Operational Security Considerations for IPv6 Networks

K. Chittimaneni, M. Kaeo, E. Vyncke

IETF 96, July 2016
Berlin, Germany
Updates for -09

- Refreshed the references, added new ones:
  - Draft-ietf-6man-hbh-header-handling
  - RFC 2993 (architectural implications of NAT)
  - RFC 6145 (stateless NAT64)
- Fixed some typos
- Acted upon most of the June reviews/comments on the mailing list.
  - Special thanks to Fred Baker, Markus deBrueen for extended review
  - Also to Erik Kline, Bob Sleigh
  - Still have to work on Lee Howard (16th of July but on -08) and the many other comments (yet to be processed)
Section 2.1, Addressing Architecture

Although initially IPv6 was thought to make renumbering easy, in practice, it may be extremely difficult to renumber \textit{without a good IP Addresses Management (IPAM) system.}

However, one aspect to keep in mind is who has \textit{administrative} ownership of the address space and who is \textit{technically} responsible if/when \textit{Law Enforcement Agency may need} there is a need to enforce restrictions on routability of the space due to malicious criminal activity.
Diffs in -09

● Section 2.1.2 Use of ULAs
  ● *It is also important to note that the IETF does not recommend the use of ULA and NPTv6.*

● Looking for the actual reference ;-) RFC 6296 ? RFC 4864 ?
Diffs in -09

- Section 2.1.4 Privacy addresses
  - ... it is advised in scenarios where user attribution is important to rely on a layer-2 authentication mechanism such as IEEE 802.1X [IEEE-802.1X] with the appropriate RADIUS accounting (Section 2.6.1.6) or to disable SLAAC and rely only on DHCPv6. ...
Diffs in -09

- Section 2.6.1.5 Stateful DHCP leases
  - The mapping between data-link layer address and the IPv6 address can be secured by using switches implementing the SAVI [RFC7513] algorithms. Of course, this also requires that data-link layer address is protected by using layer-2 mechanism such as [IEEE-802.1X].
ToDo in -10

- Document started in early 2012...
- Security is a moving target ;-) 
- Acting on all comments...
ToDo in -10

- Add section on extension headers
  - Reference draft-ietf-opsec-ipv6-eh-filtering (if work is still done), RFC 7045
  - White list approach with difference between transit/Internet routers and enterprise/edge devices
ToDo in -10 [Brian Carpenter]

- Remove references to 'dead' I-D
  - NDP throttler & co
- RFC 6877 (XLAT 464) ?
  - Unsure as for the network operation it is NAT64
- Add a privacy section
  - Unsure as it is not related to operation
ToDo in -10 [Lee Howard]

- "This is listed as Informational, but in some places is recommending best practice"
- "the tone suggesting IPv6 is new is misplaced"
  - Unsure, it is still new for people deploying it though (the audience of this I-D).
  - => will review the wording
- Proposal for the ULA + NPTv6 section ;-)
ToDo in -10 [Lee, cont.]

- Many English corrections to Frenglish ;-) 
- Section 2.3.5 (3GPP) should get some rewording (other reviewer had the same comment)
Q&A

THANK YOU!