A secure framework for protecting IPv6 Neighbor Discovery Protocol

Colin Putman

Technical Report

RHUL–ISG–2019–3

27 March 2019

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

One of the major problems to overcome in the transition from IPv4 to IPv6 is the security of the Neighbor Discovery Protocol (NDP) in IPv6, which is used to find neighbouring devices and routers on the same network link and to resolve local IPv6 addresses into link-layer addresses. Because NDP must be used as soon as a network is joined, before an IP address is chosen, it cannot use Internet Key Exchange (IKE) and so cannot be secured using IPsec as the rest of IPv6 can. It is therefore necessary for another system to be developed to secure this protocol, and while numerous proposals have been made, none have yet been found to be completely satisfactory for this purpose.

This project builds upon previous work surveying the proposals in this problem area by closely analysing a selection of the most successful or interesting proposals, focusing on those which directly extend NDP to be less vulnerable to attacks over those which specify reactive solutions based on intrusion detection systems. Particular attention is paid to SEND, currently the most complete and only industry-implemented security extension for NDP, and to the various proposals made to improve upon SEND and mitigate the drawbacks to its design. Two new, brief proposals are also made to add to the current proposals for secure router authentication, these being the use of OCSP queries to confirm that a certificate has not been revoked due to key compromise, and the use of DNSSEC reverse-lookup queries as an alternative trust anchor which does not use certificates.

In addition to providing an analytical survey of the proposals in this area, this project concludes by drawing on selected parts of the examined proposals to formulate a suggestion for a framework of improvements to SEND which aims to cover all of the major drawbacks of the protocol which previous papers have identified. The intention of this framework is to show how aspects of the proposed systems complement each other and can be combined into a more complete and efficient solution than they represent on their own. However, further scrutiny and standards action would be required, likely resulting in changes to the framework, before this solution could be adopted and implemented as an extension to NDP.