IPv6 Neighbor Discovery 보안 위협과 대응

*박수덕, 이용식, 이병호
한양대학교 정보통신학과
e-mail : *kma58@naver.com*, ys8016@*hanmail.net*

IPv6 Neighbor Discovery security treats and opposition

*Soo-Duck Park, Yong-Sig Lee, Byung-Ho Rhee
The Department of Information and Communications
Hanyang University

Abstract

IPv6 nodes use the Neighbor Discovery Protocol (NDP) to discover other nodes on the link, to determine their link-layer addresses to find routers, and to maintain reachability information about the paths to active neighbors. If not secured, NDP is vulnerable to various attacks. This document specifies security mechanisms for NDP. Unlike those in the original NDP specifications, these mechanisms do not use IPsec.

I. 서론

MIPv6의 Neighbor Discovery 프로토콜은 ICMPv6의 정보 메시지를 이용하여 노드들간에 로컬 네트워크의 토폴로지 정보를 주고 받는다. 이러한 프로토콜에 보안이 제공되지 않으면, 다양한 공격으로부터 네트워크 전체가 위협을 받을 수 있다.

본 논문은 SEND 워킹그룹에서 정의한 신뢰 모델과 보안 위협 요소 및 인접노드 탐색 프로토콜의 보안 옵션에 대해 살펴보고, 각각의 옵션이 어떻게 보안위협에 대응하고 있는지 분석하였다.[1)]

1) 본 연구는 대학 IT 연구센터 육성 지원 사업의 연구 결과로써 HY-SDR 연구센터의 연구비 지원으로 수행 되었음

II. 본론

1 CGA

SEND에서는 암호화의 공개키를 IPv6 주소와 안전함을 결부하는 방법을 제시하고 있다. 기본적으로 공개 암호키의 암호를 이용한 암호 해쉬를 계산하여 IPv6 주소의 인터페이스를 생성하는 것이다. 이러한 결과로 생성되는 IPv6 주소는 암호화하게 생성되어 CGA라 불린다. 이렇게 생성에 의해 상응하는 비밀키는 주소로부터 메시지들을 서명하기 위해 사용된다.

CGA를 생성하는 데는 세 가지의 값을 포함한다. 64비트의 서브넷 프리픽스, 주소소유자의 Public key, 그리고 보안매개변수(Sec)를 포함한다.

① 128 비트 값을 가지는 임의의 Modifier를 만든다.
② 1번에서 만들어진 Modifier 값을 오른쪽에서 왼쪽으로 입력하고 Public key와 함께 연결한다. SHA-1 값의 가장 왼쪽 112 비트가 Hash2 값이 된다.
③ 생성된 Hash2의 값 중 가장 왼쪽의 값인 16*Sec을 비교하여, 모두 0이면(or if Sec=0) Step 4로 가고, 아닐경우 Modifier 값을 1 증가시키고 Step 2로 간다.
④ 앞의 과정이 수행된 수 collision count를 0으로 세팅한다.
⑤ Modifier, subnet prefix, collision count, encoded public key, optional extension fields 값을 연결시켜 SHA-1 알고리즘을 실행한다. 이 값의 가장 왼쪽 64비트를 Hash1값으로 한다.
⑥ Hash1의 값에서 가장 왼쪽 3개의 비트는 보안 파라메타의 값을 넣고, 비트 6과 7(i.e., the "u" and "g"

bits)은 0으로 세팅한다가운데 'u'와 'g'의 비트를 넣어 최종 인터페이스 식별자를 생성한다.
⑦ 64비트 서브넷 프리픽스와 64비트 인터페이스 식별자를 연결하여 128비트의 IPv6 address 를 생성한다.
⑧ DAD 과정에서 collision 이 발생하게 되면 collision count를 증가시키고 step 5로 간다. 3번의 collision 이 발생할경우 주소생성을 중단하고 error를 보고한다.
⑨ 최종 Modifier value, subnet prefix, 최종 collision count value, encoded public key, optional extension fields 들에 의해서 CGA Parameters data structure 가 만들어 진다.

