IPv6 Security

M Babik[1], J Chudoba[2], A Dewhurst[3], T Finnern[4], T Froy[5], C Grigoras[1], K Hafeez[3], B Hoeft[6], D P Kelsey[3], F López Muñoz[7], E Martelli[1], R Nandakumar[3], K Ohrenberg[4], F Prelz[8], D Rand[9], A Sciabà[1], D Traynor[5], U Tigerstedt[10] and R Wartel[1]

[1] CERN, CH-1211 Genève 23, Switzerland
[2] Institute of Physics, Academy of Sciences of the Czech Republic Na Slovance 2 182 21 Prague 8, Czech Republic
[3] STFC Rutherford Appleton Laboratory, Harwell Campus, Didcot, Oxfordshire OX11 0QX, United Kingdom
[4] Deutsches Elektronen-Synchrotron, Notkestraße 85, D-22607 Hamburg, Germany
[5] Queen Mary University of London, Mile End Road, London E1 4NS, United Kingdom
[6] Karlsruher Institut für Technologie, Hermann-von-Helmholtz-Platz 1, D-76344 Eggenstein-Leopoldshafen, Germany
[7] Port d'Informació Científica, Campus UAB, Edifici D, E-08193 Bellaterra, Spain
[8] INFN, Sezione di Milano, via G. Celoria 16, I-20133 Milano, Italy
[9] Imperial College London, South Kensington Campus, London SW7 2AZ, United Kingdom
[10] CSC Tieteen Tietotekniikan Keskus Oy, P.O. Box 405, FI-02101 Espoo

E-mail: `david.kelsey@stfc.ac.uk, ipv6@hepix.org`

Abstract. 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.

1. Introduction

The much-heralded exhaustion of the IPv4 networking address is with us, etc. etc.

References

[1] http://hepix-ipv6.web.cern.ch

[2] All Internet Engineering Task Force Requests For Comments (RFC) documents are available from URLs such as http://www.ietf.org/rfc/rfcNNNN.txt where NNNN is the RFC number, for example http://www.ietf.org/rfc/rfc2460.txt

[3] See for instance http://www.google.com/ipv6/statistics.html. The 10% global connectivity threshold was crossed in January 2016.

[4] Hogg S, Vyncke E - IPv6 Security, Cisco Press 2009, ISBN-13: 978-1-58705-594-2