서의 MN이 CoA를 획득하게 되면 이를 자신의 홈 망의 HA에게 알려주게 된다. 그림 2.3 IPv6기본 헤더에 보내는 주소를 CoA로 설정하고 목적주소는 HA로 패킷을 구성하고 Destination Option Header에 MN의 원래 홈 주소를 추가, 다음 Mobility Header에 BU 메시지 패킷을 추가하여 HA에 보낸다. 이는 HA에 대해서 MN은 임시주소를 획득한 CoA주소를 HA에게 통지하는 것이다. BU 메시지에 추가적으로 외부 망에서 얻은 CoA와 lifetime을 포함하여 HA에게 송신한다. HA는 MN이 보낸 BU메시지를 수신함으로써 MN이 외부 망에 정착되 있는 것을 인지하고 자신의 바인딩캐시(binding cash)에 MN의 홈 주소와 CoA를 등록하고 BU에 대한 응답으로 BA 메시지를 보내어 등록이 성공적으로 이루어졌음을 알려준다. BA는 추가적으로 자신의 홈 주소, CoA, lifetime이 들어간 패킷을 MN에게 송신한다.

홈 등록(home registration)과정에서 보안적인 취약점으로 다양한 공격방법으로 노출이 되어있다. 이에 대한 보안방안으로 초기구동에 관계되어 다음절에 언급될 여러 기술들이 나와 있는 상태이지만 아직까지는 명확하게 제시된 방안이 없는 상태이다. 기존의



〔그림 2.3〕 MN과 HA의 Home Registration과정



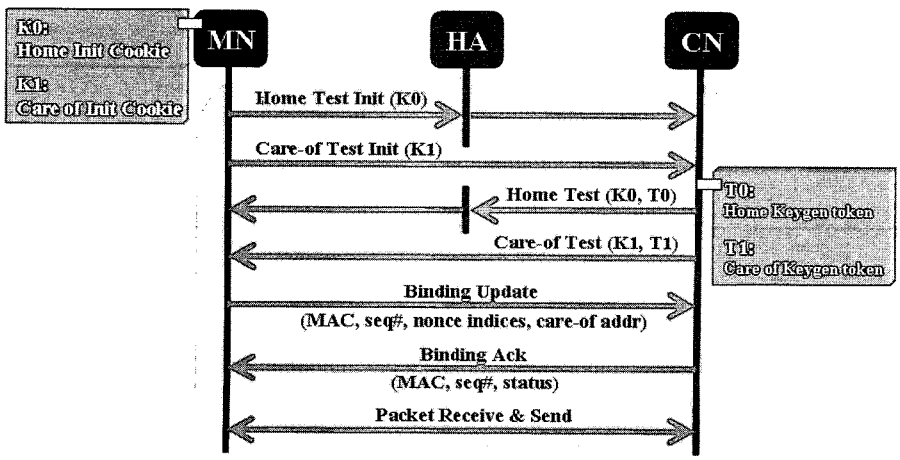
〔그림 2.4〕 CN-MN 양방향 터널링

MIPv6에서의 HA와 MN간의 인증절차는 서로간의 메시지보호를 위한 IPsec SA절차를 하게 되는데 IPsec[7]은 MN이 프리픽스(prefix)정보와 홈 주소정보를 보유되어있는 상태를 전제로 하기 때문에 초기구동시에 수동키(manual key)로 보안 설정을 해야 하는 문제가 있다.

다음은 CN이 패킷을 MN에게 보내게 되면 MN의 주소가 등록 되 있는 홈 망으로 찾아온다. 그림 2.4에서 보듯이 패킷을 받은 HA는 현재 MN이 홈 망안에 없고, 다른 망에 있다는 사실을 알고 있다. 따라서 HA는 그 패킷을 터널링(tunneling)해서 다른 망에 있는 MN으로 보낸다. 터널링한 다는 말은 이 패킷을 IPv6 패킷에 넣고, 목적지는 MN의 CoA로 해서 부치는 것이다. 처음 CN이 MN으로 데이터를 보내는 경우에는 주소를 모르기 때문에 HA로 보내야 한다.

