Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security

Yvette E. Gelogo[1], Ronnie D. Caytiles[1] and Byungjoo Park[1]*

1Multimedia Engineering Department, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
vette_mis@yahoo.com,gnsnfcknrs@yahoo.com,bjpark@hnu.kr
**Correspondent Author: Byungjoo Park* (bjpark@hnu.kr)*

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. Secure Neighbor Discovery Protocol (SEND Protocol) is a security extension of Neighbor Discovery. The SEND protocol is designed to counter the threats to NDP. This paper presents the threats and security analysis for SEND and all the possible security options for more secure IPv6 Neighbor Discovery Protocol.

Keyword: *IPV6, Secured Neighbor Discovery Protocol, CGA, NDP*

1. Introduction

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 [1].

The Neighbor Discovery Protocol (NDP) is a protocol in the Internet Protocol Suite used with Internet Protocol Version 6 (IPv6). It operates in the Link Layer of the Internet model and is responsible for address auto configuration of nodes, discovery of other nodes on the link, determining the Link Layer addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) [2].

The original NDP specifications called for the use of IPsec to protect NDP messages. However, the RFCs do not give detailed instructions for using IPsec to do this. In this particular application, IPsec can only be used with a manual configuration of security associations, due to bootstrapping problems in using IKE Furthermore, the number of manually configured security associations needed for protecting NDP can be very large making that approach impractical for most purposes [1].

Protocols for Neighborhood Discovery (ND) serve as fundamental building blocks in mobile wireless systems. Clearly, ND enables (multi-hop) communication, as it is essential for route discovery and data forwarding. ND can also support a wide range of system functionality: network access control, topology control, transmission scheduling, energy-efficient communication, as well as physical access control. Given the critical and multifaceted role of ND, its security and robustness must be ensured: ND protocols must identify as neighbors only those devices that actually are neighbors, even in hostile environments. Securing ND is however a hard problem. The very nature of wireless environments and mobile computing applications makes it easy to abuse ND and thereby

compromise systems for which ND is a building block. If not secured, NDP is vulnerable to various attacks. This paper specifies security mechanisms for NDP.

The rest of this paper is organized as follows: Section II explains background about NDP and SEND protocol; In Section III we discuss the Cryptographically Generated Addresses and its security attributes and contributions to SEND; In section IV discuss the threats and security analysis then in Section V the proposed security mechanism and lastly the concluding remarks in Section VI.

2. Background

In this section we briefly describe the current state of the technology. We assume that the reader is familiar with the basic IPv6 architecture and functions. Thus, we concentrate on explaining the Neighbor Discovery Protocol and Secured Neighbor Discovery Protocol to understand a small background about the terms and the protocols focusing on security related issues.

2.1 NDP Protocol

Nodes (hosts and routers) use Neighbor Discovery to determine the link-layer addresses for neighbors known to reside on attached links and to quickly purge cached values that become invalid. Hosts also use Neighbor Discovery to find neighboring routers that are willing to forward packets on their behalf. Finally, nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses. When a router or the path to a router fails, a host actively searches for functioning alternates [8].

Neighbor Discovery Protocol (NDP) has specific functions like Neighbor Discovery (ND), Address Auto-configuration, Router Discovery (RD), Neighbor Un-reachability Detection (NUD), Address Resolution, and Duplicate Address Detection (DAD). Figure 1 is the Neighbor Discovery Protocol function and the general overview and Figure 2 illustrate the NDP message format.

