MIPv6망에서 안전한 호스트 이동성 지원 방안

김정주* · 홍석원*

*명지대학교

Secure Host Mobility in the Mobile IPv6 Network

Jung-Ju Kim** Sugwon Hong*

*Myongji University

E-mail : kimjj77@mju.ac.kr

요 약

이동 Pv6(MIPv6)를 지원하는 네트워크에서 이동 노드(mobile node)가 새로운 네트워크로 이동했을 때 그 네트워크에서의 엑세스 라우터와 엑세스 포인트(Access Router/Access Point)를 찾아 연결해야 한다. 이때 신뢰할 수 있는 AR과 AP에 연결하지 못할 경우 여러 형태의 공격에 노출된다. 본 논문에서는 SEcure Neighbor Discovery(SEND)에서 사용하는 공개키 기반 RSA 암호화 방식을 응용하여 AR/AP와 MN이 상호 인증할 수 있는 방안을 제시한다.

ABSTRACT

In the MIPv6 network, when mobile nodes move into new newtwork, they need to find the new access router and points(AR/AP) for the newtwork. Unless they are not connected to authorized AR/APs, they can be exposed to a lot of attacks. In this paper we propose a protocol to authenticate AR/AR and MN each other. This protocol is based on the public key scheme which is used in the SEcure Neighbor Discovery(SEND) protocol.

키워드

Mobile IPv6, mobile node, Access Router/Point, Authentication, Security

Ⅰ. 서 론

이동 노드(MN)가 홈 네트워크를 이동하여 외부 네트워크에 접속하고자 할 때 접속에 사용하기 위한 외부 네트워크의 정보를 얻기 위하여 인접노드 탐색 프로토콜 메시지(ND)들을 이용한다[1]. 이 결과로 디폴트 라우터 주소, 네트워크 프리픽스, 인접노드의 MAC 주소에 대한 정보를 얻게 되고 이를 기초로 사용자의 개입 없이 네트워크에 접속할 수 있게 된다[2]. 이와 같은 네트워크 환경의 정보를 주고받는 메시지에 대한 보안이 이루어지지 않는다면 많은 위협요소에 노출될 수 있다[3]. IETF의 표준 문서인 'Neighbor Discovery for IP Version6'와 'IPv6 Stateless Address Autoconfiguration'에서는 ND 메커니즘과 주소 자동설정 메커니즘을 수행하는데 필요한 모든 메시지들이 IPsec의 AH 헤더에 의해 내용이 인증 되어야 함을 권고하고 있다[1][2]. 하지만 IPsec은 키 분배 및 성능 저하 문제 등 여러 가지 이유로 어려운 점이 존재하고, ND 메커니즘과 주소 자동설정 메커니즘은 IPv6 환경에서 통신을 수행하기 위하여 선행적으로 실행되어야 하는 과정이기 때문에 해당 메커니즘이 실행되지 않은 상태에서 IPsec 통신을 수행하는 것이 불가능할 수도 있다[2][5]. 이와 같은 문제를 해결하기 위하여 IETF의 SEcure Neighbor Discovery(SEND) 워킹그룹에서는 추가적인 키 분배와 같은 사전 작업 없이 IPv6 ND에 보안 기능을 지원하는 보안 인접 탐색 메시지와 메커니즘을 발표하였다[5].

Mobile IPv6 환경에서 이동 노드(MN)가 외부 네트워크에 접근해서 통신을 하기 위해서는 MN과 엑세스 라우터(AR)/엑세스 포인트(AP) 입장에서 보안상 고려해야 할 사항들이 있다.

첫째, AR/AP의 입장에서 현재 자신의 네트워

크에 접속하기를 원하는 MN에 대해 접속을 허가하기 위해서 MN의 정보를 알 필요가 있다.

둘째, MN의 입장에서 현재 자신이 접속하고자 하는 네트워크의 AR/AP가 정당한 AR/AP인지 확인해야 할 필요가 있다.

이를 위하여 본 논문에서는 SEND의 공개키 기반의 RSA 암호화 메커니즘을 이러한 환경에 적용 하여 발생하는 취약점들을 보완 할 수 있는 방안을 제안한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 ND 메커니즘 관련 보안 위협요소에 대해 설명한다. 3장에서는 2장에서 설명한 위협요소를 해결하기 위해서 SEND에서 제시한 메커니즘들에 대해 분석하고 4장에서는 SEND를 이용한 MN의 안전한 호스트 이동성 지원 방안에 대해 설명하고 5장에서는 결론과 향후 연구 방향에 대해서 기술한다.

