논문 2007-44TC-10-16

네트워크 기반 Mobile IPv6 보안 취약점 분석

(Security Threats Analysis for Network-based Mobile IPv6)

김 현 곤*, 서 재 현*, 오 병 균*, 안 태 남**, 김 진 형***

(HyunGon Kim, JaeHyeon Seo, ByeongKyun Oh, TaeNam Ahn, and JinHyung Kim)

요 약

호스트 기반 Mobile IPv6에서 이동 단말은 서브넷간을 이동할 때마다 세션을 유지하기 위해서 자신의 홈 에이전트와 시그널링을 수행해야 한다. 이러한 이동 단말의 시그널링 처리 부하를 제거시킨 네트워크 기반 Mobile IPv6가 제안되었다. 즉, 네트워크에 위치한 프락시 이동성 에이전트가 시그널링과 이동성 관리를 대신 수행해줌으로써 이동 단말이 이동성 관리를 처리하지 않고도 세션을 유지할 수 있게 해준다. 그러나 이동 단말의 안전한 통신을 위해서는 다양한 공격에 대응할 수 있는 보안 메커니즘들이 적용되어야 한다. 이를 위해서는 우선적으로 네트워크 기반 Mobile IPv6에 대한 보안 취약점 분석이 이루어져야 한다. 잠재적인 공격 목표는 합법적인 이동 단말의 네트워크 서비스 비용을 증가시키고, 이동 단말의 통신을 가로채 도청, 위변조를 할 수 있다. 본 논문에서는 네트워크 기반 Mobile IPv6에 대해서 보안 취약점을 식별하고 이를 상세히 분석하였다. 분석 결과는 일반적인 IPv6에서 발생할 수 있는 보안 취약점은 제외하고 네트워크 기반 Mobile IPv6에서만 존재하는 취약점으로 한정하였다.

Abstract

In the host-based Mobile IPv6, a mobile node is responsible for doing the signaling to its home agent to enable session continuity as it moves between subnets. To remove the mobile node's signalling processing load, the network-based Mobile IPv6 has been proposed recently. It allows session continuity for a mobile node without its involvement in mobility management. The proxy mobility agent in the network performs the signaling and does the mobility management on behalf of the mobile node. However, to make secure communications for a mobile node, security mechanisms against diverse attacks should be adopted. To do this, first of all security threats to the network-based Mobile IPv6 should be also identified and analyzed. Potential attack objectives may be to consume network services at the cost of a legitimate mobile node and, eavesdropping and fabrication of user traffic through interception of a mobile node's communications. This paper identifies and discusses security threats to the network-based Mobile IPv6 in details. The results of threats analysis are limited to threats that are peculiar to the network-based Mobile IPv6 except threats to IPv6 in general.

Keywords: Threats, Mobile IPv6, PMIPv6, Mobility

I. 서 론

와이브로와 같이 이동 단말이 지속적으로 이동하는 환경에서는 IP 세션의 지속적인 연결성을 보장하기 위해 이동 인터넷이라고 불리우는 IETF의 Mobile IP를 기본적으로 적용한다. IPv4를 제외하고 IPv6만을 한정해서 Mobile IP를 분류해보면 크게 호스트 기반의 Mobile IPv6[1]와 네트워크 기반의 Mobile IPv6[2~3]로 구분할 수 있다. 전자인 호스트 기반 Mobile IPv6는 충분한 연구가 이루어져 있는 상태이며 실제 deploy 수준까지 검증이 된 상태이다. 그러나 후자인 네트워크 기반 Mobile IPv6 기술은 최근 제안되었으며 통신사업자들로부터 급격한 관심을 받으면서 표준화 활동이 활발하게 이루어지고 있다.

호스트 기반 Mobile IPv6는 90년대 후반부터 오랜 기간 동안 표준화가 진행되어 왔으며 표준화가 완료될 때

* 정회원, 목포대학교 정보공학부
(Division of Information Engineering, Mokpo National University)
** 정회원, 한남대학교 민군겸용보안공학연구센터
(Security Engineering Research Center, Hannam University)
*** 정회원, 한국과학기술원 전산학과
(Computer Science, KAIST)
접수일자: 2007년8월27일, 수정완료일: 2007년10월18일

까지 많은 논쟁을 불러 일으켜 왔다. 그러나 실제 서비스를 제공할 통신 사업자들에게 매력적인 요소를 제공하지 못함으로 인해 부분적인 상용 서비스만을 제공하며 정체되어 있는 상황에 있다. 가장 근본적인 문제점은 Mobile IPv6 서비스 제공을 위해서 클라이언트인 이동 단말에 부여되는 부담이 크다는 것이다. 예를 들어, 이동 단말과 엑세스 라우터 사이의 시그널링으로 인한 무선 구간에서의 자원 사용량 증가, 성능 및 자원이 한정되어 있는 이동 단말에서의 복잡한 표준 사양 구현, 이러한 동작들로 인한 이동 단말의 전력 사용량 증가 등이다.

이러한 문제점을 인식한 IETF에서는 결국 호스트 기반 Mobile IPv6가 아닌 네트워크 기반 Mobile IPv6기술을 제안하게 되었고, 관련된 기술에 대한 논의가 진행되고 있다. 두 기술간 주요 차이점은 호스트 기반 Mobile IPv6에서는 단말이 핸드오프(정확히는 홈 에이전트와의 바인딩 업데이트)를 주도하나, 네트워크 기반 Mobile IPv6에서는 단말이 핸드오프에 관여하지 않고 네트워크에 위치한 액세스 라우터가 이동성을 지원하는 단말임을 인식하고 핸드오프를 대신 처리해준다. 따라서 이동 단말이 이동성 관련 기능을 수행하지 않음으로 인해 시그널링 처리에 따른 프로세싱 부하 제거 및 무선 자원 사용 감소 등의 장점을 가진다.

한편, 보안 취약점 분석 또한 두 가지로 분류되어 논의되어야 한다. 하나는 호스트 기반 Mobile IPv6의 취약점 분석과 다른 하나는 네트워크 기반 Mobile IPv6의 취약점 분석이다. 전자의 경우는 현재까지 많은 연구가 이루어졌으나, 후자의 경우는 네트워크 기반 Mobile IPv6 기술이 최근에 제안된 상태이므로 취약점 분석에 대한 연구가 이루어지고 있지 않은 상태이다. 이와 관련하여 본 논문에서는 현재까지 연구 초기에 있는 네트워크 기반 Mobile IPv6의 보안 취약점을 상세히 분석하였다.

논문의 구성은 다음과 같다. 제 Ⅱ장은 관련연구로서 호스트 기반 Mobile IPv6에 대해 간략히 기술하고 네트워크 기반 Mobile IPv6에 대한 동작 개요를 살펴본다. 제 Ⅲ장에서는 네트워크 기반 Mobile IPv6의 보안 취약점을 분석하기 위해 대표적인 프로토콜인 PMIPv6(Proxy Mobile IPv6)[2]를 선정하고, 인터페이스별 취약점을 상세히 분석하고 그 결과를 기술한다. 마지막으로 제 Ⅳ장에서 결론을 맺는다.

