

OPSEC

(Operational Security Capabilities for IP Network
Infrastructure)

Eric Vyncke
Gunter Van de Velde



IETF 95, 5 April 2016
Buenos Aires, Argentina

Administrivia

- Chairs:
 - Eric Vyncke
 - Gunter Van de Velde
- Jabber Scribe:
 - opsec@ietf.jabber.org
- Minutes:
 - <http://tools.ietf.org/wg/opsec/minutes>
- Note Well.
- Blue Sheets.
- Agenda Bashing.



Note Well

- This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.
- The brief summary:
 - By participating with the IETF, you agree to follow IETF processes. If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact. You understand that meetings might be recorded, broadcast, and publicly archived.
- For further information, talk to a chair, ask an Area Director, or review the following:
 - BCP 9 (on the Internet Standards Process)
 - BCP 25 (on the Working Group processes)
 - BCP 78 (on the IETF Trust)
 - BCP 79 (on Intellectual Property Rights in the IETF)



Blue Sheets

- Please fill these in
- The secretariat makes grumpy-face if we don't.

Administravia

- IETF-93/94 – no meeting
- New OPSEC Co-chair
 - Many thanks to Kiran Kumar Chittimaneni
 - Welcome to Eric Vyncke
- RFC's Published
 - RFC7610/BCP199: DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers
 - RFC7707: Network Reconnaissance in IPv6 Networks (obsoletes RFC5157)
- IESG Processing
 - --
- Other
 - --

State of the Union

- Observation: OPSEC email list activity rather light
- Observation: Most drafts are expired
 - But new work presented at this meeting
 - draft-georgescu-opsec-ipv6-trans-tech-threat-model
 - draft-winter-opsec-netconfig-metadata
 - Selected existing work revitalized

State of the Union

- Are OPSEC Goals and Milestones achieved ?
 - What is next?

OPSEC Goal

The OPSEC WG will document operational issues and best current practices with regard to network security. In particular, the working group will clarify the rationale of supporting current operational practice, addressing gaps in currently understood best practices and clarifying liabilities inherent in security practices where they exist.

Agenda – Part 1

- Administrivia
 - Chairs, 10
- SACM Vulnerability Assessment Scenario
 - draft-coffin-sacm-vuln-scenario, by Daniel Haynes
 - Time: 20 min
- A Holistic Threat Analysis of IPv6 Transition Technologies
 - draft-georgescu-opsec-ipv6-trans-tech-threat-model, by Marius Georgescu (remote)
 - Time: 20 min
- Operational Security Considerations for IPv6 Networks
 - draft-ietf-opsec-v6, by Eric Vyncke
 - Time: 10 min



Agenda – Part 2

- A Configuration File Format for Network Services on Leaf Devices
 - draft-winter-opsec-netconfig-metadata-00, by Stefan Winter
 - Time: 20 min
- MLD Security
 - draft-vyncke-pim-mld-security, by Enno Rey
 - Time: 15 min
- Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages
 - draft-gont-opsec-icmp-ingress-filtering, Fernando Gont
 - Time: 15 min
- On Firewalls in Network Security
 - draft-gont-opsawg-firewalls-analysis, by Fernando Gont
 - Time: 15 min
- Requirements for IPv6 Enterprise Firewalls
 - draft-gont-opsec-ipv6-firewall-reqs-03, by Fernando Gont
 - Time: 15 min



THANK YOU!