그러나 일단 MN에서 Destination Option의 BU로 CoA를 통보 받으면 다음 번에 CN이 MN으로 패킷을 보낼 때는 목적지 주소를 홈 주소로 하고 Routing Header안에 CoA를 넣어서 보낸다. Routing Header의 동작 원리는 Routing Header에 들어있는 주소를 반드시 거쳐야 하므로 일단 CoA로 가고, 홈 주소로 가게 된다. CoA로 가면 MN으로 도착하므로 그대로 전달하면 된다. MN은 Destination Option의 BU를 CN에게 보내준다. 여기서 CN이 MN에 대해 요청된 홈 주소와 CoA가 사용될 수 있는 값인가에 대한 확인으로 RR이 실행된다.

이 절차가 통과되어야만 CN은 BU를 수락(accept)할 수있으며 해당 CoA로 packet을 전송 할수



〔그림 2.5〕 모바일 IPv6에서 CN-MN간의 Return Routability

있다. CN은 BU를 보고 다음부터 보내는 패킷은 목적지가 홈 주소인 경우에, 목적지를 CoA로 해서 바로 보내게 된다. CN이 MN으로 패킷을 보낼 때는 목적지 주소를 홈 주소로 하고, Routing Header안에 CoA를 넣어 보낸다. Routing Header의 동작 원리는 Routing Header에 들어있는 주소를 반드시 거쳐야 하는 것이므로 일단 CoA로 가고, 홈 주소로 가게 될 것이다. CoA로 가면 벌써 MN이므로 그대로 전달하면 되는 것이다.

Ⅲ. MIPv6 보안문제

MIPv6 에서는 기본적으로 보안문제에 관해서 기술되어있다. 기존의 방식으로 해결되는 보안문제와 고려해야 할 보안 문제등을 표 3.1에서 나열하였다. 노드가 어떠한 메시지를 보내거나 패킷을 보낼 때 각각 발생할 수 있는 공격유형과 그에 관한 해결책이 제시되어있다.

〔표 3.1〕 MIPv6 보안문제와 해결책

관련 메시지 유형/형태	공격유형	공 격 방 법	해결책
BU to HA	Denial of Service	- 특정 MN의 홈 주소와 CoA를 위조 - 노드 사이에서 중간자 공격	Boot-strapping 에서의 보안
BU to CN	Replay Attack	- CoA를 위조 여러 CN에게 전송하여 공격대상에게 여러 메시지를 보내는 공격	Return Routability
Payload 패킷	위조	- Tunneling상에서 목적지 주소를 위조하여 공격 - Routing Type2를 이용하여 Firewall을 통과하여 공격	IPsec ESP
prefix 탐색	Denial Of Service	- prefix정보를 위조하여 서비스 방해 공격	인증
HAO		- Home AddressOption을 이용한 서비스 방해 공격	IPsec SA
라우팅 헤드	Reflection attack	- Type0의 라우팅 헤더를 이용한 공격	새로운 라우팅 헤더타입

3.1 HA와 CN에 보내는 BU에 관한 위협

이 공격에는 여러 가지 요소가 있다. 공격자가 특정 MN인 것처럼 행동하여 HA의 서비스를 받지 못하는 DoX공격, MN뿐만 아니라 자신이 HA인 것처럼 행동하는 Man-in-the-Midle공격, 공격대상의 MN의 CoA주소를 이용하여 다른 CN들에게 다량메시지를 공격대상에게 보내게 하는 공격, 공격자가 MN의 이전 BU를 다시 replay하여 MN의 통신을 방해하는 공격 등이 있다.

3.2 패이로드패킷(payload packet)에 관한 위협

공격자가 Home Address Destination Option을 사용하여 패킷을 보내면 이에 대한 응답 트래픽을 option에 나타난 IP주소로 보낼 수 있다. 이 경우 ingress filtering이 위조된 return address를 감지 못할 수 있다.

3.3 프리픽스(prefix)탐색에 관한 공격

모바일 프리픽스 탐색기능은 도청자에게 네트워크망 프리픽스 수명에 대한 중요한 정보를 노출 할 수도 있다. 그래서 이러한 이유로 이정보에 대해서 인증되지 않으면 안 된다. MN가 위조 프리픽스 정보를 믿고, 기존의 주소로 통신을 방해하도록 하는 공격에 대해서 응답과 요청되지 않은 프리픽스 정보는 인증되어야 한다.