II. ND 메커니즘 관련 보안 위협요소

신뢰 모델 환경에서 발생할 수 있는 위협 요소들은 3가지로 나타낼 수 있다.

① 패킷 전달 경로 우회 공격(Redirect Attack) : 악의적인 사용자가 메시지가 라우터나 합법적인 노드로 전달되지 않고 링크상의 다른 노드를 거쳐 전달되도록 유도하는 공격이다.

② 서비스 거부 공격(Denial-of-Service(DoS) Attack): 공격 대상이 되는 호스트가 특정 호스트나 네트워크 내의 다른 호스트들과 통신할 수 없는 상태가 되도록 유도하는 공격이다.

③ 패킷 flooding 공격(Flooding DoS Atack) : 공격자가 다른 노드들의 패킷을 특정 노드로 경유하여 전송되도록 만들어서 그 특정 노드에 필요 없는 트래픽을 전송하여 서비스 거부 상태가 되도록 유도하는 공격이다.

위의 요소들을 좀 더 자세히 분석하면 <표 1>과 같다.

III. SEcure Neighbor Discovery 개요

SEND 워킹그룹에서는 위에서 정의한 보안 위협 요소들을 해결하기 위해 다양한 방법으로 안전하게 ND 메시지를 보호할 수 있는 방법을 제시하고 있는데, 그중 하나가 ND 메시지의 옵션 필드에 새로운 보안 옵션 사항을 추가하는 것이다.[5]

3.1 CGA(Cryptographically Generated Address) 옵션

기존의 보안 인프라가 존재하지 않는 환경에서 보안을 제공할 수 있는 옵션으로서 ND메시지의 송신자가 요구자 주소(Claimed address)의 소유권자임을 CGA 주소를 통해서 주장한다. 그러나,

표1. 위협요소와 신뢰 모델

	공격기법	Redirect/ DoS	Message	신뢰 모델		
				1	2	3
Non router/routing related threats	NS/NA spoofing	Redirect	NA, NS	O	O	O
	NUD failure	DoS	NA,NS	X	O	O
	DAD DoS	DoS	NA, NS	X	O	O
Router/Routing involving Threats	Malicious router	Redirect	RA, RS	O	O	R
	Default router killed	Redirect	RA	O/R	O/R	R
	Good router goes bad	Redirect	RA, RS	R	R	R
	Spoofed redirect	Redirect	Redirect	O	O	R
	Bogus on-link prefix	DoS	RA	X	O	R
	Bogus address config	DoS	RA	X	O	R
	Parameter Spoofing	DoS	RA	X	O	R
Replay Attacks & Remotely Exploitable Attacks	Replay attacks	Redirect	All	O	O	O
	Remote ND DoS	Redirect	NS	O	O	O
		X:위협에 노출되어 있지 않음 O:위협요소가 있으나 해결 가능 R:위협요소에 대한 연구 필요				

CGA주소를 생성할 때 공개키를 이용하므로 모든 노드들은 자신의 CGA 주소를 생성하기 전에 공개키/개인키 쌍을 미리 보유하고 있어야 한다.

CGA의 생성을 위해서는 64비트의 서브넷 프리픽스(subnet prefix), 주소소유자의 공개키, 그리고 3 bits의 보안 파라메터(security parameter)가 필요하다.

CGA 주소는 인터페이스 식별자(Interface Identifier)를 공개키와 임시 파라미터들을 이용하여 일방향 해쉬 함수 SHA-1으로 압축한 값과 프리픽스를 이용하여 생성한다. 송신자가 생성한 CGA 주소와 함께 CGA옵션을 전송하면 수신자는 이 CGA 옵션을 이용하여 CGA 주소를 검증하게 된다. 공개키는 1,024 비트와 2,048 비트 이내의 값이어야 한다.

3.2 RSA 옵션

RSA 옵션은 ND나 RD메시지를 보내는 송신자는 자신의 주소를 CGA암호화를 이용하여 메시지를 전송한다. 수신측에서는 암호화된 주소를 공개키를 이용, 복호화하여 주소를 확인하고 송신자의 주소인지를 검사하는 절차를 거쳐 확인하게 된다. 공개키는 권한 위임 기법을 이용하여 인증서(Certificate)를 통해 제공받거나 CGA를 통해서 제공받을 수도 있고, 두 방법 모두를 통해 제공받을 수도 있다.

