National Cybersecurity Center of Excellence

Workshop on Security for IPv6 Enabled Enterprises

June 13, 2019
Emergency Procedures for NCCoE Visitors

Evacuation Emergencies

What is an Evacuation Emergency?
- Fires
- Explosions
- Earthquakes
- Indoor toxic material releases
- Indoor radiological and biological accidents
- Workplace violence

What Will Happen During an Evacuation Event?
- A building-wide alarm will sound
- Verbal instructions over the building’s public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest exit (Red Signs – Upper Right Map)
- If the Security Guard is close by and accessible, ask for further instruction
- Once outside the building, swiftly walk toward the designated meeting area near the posted sign stating “Evacuation Meeting Area” (Yellow Sign – Lower Right Map)

Shelter-In-Place (SIP) Emergencies

What is a Shelter-In-Place Emergency?
- Severe weather (hurricanes, tornadoses, etc.)
- Chemical, biological, or radiological contaminants released into the environment

What Will Happen During an Evacuation Event?
- A building-wide alarm will sound
- Verbal instructions over the building’s public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest SIP hallway or room (Yellow Signs – Upper Right Map)
- If the Security Guard is close by and accessible, ask for further instruction
Agenda

09:00 – 09:15  Welcome & Introduction to NCCoE
  Kevin Stine, NIST

09:15 – 09:30  Identifying and Removing Barrier to IPv6 Development
  Doug Montgomery, NIST

09:30 – 10:45  Enterprise Challenges
  • IPv6 Motivations and Obstacles
    Lee Howard, Retevia
  • IPv6 Adoption at a Large Enterprise
    John Burns, Wells Fargo

10:45 – 11:00  BREAK

11:00 – 12:00  Enterprise Challenges
  • Microsoft Corporate Network: Journey to IPv6
    Dawn Bedard, Microsoft
  • DoD IPv6 Context and Way Ahead
    Col. Keith Repik, DoD

12:00 – 12:15  BREAK

12:15 – 1:00  Breakout Sessions – Identifying Barriers to Deployment
  Participants will break into groups of 8-10

1:00 – 1:30  Readout, Discussion and Next Steps
National Institute of Standards and Technology
NIST is a bureau under the Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST runs a number of laboratories to assist in its mission.
Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs.
Engagement and Business Model

**DEFINE**
Define a scope of work with industry to solve a pressing cybersecurity challenge

**ASSEMBLE**
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

**BUILD**
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

**ADVOCATE**
Advocate adoption of the example implementation using the practice guide
Workshop on Security for IPv6 Enabled Enterprises
Goals and Objectives

• Motivations
  • IPv4 Address space has become a highly constrained resource in the Internet.
  • Demand for addresses continues to grow (e.g., mobile networks, IoT, cloud / virtualization)
  • USG has a strong commitment to IPv6 adoption.

• Challenges
  • Lag of adoption of IPv6 in the enterprise
  • Security concerns are often cited as barrier – maturity of products, lack of guidance, lack of documented deployment experience.

• Objectives
  • Identify challenges in secure IPv6 deployment in enterprises
  • Explore a plan for developing an NCCoE project to help accelerate the adoption on IPv6 across the enterprises
NCCoE Project Purpose and Scope

• **Purpose**
  - Demonstration project of secure IPv6 deployment in realistic scenarios using commercial products.
  - Two phases – IPv6-Everywhere and IPv6-Only.
  - Exercise and evaluate existing security guidance (e.g., NIST, IETF, others). Develop detailed NCCoE practice guides to augment.

• **Identify key IT components that will be impacted such as:**
  - 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
  - Core network infrastructure systems (e.g., switching, routing, naming) and associated monitoring and management systems

• **Identify key use cases to evaluate:**
  - Desktop to on premise service access, Enterprise access to cloud-based services, Remote access to enterprise services