3.4 HAO(Home Address Option)을 이용한 공격

HAO(Home Address Option)을 사용할 경우 발생할 수 있는 보안상의 문제점은 공격자가 DoS (Denial of Service)공격에 HAO를 사용할 수 있다는 것이다. 정확히 말하자면, HAO는 공격자가 자신의 위치를 숨길 수 있는 방법을 제공한다.

이러한 문제점을 해결하기 위해 대응노드에서 HAO를 갖고 있는 패킷을 수신했을 때, 바인딩 정보 혹은 IPsec SA(Security Association)가 존재하는 경우에만 HAO를 처리하도록 제한하는 방식을 사용한다.

3.5 라우팅 헤드를 이용한 공격

현재 MIPv6에서 사용하도록 한 Type 0의 라우팅 헤더는 호스트나 라우터에서 모두 처리 가능하며, 여러 개의 주소를 담아서 전송될 수 있기 때문에 reflection attack에 이용될 수 있다. 이 문제점에 대한 해결방안으로서, 기존의 라우팅 헤더를 사용하지 말고 새로운 Destination option, 새로운 확장 헤더 또는 새로운 라우팅 헤더 타입을 정의하여 사용하는 방식이 사용된다.

Ⅳ. Bootstrapping 메커니즘

IPv6의 이동성을 보장하는 기술로 MIPv6는 이동성 보장 및 보안적인 요소를 지원하는 표준화 작업이

마무리 단계에 도달해 있다. 하지만 보안과 성능 문제를 완전히 해결하지는 못한 상태로 별도의 워킹그룹별로 표준화를 위한 연구가 활발히 이루어지고 있으며, 그 중에서 단말이 초기구동 에서 보안적인 문제점이 대두되고 있다. 이동성 모바일은 항상 연결성을 보장을 해주어야 하기 때문에 IETF에서는 많은 가정들이 나오고 있다.

4.1 Bootstrapping의 개요

Mobile IP에서 MN가 글로벌 환경에서 인터넷이나 통신 등을 가능하게 하려면 우선 MN는 자신의 홈 주소와 홈에이전트의 주소를 알고 있어야 하고, 홈에이전트와 보안 협약(security association)을 맺고 있어야 하는 가정 하에 이동성 제공을 위한 바인딩 등록으로 가능할 수가 있다. 만일 홈에이전트 주소나 홈 주소가 부정확하거나, 타 노드의 공격대상으로 여러가지의 HA와 MN간의 공격으로 서로간에 신뢰할 수 없게 되면 주소를 기반으로 설정된 보안 협약은 신뢰할 수 없게 된다. 또한 로밍환경 시 홈 망에 의해 MN로 정보가 전송되지만 MN가 실제 환경에서 이동에 의한 제한된 수신 능력 및 전원문제로 인해 정보를 분실하는 경우가 충분히 예상할 수 있는 문제이다.

따라서 홈 망에 의한 방법이 아닌 MN에 의한 이동 컨텍스트의 동기화 방법이 제공되어야 한다. 초기구동 방식은 MN가 동적인 망 환경에 제대로 적응할 수 있도록 하는 기술로써 기본적으로 최초 부팅 시, MN의 홈 망 재구성 또는 홈 에이전트 변경 등의 예측하지 못한 환경의 변화가 발생하는 경우 이를 능동적으로 수용하고 Mobile IP의 여러 기능 요소들과 정보 교환을 통해 서비스의 신속하고 안전한 재개를 도모하기 위한 수단으로써 관리자의 직접적인 개입 없이 자동적인 과정을 통해 일관된 방식으로 서비스를 지속할 수 있도록 해 준다. MN이 외부 로밍 중에 홈 주소, 홈 에이전트 주소 또는 보안 협약을 분실하거나 유효하지 않은 정보를 가지게 되는 경우 반드시 초기구동 과정을 통해 홈 에이전트와의 이동 컨텍스트를 동기화해야 한다. 초기구동 방식은 동작 형태에 따라 3가지 관점으로 분류할 수 있다.

