Static Shared Key를 적용한 HMIPv6 LBU 인증

김보미° 김태은 주소진 전문석
숭실대학교 대학원 컴퓨터학과
{bomi°,eunii31, yetiblow, mjun}@ssu.ac.kr

Apply a Static Shared Key to Authorizing LBU of HMIPv6

Bo Mi Kim° , Taeeun Kim, So Jin Ju, Moon-seog Jun
Graduate School of Computing, Soongsil University

요 약

단말의 이동성을 지원하는 Mobile IP에서 MN이 홈 네트워크에서 먼 곳으로 이동하는 경우, 매번 BU 시그널링을 하게 되면 Registration latency가 길어져, 이로 인해 불필요한 네트워크 트래픽을 유발한다. 따라서 계층을 두어 지역적인 이동성을 관리하는 MAP을 도입한 HMIPv6가 제안되었다. HMIPv6는 지역적인 LCoA와 외부에 노출되는 RCoA를 가진다. Mobile IP 환경에서의 BU메시지 취약성은 보안이슈가 되어왔으며, HMIPv6은 두 개의 CoA를 가지므로 보안위협은 배가된다. 본 논문에서는 Static Shared Key를 사용하여 HMIPv6의 LCoA BU 시그널링 관련 메시지의 인증을 제안함으로써 Mobile WG에서 제기된 BU 시그널링의 보안 취약성을 개선하였다.

1. 서 론

인터넷의 급격한 성장과, Mobile Node(MN)가 많은 기능을 수행할 수 있도록 발전하면서 사용자들을 위한 이동 서비스 요구가 증가했다. 이에 Internet Engineering Task Force(IETF)에서는 이동성을 제공하기 위해 Mobile IP 프로토콜을 발표하였다. Mobile IPv6[1,2]에서는 위치정보를 바탕으로 MN의 이동을 지원한다. Mobile IP는 단말이 서브넷을 변경하는 경우 항상 홈 네트워크에 있는 Home Agent(HA)에 현재 위치에 대한 등록을 수행하여야 한다. 또한 경로 최적화 방법을 사용하는 경우 Correspondent Node(CN)에 대해서도 Binding Update(BU)를 수행하여야 한다. 만일 MN이 홈 네트워크에서 먼 거리로 이동한 경우 이러한 등록 방식은 긴 등록 시간을 유발하며 네트워크에 불필요한 트래픽을 유발시킨다. 지역 이동성 관리 방법은 이러한 문제를 해결하기 위하여 제안되었으며 기본 개념은 각 지역 도메인이 지역 이동성 에이전트를 가지며 지역 내의 이동성은 지역 이동성 에이전트가 처리하게 함으로써 HA나 CN에 MN의 지역적인 이동성을 숨기는 것이다.

지역 이동성을 구현하기 위한 한가지 방법으로는 Mobile IP를 계층적으로 구성하는 HMIPv6[3]가 있다. HMIPv6란 MN의 이동 특징에서 착안된 방법으로 Mobile IP에 지역성(Locality) 개념을 추가하여 지역 내 이동 발생시 지역 이동성을 총괄하는 MAP(Mobile Anchor Point)을 지역 내부와 외부의 경계에 둠으로써 경계지점에서 주소 mapping을 처리하고 MN에 대해서는 임시 HA 역할을, HA에 대해서는 MN 역할을 처리하도록 한 기술이다. 이렇게 함으로써 지역 이동 발생시 홈 등록을 위한 시그널링의 양을 크게 줄일 수 있다.

Mobile Working Group(WG)에서는 Mobile IPv6 보안 문제가 제기되면서, 이를 해결하기 위해 Mobile IPv6 Design Team(DT)을 결성하였다. 본 문서에서는 DT에서 제안한 네 가지 Mobile IPv6 보안문제 중 ' BU를 수행할 때 발생할 수 있는 공격으로부터 안전하게 BU를 수행할 수 있는 방법' 에 초점을 맞추어 HMIPv6에서 지역주소인 LCoA의 BU실행 시 시그널링 메시지의 보안 취약점을 최근 발표된 " Securing Mobile IPv6 Route Optimization Using a Static Shared Key" [4]의 Binding Management Key(Kbm) 통한 인증을 제안한다.