3.3 Timestamp and Nonce 옵션

CGA를 이용해 전송하는 메시지도 재현 공격에 노출되어 있다. SEND에서는 이러한 공격에 대응하기 위해 Timestamp, Nonce 옵션을 정의하고 있다. Timestamp는 노드가 메시지를 보내기 전에 메시지 내에 메시지가 보내진 시간을 나타내는 Timestamp 옵션을 포함하여 메시지를 전송한다. Nonce 옵션은 송신자가 메시지를 보낼 때

메시지 안에 랜덤수를 포함하여 전송한다. 일정시간이 지나면 송신자는 새로운 랜덤수를 생성하며 이전의 랜덤수를 포함한 메시지에 대한 응답이 오게 된다면 이를 폐기한다.

3.4 권한 위임 절차

각 라우터들은 이미 자신의 권한(Authority)에 대해 보증 받을 수 있는 신뢰 앵커(Trust Anchor)라고 하는 신뢰 루트를 가지고 있다. 호스트는 처음 네트워크에 접속하여 디폴트 라우터를 선택하기 전에 자신의 디폴트 라우터와 적어도 하나의 공통 신뢰 루트를 두어 인증서 사슬(Certificate Chain)을 형성하여야 한다. CPS(Certification Path Solicitation)메시지는 호스트에 의해서 보내진다. 이 메시지는 라우터와 호스트 사이의 신뢰 앵커를 형성하도록 돕는다. CPA(Certification path advertisement) 메시지는 CPS에 대한 응답으로 보내지는 메시지이며 이 메시지에는 신뢰 앵커에 대한 신뢰 루트를 포함하고 있다.

Ⅳ. Mobile IPv6 망에서 신뢰성 있는 이동성 지원 방안(Trust mobility support protocol;TMSP)

AR/AP는 현재 자신의 네트워크에 접속하기를 원하는 MN이 자신의 네트워크에 접속할 권한이 있는지 알아야 한다. 그리고 접속을 허가하기 위해서 MN에 대한 정보를 알 필요가 있다. 또한 MN은 현재 자신이 접속하려고 하는 네트워크의 AR/AP가 정당한 AR/AP인지 확인해야 할 필요가 있다. 그렇지 않으면 중간에서 MN이 보내는 메시지의 기밀성이 노출 될 수도 있고, DoS 등의 공격에 희생당할 수도 있다.

이 취약점 해결을 위해 SEND에서는 권한 위임기법을 제시하고 있다. 권한 위임 기법을 통해 라우터는 신뢰 앵커로부터 라우터로서 동작할 수 있다는 인증서를 받는다. 노드는 신뢰 할 수 있는 라우터에 대한 정보를 소유하고 있는 신뢰 앵커의 정보를 CPS와 CPA 메시지를 통해서 얻게 된다. 이후 노드는 신뢰 앵커를 통해 라우터를 신뢰할 수 있게 된다.

하지만 라우터가 신뢰 앵커처럼 행동하는 공격자를 신뢰 앵커라고 MN에게 거짓 정보를 준다면 MN는 공격에 노출되게 된다.

이를 위하여 본 논문에서는 PKI 기반의 인증 메커니즘을 MIPv6에 적용하여 AR/AP와 MN이 상호 인증 할 수 있는 프로토콜 TMSP를 제안하여 이러한 취약점들을 해결 하고자 하였다.

4.1 사전 조건

① Host는 한 개 이상의 유니캐스트 IPv6 주소를 홈 에이전트(HA)로부터 할당받아 가지고 있다. 이 주소는 도메인 기반의 계정과 연결되어 있고, 이 정보는 HA에 저장되어 있다.

② HA는 MN의 공개키를 저장하고 있다.

③ HA는 도메인 기반의 인증 시스템을 가지고 있어야 하며, MN은 각 도메인 기반의 계정을 가지고 있고, HA는 이 정보를 SAD(Security Association Database)의 형태로 유지한다.

④ HA는 주 엑세스 라우터와 엑세스 포인트(Master Access router/Access point)를 인증 할 수 있는 정보를 가지고 있다.

4.2 신뢰 라우터 찾기

SEND에서는 권한 위임 절차를 통해 신뢰 앵커라는 신뢰 루트를 찾는다. 하지만 악의적인 목적의 라우터가 가짜 신뢰 앵커에 대한 정보를 MN에게 주어 공격자가 신뢰 앵커로서 행동하여 올바르지 않은 라우터를 인증한다면 잘못된 디폴트 라우터를 선택할 위험이 있다. 따라서 TMSP에서는 2단계의 신뢰 라우터 찾기 절차를 통해서 이러한 위험을 방지한다.