4.2 전원 공급에 의한 초기구동

먼저 가장 기본적인 형태로서 이동 단말의 특성상 절전 모드로 동작하거나 장시간 배터리 전원을 끄는 경우 홈 망의 재구성으로 인한 프리픽스 정보 변경 통보를 수신하지 못하는 상황이 발생한다. 홈 망의 재구성이 발생하면 홈 에이전트는 MN에게 변경된 프리픽스를 전송하는데 프로토콜에 기술된 사양에 의해 디폴트로 5분 간격으로 3번 시도를 하며 이 기간 동안 이전 프리픽스와 새로 구성된 프리픽스가 공존하고 그 이후에는 새로운 프리픽스만 유지하게 된다. 따라서 이 기간 동안에 동작을 재개하거나 전원을 켜주지 않는다면 홈 망의 재구성 여부를 알 수 없는 상태가 되며, 기존의 홈 에이전트 및 홈 주소는 더 이상 유효하지 못한다. 더불어 홈 주소를 기반으로 설정된 보안 협약도 효력을 상실하게 된다.

4.3 고장에 의한 초기구동

홈 망에서 예측하지 못한 이벤트 발생으로 인한 초기구동 절차의 실행으로서 홈 에이전트 고장으로 인한 절체(Failover)가 일어나거나 부하 분산을 위해 다른 홈 에이전트로 대체한 경우(Switching)한 경우 또는 망재구성을 통해 홈 망의 프리픽스가 변경된 경우 초기구동 절차를 재시작 할 수 있다. 이 때 이동 컨텍스트는 무효화되고 새로 구성된다. 그 이외에 MN가 외부 로밍 중에 홈 망에 존재하는 노드와 주소 충돌이 발생하는 경우 MN의 홈 주소가 변경될 수도 있는데 이때 이동 컨텍스트는 무효화된다.

4.4 스케줄링에 의한 초기구동

보안성 향상을 위해 짧은 주기 단위로 계획된 스케줄링에 의해 초기구동 절차를 실행하는 경우로서 이는 내부 정책에 영향을 받는다. 그러나 잦은 초기구동(Boot strapping) 절차의 노출로 인해 공격의 빌미를 제공할 우려가 있고 성능의 저하를 초래할 수도 있으므로 신중히 사용해야 한다.

V. 보안 문제점 및 해결방안

대표적인 IPv6 보안 문제점은 SEND(securing neighbor discovery)로서 MN가 노드 초기구동시 현재 링크상에 존재하는 노드를 발견하는 절차를 시작하는데 이 때 공격자에 의해 거짓 노드 정보를 수신할 수 있다. 또한 라우터 발견을 통한 stateless 방식의 주소 구성 시 라우터와 노드간에 설정된 SA가 없으므로 거짓 라우터 정보를 수신하고 잘못된 주소를 구성하거나 주소 중복 검사(DAD - duplicate address detection)에서 실패하도록 만듦으로써 DoS공격 위

협이 높다. 따라서 메시지 송수신자 간에는 반드시 인증 절차가 필요하고 무결성이 보장되어야 한다. Mobile IP 기술에서 마찬가지로 MN와 홈 에이전트 간의 사전 IPsec SA설정을 통해 바인딩 메시지를 보낸다. 그러나 MN이 로밍 환경시 발생할 수 있는 보안문제이다. MN이 다른 외부로 이동하는 경우 먼저 MN와 외부노드 사이에 인증절차가 우선 이루어져야 하는데 이 과정에서 위협에 노출되는 경우 치명적인 피해를 입을 수가 있기 때문이다. 이동, 컨텍스트는 MN의 홈 주소, 홈 에이전트 주소 및 MN와 홈 에이전트간에 사전에 설정된 보안 협약(SA)를 포함한다. 이러한 협약이 이동 중이나 전원공급의 문제, 또한 특정한 공격에 의한 문제로 인해 3가지 정보(authentication, authorization account)중 하나라도 분실하는 경우 컨텍스트는 무효화 된다. 만일 홈 주소를 분실한 경우 DNS나 DHCP 확장 기능을 이용해서 주소를 얻는 방법을 생각할 수 있다. 그러나 DNS나 DHCP 엔티티에 대한 보안 기능이 우선 되어야 한다. 홈 에이전트 주소를 분실한 경우, 홈 주소의 프리픽스 정보를 기반으로 애니캐스트 메시지를 통해 홈 에이전트 주소 발견 절차를 시도할 수 있지만 이 역시 보안의 취약성으로 인해 위험이 존재한다.