2. 관련연구

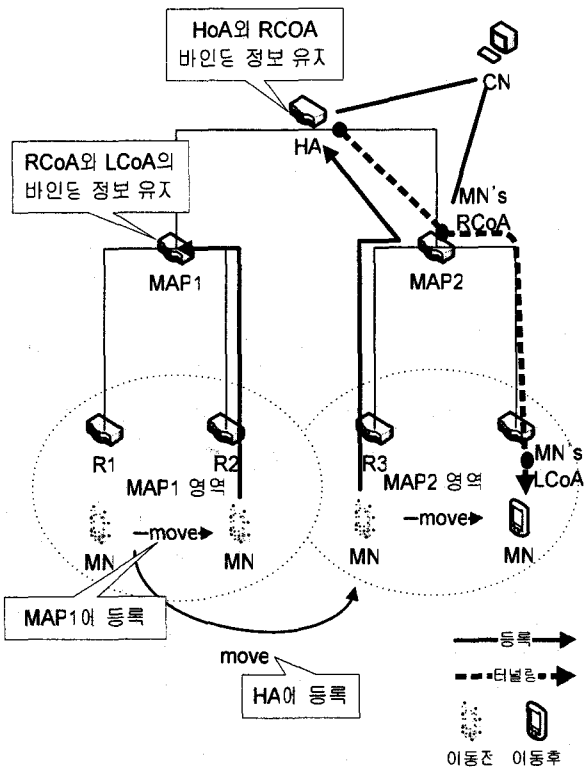
2.1 Hierarchical Mobile IP

Mobile IPv6는 서브넷을 이동할 때마다 CN과 HA에

대한 BU를 수행해야 한다. CN에 대한 BU를 인증하기 위하여 사용되는 RR(Return Routability)의 경우 최소 1.5 라운드 트립 지연(round trip delay)이 발생한다. 따라서 이러한 지연으로 인하여 핸드오버 시에 서비스의 단절이 발생하게 된다. 또한 백본 망에서의 시그널링 트래픽 증가, CN 및 HA의 무선 구간에서의 시그널링 증가를 가져온다. 따라서 지역적 이동성을 관리하는 지역 앵커를 도입한다면 BU에 필요한 지연을 줄일 수 있을 뿐만 아니라 이러한 이동성 시그널링의 양을 줄일 수 있다. HMIPv6에서는 이를 위하여 MAP(Mobile Anchor Point)를 도입한다. MAP은 경계지점에서 주소 사상(mapping)을 처리하고 개념적으로 MN에 대해서는 임시 HA 역할을, HA에 대해서는 MN 역할을 처리한다. 동일한 MAP 영역 내에서의 이동은 CN과 HA에게 숨겨지게 된다. HMIPv6에서 이동 단말은 3가지 주소를 가지게 된다. 즉, 홈 네트워크에서 구성한 고유한 Home of Address(HoA), 액세스 네트워크에서 구성한 on-link CoA(LCoA) 그리고 MAP을 기반으로 구성한 Regional CoA(RCoA)를 가진다. CN과 HA는 CN의 위치를 RCoA로 인식하며 이 주소로 데이터를 전송한다. MAP은 RCoA와 LCoA 간의 바인딩 정보를 이용하여 데이터를 최종적으로 MN에게 전달한다.

HMIPv6는 MAP이라는 새로운 개체가 필요하지만 MN에 대해서는 최소 확장만이 필요하고 CN과 HA에 변경이 요구되지는 않는다. 또한 Mobile IPv4에서 계층적인 구조를 제공하는 Mobile IPv4 Regional Registration과는 구조적인 유사성으로 인하여 자연스러운 발전이 가능하다는 장점을 가진다.

