Operational Security Considerations for IPv6 Networks

draft-ietf-opsec-v6 (-17)

Eric Vyncke
Kiran Kumar Chittimaneni
Merike Kaeo
Enno Rey

IETF-105 V6OPS WG
Objectives

“This document analyzes the operational security issues in several places of a network (enterprises, service providers and residential users) and proposes technical and procedural mitigations techniques. Some very specific places of a network such as the Internet of Things are not discussed in this document.”

It’s about providing security-oriented input to operations. We notice that, within the operators’ community, there’s quite some interest in such input coming from the IETF (similar to RFC 7381).
Overview

• This has been a OPSEC WG doc since Sep 2012
  – Quite a vast domain... And moving target with new relevant documents popping up

• Informational document, 50 pages and 116 informative references
  – This memo summarizes and refers to other documents

• The doc provides Operational Security Considerations for IPv6 Networks

• The goal is to provide operators with a reference doc that helps operators secure IPv6 networks
Structure & Main Elements

- Generic Security Considerations (50% of the document)
- Enterprise Specific Sec Considerations
- Service Providers Specific Considerations (*BGP, transition mechanisms, LI*)
- Residential Users Security Considerations (*mainly refers to RFC 7084 / 6092*)
Generic Security Considerations

- Addressing Architecture (ULA, DHCPv6, SLAAC, privacy considerations, ...)
- Extension Headers (order, Hbh, fragmentation, ...)
- Link-Layer Security (NDP rate limiting & filtering, securing DHCP, 3GPP, ...)
- Control Plane Security (control & management protocols, packet exceptions)
- Routing Security (authentication of peers, routing updates, route filtering, ...)
- Transition/Coexistence Technologies (dual-stack, encapsulation, translation)
- General Device Hardening
Where the Draft Stands Today

- Obviously some of the sections have sparked heavy discussions on the mailing list and in meetings
  - PI vs PA, ULAs, NPTv6, ...
  - To solve the discussions => either removed text or pointed to other documents

- We think that a reasonable balance of discussing options while at the same time providing some guidance has been reached in the interim.
  - Referencing other documents further increases efficiency.
FYI Acknowledgements

“The authors would like to thank the following people for their useful comments: Mikael Abrahamsson, Fred Baker, Mustafa Suha Botsali, Brian Carpenter, Tim Chown, Lorenzo Colitti, Markus de Bruen, Tobias Fiebig, Fernando Gont, Jeffry Handal, Lee Howard, Panos Kampanakis, Erik Kline, Jouni Korhonen, Mark Lentczner, Jordi Palet, Bob Sleigh, Tarko Tikan, Ole Troan, Bernie Volz (by alphabetical order).”
Next Steps

• Authors have requested OPSEC WG Last Call
• We’d like to ask you (V6OPS) for review and/or participation in *opsec WGLC*.
  – The document serves a purpose very much aligned with the goals of *v6ops*. We’re in the same boat.

• We, as authors, thank you in advance for your efforts and contributions!

• The authors feel that there is tremendous value in having a doc that provides operations with important security considerations for IPv6 networks
Thanks for Your Time

Questions?