PANEL: Securing the Internet's Exterior Routing Infrastructure

Sue Hares (Merit, United States)
Sandra Murphy, TIS Labs at Network Associates
Charles Lynn, BBN Technologies
Tony Li, Juniper Networks, Inc.
Curtis Villamizer, ANS Communications

The Internet's exterior routing infrastructure is highly vulnerable to a variety of attacks, both in theory and in practice, due to the lack of a scalable means to verify the legitimacy and authenticity of the relevant control traffic. This infrastructure is based on a distributed system composed of routers grouped into management domains called Autonomous Systems (AS's). Routing information is exchanged between routers (aka "speakers") on the borders of the AS's using the Border Gateway Protocol (BGP-4). BGP's vulnerability has been clearly demonstrated by a number of recent unintentional "attacks" involving misconfigured routers. In these cases, incorrect routing information was advertised by the misconfigured routers and unquestioningly accepted by other routers, leading to mis-routing of traffic and many hours or even days of disrupted communications.

Correct operation of BGP depends upon the integrity, authenticity, and recency of the routing UPDATEs as well as each BGP speaker's correctly processing, storing, and distributing this information. The nature of the information to be verified (e.g., authorization of the BGP speaker sending/receiving an UPDATE, the content of the UPDATE (unreachable destinations for which routes are to be withdrawn, IP address prefixes for new routes, the path (a sequence of AS's) to those destinations, etc.) and the very large number of routes (approximately 50,000) and UPDATEs (approximately 1 million/day for a speaker located at a Network Access Point (NAP)) combine to make the securing of BGP a challenging problem.

During this panel session, the first panelist will present a security analysis of BGP, outlining its vulnerabilities. Each of the 3 remaining panelists will then present a different approach to addressing one or more of these vulnerabilities.