HMIPv6에서 BU는 지역 등록과 일반적인 등록으로 구분된다. MN이 MAP이 관리하는 영역에 진입하면 라우터의 주기적인 Router Advertisement(RA) 메시지를 받는다. 이 RA에는 해당 라우터가 MAP의 영역 내에 있음을 알리는 MAP 옵션을 포함하고 있다. MAP 옵션이 포함된 RA를 받은 MN은 라우터상의 LCoA와 MAP 상의 RCoA를 stateless auto-configuration[5] 형태로 생성한다. LCoA와 RCoA를 구성한 후 MN은 LCoA를 소스 주소로하고, MAP 주소를 목적지 주소로, RCoA를 home address option으로 하여 지역적 바인딩 메시지를 보낸다. MAP은 LCoA와 RCoA를 바인딩 하여 Binding Acknowledge 메시지를 MN에게 돌려준다. 지역적 바인딩이 성공적으로 이루어지면 MN은 HA와 CN에 대하여 Mobile IPv6에서 규정된 BU를 수행한다. 이 BU 메시지는 소스 주소를 RCoA, 목적지 주소를 HA/CN의 주소로, home address option에는 MN의 HoA를 담아서 BU 메시지를 보내게 된다. 만일 MN이 MAP1 영역 내의 다른 라우터(R2)로 이동하는 경우 HA/CN에 대해서는 동일한 RCoA를 가지므로 HA로의 BU는 필요로 하지 않고, LCoA를 갱신하는 지역적 BU만이 필요하게 된다. 따라서 동일한 MAP 영역 내에서의 MN의 이동은 HA/CN에 투명하게 이루어지게 된다. 등록이 완료된 이후 MN으로 전달되는 데이터가 있으면 이 데이터는 RCoA로 전달되며 MAP은 이 데이터를 터널링을 통해 MN의 LCoA로 전달한다. MN이 CN으로 데이터를 전송하는 경우 MAP 간의 터널링을 통해서 전송하며, CN과의 직접적인 전송을 하고자 하는 경우 RCoA를 소스 주소로 하여 CN으로 직접 데이터를 전송할 수도 있다.



(그림 1) HMIP Operation

2.2 Static Shared Key를 사용한 Securing Mobile IPv6 Route Optimization

Mobile IPv6 에서 Route Optimization(RO) 메시지의

시그널링 메시지를 보호하기 위해 low-latency 보안 구조로 고안된 이 기법은 MN과 CN이 사전 협약된 데이터를 이용하여 Binding Management Key(Kbm)를 생성하여 BU 메시지를 안전하게 인증 할 수 있도록 고안된 방법이다.

기본적인 구조로 Mobile IPv6[2]와 같이 주기적인 RR 테스트를 사용하여 MN의 HoA와 요청되는 CoA의 유효성 검사를 한다. 이 구조는 MN의 HA이상의 신뢰할 수 있는 장치를 구성하는 대신에 MN과 CN 공유할 수 있는 비밀키를 가진다. 결과로 routability 검사에 관련된 메시지들은 생략될 수 있으며, 이로 인해 상당한양의 지연을 줄이게 된다. 이 기법은 Kbm을 위한 데이터(patameters)를 공유 하므로 회사 내부나 특정 사용자 간의 연결 등의 제한된 구조에서 유용하다.

Kbm을 생성함으로써 바인딩 관리 메시지의 인증이 가능하며, 특히 BU와 Binding Acknowledgement(BA) 인증에 유용하다. 키를 생성하기 위해 다음과 같은 데이터를 필요로 한다.