Ⅱ. 관련 연구

1. 호스트 기반 Mobile IPv6

Mobile IP란 모바일 장치가 이동하는 중에도 자신이 초기에 할당 받은 영구적인 홈 주소를 유지하면서 인터넷 서비스를 끊김 없이 제공받을 수 있게 해주는 이동 인터넷 기술이다. IPv6 주소체계를 갖는 네트워크에서 이동 인터넷을 가능하게 해 주는 대표적인 프로토콜로서 RFC3755 표준에 정의된 호스트 기반 Mobile IPv6를 들 수 있다[1]. 유선 환경에서 IPv6 노드가 이동하게 되면 그 노드가 속해 있는 서브넷이 바뀌게 되므로 초기에 할당 받은 홈 주소가 바뀌어야 하고, 그 결과로 현재 진행 중인 응용 세션이 단절되게 된다. 호스트 기반 Mobile IPv6는 이러한 주소의 변경을 응용 단으로부터 감추어줌으로써 끊김 없는 응용서비스를 제공한다.

2. 네트워크 기반 Mobile IPv6

가. 기술 도입 배경

호스트 기반 Mobile IPv6는 IPv6 노드의 이동성을 제공한다. 이를 위해 이동 단말의 IPv6 스택에서는 Mobile IPv6 클라이언트 기능을 수행해야 한다. 이동 단말과 홈 에이전트간의 시그널링은 이동 단말의 홈 주소와 임시 주소간의 바인딩을 생성하고 유지한다. Mobile IPv6는 호스트의 IPv6 스택에 통합하는 형태로 설계되었다. 그렇지만 현재에도 Mobile IPv6 기능을 가지지 않는 IPv6 스택이 존재하며, 추후에도 Mobile IPv6 기능이 탑재되지 않을 가능성이 크다. 따라서 모든 호스트에서 IPv6 스택에 Mobile IPv6 기능을 탑재하는지 여부와 상관없이 노드의 이동성을 지원하는 것이 필요하다.

PMIPv6[2~3]는 네트워크측의 프락시 이동성 에이전트를 통해, RFC3775의 Mobile IPv6 시그널링과 홈 에이전트를 재사용함으로써 IPv6 노드들의 이동성을 지원한다. 이러한 접근 방식은 이동 단말이 이동성 관리를 위해 요구되는 시그널링에 관여하지 않게 할 수 있다. 네트워크의 프락시 에이전트는 시그널링과 이동 단말을 대신해 이동성 관리를 수행한다. Mobile IPv6 시그널링과 홈 에이전트 기능을 확장하고 재사용하기 때문에 프락시 Mobile IPv6 즉, PMIPv6라고 한다.

나.주요 엔티티 기능과 용어

PMIPv6에서 적용되는 주요 엔티티의 기능과 관련 용어는 아래와 같다.

□ Local Mobility Anchor(LMA) : PMIPv6 도메인에서 이동 단말(Mobile Node; 이하 MN)을 위한 홈 에이전트(Home Agent; 이하 HA)이다. 그리고 MN

의 홈 프리픽스를 위한 토폴로지상에서 앵커 포인트이며, MN의 reachability 상태를 관리하는 엔티티이다. LMA는 호스트 기반 Mobile IPv6 기본 규격에 정의된 HA의 능력을 가지며 PMIPv6를 지원하기 위한 추가적인 능력을 갖는다.

- ☐ Mobile Access Gateway(MAG) : 액세스 링크에 부착되어 MN의 이동성과 관련된 시그널링을 관리하는 기능을 수행한다. 그리고 MN이 액세스 링크에 접속되었는지 여부를 추적하는 역할을 하며 MN을 대신해 LMA와의 시그널링을 수행하는 역할을 하는 엔티티이다.
- ☐ MN's Home Address(MN-HoA) : PMIPv6 도메인 내에서의 MN의 홈 주소이다. 즉, 하나의 PMIPv6 도메인내에서 MN에 의해 얻어진 주소이다. MN은 PMIPv6 도메인의 범주에서 네트워크에 접속되어 있는 동안에는 이 주소를 지속적으로 사용한다.
- ☐ Proxy Care-of Address(Proxy-CoA) : MAG의 인터페이스 상에서 설정된 주소이며 LMA와 MAG간에 터널 전송 종단점이다. LMA는 이 주소를 MN의 임시 주소로 사용하며 MN을 위한 바인딩 캐시 엔트리에 이 주소를 등록한다.
- ☐ Proxy Mobile IPv6 Domain(PMIPv6-Doamin) : 로컬로 구역화된 이동성 관리 도메인이다.
- ☐ MN's Home Network Prefix(MN-HNP) : PMIPv6 도메인에서 MN이 항상 보이는 on-link 프리픽스이다. MN-HNP는 MN의 LMA에 토폴로지적으로 앵커된 것이다. MN은 이 프리픽스로부터 하나의 주소와 연관된 인터페이스를 설정한다.
- ☐ MN Identifier(MN-ID) : 액세스 인증의 일부로서 네트워크에 주어지는 MN의 ID이다. 일반적으로 액세스 기술에 특정 지어지는 MN의 NAI(Network Access Identifier)와 같은 ID이다.

다. 동작 개요

PMIPv6는 구역이 한정된 로컬 네트워크에서 MN에게 어떠한 이동성 관련된 시그널링도 요구하지 않으면서, 네트워크 기반 이동성 관리를 지원한다. PMIPv6 도메인내에서 이동하는 모든 MN들은 일반적으로 정책 저장소(policy store)에서 MN의 정책 프로파일을 조회하고 이를 통해 획득한 ID 또는 MN-ID와 같은 ID에 의해 식별된다. 정책 프로파일은 일반적으로 네트워크 기반 이동성 서비스의 특성, MN의 홈 네트워크 프리픽스, 제한된 주소 설정 모드, 로밍 정책, 네트워크 기반

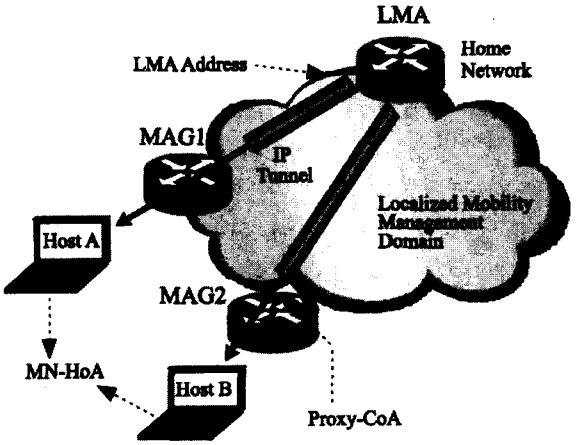


그림 1. PMIPv6 네트워크 토폴로지 및 도메인
Fig. 1. Network topology and domain of PMIPv6.

이동성 서비스를 지원하기 위한 필수적인 파라미터 등을 포함한다. 그림 1에 PMIPv6 네트워크 토폴로지 및 도메인을 도시하였다.

