PMIPv6에서의 안전한 핸드오버 기법

나상호*, 신영록*, 허의남*
*경희대학교 컴퓨터공학과
e-mail:{shna, ekseldwe, johnhuh}@khu.ac.kr

Secure Handover Scheme for PMIPv6

Sang-Ho Na*, Young-Rok Shin*, Eui-Nam huh*
*Dept of Computer Engineering, Kyung-Hee University

요 약

노드의 이동성을 지원하는 Mobile IPv6에서는 단말과 홈 에이전트 간 시그널링 처리로 인한 부하를 줄이기 위해 Proxy Mobile IPv6가 제안되었다. 그러나, Proxy Mobile IPv6 역시 서브넷 이동에 따른 재인증 프로세스로 인해 지연이 발생하며 현재까지 Mobile IPv6와는 달리 보안 취약점에 대한 분석과 그에 맞는 보안 기법이 미비한 상황이다. 본 논문에서는 현재까지의 Proxy Mobile IPv6에 대한 보안 취약점 분석을 통해 안전한 핸드오버 기법을 제안한다.

1. 서론

앞으로의 인터넷 환경은 현재의 와이브로와 같이 다양한 모바일 단말에 대한 지속적인 이동성을 지원해야 한다. 이를 위해 IETF에서 Mobile IPv6를 제정하였으며 실제 환경에 적용을 위한 검증이 완료 되었으나 이동 단말과 홈 에이전트 간 시그널링 처리로 인한 부하로 인해 네트워크 기반에서 이동성을 지원하는 Proxy Mobile IPv6(PMIPv6)가 제안되었다. 그러나, 최근까지 PMIPv6에 대한 보안 취약점 분석이 미비하며, 그에 따른 안전한 보안 기법이 필요하다. 본 논문에서는 PMIPv6에 대한 보안 취약점 분석을 바탕으로 802.11n 환경의 PMIPv6에서 안전한 핸드오버 기법을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서 보안 취약점에 대한 분석을 통해 3장에 안전한 핸드오버 기법을 제안하고, 4장 결론을 통해 향후 연구 방향을 제시한다.

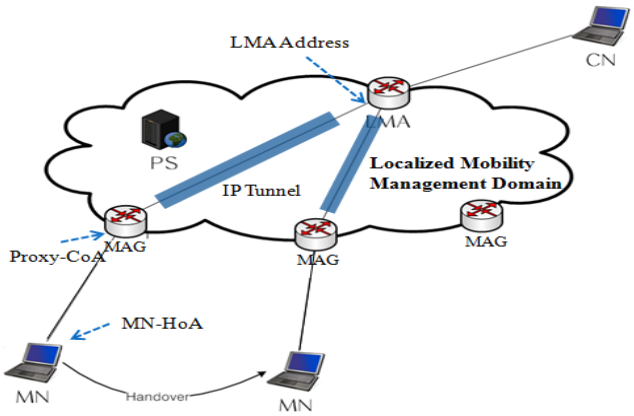
2. PMIPv6의 보안 취약점 분석

PMIPv6는 로컬 도메인에서 Mobile Node(MN)의 이동성 지원을 위하여 네트워크 기반의 관리 시스템을 제공하며 다음 [그림1]과 같은 구성을 가진다.

PMIPv6는 네트워크 인터페이스를 기준으로 크게 MN-MAG, MAG-LMA, LMA-CN의 세 구간으로 이루어져 있으며, 이를 바탕으로 보안 취약점[1]을 분석할 수 있다.

MN-MAG 구간에서 MAG는 지속적으로 MN의 이동을 모니터링하고 MN는 MAG에 의하여 안전하게 바인딩 되어야 한다. 그러나, 공격자는 패킷 리다이렉션과 핸드오프 시그널 변조를 통해 경로 업데이트 메시지 손실, 잘못된 바인딩 업데이트 메시지 등을 유발하여 네트워크 자원 소비를 유도하여 서비스 거부 공격 등에 이용할 수 있다.