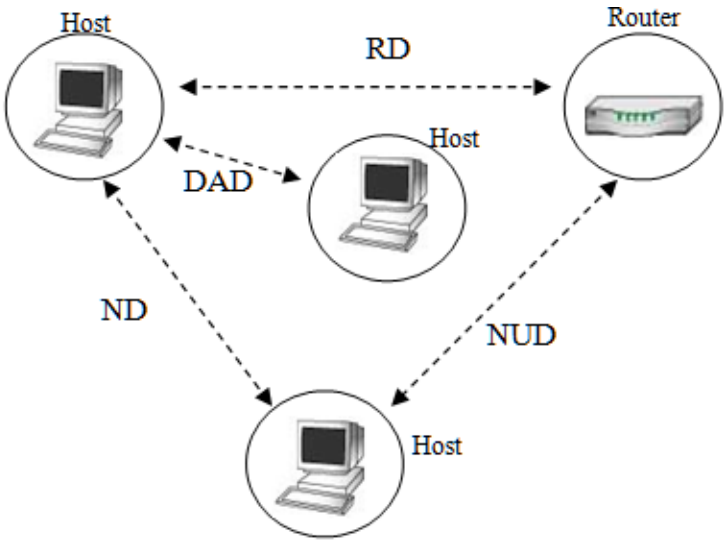

Figure 1. Neighbor Discovery Protocol Overview

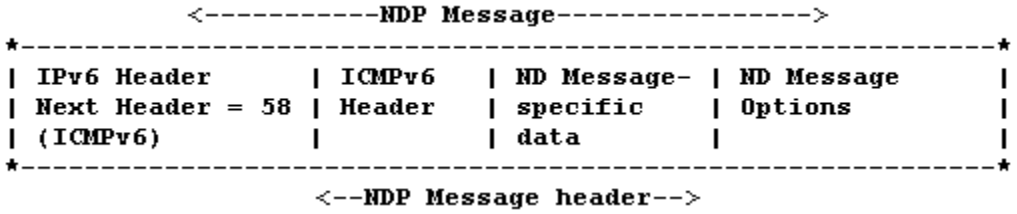

Figure 2. The NDP Message Format

2.2 SEND Protocol

The Secure Neighbor Discovery (SEND) protocol is designed to counter the threats to NDP. SEND is applicable in environments where physical security on the link is not assured (such as over wireless) and attacks on NDP are a concern. As NDP is used by both hosts and routers, it is more vulnerable to various attacks unless secured. To encounter the threats to NDP, Secure Neighbor Discovery (SEND) protocol is designed.

SEND uses CGAs, a cryptographic method for binding a public signature key to an IPv6. CGAs are used to make sure that the sender of a neighbor discovery message is the "owner" of the claimed address. A public-private key pair is generated by all nodes before they can claim an address. A new NDP option, the CGA option, is used to carry the public key and associated parameters. CGA is formed by replacing the least-significant 64 bits of the 128-bit IPv6 address with the cryptographic hash of the address owner's public key. The messages are signed with the corresponding private key. Only if the source address and the public key are known can the verifier authenticate the message from that corresponding sender [6].

The SEND protocol requires no public-key infrastructure. Valid CGAs may be generated by any sender, including a potential attacker, but they cannot use any existing CGAs. Public key signatures protect the integrity of the messages and authenticate the identities of those who send them. The authority of a public key is established via a number of processes depending on the configuration and the type of message that's being protected.

3. Cryptographically Generated Addresses

Cryptographically generated addresses (CGA) are IPv6 addresses where up to 64 address bits are generated by hashing the address owner's public key. The address owner uses the corresponding private key to assert address ownership and to sign messages sent from the address without a PKI or other security infrastructure. The CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery and mobility protocols. It can also be used for key exchange in opportunistic IPSec. The idea of hashing CGA idea originated in a paper on child-proof authentication for Mobile IPv6 [5]. CGA are IPv6 addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from public key and auxiliary parameters. The binding between the public key and the address can be verified by re-computing the hash value and by comparing the hash with the interface identifier. Messages sent from an IPv6 address can be protected by attaching the public key and auxiliary parameters and by signing the message with the corresponding private key. The protection works without a certification authority or any security infrastructure [4].

4. Threats and Security Analysis

As NDP is used by both hosts and routers, it is more vulnerable to various attacks unless secured. To encounter the threats to NDP, Secure Neighbor Discovery (SEND) protocol is designed. Various protocol options are given below.

- *Cryptographically Generated Addresses (CGA) Option*

  The CGA ensures that the sender of an NDP message is the owner of the claimed address. Before claiming an address, each node generates a public-private key pair and the CGA option verifies this key [1, 3].

- *RSA Signature Option*

  The public key signatures maintain the integrity of the messages and authenticate the sender identity. The RSA Signature option protects messages by requiring public-key based signatures attached to every NDP message [1, 3].

- *Timestamp Option*

  The Timestamp option provides replay protection and ensures that unsolicited advertisements and redirects have not been replayed [1].

- *Nonce Option*

  An unpredictable random or pseudo-random number generated by a node and used exactly once. In SEND, nonces are used to assure that a particular advertisement is linked to the solicitation that triggered it [1].

- *Certification Path Solicitation*

  Authorization is provisioned for both routers and hosts with routers getting certificates from a trust anchor and hosts getting configured to authorize routers. Separate certification path solicitation and advertisement messages are used to know the certification path to the trust anchor. Hosts will send the Certification Path Solicitations [1].

The following are the threats and SEND security responses:

- *Neighbor Solicitation/Advertisement Spoofing*

  - SEND requires the RSA Signature and CGA options to be presented in solicitations.

