NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Workshop on Security for IPv6 Enabled Enterprises

The National Institute of Standards and Technology (NIST) announces a workshop on Security for Ipv6 Enabled Enterprise IT Systems. The workshop will be held on June 13, 2019 at the National Cybersecurity Center of Excellence (NCCoE), 9700 Great Seneca Highway, Rockville, Maryland.

Internet Protocol version 6 (IPv6) is the Internet's next-generation protocol, designed to replace the legacy IPv4 protocol that has been in use since 1983. Internet Protocol (IP) addresses are the global numeric identifiers necessary to uniquely identify entities that communicate over the Internet. The available free pool of IPv4 addresses was exhausted in 2015, and the demand for global IP addresses continues to grow exponentially as the number of users, devices and virtual entities connected to the Internet increases. In the last 5 years, IPv6 momentum in industry has dramatically increased, with large commercial IPv6 deployments in several industry sectors (e.g., data centers, cellular carriers, content providers) now driven by business goals of reducing cost, decreasing complexity, improving security and eliminating barriers to innovation in networked information systems.

While there has been significant IPv6 deployment progress in some use case scenarios, widescale adoption in general enterprise settings continues to lag. There are significant potential benefits to transitioning enterprise networks to IPv6, but questions remain about the viability of technologies and deployment guidance necessary to do so securely.

Call for Presentations

The purpose of this workshop is to identify perceived issues and challenges in secure IPv6 deployment in enterprises as planning input to a planned NCCoE demonstration project in this area. NIST will present its preliminary plans for this project and we solicit presentations from industry and other parties on their views of the challenges in secure IPv6 deployment in the enterprise, and/or enabling technologies and best practices to address perceived challenges. The agenda will be finalized on June 7, 2019. Applications to present should be sent to ipv6-transition@nist.gov no later than **May 30, 2019**.

Register today.

Questions about workshop participation should be sent to: ipv6-transition@nist.gov

A primary focus of the workshop and subsequent NCCoE demonstration project is to examine the extent to which current commercially available security technologies can support wide scale deployment and use of IPv6 in a range of enterprise use case scenarios. Initially the project will focus on dual-stack deployments and then in subsequent follow on efforts, focus on IPv6-only deployments. In both scenarios, the use of common IPv4-IPv6 transition mechanisms will be addressed. Example enterprise security technologies to be considered include:

- Identity and access management systems;
- Access control and policy enforcement systems, threat intelligence and reputation systems;
- Virtual private networks and remote access technologies;
- Firewalls and intrusion detection / protection systems, end-point security systems;
- Security incident and event management systems; and,

- Core network infrastructure systems (e.g., switching, routing, naming) and associated monitoring and management systems.

Enterprise IPv6 security technologies will be demonstrated in common usage scenarios. Example enterprise use case scenarios to be addressed include desktop to on premise service access; enterprise access to cloud-based services; and, remote access to enterprise services.

A second focus of the workshop and subsequent planned NCCoE project is to examine the state of existing standards, guidance and industry best practice documentation; to demonstrate the viability of implementing such specifications with commercially available products; and, to identify gaps in the knowledgebase that should be filled with additional guidance and specifications. The proof-of-concept demonstration project will exercise existing guidance from NIST and the Internet Engineering Task Force. It is anticipated that outcomes of the project will inform updates to the NIST guidelines and recommendations.

NIST explicitly solicits input from workshop participants on all aspects of the planned NCCoE demonstration project including the proposed scope, use cases and technologies to be considered, and sources of specifications and guidance. Once the project description in finalized NIST will solicit organizations to directly collaborate in the technical project and the development of its outputs.

Registration is Open
To register for this free workshop, please complete this short form by June 11, 2019. For our international visitors, registration is suggested no later than June 6, 2019, to allow for the registration process. Please download the file and fax the hard copy to (301-975-0321). Once the form has been faxed, email deborah.mowatt@nist.gov or keri.bray@nist.gov to confirm receipt.

DETAILS
Thursday, June 13, 2019
8:30 a.m. – 1:30 p.m.

The NCCoE
9700 Great Seneca Hwy
Rockville, MD 20850