MN이 하나의 PMIPv6 도메인에 진입하고 액세스 인증이 한번 성공적으로 실행되면 네트워크는 MN이 항상 홈 네트워크에 있다는 것을 보장하고, 더 나아가 MN이 액세스 링크상에서 자신의 홈 주소를 얻을 수 있게 해 주며, 임의의 주소 설정 절차를 수행할 수 있도록 해준다. 즉, MN은 홈 네트워크 프리픽스를 할당 받으며 PMIPv6 도메인내에서 로밍하는 곳이 어디든지 간에 이 주소를 항상 사용할 수 있다. MN의 관점에서 보면 PMIPv6 도메인은 자신의 홈 링크 또는 하나의 링크로 보여진다.

PMIPv6에서는 MAG라는 새로운 엔티티를 도입하였다. 이 엔티티는 MN이 앵커되는 액세스 링크상에 위치하며 MN을 대신해 이동성 관련된 시그널링을 수행한다. LMA의 관점에서 보면 MAG는 MN을 대신해 Mobile IPv6 시그널링 메시지를 보낼 수 있도록 인가된 네트워크내 특별한 엔티티이다. MAG에 연결된 액세스 링크로 MN이 접속(attach)할 때, MN은 액세스 인증 절차의 일부로서 자신의 ID인 MN-ID를 제공한다. 성공적인 액세스 인증 후, MAG는 AAA(Authentication, Authorization and Accounting)[4~5] 인프라와 같은 정책 저장소로부터 MN의 프로파일을 얻는다. MAG는 액세스 링크상에서 MN의 홈 네트워크를 에뮬레이션하기 위한 모든 정보를 갖게 된다. MAG는 자신의 홈 네트워크 프리픽스를 방송하여 MN에게 주기적인 라우터 광고 메시지를 송신하기 시작한다.

액세스 링크상에서 라우터 광고 메시지를 수신한 MN은 액세스 링크에서 허용된 모드를 기반으로 할당

에 의한 주소 자동생성(statefull) 또는, 임의에 의한 주소 자동생성(stateless) 설정 모드를 사용하여 자신의 인터페이스와의 주소 설정을 시도한다. 성공적인 주소 설정 절차 후에 MN은 자신의 홈 네트워크 프리픽스로부터 하나의 주소를 얻게 된다.

MN의 현재 위치를 LMA에 업데이트 하기 위해서 MAG는 LMA로 프락시 바인딩 업데이트 메시지를 송신한다. 이 메시지는 MN의 NAI ID, 홈 네트워크 프리픽스 옵션이 포함된다. 이 메시지의 소스 주소는 자신의 egress 인터페이스상의 MAG 주소가 된다. 프락시 바인딩 업데이트 요청을 수신하면, LMA는 터널상에서 MN의 홈 네트워크 프리픽스로 경로를 설정하고 MAG에게 응답으로 프락시 바인딩 업데이트 응답 메시지를 전송한다. 이 메시지를 수신한 MAG는 자신과 LMA 사이에 터널을 설정하고 이 경로를 디폴트 경로에 추가시킨다. 이후, MN으로부터 수신한 모든 트래픽은 터널을 통해 설정된 LMA로 라우팅된다.

이 시점에서 MN은 현재의 접속점(point of attachment)에서 자신의 홈 네트워크 프리픽스로부터 유효한 홈 주소를 갖는다. Serving MAG와 LMA는 MN에게 수신된 또는, MN이 송신한 트래픽을 처리하기 위해서 적절한 라우팅 상태를 갖는다. 토폴로지적으로 MN의 홈 네트워크 프리픽스에 대해 앵커 포인트가 되는 LMA는 MN의 통신 상대 노드가 송신하는 모든 패킷을 수신한다. LMA는 터널을 통해 MAG에게 수신된 패킷들을 포워딩한다. 터널의 반대편에서 MAG는 수신된 패킷의 터널 헤더를 제거한 후, MN의 액세스 링크에게 패킷을 포워딩한다.

MAG는 일반적으로 액세스 링크상에서 디폴트 라우터로 동작한다. MN이 통신 상대 노드로 송신하는 모든 패킷은 MAG에 의해 수신되며 이 패킷은 터널을 통해 LMA로 포워딩된다. 터널의 반대편인 LMA는 패킷의 터널 헤더를 제거한 후에 패킷을 목적지인 상대 노드로 라우팅한다.

III. 네트워크 기반 Mobile IPv6 보안 취약점 분석

네트워크 기반 Mobile IPv6는 그림 2와 같이 크게 3개의 인터페이스로 정의할 수 있다. 즉, MN과 액세스 라우터 역할을 수행하는 MAG간 인터페이스, MAG와 HA 역할을 수행하는 LMA간, 그리고 LMA와 MN의 통신 상대인 CN(Correspondent Node; 이하 CN)간 인

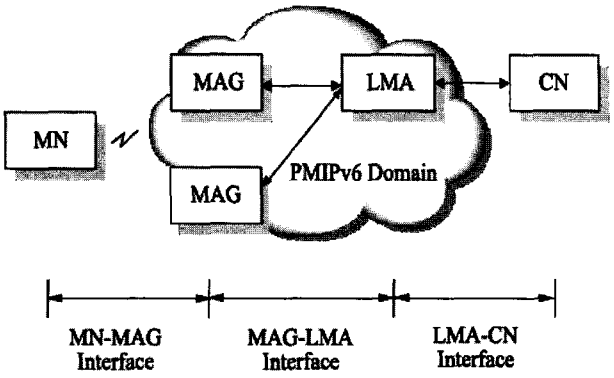


그림 2. 네트워크 기반 Mobile IPv6 인터페이스
Fig. 2. Interface of network-based Mobile IPv6.

터페이스이다. 보안 취약점은 크게 상기 3개의 인터페이스로 분류하여 분석하였다. 각 인터페이스에 대한 취약점은 기존의 IPv6에 이미 존재하는 취약점을 그대로 가지고 있으며, 네트워크 기반 Mobile IPv6 프로토콜 고유의 취약점이 새롭게 나타날 것이다[6~11]. 본 논문에서는 네트워크 기반 Mobile IPv6 프로토콜 고유의 취약점만을 분석 대상으로 한정하였다.

1. MN-MAG 인터페이스 보안 취약점

MAG는 링크 계층 또는 IP 계층 메커니즘을 기반으로 하여, 자신의 로컬 액세스 링크에 MN이 접속(arrival)되었는지 아니면 이탈(departure)하였는지를 모니터링 한다. 액세스 링크상에서 시그널링을 통해 발생하는 모든 오퍼레이션은 MN의 ID로 안전하게 바인딩되어야 한다. 이 바인딩을 이용하여 MAG는 MN에게 시그널링을 전송한다. 따라서 제 3자에 의해 MN의 위장, DoS 공격, 끼어들기 (Man-In-The-Middle; 이하 MITM) 공격에 노출되지 않기 위해서는 바인딩 자체가 스푸핑에 강해져야 한다. MN-MAG 인터페이스의 보안 취약점을 분류해보면 아래 <표 1>과 같다.

표 1. MN-MAG 인터페이스 보안 취약점
Table 1. Security threats to MN-MAG interface.