- *Neighbor Unreachability Detection Failure*

  - SEND requires a node responding to Neighbor Solicitations probes to include an RSA Signature option and proof of authorization to use the interface identifier in the address being probed

- *Duplicated Address Detection DoS Attack*

  - SEND requires including an RSA Signature option and proof of authorization in the Neighbor Advertisements sent as responses to DAD

- *Router Solicitation and Advertisement Attacks*

  - SEND requires Router Advertisements to contain an RSA Signature option and proof of authorization

- *Replay Attacks*

  - SEND includes a Nonce option in the solicitation and requires the advertisement to include a matching option.

SEND enhances this insecure protocol by employing cryptographically generated addresses (CGA) to encrypt NDP messages. This method is independent of IPSec, which is typically used to secure IPv6 transmissions. The introduction of CGA helps to nullify neighbor/solicitation/advertisement spoofing, neighbor unreachability detection failure, DOS attacks, router solicitation, and advertisement and replay attacks. The SEND protocol requires no public-key infrastructure. Valid CGAs may be generated by any sender, including a potential attacker, but they cannot use any existing CGAs. Public key signatures protect the integrity of the messages and authenticate the identities of those who send them. The authority of a public key is established via a number of processes depending on the configuration and the type of message that's being protected.

6. Conclusion

IPv6 Neighbor Discovery Protocol is vulnerable to attacks. Secure Neighbor Discovery Protocol (SEND Protocol) is a security extension of NDP. It introduces different kind of security options in order to secure the connection while moving from one node to another node. It is better to understand what are the security options and the possible attacks that can be launched. There have been a lot of proposed security to secure IPv6 in different aspect but there is no concrete solution. Hence, it is better to understand which among these options is applicable for certain requirements. In this paper, we introduce threats and security analysis for SEND and different security options for enhanced Secured Neighbor Discovery Protocol.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0024401, 2011-0026286).

References

[1] Request for Comments: 3971, “SEcure Neighbor Discovery (SEND),”http://tools.ietf.org/html/rfc3971.

[2] Request for Comments: 1122, “Requirements for Internet Hosts - Communication Layers”, http://tools.ietf.org/html/rfc1122.

[3] Secure Neighbor Discovery (SEND), http://ipv6.com/articles/research/Secure-Neighbor-Discovery.htm.

[4] RFC: 3972 , “Cryptographically Generated Addresses (CGA)”, http://www.ietf.org/rfc/rfc3972.txt.

[5] “Designing secure Internet protocols “, http://research.microsoft.com/en us/projects/secureprotocols/default.aspx.

[6] http://www.techopedia.com/definition/24857/secure-neighbor-discovery-protocol-send-protocol.

[7] J. Arkko, et. al., “Securing IPv6 Neighbor and Router Discovery”, WiSe ’02, **(2002)** September 28, Atlanta, Georgia, USA.

[8] RFC: 4861, “Neighbor Discovery for IP version 6 (IPv6)”, http://tools.ietf.org/html/rfc4861.

Authors

Yvette E. Gelogo

2006~2010 Bachelor of Science in Information Technology, Western Visayas College of Science and Technology, Philippines

Currently, Master of Science in Multimedia Engineering, Hannam University, Daejon, Korea

Research Interests: Mobile Computing, Multimedia Communication, Ubiquitous Healthcare, Ubiquitous Learning, Biometrics, Information Security.

Ronnie D. Caytiles

1995-2000 Bachelor of Science in Computer Engineering, – Western Institute of Technology, Iloilo City, Philippines

2008-2010 Master of Science in Computer Science – Central Philippine University, Iloilo City, Philippines

Currently, Integrated Course for M.S. and Ph.D. in Multimedia Engineering, Hannam University, Daejon, Korea.

Research Interests: Mobile Computing, Multimedia Communication, Information Technology Security, Ubiquitous Computing, Control and Automation.

Byungjoo Park

He received the B.S. degree in electronics engineering from Yonsei University, Seoul, Rep. of Korea in 2002, and the M.S. and Ph.D. degrees (first-class honors) in electrical and computer engineering from University of Florida, Gainesville, USA, in 2004 and 2007, respectively. From June 1, 2007 to February 28, 2009, he was a senior researcher with the IP Network Research Department, KT Network Technology Laboratory, Rep. of Korea. Since March 1, 2009, he has been a Professor in the Department of Multimedia Engineering at Hannam University, Daejeon, Korea. He is a member of the IEEE, IEICE, IEEK, KICS, and KIISE. His primary research interests include theory and application of mobile computing, including protocol design and performance analysis in next generation wireless/mobile networks.