- 공용키(Shared Key: Kcn) 생성을 위한 최소 20 octet 이상의 keygen token
- CoA 생성을 위한 임시 keygen token
- HoA 생성을 위한 임시 keygen token

keygen token과 다른 파라미터들은 Mobile IPv6[2] 의 RR 파트에 명시된 값들을 사용하며, Kbm 역시 같은 방법으로 생성된다. Kbm을 이용한 BU의 Sequence Number 값을 통해 Replay Attack을 방지할 수 있다. CN이 최근 사용된 Sequence Number를 인지하지 못하는 경우 악의적인 노드가 이전의 BU 메시지를 사용하여 Replay attack을 하거나 CN을 속여 다른 CoA로 라우팅 되게 할 수도 있기 때문에, 이 기법은 사전에 계산된 Kbm 값을 사용하여 SN 필드의 최신 값을 안전하게 공유할 수 있게 된다.

실제 시스템에서의 실용적인 보안수준과, 문서에서 요구된 보안수준을 고려하여, 수동적인 Kbm의 생성은" Guidelines for Cryptographic Key Management" [7] 에서 명시된 바를 준수해야 한다. 또한 Dictionary Attack 을 방지하기 위해 데이터가 아닌, BU의 인증에만 사용되어야 한다.

이 기법은 간단하며, 기존의 Mobile IP를 구성하는 개체 이외의 새로운 보안 개체를 필요로 하지 않으므로 같은 관리체계를 가지는 개체간의 BU를 안전하고, 간단하게 인증할 수 있다.

3. 제안방안

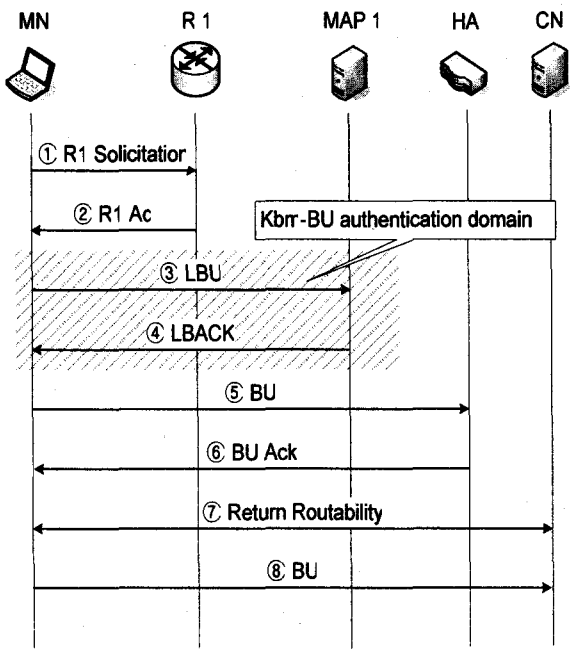
3.1 Mobile IP BU 보안 취약성 분석

Mobile IPv6 가 표준으로 제정되기 이전 환경에서는 시그널링 메시지를 강력하게 보호하기 위해 IPsec[6]을 이용하여 BU 메시지를 보호하도록 하였는데, BU 를 강력하게 인증하기 위해 이 방법을 사용하려면 글로벌 PKI(Public Key Infrastructure) 구조를 구축해야 하고, 이것은 현재 인터넷 상황에서 가능하지도 강조되지도 않는다. 대신 MN 과 CN 사이에 BU 를 안전하게 교환하기 위해서 Binding Security Association(BSA)를 설정하는 등의 약한 인증방법이 사용된다. BU 시그널링 시 발생할 수 있는 보안 문제를 경우 별로 살펴보면 다음과 같다. 첫 번째로 MN 이 HA 로 BU 메시지를 전송할 때, attacker 는 어떤 MN 에 대해 현재 위치한 곳과 다른 곳에 위치해 있다는 정보를 줄 수 있고, HA 가 이 정보를 받아들이면, MN 은 패킷을 받지 못하는 반면 다른 노드가 원하지 않는 패킷을 수신하게 된다. 두 번째로, CN 으로 BU 메시지를 전송할 때, 악의적인 MN 이 자신의 HoA 를 victim 의 HoA 로 설정하여 거짓 정보를 알릴 경우, CN 이 그 정보를 받아들인다면, CN 에서 victim 으로 전송하고자 하는 패킷은 MN 을 거치게 되므로 MN 은 availability 와 confidentiality 를 모두 위협한다. MN 이 자신의 CoA 를 거짓으로 알리는 경우, CN 은 MN 으로 보내는 패킷을 모두 거짓 CoA 로 전송하여 DoS(Denial of Service) 공격을 할 수 있다. CN 으로 의미 없는 BU 메시지를 한꺼번에 다량 전송할 경우에는 CN 의 자원을 고갈시켜 유효한 패킷을 처리할 수 없게 만들기도 한다. 또한 Attacker 는 오래된 BU 메시지를 replay 하여 패킷들을 MN 의 예전 위치로 전달시켜 패킷을 수신하지 못하게 만들 수 있다.