번호	보안 취약점	
1	동일 링크상에서 패킷 리다이렉션	
2	서로 다른 링크상에서 MITM 공격	서로 다른 MN의 핸드오프에 대한 공격
3		동일한 MN의 핸드오프에 대한 공격
4	서비스 거부 공격	
5	IP 스푸핑	

가. 동일 링크상에서 패킷 리다이렉션

MN의 ID를 꾸며내거나 위조할 수 있는 공격자는 MAG를 속여서 MN의 데이터 패킷들을 공격자에게 리다이렉션할 수 있다. 공격자는 자신과 동일 링크(on-link)에 또는, 서로 다른 링크(off-link)에 있는 MN에 대하여 위장공격을 할 수 있다. 만약 공격이 동일 링크에서 발생할 경우, 패킷은 MN에서 공격자로 전달된다. 즉, 원래의 패킷이 MN에서 MAG로 전달되어야 하나 리다이렉션 공격으로 인해 MAG는 패킷을 수신할 수 없게 된다. 이로 인해 MAG와 LMA간에 경로 업데이트 시그널링이 발생되지 않는다. 동일 링크상에서의 공격은 안전한 이웃 발견(Secure Neighbor Discovery) 메커니즘을 사용하지 않을 경우, 일반적인 IPv6 네트워크에서도 발생할 수 있다[12~13].

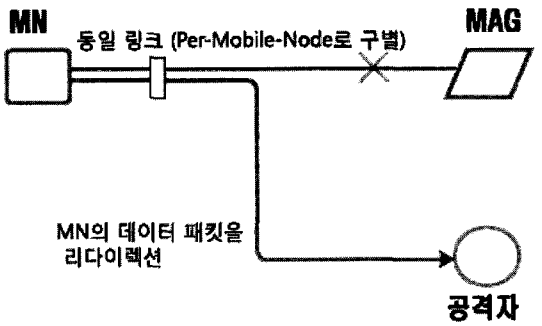


그림 3. 동일 링크상에서 패킷 리다이렉션
Fig. 3. Packet redirection on the same link.

나. 서로 다른 링크상에서 MITM

서로 다른 링크상에서의 위장은 MN의 핸드오프 시그널링을 공격자가 획득하고 위변조하는 것이다. 즉, 공격자가 MAG를 속여서 MN이 그 MAG의 다른 액세스 링크로 핸드오프 되었다고 믿게 한다. 이 공격은 두 가지 경우를 예측해 볼 수 있는데 하나는 공격자와 MN이 서로 다른 MAG에 접속되는 분리된 링크상에 있는 경우이고, 다른 하나는 공격자와 MN이 동일한 MAG에 연결된 가상의 Per-Mobile-Node 링크로 분리된 경우이다.

전자의 경우를 그림 4에 도시하였다. 이 예에서는 공격자가 MN이 새로운 링크 2로 핸드오프 되었다고 속임으로써, 각기 다른 두 MAG는 각각의 MN에 대해 둘 다 독립적으로 LMA와 경로 업데이트 시그널링을 수행할 것이다.

후자의 경우를 그림 5에 도시하였다. 이 경우, 경로 업데이트 시그널링은 단지 한번만 수행되며 패킷은

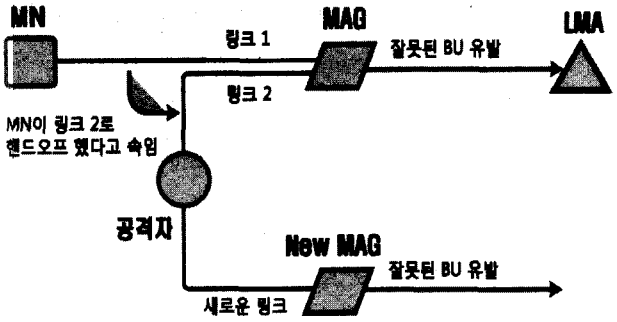


그림 4. 서로 다른 MN의 핸드오프시 서로 다른 링크상에서 MITM 공격
Fig. 4. MITM attack on the different link during the different MN's handoff.

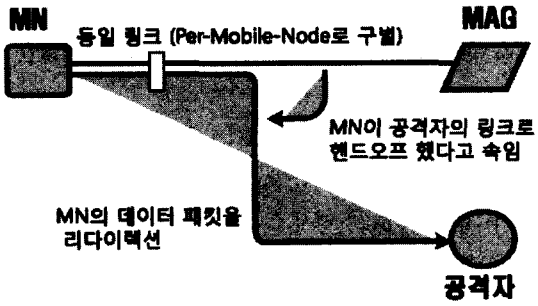


그림 5. 동일한 MN의 핸드오프시 서로 다른 링크상에서 MITM 공격
Fig. 5. MITM attack on the different link during the MN's handoff.

MN에서 공격자로 전달된다. 즉, 원래의 패킷이 MN에서 MAG로 전달되어야하나 리다이렉션 공격으로 인해 MAG는 패킷을 수신할 수 없게 된다. MN은 새로운 핸드오프 시그널링을 수행함으로써 공격자로부터 자신의 트래픽을 항상 다시 획득할 수 있다. 그러나 일반적인 MN들은 이러한 종류의 공격에 적절하게 대응할 수 없다. 만약에 네트워크 스택들이 적절한 기능을 보유하고 있더라도 링크 또는, IP 계층에서 매우 짧은 시간내에 대응하기 어렵다. 그러나 정해진 시간내에 MN이 경로 업데이트를 수행할 것이므로 공격의 영향은 크지 않을 것이다. 이러한 공격의 영향은 MN이 다음 순서의 핸드오프를 다시 시작하기 위해 시그널링을 초기화하기 전까지 지속된다.

위장 공격들은 MN과 네트워크간 핸드오프 시그널링이 반드시 인증되고, 무선 링크 계층에 의해 완전하게 제어되는 셀룰러 네트워크의 예와 같이, 링크계층에서 막을 수 있다. 셀룰러 액세스에서는 동일 링크상에서 그리고 서로 다른 링크상에서도 위장공격이 매우 어렵도록 다양한 암호학적 그리고 비암호학적 공격에 대한 대응책을 제공한다. 그렇지만 핸드오프 동안 링크계층

인증과 인가를 지원하지 않는 셀룰러 외에 기술들은 위장 공격들이 가능하다. 다시 말하면 PMIPv6에서도 위장 공격이 충분히 가능하다.

다. 서비스 거부 공격

핸드오프 시그널링을 변조할 수 있는 공격자는 PMIPv6 도메인에 대해서 DoS 공격을 할 수 있다. 예를 들어, 공격자가 MAG를 속여서 다수의 MN들이 로컬 액세스 링크에 접속되었다고 믿게 한다. 그리고 가상의 링크상에 각 MN에 대해 LMA와의 경로 업데이트 시그널링을 시작하도록 유도한다. 이 공격의 결과로 제어평면에서 과도한 시그널링 오버헤드가 생길뿐만 아니라 LMA와 MAG의 라우팅 테이블에 다수의 불필요한 엔트리들이 만들어진다.

라우팅 테이블이 예상보다 커지면 그 결과로 LMA는 정상적인 경로 업데이트 요청을 거절하게 될 것이고, MAG가 자신의 로컬 액세스 링크상에서 이루어지는 정상적인 MN들의 핸드오프를 무시하게 만든다. 또한 경로 룩업이 많아지기 때문에 LMA와 MAG에서 인 바운드(inbound) 및 아웃 바운드(outbound) 데이터 패킷들의 포워딩 속도가 감소할 것이다. 그리고 동일한 이유로 제어평면 패킷들의 응답 또한 느려질 것이다.

