이동성 지원을 위한 Mobile IPv6 관련 보안 이슈

TTA IPv6 프로젝트그룹 부의장, 삼성전자 전문연구원 **이 병 준**

1. 서론

본 고에서는 현재 인터넷 프로토콜에 관한 표준문서를 제정하고 있는 IETF (Internet Engineering Task Force) 국제 표준화 기구에서 작업중인 Mobile IPv6 관련 보안이슈에 대한 고찰과 관련 표준화 동향을 소개하고자 한다. Mobile IPv6 표준화 문서작업은 mip6 WG(Mobility for IPv6 Working Group)에서 진행되고 있다[1]. 비교적 많은 양의 표준문서 작업 내용을 이곳에 자세히 소개하기에는 할당된 지면의 제약이 있으므로, 이곳에서는 개략적인 이슈를 소개하고, 대신 관련 표준 문서들을 참고문헌으로서 포괄적으로 리스트 해보고자 한다.

2. Mobile IPv6 프로토콜

Mobile IPv6 [2]는 IPv6 주소체계하의 네트워크에서 이동성 지원을 위한 프로토콜로서, 이러한 환경에서의 보안 이슈들을 열거하기 전에 Mobile IPv6 프로토콜에 대해 간략히 기술한다.

IPv6 기반의 애플리케이션을 탑재한 모바일 기기가 이동하는 중에 기기가 속해있는 서브넷(Subnet)이 바뀌게 되면, 그 기기가 가지고 있는 IPv6 주소가 바뀌어야 하고, 그 결과로 현재 진행중인 애플리케이션 세션(application session)이 끊어지게 된다. Mobile IPv6 프로토콜은 이러한 주소의 변경을 애플리케이션 단으로부터 감추어 줌으로써 문제를 해결하고자 하는 것이다. Mobile IPv6에 관한 더욱 상세한 기술은 표준문서

RFC 3577[2]와 참고문헌[3]에서 찾아 볼 수 있다.

3. Mobile IPv6 관련 기본 보안 이슈들

어떠한 종류의 이동성 지원 솔루션이나 프로토콜들도 이동에 따른 속성이나 지원 메커니즘을 이용한 보안 관련 공격에 대한 방어수단을 제공하여야 한다. Mobile IPv6 프로토콜이 동작하는 상황에서 예견될 수 있는 대부분의 위협들은 위조된 BU(Binding Update) 시그널링 메시지와 관련된 DoS(Denial-of Service) 공격을 생각할 수 있으며, 다른 종류의 위협들은 Man-in-the-Middle, Hijacking 등이 있을 수 있다.

이러한 보안 위협들에 대한 대처 방안으로서 Mobile IPv6 표준문서는 기본적으로모바일 기기(Mobile Node - MN)가 홈 에이전트(Home Agent - HA)와 CN(Correspondent Node)이 주고받는 BU(Binding Update) 메시지, 그리고 이동 프레픽스(Mobile Prefix) 발견 메시지를 보호하는 것, 그리고 데이터 패킷 자체를 보호하는 메커니즘 등을 정의하고 있으며, 각각의 사례에 대한 보안 메커니즘을 다음에 기술한다.

3.1 MN과 HA 간의 BU 시그널링 메시지 보안

모바일 기기(MN)와 홈 에이전트(HA) 간에는 BU(Binding Update) 시그널링 메시지의 무결성(Integrity)과 확실성(Authenticity)을 보장하기 위하여 반드시 IPsec 보안제휴(Security Association - SA) 메커니즘을 사용하여야 한다. 또한 MN과 HA는 반드시 ESP(Encapsulating Security Payload)를 트랜스포트 모드(Transport Mode)에서 지원하여야 하며, non-NULL payload 인증 알고리즘을 사용하여 데이터 소스의 인증, connectionless 무결성 그리고 선택사양인 anti-replay 방지 등을 제공할 수 있어야 한다.

IPsec 프로토콜을 사용하여 모바일 기기(MN)와 홈 에이전트(HA) 간의 통신을 안전하게 보장하는 메커니즘 및 예제들에 대한 더욱 상세한 기술은 표준문서[4]에서 찾아볼 수 있다.

3.2 MN과 CN 간의 BU 시그널링 메시지 보안

모바일 기기(MN)와 통신하는 Correspondent Node(CN)로 보내지는 BU 시그널링 메시지를 보호하기 위해서는 위에서 언급한 IPsec SA 메커니즘이나 인증 구조기반(authentication infrastructure)이 MN과 CN 간에 필요치는 않다. 그 대신 리턴 라우터빌리티(Return Routability - RR)라 불리는 절차를 이용하여 적법한 모바일 기기가 CN에게 BU 메시지를 보내고 있다는 것을 확인만 하면 된다. 이러한 RR을 이용한 보안방법의 장점과 약점 등의 구체적인 기술은 표준문서[2]에 정의되어 있다.