또한 ICMP(internet control message protocol) 기반의 홈 에이전트 발견 메시지는 핑(Ping) 공격 및 트래픽 폭주 등을 막기 위해 설치된 VPN(virtual private network) 등의 보안 엔티티에 의해 차단될 수 있으므로 궁극적으로 신뢰할 수 있는 엔티티를 포함하는 홈 에이전트 발견이 선호되어야 할 것이다. 만일 보안 협약을 분실하였다면, 홈 주소 및 홈 에이전트 주소를 기반으로 동적인 보안 협약 검색이 가능하며 보안 협약이 만료되거나 존재하지 않는 경우 동적인 보안 협약 설정 절차를 실행할 수 있다. 이때 IPsec 기반으로 수동 키 입력 방식이 사용될 수도 있지만 홈 망 재구성 및 홈 주소 변경으로 인한 이동 컨텍스트 변경 시 이를 수동으로 지정해 주는 것은 사실상 불가능하다.

IKEv1(internet key exchange version 1)[8]을 이용한 동적 보안 협약 재구성은 이미 홈 주소를 알고 있다는 가정 하에 진행되므로 홈 주소 분실 시에는 쓸모가 없게 된다. 또한 확장성 면에 있어서도 만족할 만한 성능을 제공하지 못한다. 그러므로 초기구동 절차 시 보안 위협을 최소화하기 위해서 초기구동 절차에 참여하는 엔티티 및 이들 간의 트랜잭션을 최소화해야 하고 VPN이나 기타 방화벽 환경을 고려하여 신뢰성 있는 엔티티를 참여시키는 방법이 제공되어야 할 것이다.

앞서 말했듯이 초기구동에 관련된 보안 적인 문제점들의 해결방안으로 IETF WG에서 여러 제안들이 나오고 있다. 크게 해결방안으로 보면은 초기구동에 관한 해결방안으로는 인프라를 사용하는 방법과 인프라없이 사용하는 2가지로 나누어 볼 수 있다.

5.1 인프라없이 사용 방안

IPsec 수동 키 입력 방식은 Bootstrapping에서 자동설정으로 이루어져야 하는데 실제로 수동 키 방식으로 사용하기 때문에 사실상의 관리가 불가능 하므로 채택이 어려우며, IKEv1의 사용은 MN의 홈 주소를 이미 알고 있다는 가정 하에 실행되므로 초기구동 절차의 보안 문제점에 대한 완전한 해결 방법을 제공하지 못한다. 또한 보안협약 설정에 있어서 너무 많은 정보의 교환이 발생하므로 프로토콜 동작 자체가 이동 환경에 적합하지 않으므로 이를 최소화 할 수 있는 노력의 일환으로 IKEv2(internet key exchange version 2)[9]에 대한 표준화 작업이 진행 중에 있다. CGA를 이용하는 경우 제공되는 보안 강도가 높고 절차가 간단하지만 각 MN에서 처리해야 하는 암호학적 연산의 양이 많아지므로 일반적으로 이동 단말의 낮은 성능을 고려할 때 적용이 어렵다.

5.2 인프라사용 방안

PANA[10]는 특정 AAA[11] 인프라구조를 이해하지 않고도 클라이언트가 백엔드 AAA 서버와의 연동을 통해 자신을 인증할 수 있도록 하는 인프라 제공을 목적으로 하고 있으며 EAP(extended authentication protocol) 확장을 통해 표준 정의가 진행 중이다. PANA 단독으로 사용하는 것은 의미가 없으며 기존의 인프라와의 연동을 통해 인증을 진행하므로 보안 강도는 기존 인프라의 보안 및 성능에 좌우된다. PKI는 인증서 관리 및 공인 인증기관의 설치 등의 추가 비용이 많으며 실시간 인증 구조에 적합하지 않다. 또한 규모면에서 보면 소규모 인증 시스템에는 적합하지 않은 고비용 저효과를 제공하므로 이동 단말에 대한 초기구동 절차상에 많은 부하 요인이 작용한다.

AAA는 기존 AAA 프로토콜인 RADIUS에서는 날로 증가하는 망 구성의 복잡도를 수용하기 어려움이 있기때문에 복수의 사업자에 의해 관리되는 통신망 상에서 로밍 인증 및 접근 제어를 수행하는데 적합하지 않는 문제가 있다. 그리고 RADIUS는 PAP, CHAP

등의 비교적 보안 강도가 낮은 방식의 인증구조를 가지고 있어 UDP기반의 취약한 전송 구조, 서버 오류에 대한 미흡한 대응, 송수신 패킷에 대한 보안성 결여, 동적인 이동 환경 적용을 위한 확장성 결여, 과다한 트랜잭션 발생으로 인한 인증 비용 증가, 프로토콜 제한으로 인한 파라메터 확장성 결여 등 그대로 적용하기에는 미흡한 점이 많다. 따라서 현재 IETF AAA에서는 이와 같은 RADIUS의 문제점을 보안하기 위해 새로운 AAA프로토콜인 DIAMETER를 표준화하고 있다.