이 공격의 또 다른 측면 효과는 PMIPv6 도메인 전체적으로 LMA가 외부 공격자로부터 수신한 패킷을 플러딩할 여지가 높아지게 된다. 즉, 경로 수가 많아지면 PMIPv6 도메인 내에서 랜덤 IP 주소로 패킷이 플러딩될 확률이 높아진다. 그리고 다수의 경로들은 LMA에 존재하는 라우팅 테이블에 매치되고 MAG로 터널링 된다. 이는 결국 로컬 액세스 링크상에서 과도한 주소 해석(resolution)으로 이어진다. 그리고 소수의 플러딩 패킷들은 라우팅 테이블에 엔트리가 존재하지 않음으로 인해 LMA에서 직접 드롭될 수 있다.

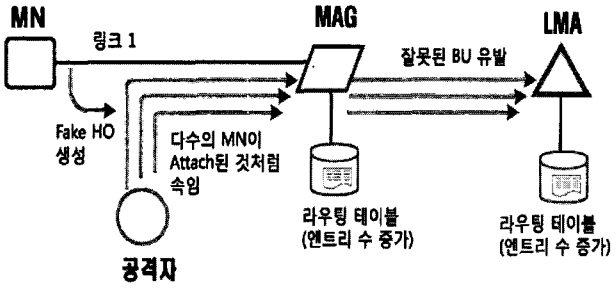


그림 6. 서비스 거부 공격
Fig. 6. Denial of service attack.

라. IP 스푸핑

공격자들은 대부분 반사(reflection) 공격을 위해 또는, 자신의 ID를 숨기기 위해 IP 스푸핑 공격을 한다[14]. PMIPv6 도메인내에서도 MN과 MAG간 그리고 MAG와 LMA간 IP 스푸핑 공격을 가할 수 있다. 이러한 위협은 액세스 네트워크 내에서 라우터에 있는 네트워크 ingress 필터링을 광범위하게 설치함으로써 합리적인 수준으로 억제할 수 있다. 필터링은 포워딩될 패킷들내 IP 소스 주소의 프리픽스에 대해 토폴로지적인 정확성(correctness)을 보장하는 범위까지 IP 스푸핑을 막을 수 있다. 액세스 네트워크에 필터링이 설치된 곳에서는 IP 주소가 라우터의 로컬 액세스 링크에서 유효하기만 하면 모든 패킷들은 포워딩될 수 있다.

한편, 공격자는 on-link 프리픽스와 연관된 잘못된 인터페이스 ID를 이용할 수 있다. 그러나 반사 공격이 보통 off-link를 목표로 하고 있고, 토폴로지적으로 정확한 IP 주소 프리픽스를 강제로 사용하는 것은 ID를 숨김으로 생기는 효과를 반감시키기 때문에 네트워크 ingress 필터링은 현재 제시할 수 있는 적절한 솔루션이라 할 수 있다. 다르게 표현하면, 프리픽스들이 PMIPv6 도메인에서 특정한 링크에 한정되지 않으므로 ingress 필터링만을 사용해서는 토폴로지적인 정확성을 보장하기 어렵다. 따라서 off-link상에서 다른 IP 소스 주소의 패킷을 전송하는 공격을 막기 위해서는 IP 주소 소유자를 증명할 수 있는 추가적인 메커니즘이 필요하다.

2. MAG-LMA 인터페이스 보안 취약점

MAG와 LMA간 인터페이스 상에서 실행되는 PMIPv6 프로토콜은 MN들의 데이터 트래픽에 대한 경로를 설정하고 갱신하고 제거한다. 이 인터페이스에 대한 공격은 크게 LMA 침해 또는 합법적인 LMA 가장, MAG 침해 또는 합법적인 MAG 가장, MITM 공격 등

표 2. MAG-LMA 인터페이스 보안 취약점
Table 2. Security threats to MAG-LMA interface.

번호	보안 취약점
1	MAG와 LMA간 경로 재설정에 따른 위협
2	네트워크 프리픽스 위장
3	침해된 MAG를 통한 패킷 리다이렉션
4	침해된 MAG를 통한 MN의 트래픽 손실
5	침해된 MAG에 의한 LMA 서비스 거부 공격
6	MAG의 ID 위조
7	MAG와 LMA간 끼어들기

을 통해 이루어진다. MAG-LMA 인터페이스의 보안 취약점을 분류해보면 <표 2>와 같다.

가. MAG와 LMA간 경로 재설정에 따른 위협

침해된 LMA는 MN으로의 서비스를 거절하기 위해서 합법적인 MAG로부터의 경로 업데이트 요청을 무시할 수 있다. 또한 침해된 LMA와 MAG간에 잘못된 경로를 만들고 이를 통해 리다이렉션된 MN의 트래픽을 침해된 LMA가 수신할 수 있도록 MAG를 속인다. 즉, MAG에 의해 포워딩되는 트래픽이 다른 LMA로 리다이렉션 되도록 하는 것이다. 또한, MN의 서비스를 거절하기 위해 간단하게 기존에 설정된 MAG 경로를 드롭할 수 있다. 또한, MN의 데이터 트래픽이 LMA를 거치기 때문에 침해된 LMA는 트래픽을 가로채거나 검사하거나 수정하거나 제거하거나 공격자와 결탁된 목적지로 리다이렉션할 수 있다. 공격자는 MAG로 전달되는 트래픽을 또는, 특정한 MN으로 전달되는 트래픽만을 선택적으로 차단할 수 있다.

침해된 LMA는 모든 패킷들이 하나의 MAG로 향하도록 자신의 라우팅 테이블을 조작할 수 있다. 즉, 특정 MAG에 접속된 액세스 링크와 특정 MAG에 대해 DoS 공격을 하는 것이다. 또한, 이러한 위협들은 MAG에게 공격자 자신이 합법적인 LMA라는 것을 믿도록 속임으로써 더욱 위협적일 수 있다. 공격자는 MN의 트래픽을 리다이렉션 하기 위해서 또는, MN의 트래픽을 거절하기 위해서 위에서 기술한 바와 같이 MAG에게 잘못된 경로 변경을 유도하거나 MAG로부터의 경로 업데이트 요청을 무시함으로써, MAG가 합법적인 LMA 대신에 공격자와 경로 업데이트 시그널링을 하도록 유도한다. 공격자는 MAG에게 자신의 존재를 알려줄 수 있기 때문에 합법적인 LMA와 MAG간에 원래의 제어평면 경로상에 위치할 필요는 없다. LMA와 MAG 사이에 연관을 설정할 때, 상호 인증이 실패할 경우에는 공격자가 이를 이용해 위장 LMA를 설정할 수 있다.

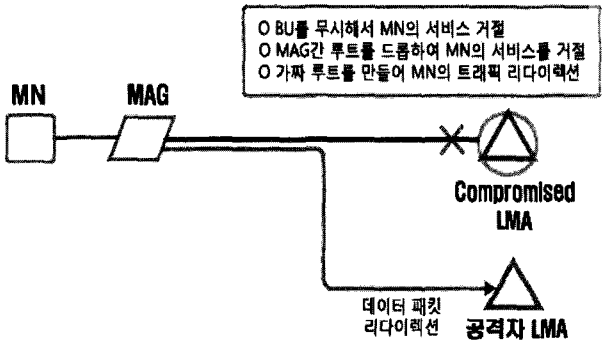


그림 7. 경로 재설정에 따른 위협
Fig. 7. Threats to path redefine.

