SEcure Neighbor Discovery protocol 취약점에 관한 연구

박진호 김정식 조재익 임을규
한양대학교 정보통신대학
pjh0347@yahoo.co.kr bisa1004@hanmail.net whisperi@hanmail.net imeg@hanyang.ac.kr

The Study of SEcure Neighbor Discovery protocol Vulnerability

Park Jin Ho Kim Jung Sik Cho Jae Ik Im Eul Gyu
College of Information & Communications, Hanyang Univ.

요 약

IPv6 네트워크 환경에서는 Neighbor Discovery protocol (NDP)을 이용하여 동일 링크에 연결된 노드 사이에 이웃 노드에 관한 정보를 교환하는데 이런 정보에 대한 보안성 제공은 필수적이지만 초기의 이웃 탐색 프로토콜에서 제공되지 않았다. 이에 대한 해결법으로 IETF에서는 SEND(SEcure Neighbor Discovery) 그룹을 조직하여 NDP 보호 메커니즘 표준을 만들었지만 아직 그 기능과 성능에 대해 개선을 위한 연구가 진행 중이다. 본 논문에서는 보안 이웃 탐색 프로토콜에 대한 분석을 통해 취약점을 정리하고 이론적 대응방안을 거시적으로 제시하며, 뒷부분에서는 취약점 중 하나인 서비스 거부 공격(DoS)에 대해 조금 더 자세하게 생각해 보았다.

1. 서 론

현재 사용하고 있는 IPv4는 주소고갈의 문제로 인해서 가까운 미래에는 주소공간이 획기적으로 확장된 Internet Protocol Version 6 (IPv6)를 사용하게 될 것이다. IPv6에는 확장된 주소공간뿐만 아니라 간단한 헤더 구조, 유연해진 확장과 옵션, 강력해진 QoS 기능, IPsec 기본탑재로 높아진 보안성, 이동성 등 여러 기능이 보완 되었다.[1]

IPv6 네트워크 환경에서는 ICMPv6에 다섯 가지의 메시지 타입을 따로 정의하여 이웃 탐색 프로토콜(Neighbor Discovery Protocol)을 구현하고 있다. 이 프로토콜은 라우터 탐색, 프리픽스 탐색, 파라미터 탐색, 주소 자동 설정[3], 주소 해석, 다음 홉 결정, 인접 노드 접근 불가 탐지, 중복된 주소 탐지, 리다이렉트 등의 기능이 있다.

이웃 탐색 프로토콜은 자체적 보안 메커니즘이 없다. IPv6에서는 확장 헤더 형식으로 IPsec을 지원하여 보안성을 제공하지만 ICMPv6에서 구현된 이웃 탐색 프로토콜은 ICMPv6 프로토콜 자체적 보안 메커니즘을 제공하지 않기 때문에 이웃 탐색 프로토콜에 대해 스니핑, 스푸핑, 위변조 등의 공격이 가능하다. 이문제 해결을 위해 이웃 탐색 프로토콜에 보안성을 제공하는 보안 이웃 탐색 (SEcure Neighbor Discovery, SEND) 메커니즘을 IETF의 SEND 그룹에서 표준화 시켰다. 기본적인 원리는 이웃 탐색 프로토콜에 새로운 메시지 타입과 보안 옵션을 제공하는 것이다.

이렇게 보안 메커니즘을 제공하고 있지만 연구 단계에 있기 때문에 아직 알려지지 않은 취약점이 존재할 가능성이 있다. 본 논문에서는 "이웃 탐색 신뢰 모델과 보안 위협 요소(Neighbor Discovery trust models and threats)" 즉, 이웃 탐색 프로토콜에 보안성 제공을 위한 해결책을 구상할 때 더욱 체계적인 평가 기준을 두어 견고한 메커니즘 구상에 도움을 주기 위해 제시된 내용을 소개하고 각 상황별 공격과 그에 대한 대응법이 있는지 알아본다.

앞의 내용을 바탕으로 SEND의 취약점 분석과 대응방안을 생각해 보고 특별히 주목받고 있는 DoS 취약점에 대해 조금 더 구체적으로 대응 방안을 제시한다.

본 논문에서는 2장과 3장에서 이웃 탐색 프로토콜과 보안 이웃 탐색 메커니즘(SEND)에 대해 설명하고, 4장에서 신뢰 모델과 보안 위협 요소에 대한 내용을 살펴본 후, 5장에서 SEND의 취약점 분석 및 대응방안의 제안과 구체적으로 DoS 공격에 대한 내용을 다루고, 6장에서는 연구 내용을 정리하고 향후 연구 방향에 대해서 설명한다.

2. Neighbor Discovery Protocol

이웃 탐색 프로토콜은 IPv6 네트워크 환경에서 동일 링크에 연결된

* 본 연구는 한국과학재단 특정기초연구(과제번호 : R01-2006-000-11196-0)지원으로 수행되었음.