2 RSA Signature

모든 ND나 RD 메시지를 개인키를 이용하여 메시지 서명함(공개키 기반 서명)으로써 송신자의 Identifier를 인증하고 메시지의 무결성을 제공하는 옵션이다. 공개키는 권한 위임 기법을 이용하여 인증서(Certificate)를 통해 제공받거나 CGA를 통해서 제공받을 수도 있고, 두 방법 모두를 통해 제공받을 수도 있다.

3 Timpstamp and Nonce

Timpstamp와 Nonce 옵션은 Timestamp option의 목적은 unsolicited advertisements 와 redirect 메시지의 replay 공격에 대응하는 것이다. Nonce option의 목적은 노드에 의해 보내어진 solicitation의 응답으로 새롭게 만들어진 advertisement 라는것을 증명하는 것이다. 송신자는 모든 ND 메시지에 Timestamp 옵션을 포함하고 Solicitation/Advertisement 메시지에는 Nonce 옵션을 포함하여 전송하여야 한다.

4 Authorization Delegation Discovery

각 라우터들은 이미 자신의 권한(Authority)에 대해 보증받을 수 있는 Trust Anchor 의 신뢰 루트를 가지고 있다. 호스트는 처음 네트워크에 접속하여 디폴트 라우터를 선택하기 전에 자신의 디폴트 라우터와 적어도 하나의 공통 신뢰 루트를 두어 Certificate Chain 을 형성하여야 한다. 이와 같은 문제를 해결하기 위해 새로운 ICMPv6 메시지인 CPS(Certification Path Solicitation)와 CPA(Certification Path Advertisement)를 정의하였다. 이 메시지들을 통해 호스트는 라우터를 지정하기 전에 라우터 존재 유무와 Certificate Chain 정보를 얻을 수 있다. 호스트는 라우터로부터 인증서 사슬 정보를 획득하기 위해 CPS 메시지 내에 자신의 Trust Anchor 목록을 포함하여 전송하고, 라우터는 이에 대한 응답으로 자신의 인증서나 Trust Anchor 목록을 포함한 CPA 메시지를 호스트로 전송한다.

Ⅲ. SEND에 의한 위협요소 대응

SEND에서 정의된 옵션과 메시지들은 라우터와 호스트들 사이의 신뢰를 형성하게 한다. CPS, CPA를 통하여 라우터를 신뢰하게 되며, RSA를 CGA를 이용하여 호스트들 사이에 신뢰형성을 가능하게 한다.

공격자는 ND 메시지를 위조하려 하지만, 메시지 내의 주소는 CGA로 암호화 되어 주소를 알아낼 수 없다. 만일 공격자가 메시지를 전송하여 상대호스트가 메시지를 받는다고 하더라도 RSA Signature 를 분석하여 송신자 주소와 서명내의 주소를 비교하여 송신자를 인증하게 된다.

Ⅳ. 결론 및 향후 연구 방향

지금 현재 전 세계는 IPv6로의 전환을 시작하고 있는 단계이며, 많은 기업에서는 IPv4의 제품에 IPv6의 기능을 탑재한 제품을 출시하고 있다. 따라서 현존하는 위협요소들에 대한 충분한 대처가 필요할 것이며, SEND에서 제시하고 있는 여러 가지 매커니즘에 대한 보안 시스템 적용이 필요한 시점이다. SEND를 통해 MIPv6의 보안 취약점은 대부분 해결이 되었지만, 일부 RD 메시지에 대한 공격(Default router killed, Good router goes bad)에 대해서는 완벽히 해결하지 못하고 있다. 이에 대한 충분한 연구와 개선이 필요하다.

참고문헌

[1] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.
[2] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
[3] Jari Arkko, James Kempf, Brian Zill, Pekka Nikander. "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.
[4] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.
[5] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", June 2004.