Could IPv6 Improve Network Security? And, If So, at What Cost?

Brent Rowe and Michael Gallaher
RTI International
browe@rti.org

Abstract

Industry stakeholders and Internet experts generally agree that IPv6-based networks in many ways would be technically superior to IPv4-based networks. The redesigned header structure in IPv6, including new flow labels, and the enhanced capabilities of the new protocol could provide significant security benefits to Internet users, network administrators, and applications developers. However, there is disagreement about the characteristics and timing of the security benefits associated with IPv6. Some experts believe that IPv6 could spur increased research and development of and interest in transitioning to a new network security model, in which techniques such as Internet Protocol Security (IPSec) could be more commonly and effectively used. However, the costs of a transition to IPv6 could be substantial and the benefits are still rather speculative.

In this paper, we will discuss the question of whether IPv6 could help improve computer network security, and if so, at what cost. Based on a study we performed for the Department of Commerce IPv6 Task Force, our paper provides a qualitative assessment of the potential security effects of a transition to IPv6 as well as a quantitative analysis of the cost of IPv6 adoption to be borne by users, ISPs, and vendors in the U.S. The results of our analysis should be useful to both industry and government in decisions related to investments in network security and IPv6.