1단계는 네트워크 내에서 한 라우터만을 신뢰하는 것이 아니라 다른 노드들이 이미 신뢰 할 수 있는 라우터라고 인지하고 있는 라우터만을 신뢰 한다. 예를 들면, 노드들의 50%이상이 신뢰할만한 라우터라고 CPA 메시지 안에 특정 라우터에 대한 정보가 포함되어 보내진다면 새로운 노드 또한 그 라우터를 신뢰하여 자신의 임시 디폴트 라우터로서 등록을 하게 되는 것이다.

2단계는 1단계에서 임시로 등록한 AR/AP가 신뢰 할 수 있는 AR/AP인지 판단하기 위하여 MN은 임시 디폴트 라우터로 등록한 AR/AP에게 자신의 공개키가 저장되어 있는 도메인 형태의 HA의 위치정보, HA 내에서 자신의 식별자, 그리고 MN의 개인키로 암호화된 nonce가 포함된 메시지를 전송한다. 이것을 받은 AR/AP는 HA에게 MN의 공개키를 요청하여 MN의 공개키를 얻게 된다.

AR/AP는 전송 받은 공개키를 이용하여 MN이 보냈던 nonce를 복호화 하고 AR/AP 자신의 공개키 정보와 네트워크 프리픽스등의 네트워크에 접속하기 위한 정보를 포함한 응답 메시지를 MN에게 전송한다. 이 메시지를 받은 MN은 nonce정보와 자신이 보냈던 nonce정보와 비교한다.

두 nonce가 같으면 자신이 통신하고 있는 AR/AP가 HA가 인증하는 올바른 AR/AP라고 인식하고 AR/AP가 보내준 정보로 네트워크에 접속하게 된다.

만약 AR/AP가 전송한 nonce가 자신이 보냈던 nonce와 다르다면 MN은 임시 등록했던 AR/AP를 삭제하고 새로운 AR/AP를 찾기 위해서 1단계부터 다시 수행한다.

4.3 AR/AP의 인증

각각의 AR/AP는 계층적인 구조로 되어 있으며 최 상위에 있는 Master AR/AP(MAR/MAP)

가 하위의 모든 AR/AP를 인증한다. 상대적으로 MAR/MAP는 숫자가 적으므로 Mobile IPv6 서비스를 제공하는 네트워크의 HA에 등록되어 있을 수 있다. 가장 하위의 AR/AP는 HA가 MAR/MAP를 인증함에 따라 그 신뢰성이 인증된다.

V. 결론 및 추후과제

본 논문은 IPv6 환경에서 사용되는 인접 탐색 프로토콜(ND)과 SEND 워킹그룹에서 제시하고 있는 암호화 방법과 위협요소에 대해 소개 하였고, SEND의 공개키 기반 RSA방식의 암호화 방법을 Mobile IPv6에 적용하여 MN와 AR/AP가 상호 인증할 수 있는 방안을 제안하였다. 이 방안을 통해 MN는 신뢰할 수 있는 AR/AP에 접속하여 안전한 메시지 교환이 가능하며, AR/AP는 공격자가 네트워크에 무단 접속하여 악의적인 행위를 하는 것을 차단 할 수 있다.

또한 MN과 AR/AP가 서로의 공개키를 소유하고 있으므로 두 인터페이스사이에 보안을 요구하는 메시지를 주고받는 경우 서로의 개인키로 암호화 하여 전송한다면 기밀성, 무결성을 보장받게 될 수 있을 것으로 기대한다.

또한 MN이 네트워크를 떠날 경우 네트워크의 AR/AP는 MN에 대한 정보를 가지고 있으므로 과금 처리를 할 수 있다. 이를 위해서는 별도의 AAA를 두어 운영해야 할 것이다.

참고문헌

[1] C. Perkins, Neighbor Discovery for IP Version 6(IPv6), RFC2461, December 1998.

[2] S. Thomson and T. Narten, IPv6 Stateless Address Autoconfiguration, RFC2462, December 1998.

[3] A. Conta and S. Deering, Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6), RFC 2436, December 1998.

[4] P. Nikander, ED, J. Kempf, and E. Nordmark, IPv6 Neighbor Discovery(ND) Trust Models and Threats, RFC3756, May 2004.

[5] J. Arkko, Ed, J Kempf, B. Zill and P. Nikander, SEcure Neighbor Discovery(SEND), RFC3971, Mar 2005.

그림 1 TMSP 흐름도