Contribution ID: **304** Type: **Poster**

IPv6 Security

Tuesday, 11 October 2016 16:30 (15 minutes)

IPv4 network addresses are running out and the deployment of IPv6 networking in many places is now well underway. Following the work of the HEPiX IPv6 Working Group, a growing number of sites in the Worldwide Large Hadron Collider Computing Grid (WLCG) have deployed dual-stack IPv6/IPv4 services. The aim of this is to support the use of IPv6-only clients, i.e. worker nodes, virtual machines or containers.

The IPv6 networking protocols while they do contain features aimed at improving security also bring new challenges for operational IT security. We have spent many decades understanding and fixing security problems and concerns in the IPv4 world. Many WLCG IT support teams have only just started to consider IPv6 security and they are far from ready to follow best practice, the guidance for which is not easy to find. The lack of maturity of IPv6 implementations together with the increased complexity of the protocol standards and the fact that the new protocol stack allows for pretty much the same attack vectors as IPv4, raise many new issues for operational security teams.

The HEPiX IPv6 Working Group is producing guidance on best practices in this area. This paper will consider some of the security concerns for WLCG in an IPv6 world and present the HEPiX IPv6 working group guidance both for the system administrators who manage IT services on the WLCG distributed infrastructure and also for their related security and networking teams.

Secondary Keyword (Optional)

Network systems and solutions

Primary Keyword (Mandatory)

Security and policies

Tertiary Keyword (Optional)

Primary authors: KELSEY, Dave (STFC - Rutherford Appleton Lab. (GB)); PRELZ, Francesco (Università degli Studi e INFN Milano (IT))

Co-author: WARTEL, Romain (CERN)

Presenter: PRELZ, Francesco (Università degli Studi e INFN Milano (IT))

Session Classification: Posters A / Break

Track Classification: Track 8: Security, Policy and Outreach