나. 네트워크 프리픽스 위장

공격자가 정상적인 LMA와 MN이 접속한 MAG 사이의 데이터평면 경로상에 있거나 또는, 경로상에 있지 않더라도 MN으로부터의 또는 MN에게로의 데이터 트래픽을 가로채거나 검사하거나 수정하거나 드롭하거나 리다이렉션할 수 있다. 공격자가 정상적인 데이터평면 경로상에 위치하지 않을 경우에는 MN의 IP 주소 설정에 사용되는 프리픽스를 재정의해서 PMIPv6 프로토콜을 지렛대로 활용할 수 있다. 즉, 공격자가 자신에게로의 경로로 프리픽스를 재지정할 수 있다.

공격자가 정상적인 데이터평면 경로를 끊음으로 인해 MN의 outgoing 데이터 패킷들이 영향을 받는지 여부는 PMIPv6 도메인내에서 특정 데이터 패킷 포워딩 메커니즘에 따라 달라질 수 있다. 예를 들어, 만약 IP-in-IP 엔캡슐레이션 또는, 동등한 접근 방법이 데이터 패킷의 아웃 바운드에 사용된다면 패킷들은 공격자를 통해 강제로 라우팅될 수 있다. 즉, 표준 IP 라우팅은 합법적인 LMA를 통해 릴레이될 수 있으며 이로 인해 공격자를 통해 우회될 수 있다.

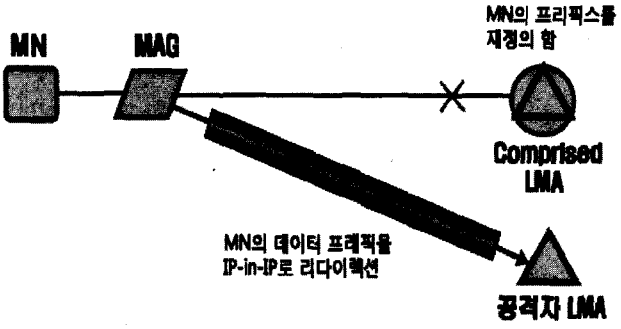


그림 8. 네트워크 프리픽스 위장
Fig. 8. Network prefix impersonation.

다. 침해된 MAG를 통한 패킷 리다이렉션

침해된 MAG는 MN의 인가 없이도 자신의 임의의 액세스 링크로 MN의 트래픽을 리다이렉션할 수 있다. 이 공격은 일반적인 라우팅 프로토콜에서 발생하는 공격과 동일하게, 악의의 스터브 라우터가 MN을 위해 가짜 호스트 경로를 삽입하는 것이다.

일반적으로 링크 상태(link state)에서의 서브넷 프리픽스 위조 또는, 디스턴스 벡터 라우팅 프로토콜을 이용한 위조는 포워딩 동작에 있어서 유효한 경로를 얻기

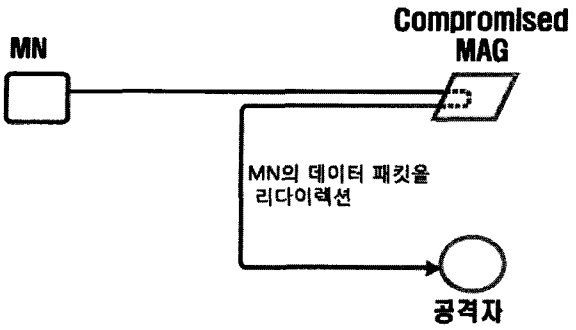


그림 9. 침해된 MAG를 통한 패킷 리다이렉션
Fig. 9. Packet redirection through compromised LMA.

위해서 다수의 라우터가 동원된다. 그러나 위장 호스트 경로는 합법적인 라우터들에 의해 광고된 라우팅 정보들보다 우선적으로 적용된다. 따라서 다수의 라우터들을 동원하지 않더라도 공격이 쉽게 성공될 수 있다. 라우팅 프로토콜에서의 리다이렉션과 PMIPv6에서의 리다이렉션의 차이점은 전자는 다수의 라우터내의 라우팅 테이블에 영향을 주고, 후자는 단지 침해된 MAG와 LMA가 관여되는지의 차이이다.

라. 침해된 MAG를 통한 MN의 트래픽 손실

침해된 MAG는 자신의 로컬 액세스 링크상에 있는 MN의 존재를 무시할 수 있으며 LMA에 MN의 등록을 생략 또는 무시할 수 있다. 이로 인해 MN의 트래픽이 유실될 수 있다. 또한, 침해된 MAG는 MN의 전원이 오프된 것처럼 LMA를 속여 MN의 등록을 해제 시킴으로써 MN의 정상적인 통신을 방해할 수 있다.

더 나아가 침해된 MAG는 MN이 다른 MAG로 이동할 때까지 반복적으로 이러한 공격을 지속하여, MN이 네트워크 엑세스 인증 절차를 지속적으로 재시도 하도록 유도할 수 있다. MN은 이러한 상황을 처리할 수는 있으나 회복 절차가 길어지고 이로 인해 outgoing 통신 세션이 중단될 수 있다.

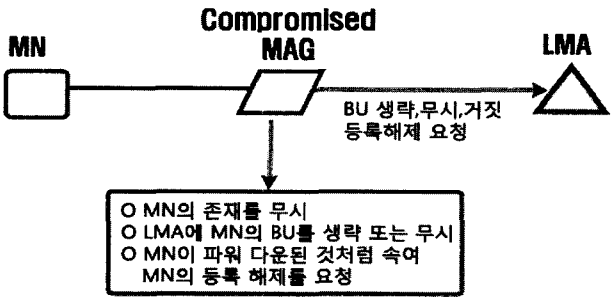


그림 10. 침해된 MAG를 통한 MN의 트래픽 손실
Fig. 10. Packet loss by compromised LMA.

마. 침해된 MAG에 의한 LMA 서비스 거부 공격

LMA에 대한 DoS 공격이 MAG를 손상시키는 또 다른 위협이 된다. 침해된 MAG는 다수의 MN들이 자신에게 접속된 것처럼 LMA를 속일 수 있다. 이 경우, LMA는 존재하지 않는 각각의 MN에 대해 라우팅 테이블 엔트리를 만들게 되고 이로 인해 라우팅 테이블이 예상치 못하게 커지게 되면, 결과적으로 LMA는 합법적인 경로 업데이트 요청을 처리하지 못할 수 있다. 또한, 경로 룩업이 지연되고, 데이터 패킷들의 포워딩 속도가 느려지며, 같은 이유로 제어평면 패킷의 응답이 느려진다. 라우팅 테이블 엔트리의 수가 많아질 경우에 또 다른 불리한 측면은 전체 PMIPv6 도메인에서 외부 공격자에 의해 LMA가 불필요한 패킷을 플러딩할 수 있게 된다는 것이다.