이런 공격들을 막기 위해서 MN 이 BU 메시지를 전달할 때 HA 로는 IPsec ESP(Encapsulation Security Payload)를 사용하여 패킷을 보호하고, CN 으로 BU 메시지를 전송할 때에는 보안을 위한 기본 메커니즘으로 RR 을 이용하여 HoA 와 CoA 가 도달가능한지를 확인한 후 메시지를 전송하는 방식을 적용하고, 필요한 경우에 RR 방식보다 더 강력한 메커니즘을 추가적으로 사용하는 방향으로 결론 지어졌다.

3.2 Static Shared Key 적용방안

기존의 Mobile IP와 비교하여 이동성을 고려하여 시그널링 메시지를 크게 줄일 수 있었지만, MAP을 두어 지역 이동성을 고려한 HMIPv6 기법의 문제점 중 하나는 보안 위협성 증가이다. HMIPv6 구조상 MN은 두 개의 CoA를 구성해야 하고 이 정보는 AR(Access Router)로부터 advertisement 메시지를 통해 제공받게 되므로 BU 보호에 관련해서 기존의 Mobile IP구조에 비해 보안 위협이 배가 되며, MAP에 바인딩 Flooding 공격이 가해질 경우 MAP은 DoS 위협에 노출되며, 해당 MAP 하에 속해있는 MN들의 통신에 장애가 될 수 있다. HMIP은 특별한 보안규정을 명시하지 않으므로 다른 구조에 의한 BU의 인증은 반드시 필요하다. 따라서 본 논문에서는 Static Shared Key를 사용하여 BU 시그널링 메시지를 보호하고자 한다.



(그림 2) Kcm 적용을 위한 HMIP Message Flow

(그림 2)에서는 " Securing Mobile IPv6 Route Optimization Using a Static Shared Key" 의 Kbm을 적용하여 바인딩 시그널링에 사용되는 메시지를 인증하는 영역을 나타낸다. MN이 MAP1내의 다른 라우터 영역으로 이동을 감지하면 현재 속해있는 네트워크의 라우터인 R1에서 새로운 R2의 링크를 획득하기 위해 MAP1에게 ③LBU로 LCoA를 요청하게 된다. Kbm을 위한 데이터(patameters)를 공유하고 있는 MAP1은 사전 협약된 파라미터로 계산된 Kbm을 이용하여 최근 사용된 Sequence Number 비교와 DAD(Duplicate Address Detection) 등을 수행하고 유효한 LCoA 여부에 관한 ④LBACK 메시지를 전송하게 되고, 이 때 HA와 CN 혹은 다른 MAP이 알아챌 수 없는 LCoA만이 변경된다. 따라서 MN은 HA에게 BU를 전송하는 것이 아니라 MAP1 내에서만 BU 시그널링이 발생하게 된다. 따라서 같은 MAP 소속되어 있는 객체간에 발생하는 이 지역적인 BU메시지를 Kbm을 적용하여 인증하면 Redirect, Flooding, Resource Exhaustion, DoS 공격과 이외에도 인증되지 않은 BU메시지로 인해 발생할 수 있는 몇몇의 알려진 잠재적인 공격[8,9,10]에 대응함으로써 보안 요구조건에 부합함과 동시에 적은 비용으로 외부 노드의 공격에 대응할 수 있는 안전한 방식을 취하게 된다.