3.3 이동 프레픽스 발견(Mobile Prefix Discovery) 관련 보안

모바일 기기(MN)와 홈 에이전트(HA)는 IPsec 보안제휴(Security Association) 메커니즘을 사용하여 이동 프레픽스(Mobile Prefix) solicitation과 advertisement 시그널링 메시지를 보호하여야 한다. 또한 위에서 언급한 MN과 HA 간의 BU 시그널링 메시지 보안의 경우와 마찬가지로, 반드시 ESP(Encapsulating Security Payload)를 트랜스포트 모드(Transport Mode)에서 지원하여야 하며, non-

NULL payload 인증 알고리즘을 사용하여 데이터 소스의 인증, connectionless 무결성(Integrity) 그리고 선택사양인 anti-replay 방지 등을 제공할 수 있어야 한다.

3.4 데이터 트래픽 패킷 보안

모바일 기기(MN)와 Correspondent 노드(CN) 간에 주고받는 데이터 패킷을 보호하는 방법은, 고정 기기가 IPv6 주소체계에서 사용하는 방법(예, IPsec, 등)을 사용하면 되지만, Mobile IPv6 프로토콜이 선택사양으로서 홈 어드레스 데스티네이션 옵션(Home Address Destination Option), 라우팅 헤더(a routing header), 그리고 터널링 헤더(tunneling header) 등을 패킷 페이로드(payload) 내에 사용하므로 이에 대한 대응방법이 필요하게 된다. 이러한 대응 메커니즘에 대한 구체적인 정의는 역시 표준문서[2]에서 찾아 볼 수 있다.

4. 추가적인 보안이슈와 대응 메커니즘

위에서 언급한 Mobile IPv6 관련한 기본적인 보안 이슈와 대응 메커니즘 이외에도, 현재 IETF mipv6 WG에서 공식문서로 추가 작업하고 있는 보안이슈와 메커니즘을 아래에 소개한다. 그 이외에도 mipv6 WG에서는 아직 공식문서로 작업하고 있지 않지만, 개인 기고문(individual draft) 등을 통해 제기된 보안 이슈 및 해결방안, IRTF(Internet Research Task Force) 표준화 기구에서 고려되고 있는 이슈 등도 다루어본다.

4.1 공식 mipv6 WG에서 추가로 작업중인 보안 이슈들

- 리턴 라우터빌리티(Return Routability - RR)에서 문제가 되는 전송지연을 줄이기 위해 모바일 기기(MN)와 correspondent node(CN) 간의 기계산된 binding management key를 사용하는 것과 IPsec을 사용하는 방법 등이 표준화 문서[5, 6]에서 정의되고 있다.

- 표준문서[7]에서는 모바일 기기와 CN 간에 IPsec을 사용하지 않고 시그널링 메시지 보안을 유지하는 메커니즘을 정의하고 있는데, 이는 실제로 Mobile IPv6 프로토콜이 네트워크 환경에서 구현 적용되는데 보다 유용성(flexibility)을 제공할 수 있도록 하고자 함이다. 이러한 적용의 예로서는 3세대 이동통신망 규격을 정의하고 있는 3GPP2 문서에서도 발견할 수 있다.

- 표준문서[8]에서는 현재 IPv4 주소체계의 인터넷에서의 보안장치로 널리 구축되어 있는 방화벽(Firewall) 운영이슈에 대한 논의를 기술하고 있다. IPv6 네트워크 이동성 지원을 위한 Mobile IPv6 표준 프로토콜이 제정된 지 얼마되지 않을 뿐 아니라, 운영경험도 일천한 이유로 대부분의 IPv6용 방화벽 메커니즘들은 Mobile IPv6를 고려하지 못하고 있는 실정이다. 그러나 이러한 문제들이 해결되지 않는한, 기존의 방화벽들이 원활한 프로토콜의 동작을 방해할 수 있을 뿐만 아니라, Mobile IPv6가 광범위하게 적용되는데 커다란 장벽이 될 것이다. 더욱이 이러한 이슈들은 기업망을 보호하는 방화벽의 문제일 뿐만 아니라, GPRS/UMTS 그리고 cdma2000과 같은 3세대 이동통신 네트워크에서도 문제를 야기시킬 수 있을 것이다.

- 표준문서[9]에서는 새롭게 개정된 IPsec 아키텍처와 IKEv2(Internet Key Exchange Protocol

version 2)를 이용한 Mobile IPv6 프로토콜의 동작을 기술하고 있다.