MAG-LMA 구간은 MAG, LMA 위장과 침해를 통해 패킷 리다이렉션, 트랙픽 손실 및 서비스 거부 등의 공격이 가능하며, 마지막으로 LMA-CN 구간에서는 CN을 가장한 공격자의 대량 패킷 전송으로 LMA에 대한 서비스 거부 공격에 대한 위협이 존재한다.



[그림 1] PMIPv6 네트워크

이처럼 PMIPv6에서 다양한 보안 위협은 PMIPv6의 구성 엔티티인 Mobile Node(MN), Mobile Access Gateway (MAG), Local Mobility Anchor(LMA) 간 상호 신뢰성 확보 방안(인증), MN의 핸드오버 시 메시지 출처 인증(부인봉쇄) 및 데이터 전송 상의 기밀성과 무결성 보장 등의 보안 서비스를 위한 강력한 보안 메커니즘이 필요하다.

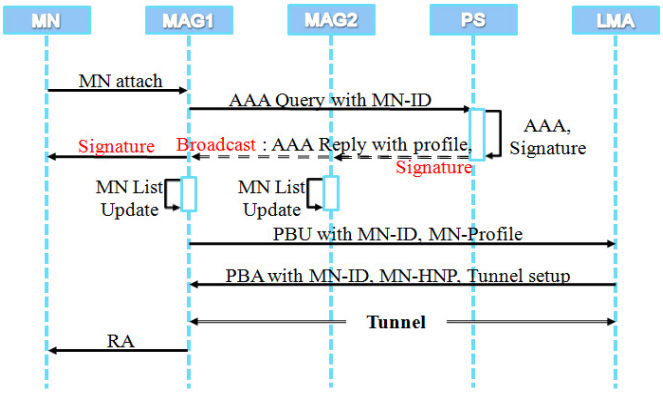
그 중에서도 MN의 핸드오버 시 시그널링 메시지 위·변조는 신분 위장, 패킷 리다이렉션, MITM(Man-in-the-Middle) 공격 그리고 서비스 거부 공격 등 다양한 공격의 루트로 사용될 수 있다. 따라서 다음 3장에서는 PMIPv6에서의 보안 취약점을 보완할 수 있는 안전한 핸드오버 기법을 제안한다.

3. PMIPv6의 안전한 핸드오버 기법

PMIPv6에서의 기존 핸드오버 기법은 주로 MN의 이동 시 재인증에 따른 지연을 줄이기 위한 방법[2, 3]들이 연구되고 있다. 본 논문에서는 안전한 핸드오버를 위하여 최초 모바일 노드 인증 및 핸드오버 시 인증 기법을 제안한다.

1) 최초 MN 인증

최초 MN가 인증 후 MN-ID 정보를 핸드오버 시 활용하기 위하여 각 MAG는 인증 완료 된 MN-ID 리스트를 가지고 있으며, 최초 MN의 세부 인증 기법은 [그림2]와 같다.



[그림 2] MN의 최초 인증

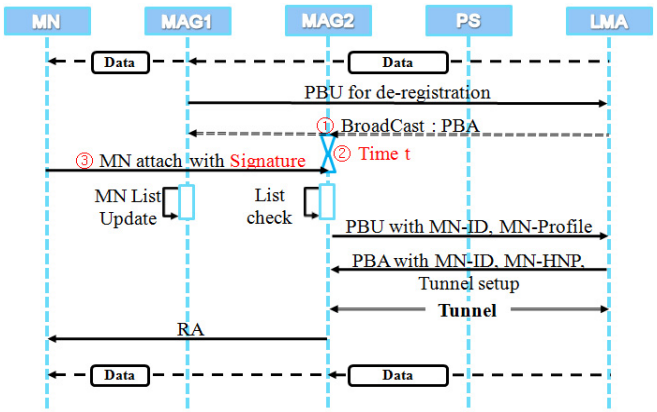
MN가 최초 접속하여 인증 시 PS(Policy Server)는 각 MN의 정보를 이용하여 Signature를 생성하고 AAA Reply 메시지와 함께 로컬 도메인의 모든 MAG에게 브로드캐스트한다. 메시지를 받은 MAG는 자신이 가진 MN-ID 리스트를 업데이트 한다. MN는 MAG와의 안전한 세션을 통해 Signature를 받아 통신 시 메시지 출처 인증에 사용한다.

