Chapter 8
SEcure Neighbor Discovery: A Cryptographic Solution for Securing IPv6 Local Link Operations

Ahmad AlSa'deh
Hasso-Plattner-Institute, Germany

Hosnieh Rafiee
Hasso-Plattner-Institute, Germany

Christoph Meinel
Hasso-Plattner-Institute, Germany

ABSTRACT

SEcure Neighbor Discovery (SEND) was proposed to counteract threats to the Neighbor Discovery Protocol (NDP). It is a strong security extension that can make the IPv6 local link very safe. SEND relies on dynamically Cryptographically Generated Addresses (CGAs) and X.509 certificates. However, SEND is not easily deployed and is still vulnerable to some types of attacks. This chapter evaluates the practical considerations of a SEND deployment taking a cryptographic approach as a means of securing the IPv6 local link operations. It reviews the remaining vulnerabilities and gives some recommendations with which to facilitate SEND deployment.

INTRODUCTION

The free pool of IPv4 address space will be depleted soon. On 3 February 2011, the Internet Assigned Numbers Authority (IANA) (2012, March 14) allocated the last remaining blocks of IPv4 address space to the Regional Internet Registries (RIRs). Therefore, the world is responding by transitioning from IPv4 to IPv6. On 8 June 2011, top websites and Internet Service Providers (ISPs) around the world joined together with more than 1000 other participating websites in a "World IPv6 Day". Because of the success of this global-scale event, the Internet Society organized the "World IPv6 Launch Day" on 6 June 2012 (Internet Society, 2012). On this day major ISPs and companies around the world permanently enabled IPv6 for their products and services.

DOI: 10.4018/978-1-4666-4030-6.ch008

However, businesses need to migrate to IPv6 in a secure manner in order to avoid the possible security risks inherent in an IPv6 deployment. One of the security concerns comes from the new IPv6 features and mechanisms, which can expose the network to new security threats. For instance, StateLess Address Auto-Configuration (SLAAC) (Thomson, Narten, & Jinmei, 2007) and Neighbor Discovery (ND) (Narten, Nordmark, Simpson, & Soliman, 2007) messages are essential portions of the IPv6 suite. Both ND and SLAAC, together, are known as Neighbor Discovery Protocol (NDP). IPv6 nodes use NDP for several critical functions: to discover other nodes (routers/hosts) on the link, to find the mapping between the MAC and link local addresses, to detect duplicate addresses, and to maintain reachability information about the paths to active neighbors. Also, NDP plays a crucial role in mobile IPv6 (MIPv6) networks (Perkins, Johnson, & Arkko, 2011). However, NDP is vulnerable to spoofing and Denial-of-Service (DoS) attacks (Nikander, Kempf, & Nordmark, 2004) and attackers have already developed a set of tools to use in attacking ND functionalities (Hauser, 2012).

NDP specifications do not include any security provisions. It was designed to work in trustworthy links where all nodes on the link trust each other. However, we cannot assume that being on the same network is trustworthy as this assumption does not hold in number of different scenarios, such as, over wireless networks, where anyone can join a local link either with minimal or with no link layer authentication. Today people use public networks such as Wireless LAN at airports, hotels, and cafes, where a malicious user can impersonate legitimate nodes by forging NDP messages to generate serious attacks. RFC 3756 (Nikander, et al., 2004) shows a list of potential threats to NDP. Therefore, if NDP is not secured, it will be vulnerable to these various attacks. Some such attacks are Neighbor Solicitation (NS)/ Advertisement (NA) spoofing, Neighbor Unreachability Detection (NUD) faller, Duplicate Address Detection (DAD), Denial of Service (DoS), Malicious Last Hop Router, Spoofed Redirect Message, Bogus On-Link Prefix, Parameter Spoofing, and Replay attacks.

Therefore, RFC 3971 "SEcure Neighbor Discovery (SEND)" (Arkko, Kempf, Zill, & Nikander, 2005) was proposed as a set of enhancements to make the IPv6 neighbor and router discovery secure. SEND was designed to ensure message integrity, prevent IPv6 address theft, prevent replay attacks, and provide a mechanism for verifying the authority of routers. It uses Cryptographically Generated Addresses (CGA) (Aura, 2005), digital signature, and X.509 certification (Lynn, Kent, & Seo, 2004) to offer significant protection for NDP. A SEND-enabled node must generate or obtain a public-private key pair before it can claim an address. Then it generates the CGA address based on the public key and other auxiliary parameters. The associated private key is used to sign the outgoing ND messages from that address. For router authorization, every router must have a certificate from a trust anchor and the hosts provisioned with a trust anchor(s) list and picks routers that can show a valid certificate from a trust anchor. The SEND verifier node checks that the received address is a hash of the corresponding public key and that the signature, from the associated private key, is valid. If both verifications are successful, then the verifiers know that the address is not a stolen address and that it is from the address corresponding to public private key pairs.

Although SEND is considered to be a promising technique with which to protect NDP and to make IPv6 a very safe protocol, its deployment is not easy and thus is very challenging. SEND lacks mature implementations by developers of operating systems. It is compute-intensive and bandwidth-consuming. Moreover, SEND itself can be vulnerable to some types of attacks.

This chapter will introduce SEND functionalities and messages, discuss the practical considerations of SEND deployment as a cryptography solution in securing IPv6 local networks, survey