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. Lòpez 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]

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

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. We 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.

What does the adoption of IPv6 (*already* present and latent in most networks) bring to the IP operational security practices ?

What's new and significant ?

Should I worry, like, *now* ?

Checklist for Administrators

I. Ensure all security/network monitoring/logging are IPv6-capable
II. Filter IPv6 packets that enter and leave your network/system
III. Filter/disable IPv6-on-IPv4 tunnels
IV. Deploy RA-Guard or otherwise deal with Rogue RAs
V. Filter ICMPv6 messages wisely
VI. Allow special-purpose headers only if needed
VII. Make an addressing plan
VIII. Decide whether to use DHCPv6 or SLAAC+DynDNS
IX. Use synchronised IPv4/v6 access rules
X. Do not be tempted by transition technologies

More details in our paper...

Checklist for Developers

I. Code that replaces IPv4 transport with IPv6 is expected to behave as well and to be tested at least as well as existing code: plan for *extensive* testing
II. Make sure that the choice/ordering/preference of source and destination IP addresses follows what is administratively chosen and configured at the OS level
III. Existing IPv4 security measures should not be removed, worked around or simply forgotten when porting code for IPv6

More in our paper...

New IPv6 features

Many more ICMP message types!
➔Cannot filter all of them (MTU discovery has to work)
➔*Must* filter some of them
➔RFC4890 gives advice

New methods for auto-configuring addresses, routes, DNS
➔Good for the end-user
➔*Must* do something against rogue Router Advertisements (see RFC6104)

Not really a feature of IPv6 proper, but much of the network stack and application code is enticingly fresh!

Longer IP addresses
➔Hey, everyone knows *that*.
➔They may slow down brute force scans.
➔But no bad guy is that crude...

Transitional technologies (e.g. tunnels) have intrinsic vulnerabilities but don't need to be there forever...

Cannot fragment packets en-route
➔Minimum MTU: 1280
➔But you can still hurt yourself and send small fragments if you wish
➔Some good news, at least

Business as usual *

Broadcasts and Multicasts are still there, with a vengeance

Can still pollute Ethernet address discovery (ND instead of ARP)

Can still try forging and injecting packets into the local network

Can still run a rogue DHCP server

Can still use IP headers for out-of-band communications

Upper-layer protocols did not change!

*: As long as all network monitoring and administration tools are up-to-date and (therefore) aware of IPv6.

CHEP 2016 San Francisco – October 10-14

(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, Finland