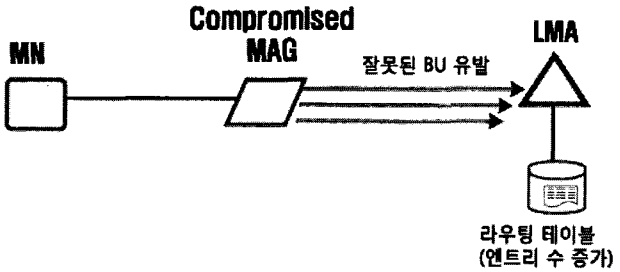


그림 11. 침해된 MAG에 의한 LMA 서비스 거부 공격
Fig. 11. LMA DoS attack through compromised MAG.

바. MAG의 ID 위조

공격자가 MAG의 ID를 위조할 경우, MN과 LMA 사이는 MITM 공격에 노출될 수 있다. 공격자는 MN에게 인가된 MAG로 행동할 수 있으며 경로 업데이트 시그널링을 수행하는데 있어서 LMA를 관여하게 만든다.

이로 인해 공격자는 합법적인 MAG와 LMA간에 교환되는 시그널링 패킷을 훔쳐보며 나중에 이들 패킷을 재생할 수도 있다. 공격자는 특정한 횟수로 특정한 MN

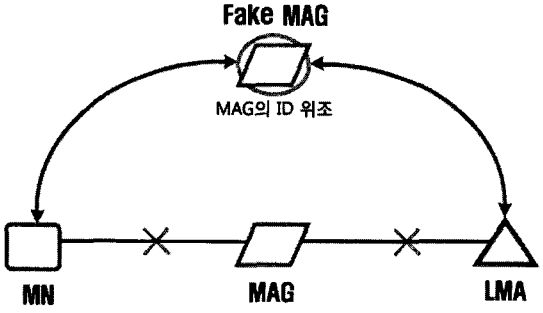


그림 12. MN의 ID 위조
Fig. 12. MN's ID forgery.

에 대한 트래픽을 선택적으로 비활성화 시키는 동작을 임시적으로 수행할 수도 있다.

사. MAG와 LMA간 끼어들기

합법적인 MAG와 합법적인 LMA 사이에 끼어든 공격자는 양쪽 제어평면 시그널링과 데이터평면 트래픽에 대하여 MITM 공격을 할 수 있다. 만약 공격자가 정상적인 제어평면 경로상에 있다면, 공격자는 위조, 변경, 거짓의 경로 설정을 위해서 또는, 현재 액티브하게 사용되고 있는 경로를 제거하기 위해서 경로 업데이트 패킷을 드롭할 수 있다. 유사하게, 정상적인 데이터평면 경로상에 공격자가 있다면, 가로채기, 검사, 변경, 드롭, 또는 MN으로의 데이터 패킷들을 리다이렉션 할 수 있다.

MAG와 LMA 사이에 위치한 침해된 스위치 또는 라우터가 유사한 위협을 일으킬 수 있다. 제어평면 경로상에 있는 스위치나 라우터는 위조, 변경, 제어평면 패킷들을 드롭할 수 있으며 이로 인해 경로설정에 방해를 받을 수 있다. 데이터평면 경로상에 놓여있는 스위치나 라우들은 가로채기, 검사, 변경, 데이터 패킷 드롭, 또는 그들의 원래 경로로부터 패킷을 다른 곳으로 전환시키기 위해서 IP 주소를 재작성할 수 있다.

더 나아가 MAG와 LMA 사이에 위치한 공격자는 경로 업데이트 시그널링을 수행하는데 있어서 LMA에게는 합법적인 MAG로, MAG에게는 합법적인 LMA로 위장할 수 있다. 공격자는 MAG와 LMA간 정상적인 제어평면 경로상에 있지 않더라도 경로 설정을 방해할 수 있다. 정상적인 데이터평면 경로를 차단한 공격자는 MN으로 전달되는 인 바운드 데이터 패킷을 우선적으로 LMA에서 공격자에로, MN의 MAG에게로, 최종적으로 MN에게로 라우팅되어 지도록 동작한다. 이러한 공격이 소스가 MN인 outgoing 데이터 패킷들의 경로에 영향을 주는지 여부는 PMIPv6 도메인내에서 특정 한 데이터 패킷 포워딩 메커니즘에 따라 결정된다.

3. LMA-CN 인터페이스 보안 취약점

이 인터페이스에서 유일하게 발생할 수 있는 위협은 공격자가 CN을 가장해서 LMA에게 대량의 데이터 패킷을 전송하는 것이다. 랜덤 IP 주소로 송신되는 플러딩 패킷은 LMA의 기존 라우팅 테이블 앤트리와 매치되므로 이 단계에서 불필요하게 LMA의 프로세싱 자원을 고갈시킬 수 있다.

PMIPv6 도메인은 서로 다른 MN에 대해서 데이터 트래픽을 송수신하기 위해 각각의 LMA와 MAG간 개별적인 호스트 경로를 사용한다. 따라서 경로들을 생성하고 유지하고 제거하기 위해서 PMIPv6 도메인내에서 제어 트래픽이 유발된다.

LMA에 대한 DoS 공격은 PMIPv6 도메인내에서 MN들에 의해 잠재적으로 사용되고 있는 임의의 IP 주소들로 패킷을 전송함으로써 이루어질 수 있다. 경계 라우터와 같이 LMA는 토폴리지적으로 최상위에 위치함으로서 대량의 데이터 트래픽이 통과되므로 모든 플러딩 패킷들을 처리해야 하고, 이들 패킷들 각각에 대해 라우팅 테이블 룩업을 수행해야 한다. LMA는 IP 목적지 주소가 자신의 라우팅 테이블에 등록되지 않은 패킷들을 버릴 수 있다. 그러나 그 외에 패킷들은 반드시 캡슐레이션하고 포워딩해야 하고, 수신측에서는 불필요한 플러딩 패킷들도 반드시 역 캡슐레이션해야 한다. 이로 인해 링크 대역(bandwidth)이 소모되고, 수신자의 프로세싱 자원이 소모되기 때문에 타겟 MAG와 그 MAG의 로컬 액세스 링크에 접속된 모든 MN들은 쉽게 피해를 당할 수 있다. 이 위협은 일반적인 IPv6 경계 라우터에서 이루어지는 DoS 공격과 동일하다. 그러나 라우팅 테이블 룩업은 LMA가 플러딩 패킷들의 일

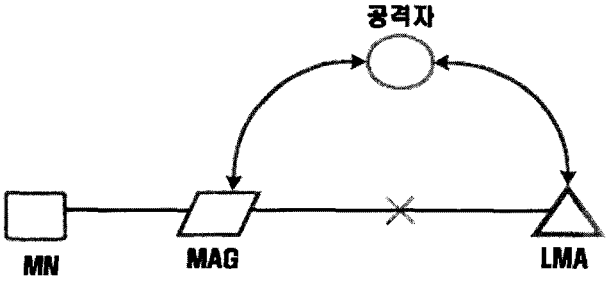


그림 13. MAG와 LMA간 끼어들기
Fig. 13. MITM attack between MAG and LMA.

