## BSDCan 2010: The Technical BSD Conference

*May 13–14, 2010*
*Ottawa, Canada*

- ***Security Implications of the Internet Protocol version 6 (IPv6)***

*Fernando Gont, Universidad Tecnológica Nacional/Facultad Regional Haedo (Argentina) and United Kingdom's Centre for the Protection of National Infrastructure*

*Summarized by Alan Morewood (morewood@computer.org)*

*Editor's Note: As a Gold Sponsor of BSDCan 2010, USENIX invites attendees to submit reports for publication in* ;login:. *We received this very timely summary about issues with implementing IPv6 in production networks.*

Although there where frequent references to the sysctl parameters that allow BSD to tweak various kernel settings, Fernando's talk was focused at a higher level, explaining the fundamental concerns uncovered during his ongoing research with the UK's Centre for the Protection of National Infrastructure (CPNI).

The three most important messages from the presentation may be: to train design and operations staff on IPv6 before deployment; that there are significant similarities and differences between IPv4 and IPv6 but that myths and marketing are unreliable sources to distinguish the differences; and, finally, for developers to always provide a limit to functionality which uses kernel resources.

To have features similar to an organization's existing IPv4 firewall, one needs to have similar policy enforcement mechanisms available, so careful evaluation of vendor's IPv6 equipment is necessary. Some settings, such as ICMPv6 redirect, are not entirely necessary for operation according to Gont, only for optimization. A strong knowledge of architecture will mean that redirects are not necessary for operation or optimization. Education and training would allow for the right configuration; while knowledge of IPv4 and related utilities is useful, there are some differences in the details.

Know the details, not the hype, suggested Gont. Early in the presentation, Gont made reference to a myth that, due to the large IPv6 address space, scanning for valid addresses will be infeasible. This presumption is predicated on the idea that the space is used in a random and uniformly sparse manner, but studies have shown that deployment methods actually used have many factors which lead to significant predictability. These include sequential manual address assignment, sequential MAC address assignments typical of an enterprise environment, and addresses based on IPv4, all found within the Host ID field. It was noted that with the default MAC-based HostID assignment, individual hosts can be tracked when connected to different networks, causing possible privacy concerns.

Gont pointed out that while OpenBSD had many of the tweaks necessary to safeguard resource usage and limit other IPv6 vulnerabilities, there were still areas of concern not covered and that the default settings were not the most conservative, allowing for full functionality. Some BSD implementations did not enforce minimum fragment or packet sizes, none filtered MAC addresses reserved for broadcast and multicast, and some did not have tweaks to disallow autoconfiguration from manipulating routing configuration, all facilitating various abuses.

An example of resource utilization issues is that a device can receive multiple network addresses, at least one per valid network prefix in operation on a link. Without a limit, an attacker may impose thousands of addresses on a host's network interface via the autoconfiguration features, causing excessive resource use on the host. Similar resource issues were brought forward for fragment processing, link layer address cache sizes, and many other important functions. An audience member noted that putting limits on these parameters could prevent correct operation while under attack, which was acknowledged, but all agreed that having an operational kernel facilitated corrective action.

Many more concerns were presented, such as the use of fragmentation which, despite the new restrictions on overlapping fragments (RFC5722), may still allow firewall rule bypassing. More details on this and other issues are still not public, for security reasons. They are working with vendors and other relevant parties to correct protocol and implementation issues.