2) 핸드오버 시 MN 인증

MN가 이동할 경우(그림3) 이를 감지한 MAG는 LMA에 알리고 LMA는 MN가 핸드오버할 것임을 로컬 도메인의 모든 MAG에게 ①PBA(Proxy Binding Acknowledgment)로 브로드캐스트 하여 알린다. 각 ②MAG는 시간 t 동안 MN의 Attach 메시지를 기다리고, ③시간 t 내에 MN의 Attach메시지를 받는 경우 자신이 가진 리스트 확인을 통해 MN를 인증하고 LMA에게 PBU(Proxy Binding Update) 메시지를 보낸다. 이때, MN로부터 Attach 메시지를 받지 못한 MAG는 자신의 MN-ID 리스트를 업데이트하고 만약 MN가 시간 t 내에 다른 MAG에 접속하지 못한 경우 MAG가 가진 MN-ID 리스트에서 삭제되므로 재인증(최초 MN 인증) 프로세스를 거쳐야 한다.

3) 핸드오버를 이용한 공격 탐지

RFC5213에서 기술하고 있듯이 LMA-MAG 간 보안은 IPsec을 이용하여 시그널 및 데이터 보안을 보장한다. 따라서 LMA, MAG를 신뢰할 수 있을 때, 다양한 네트워크 공격의 시발점은 MN의 위장을 통한 거짓 핸드오버 시그널 발생이라고 할 수 있다. 제안하는 핸드오버 기법은 [그림 3]의 세 가지 절차(① ~ ③)을 통해 MN의 핸드오버 시 공격자의 거짓 핸드오버 메시지, MN의 ID 위장을 탐지할 수 있다. LMA로 부터의 PBA메시지를 받은 시점부터 일정한 시간(t)동안 MN로부터 Attach 메시지가 도착하지 않는 경우, 메시지를 받았으나 최초 인증 시 생성된 Signature와 다른 경우 해당 메시지로 공격으로 판단하게 된다.



[그림 3] 핸드오버 시 MN 인증

4. 결 론

PMIPv6는 IETF에 의하여 제정된 뒤 많은 연구가 이루어지고 있다. 그러나, PMIPv6의 탄생 배경과 맞물려 보안의 측면보다는 그 성능 향상[4]을 위한 연구가 주로 이루어지고 있다. 본 논문에서는 PMIPv6에서의 공격 위협 분석을 통해 안전한 핸드오버 기법을 제안하였다. 향후 PMIPv6 환경에서의 6LoWPAN 네트워크 내 MN의 이동성 지원 방안에 대하여 연구하고자 한다.

Acknowledgment

"이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2009-0069457)."

참고문헌

[1] 김현곤, 서재현, 오병균, 안태남, 김진형, “네트워크 기반 Mobile IPv6 보안 취약점 분석”, 전자공학회 논문지, 제44권, 10호, 2007. 10

[2] 김수득, 이종혁, 정태명, “Proxy Mobile IPv6에서의 안전한 Fast Handover 기법”, 한국인터넷정보학회 학술발표대회 논문집, 2009

[3] 이혜진, 김기일, “PMIPv6의 성능 향상을 위한 연구 동향”, 한국인터넷정보학회, 제9권 제4호, pp. 15~21, 2008. 12

[4] 이성근, 전유찬, 임태형, 박진우, “향상된 핸드오프를 지원하는 망 기반의 이동성 지원 방안”, 한국통신학회논문지, Vol. 34 No.1, 2009. 01

[5] S. Gundavelli, Ed., K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", RFC5213 (http://tools.ietf.org/html/rfc5213), 2008. 10