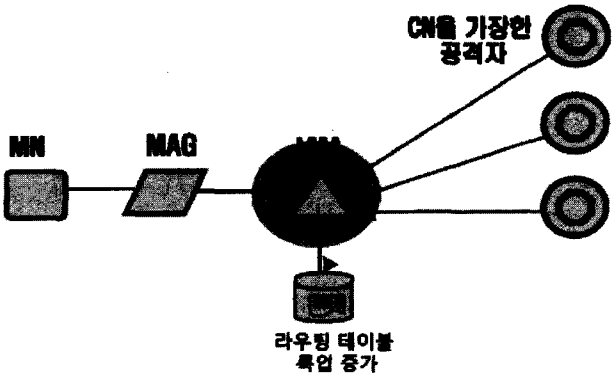


그림 14. CN을 가장한 LMA 서비스 거부 공격
Fig. 14. LMA DoS attack by CN impersonation.

부를 미리 드롭하게 해주거나 또는, 반대로 드롭할 수 없는 패킷들을 위해 추가적인 터널링 부하를 요구한다. 이 점이 일반적인 IPv6에서의 공격의 영향과 다르다.

관련된 공격으로서 공격자는 글로벌 라우팅이 가능한 LMA 또는 PMIPv6 도메인내의 다른 엔티티의 IP 주소를 획득하고, 그 IP 주소에 대해 DoS 공격을 감행할 수 있다. PMIPv6는 일반적으로 MN들이 PMIPv6 도메인내에서 임의 엔티티의 글로벌한 IP 주소를 획득할 수 없기 때문에 이러한 공격에 대해 대응할 수 있다. 따라서 PMIPv6 도메인은 토폴로지적으로 침해된 MN의 정보 추출 가능성을 제한하고, 이들 IP 주소가 통과될 수 없도록 함으로써 원격 공격자를 차단한다. 만약 MAG들과 LMA들이 글로벌 라우팅이 가능한 IP 주소들을 가졌다면, 공격자가 IP 주소 스캐닝을 수행할 수 있는 가능성이 있다. 그러나 IPv6 주소 공간이 크므로 스캐닝에 상당히 많은 시간이 소모된다.

Ⅳ. 결 론

네트워크 기반 Mobile IPv6는 기존의 호스트 기반 Mobile IPv6가 가지고 있는 단점인 이동 단말에 부여되는 과도한 시그널링 부하, 무선자원 비효율성, 과도한 전력 사용량 등의 문제점들을 해결할 수 있는 대안으로 제시되고 있다. 그러나 이동 단말의 안전한 통신을 위해서는 다양한 공격에 대응할 수 있는 보안 메커니즘들이 적용되어야 한다. 이를 위해서는 우선적으로 네트워크 기반 Mobile IPv6에 대한 보안 취약점 분석이 이루어져야 한다. 본 논문에서는 네트워크 기반 Mobile IPv6의 보안 취약점을 식별하고 이를 상세히 분석하였다. 보안 취약점 분석에 있어서 네트워크 기반 Mobile IPv6가 3개의 인터페이스로 정의되므로 각 인터페이스별로 보안 취약성을 분류하고 분석하였다. 한편, 본 논문에서는 보안 메커니즘을 적용하기 이전 상태에서의 보안 취약점을 분석하였으나 추후, 다양한 보안 메커니즘 적용에 따른 보안 취약점을 분석할 필요가 있다.

참 고 문 헌

[1] D. Johnson, C. Perkins, and J.Arkko, "Mobility Support in IPv6", *RFC3755*, July 2003.

[2] S. Gumdavelli, K. Leung, et al., "Proxy Mobile IPv6", *draft-ietf-netlmm-proxymipv6-01.txt*, June 2007.

[3] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Goals for Network-based Localized Mobility Management", *RFC4831*, 2006.10

[4] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", *RFC2977*, October 2000.

[5] 김현곤 외 6명, "AAA 정보보호 기술 표준화 동향", *전자통신동향분석*, 제20권 제1호, 2005년 2월

[6] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Problem Statement for Network-based Localized Mobility Management", *RFC4830*, September 2006.

[7] C. Vogt, J. Kempf, "Security Threats to Network-Based Localized Mobility Management (NETLMM)", *RFC4832*, April 2007.

[8] 한국정보보호진흥원, "*IPv6 보안 기술 해설서*", 2005년 10월

[9] 한국정보보호진흥원, "*와이브로 보안기술 해설서*", 2006년 8월

[10] 정보홍, 임재덕, 김영호, 김기영, "IPv6 환경의 보안 위협 및 공격 분석", *전자통신동향분석*, 제22권 제 1호, pp.37-50, 2007년 2월

[11] 신명기, 김형준, "IPv6 전환 환경에서의 보안 기술 분석", *전자통신동향 분석*, 제21권 제5호, pp.163-170, 2006년 10월

[12] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", *RFC 3756*, May 2004.

[13] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery(SEND)", *RFC 3971*, March 2005.

[14] CERT Coordination Center, "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", September 1996.

저 자 소 개

김 현 곤(정회원)

1992년 금오공과대학교 전자공학과 학사
1994년 금오공과대학교 전자공학과 공학석사
2003년 충남대학교 전자공학과 공학박사
1994년~2005년 한국전자통신연구원 정보보호연구단 팀장
2005년~현재 목포대학교 정보공학부 정보보호전공 조교수
<주관심분야 : RFID/USN 정보보호, 이동통신 정보보호, 개인 프라이버시 보호>

오 병 균(정회원)

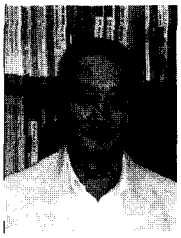
1970년 공주사범학교 수학과 학사
1984년 조선대학교 전자계산학과 석사
2000년 단국대학교 전자공학과 박사
1984년~현재 목포대학교 정보공학부 정보보호전공 교수
<주관심분야 : 시스템 보안, 컴퓨터 구조>

김 진 형(정회원)

1971년 서울대학교 공과대학 학사
1979년 UCLA 시스템공학 석사
1983년 UCLA 전산학과 박사
1971년~1973년 KIST 연구원
1981년~1985년 Hughes Research Laboratories 선임연구원
1985년~현재 KAIST 전산학과 교수
1990년 IBM Watson 연구소 방문연구원
2002년~2003년 삼성SDS 방문연구원
<주관심분야 : 인공지능, 패턴인식>

서 재 현(정회원)

1985년 전남대학교 계산통계학과 학사
1988년 중앙대학교 전자계산학과 석사
1988년~1996년 송원대학교 전임강사
1996년 전남대학교 전산통계학과 박사
1996년~현재 목포대학교 정보공학부 정보보호전공 교수
<주관심분야 : 정보보호, 시스템 및 네트워크보안, 컴퓨터 네트워크>



안 태 남(정회원)

1975년 육군사관학교 전자공학과 학사
1979년 서울대학교 자연대학 계산통계학과 학사
1983년 美해군대학원 전산학 석사
1989년 美루지애나(라파엣) 대학 전산학 박사
2006년~2007년 8월 KAIST 전산학과 초빙교수
2007년 9월~현재 한남대학교 민군겸용보안공학 연구센터 초빙교수
<주관심분야 : 정보보안, 부호이론>