# OPSEC WG

Joel Jaeggli
and
Joel Abley

# Agenda

- (5 minutes) Rechartering status.
- (5 minutes) Document status.
- (10 minutes) Briefly discuss and collect feedback for Fernando on:
  - `draft-gont-opsec-icmp-filtering-00`
- (10 minutes) SAVI working group overview
- (15 minutes) whether that is worth pursuing and if so, what would be the direction for that effort.
  - `Draft-savola-rtgwg-backbone-attacks-03`

# Rechartering Status.

- Fatigue on existing milestones.
- New working group chairs 12/12 2007.
- Proposed charter update discussion 12/18-1/10/2008
  - Well received
  - Minor changes
- Last called 07/09/2008
- Forwarded to the IESG on 07/21

# Charter

Goals:
The OPSEC WG will document best current practices with regard to network security. In particular an effort will be made to clarify the rational supporting current operational practice, address gaps in currently understood best practices for forwarding, control plane, and management plane security and make clear the liabilities inherent in security practices where they exist.

Scope:
The scope of the OPSEC WG is intended to include the protection and secure operation of the forwarding, control and management planes.

Documentation of best common practices, revision of existing operational security practices documents and proposals for new approaches to operational challenges are in scope.

# Charter

Method:
It is expected that the work product of the working group will fall into the category of best current practices documents. Taxonomy or problem statement documents may provide a basis for best current practices documents.

Best Current Practices Document
For each topic addressed, a document will be produced that attempts to capture current practices related to secure operation. This will be primarily based on operational experience. Each entry will list:

* threats addressed,
* current practices for addressing the threat,
* protocols, tools and technologies extant at the time of writing that are used to address the threat,
* the possibility that a solution does not exist within existing tools or technologies.

# Charter

Taxonomy and Problem Statement Documents
A document which attempts to describe the scope of particular operational security challenge or problem space without necessarily coming to a conclusion or proposing a solution. Such a document might be a precursor to a  best common practices document.

While the principal input of the Working Group are operational experience and needs, the output should be directed both to provide guidance to the operators community as well as to Working Groups that develop protocols or the community of protocol developers at large, as well as to the implementers of these protocols.

Non-Goals:
The Operations security working group is not the place to do new protocols or requirements documents.

New protocol development or requirements work should be addressed in a working group chartered in the appropriate area or as individual submissions. The OPSEC WG may take on documents related to the practices of using such work.

# Sticking Point

- Milestones are a bit thin.
- Want to keep the working group around to bring problems from the network operations space into.
- Alternative would probably be to fold this into OPSAWG

# Status of Existing Documents

*Working Group Documents:*

| Draft name | Rev. | Dated | Status | Comments, Issues |
|---|---|---|---|---|
| ***Active:*** | | | | |
| draft-ietf-opsec-efforts | -08 | 2008-06-06 | Active | |
| ***Recently Expired:*** | | | | |
| draft-ietf-opsec-logging-caps | -04 | 2007-08-24 | Expired | |
| ***Published:*** | | | | |
| **Draft name** | **Rev.** | **Dated** | **Status** | **Obsoleted by/*(Updated by)*** |
| draft-ietf-opsec-current-practices | -07 | 2006-08-30 | RFC 4778 | |
| ***Expired:*** | | | | |
| draft-ietf-opsec-filter-caps | -09 | 2007-07-13 | Expired | |
| draft-ietf-opsec-framework | -05 | 2007-04-03 | Expired | |
| draft-ietf-opsec-infrastructure-security | -01 | 2007-04-10 | Expired | |
| draft-ietf-opsec-misc-cap | -00 | 2006-02-22 | Expired | |
| draft-ietf-opsec-nmasc | -00 | 2006-03-01 | Expired | |
| draft-ietf-opsec-routing-capabilities | -03 | 2007-06-15 | Expired | |

---

*Related Active Documents (not working group documents):*

*(To see all opsec-related documents, go to opsec-related drafts in the ID-archive)*

| | | |
|---|---|---|
| draft-gont-opsec-icmp-filtering | -00 | 2008-03-30 |
| draft-jones-opsec-framework | -01 | 2004-10-21 |

Draft dependency graphs

# Looking forward to new work.

- Not yet submitted
  - `draft-kumari-blackhole-urpf-00.txt`
    - Expands on rfc 3882
  - `draft-kumari-blackhole-community-00.txt`
    - Asks iana for a standard blackhole community attribute

# draft-gont-opsec-icmp-filtering-00

- Got a fair amount of commentary on the list, most of it positive.
- Believe that as of of 05/06 based on mailing list discussion we have consensus to adopt it as a working group document.

# SAVI

- Newly chartered working group.
- I personally am very interested in the operational implications of of SAVI-like validation schemes.
- The application of SAVI to non-end-system hosts.
- Invited SAVI folks to present to this group as a result.

# Draft-savola-rtgwg-backbone-attacks-03

- Pekka wanted this discuss this draft.
- Previously in the routing area working group.
- Given the broad security implications it should be relevant under our new charter.