ISP Internet Routing Security Practices and Partnerships

January 2024

The Communications Sector Coordinating Council (CSCC) recognizes the key role that transit and peering play in the Internet ecosystem and have embraced routing security measures that prioritize protecting critical functions from Internet protocol risks. As made explicit in the National Cybersecurity Strategy Implementation Plan (National Cybersecurity Initiative), making progress will require "close collaboration between public and private sectors to reduce our risk exposure without disrupting the platforms and services built atop this infrastructure."

Herein, the CSCC identifies robust and concrete actions that Internet Service Providers (ISPs) have undertaken to advance Internet routing security. ISPs' proactive, continuous efforts ought to undergird and encourage activities by other participants of the ecosystem to follow ISPs' lead in good Internet routing hygiene.

While the concrete measures identified below represent a major successful collective effort by many ISPs, ISPs constitute only a small part of the ecosystem – as evidenced by the National Cybersecurity Initiative. It is crucial for all stakeholders to acknowledge that routing security is a team sport, and for other parts of the ecosystem to also be expected to do their part for the collective good of the Internet. In particular, the paradigm must include participation in security measures by network operators other than ISPs, as well as hardware and software vendors, registries, and other relevant entities, across the board.

Indeed, actions undertaken by ISPs cannot unilaterally protect against the sorts of risks and attacks about which stakeholders like CISA, DOJ, and DoD have expressed concern. For example, the well-publicized incident where Department of Energy traffic was misrouted through China will be *partly* addressed by ISPs' RPKI-ROV practice to filter out spoofed route announcements, but ISPs cannot use RPKI to filter BGP updates for which ROAs have not been created – so their filtering will only address this challenge to the extent entities like the Department of Energy (and other critical infrastructure) also embrace the need to register ROAs; and while there has been progress, more remains to be done. IP address owners are the only ones capable of registering ROAs for their network addresses – ISPs do not have authority to register ROAs for any addresses other than their own.

Moreover, even if all U.S. based entities create ROAs and ROV is broadly deployed in the U.S., if the prefix for an American entity is spoofed by a malicious actor in a foreign country, then it will still attract traffic and won't be filtered out unless ROV is well deployed in foreign networks.

If, however, other participants of the ecosystem were to follow American ISPs' lead in good internet routing hygiene, adopting the practices ISPs have already adopted, the National Cybersecurity Strategy's routing initiative would be highly successful.

	ISP Internet Routing Security Practices and Partnerships
1	Large U.S. operators are presently conducting RPKI Route Origin Validation (ROV) on routers used for interconnecting with other large operators.
2	U.S. operators work with (or will do so upon request) customers who own or operate their own IP address space or prefixes and request help in validating that those customer's Route Origin Authorizations (ROAs) are not misconfigured and are implemented accurately.
3	U.S. ISPs are continuing to efficiently and effectively implement ROAs to address space that they own based on a risk-based framework that prioritizes where ROAs will create the most benefit.
4	U.S. operators have participated in many efforts to address routing security. They will continue to support efforts to educate smaller ISPs and other network operators through lessons-learned sessions and other practical tips/assistance.
5	U.S. operators have led and participated in efforts at standards bodies such as the Internet Engineering Task Force (IETF) as well as industry best practice initiatives such as Mutually Agreed Norms for Routing Security (MANRS) to develop new solutions and best practices to enhance routing security. They will continue to participate in industry organizations and initiatives to help identify new technological solutions and best practices focused on internet routing security.
6	U.S. operators have participated in information exchange/periodic high side meetings with national security agencies about the latest routing security issues. U.S. operators will continue these efforts and will consider recommended actions from these meetings as part of their risk-based program to enhance routing security. They will strive to promulgate enhancements to their routing practices via existing information sharing channels (e.g., Comm-ISAC, CSCC, NANOG).