4. 결론 및 향후 과제

이 문서에서는 HMIPv6에서 동일한 MAP내에서 MN의 이동으로 인하여 LCoA 변경 요청 시 발생하는 바인딩 시그널링 메시지를 인증하기 위해서 제한적인 지역 내에서 효율적으로 BU를 인증하도록 고안된 " Securing Mobile IPv6 Route Optimization Using a Static Shared Key" [4] static shared key인 Kbm을 사용하여 LBU와 LBACK메시지에 포함시켜 최신의 Sequence Number를 유지하고, BU에 가해질 수 있는 잠재적인 공격에 대응할 수 있는 방안을 제시하였다.

향후 Mobile IPv6 환경하의 MN은 더욱 자유로운 이동성을 요구할 것이다. MN이 외부 네트워크로 이동하였을 때 해당 네트워크에서 할당 받은 CoA와 홈 네트워크의 HoA를 HA에 바인딩 함으로써 MN은 연속적인 연결을 유지 할 수 있다. 이렇게 MN이 다른 네트워크로 이동하는 것을 Handover라고 하는데 이때 MN은 통신을 할 수 없는 Handover Latency를 가지게 된다. 이러한 지연은 특히 실시간 전송에 있어서 큰 문제를 드러낸다. Fast Handover[11]는 이러한 Handover Latency를 줄임으로써 MN에게 보다 나은 서비스를 제공한다. 보안문제를 해결한 HMIPv6와 FMIP의 적절한 결합을 적용시킨 구조야말로 지연을 더욱 줄일 수 있는 이상적인 구조가 될 것이며, 향후 과제로는 HMIPv6와 FMIP의 결합과 더불어 본 문서에서 제안한 Static Shared Key

방식을 적용하여 지역적인 BU 시그널링 메시지를 인증하면 외부 공격에 더욱 안전한 low-latency Mobile 네트워크를 구성하게 될 것이다.

5. 참고문서

[1]S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", Request for Comments 2460, Internet Engineering Task Force, December 1998

[2]D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", Request for Comments 3775, Internet Engineering Task Force, June 2004

[3]H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, " Hierarchical Mobile IPv6 Mobility Management (HMIPv6)" , Request for Comments 4140, Internet Engineering Task Force, August 2005

[4]C. Perkins, " Securing Mobile IPv6 Route Optimization Using a Static Shared Key" , Request for Comments 4449, Internet Engineering Task Force, June 2006

[5]S. Thomson, T. Narten, " IPv6 Stateless Address Autoconfiguration" , Request for Comments 1971, Internet Engineering Task Force, August 1996

[6]S. Kent, R. Atkinson, " Security Architecture for the Internet Protocol" , Request for Comments 2001, Internet Engineering Task Force, November 1998

[7]S. Bellovin, R. Housley, " Guidelines for Cryptographic Key Management " , Request for Comments 4107, Internet Engineering Task Force, June 2005

[8]Aura, T., Roe, M. and Arkko, J., Security of Internet Location Management, In Proc. The 18th Annual Computer Security Applications Conference, Las Vegas, 2003

[9]Aura, T., Mobile IP Security, Security Protocols: The 10th Int' l Workshop, Cambridge, U.K., Apr. 17-19, 2002, LNCS 2845, Springer Verlag 2003

[10]O' Shea, G. and Roe, M., Child-proof Authentication for MIPv6 (CAM), ACM Computer Communications Review, 31 (2), July 2001

[11]R. Koodli, Ed. " Fast Handovers for Mobile IPv6" , Request for Comments 4068, Internet Engineering Task Force, July 2005