IPv6 guide provides path to secure deployment of next-generation Internet protocol
6 January 2011

As the day draws nearer for the world to run out of the unique addresses that allow us to use the Internet—now predicted to happen by the end of 2012—researchers at the National Institute of Standards and Technology (NIST) have issued a guide for managers, network engineers, transition teams and others to help them deploy the next generation Internet Protocol (IPv6) securely.

Guidelines for the Secure Deployment of IPv6 (NIST Special Publication 800-119), describes the features of IPv6 and the possible related security impacts, provides a comprehensive survey of mechanisms to deploy IPv6 and suggests a deployment strategy for a secure IPv6 environment.

The ballooning popularity of devices, such as smart phones and netbooks, tied to the Internet is rapidly depleting the number of so-called IP addresses available under the current Internet Protocol version 4 (IPv4), so the networkers of the world are preparing to move to the next generation, IPv6. Among other improvements, IPv6 has a vastly greater number of potential addresses—several billion per each of the world's current population of about 6.9 billion people.

To ensure that the federal government is prepared for IPv6, the Office of Management and Budget has mandated federal agencies to begin deploying the new protocol. NIST developed the IPv6 security guidelines in support of the Federal Information Security Management Act (FISMA). The publication is designed to help federal agencies avoid possible security risks that could occur during IPv6 deployment. It also could be useful for the private sector and other organizations.

"The Internet protocol pervades every aspect of computer communications," explains lead author Sheila Frankel, "so deploying IPv6 is a major task." With detailed planning, she says, organizations can navigate the process smoothly and securely. Most organizations will be operating IPv6 and IPv4 concurrently.

"Security will be a challenge, however, because organizations will be running two protocols and that increases complexity, which in turn increases security challenges," Frankel says. SP 800-119 describes the security challenges organizations may face as they deploy IPv6. Those challenges include fending off attackers that have more experience than an organization in the early stages of IPv6 deployment and the difficulty of detecting unknown or unauthorized IPv6 assets on existing IPv4 production networks. The publication provides information to be considered during the deployment planning process and makes recommendations to mitigate IPv6 threats.

More information: SP 800-119, Guidelines for the Secure Deployment of IPv6, may be downloaded in pdf format from csrc.nist.gov/publications/nist ... 00-119/sp800-119.pdf . An index to the NIST 800-series special publications on computer security is available at csrc.nist.gov/publications/PubsSPs.html .

Provided by National Institute of Standards and Technology