Ⅵ. 결 론

MIPv6에서는MN가 로밍 환경에서의 MN와 홈 네트워크간의 인증절차로 인한 보안적인 문제를 다루어 보았다. 이를 초기구동에서의 문제점이라고 하는데 IETF WG에서 초기구동 시 보안해결 방안으로 많은 기술들이 나오고 이에 대해서 앞서 열거 하였다. 그중 해결방안으로 대두되고 있는 것은 AAA를 따른 DIAMETER 인증방식인데 이에 대한 표준화가 이루어지고 있는 상태이다. 로밍 환경에서의 초기구동 절차는 무엇보다도 모바일 환경에서 가장 중요하고 시급히 해결하여야 하는 문제이다. 표준화가 이루어지고 있는 AAA인증방식의 DIAMETER를 적용하여 실제 로밍 환경에서 홈 망간에 인증방식을 고려하여 연구해야 할 것이다.

참 고 문 헌

[1] D. Johnson, C. Perkins and J. Arkko," Mobility Support in IPv6, "RFC 3775, June 2004.

[2] A. Patel, "Problem Statement for bootstrapping Mobile IPv6," draft-ietf-mip6-bootstrap-ps-01.txt, Oct 2004.

[3] J. Arkko, T. Aura and J. Kempf," Security IPv6 Neighbor and Router Discovery," Microsoft Recearch 2003.

[4] S.Thomson and T.Narten," IPv6 Stateless Address Autocofiguration," RFC 2462, Dec 1998.

[5] J.Arkko, J.Kempf, B.Sommerfeld, B.Zill and P.Nikander," Secure Neighbor Discovery," draft-ietf-send-ndopt-06.txt, July 2004.

[6] T.Aura," Cryptographically Generated Addresses(CGA)," draft-ietf-end-cga-06.txt, April 2004.

[7] J. Arkko, V. Devarapalli and F. Dupont," Using IPsec to Protect Mobile IPv6 Signaling Between," RFC3776, June 2004.

[8] Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov 1998.

[9] V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture," draft-ietf-mip6-ikev2-ipsec-00.txt, Oct 2004.

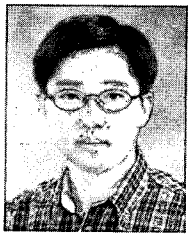
[10] J. Jee, J. Nah and K.Chung," Diameter Mobile IPv6 Bootstrapping Application using PANA," draft-jee-mip6-bootstrap-pana-00.txt, Oct 2004.

[11] B. Aboba and J. Wood," Authentication, Authorization and Accounting (AAA) Transport Profile," RFC 3539, June 2003.

〈著 者 紹 介〉

전 용 수 (Yong Su Jeon)

2004년 2월 : 동의대학교 소프트웨어공학과 졸업(공학사)
2004년~현재 : 동의대학교 컴퓨터·소프트웨어공학부 석사과정



이 종 민 (Jong Min Lee)

1992년 2월 : 경북대학교 컴퓨터공학과 졸업(공학사)
1994년 2월 : 한국과학기술원 전산학과졸업(공학석사)
2000년 2월 : 한국과학기술원 전자전산학과 전산학전공 졸업(공학박사)
1999년~2002년 : 삼성전자 무선사업부 책임연구원

2002년~현재 : 동의대학교 컴퓨터·소프트웨어공학부 조교수

권 오 준 (Oh-Jun Kwon)
정회원

1986년 2월 : 경북대학교 전자공학과 졸업(공학사)
1992년 2월 : 충남대학교 대학원 전산학과(이학석사)
1998년 2월 : 포항공과대학교 대학원 전자계산학과(공학박사)
1986년 1월~2000년 2월 : 한국전자통신연구원 선임연구원
2000년 3월~현재 : 동의대학교 컴퓨터·소프트웨어공학부 조교수