4.2 기타의 Mobile IPv6 관련 보안 이슈들

위에서 언급한 공식적인 표준 문서들 이외에도, Mobile IPv6 프로토콜을 적용 운영함에 있어서 보다 더 효율적이고 안정적으로 보안이슈를 해결할 수 있는 메커니즘 등의 제안을 기술하고 있는 개인 기고 문서들이 있는데[10, 11, 12], 이러한 개인기고 문서들은 mip6 WG에서 많은 논의를 거쳐 공식적인 작업문서로서 승격될 것이다.

마지막으로 IETF의 mipshop(Mobile IPv6 Signaling and Handoff Optimization) WG에서는 Mobile IPv6 프로토콜 동작 시 발생하는 시그널링 오버헤드(overhead)로 인한 비효율성 문제와, 모바일 기기의 핸드오프 도중의 지연시간 및 패킷 손실을 최소화하기 위한 최적화 메커니즘을 표준문서[13]에서 정의하고 있는데, 이 문서에서는 어떻게 모바일 기기(MN)가 핸드오프 이전의 엑세스 라우터(Previous Access Router - PAR)와 보안제휴(Security Association - SA)를 맺어야 하는지에 대한 부분이 기술되어 있지 않다. 이러한 MN-PAR 간의 SA 메커니즘에 대한 연구 및 정의는 현재 IETF 표준화 기구의 연구단체인 IRTF (Internet Research Task Force)의 MobOpts RG (IP Mobility Optimization Research Group)[14]에서 다루어지고 있으며, 관련 기술내용은 IRTF 표준문서[15, 16]에서 찾아볼 수 있다.

5. 맺는말

IPv6 주소체계하에서 이동성 지원을 위한 프로토콜인 Mobile IPv6의 원활한 서비스를 위해서는 보안 메커니즘이 중요한 기능 중의 하나이지만, 여타 표준기반의 서비스들과는 달리 해결하기가 까다로운 문제이기도 하다. 그 중요한 이유로서는, 첫째, 이동하는 통신단말들이 IPv6 네트워크 안에서 아무때나 임의의 장소에 위치할 수 있으며(예: MN-HA, MN-CN, MN-AR), 둘째, 실시간의 트래픽을 빠른 이동성 환경에서 지원해야 하며, 셋째, 제한된 무선자원과 단말의 프로세싱 성능의 (processing capacity) 제한 등이 추가적인 제약조건이 된다.

현재로서는 IPv6, 나아가서는 Mobile IPv6 기반의 네트워크의 전개, 운영에 관한 경험이 상대적으로 성숙하지 못한 상황에서, 관련 보안 이슈에 대한 깊은 이해가 이루어지고 있지 못하고 있으며, 이러한 이유로 향후 심도있는 연구와 표준화 노력이 더욱 요구된다고 하겠다.

참고문헌

1. http://www.ietf.org/html.charters/mip6-charter.html
2. D. Johnson, et al. “Mobility Support in IPv6,” RFC 3775, June 2004.
3. Hesham Soliman, “Mobile IPv6 - Mobility in a Wireless Internet,” Addison-Wesley, 2004.
4. J. Arkko, et al. “Using IPsec to protect Mobile IPv6 signaling between mobile nodes and home agents,” RFC 3776, June

2004.

5. C. Perkins, "Precomputable Binding Management Key Kbm for Mobile IPv6," draft-ietf-mip6-precfgkbm-01.txt, October 2004.

6. F. Dupont and J. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes," draft-ietf-mip6-cn-ipsec-00.txt, January 2005.

7. A. Patel, et al. "Authentication Protocol for Mobile IPv6," draft-ietf-mip6-auth-protocol-04.txt, February 2005.

8. F. Le, et al. "Mobile IPv6 and Firewalls: Problem Statement," draft-ietf-mip6-firewalls-02.txt, May 2005.

9. V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture," draft-ietf-mip6-ikev2-ipsec-01.txt, February 2005.

10. A. Yegin, "AAA Mobile IPv6 Application Framework," draft-yegin-mip6-aaa-fwk-01.txt, February 2005.

11. HeeJin Jang, A. Yegin, J. Choi, "DHCP Option for Home Agent Discovery in MIPv6," draft-jang-dhc-haopt-01.txt, April 2005.

12. J. Bournelle, "Bootstrapping Mobile IPv6 using PANA," draft-bournelle-pana-mip6-00.txt, December 2004.

13. R. Koodli, ed. "Fast Handovers in Mobile IPv6," draft-ietf-mipshop-fast-mipv6-03.txt, October 2004.

14. http://www.irtf.org/charters/mobopts.html

15. J. Kempf, "Bootstrapping a Symmetric IPv6 Handover Key from SEND," draft-kempf-mobopts-handover-key-00.txt, June 2004.

16. A. Yegin, "Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication," draft-yegin-eap-boot-rfc3118-01.txt, January 2005. TTA