Operational Security Capabilities and Practices for IP Network Infrastructure

Last Modified: 2004-**08-03**

Chairs:

<tbd>

Operations and Management Area Director(s):

Bert Wijnen <bwijnen@lucent.com>
David Kessens <david.kessens@nokia.com>

Operations and Management Area Advisor:

David Kessens <david.kessens@nokia.com>

~~**Security Area Director(s):**~~

~~**Russell Housley <housley@vigilsec.com>**~~
~~**Steven Bellovin <smb@research.att.com>**~~

Security Area Advisor:

Steven Bellovin <smb@research.att.com>

Mailing Lists:

General Discussion: opsec@ops.ietf.org
To Subscribe: opsec-request@ops.ietf.org
In Body: subscribe
Archive: http://ops.ietf.org/lists/opsec/

Description of Working Group:

Problem Statement

Security issues in operational networks are complex, and not universally well understood. Improving the security awareness and education of network operators and vendors is important in order to improve the operational security of the Internet and other network infrastructures. Much of this knowledge exists in the minds of network operators.

Goals

The goal of the Operational Security Working Group is to codify knowledge about capabilities and best current practices that may be used to deploy and operate secure managed network elements providing transit services at the data link and IP layers.

Scope

The working group will produce requirements appropriate for **devices used in**:

* Internet Service Provider (ISP) Networks
* Enterprise Networks

The following areas are excluded from the charter at this time:

* Wireless devices
* **Small Office Home Office (**SOHO**)** devices
* Security devices (firewalls, **Intrusion Detection Systems**, Authentication Servers)
* Hosts

Methods

A framework document will be produced describing the scope, format, intended use and sequence of future documents. A series of **Best Current Practice (**BCP**)** documents will be produced covering various areas of security management functionality. Profiles documents will be produced, citing the BCPs, which list the requirements relevant to different operating environments. Profiles might list different requirements for devices in different roles: core, edge, peering, aggregation, access, etc.

http://www.ietf.org/internet-drafts/draft-jones-opsec-06.txt will be used as a jumping off point.

Much of the operational security knowledge that needs to be codified resides with operators. In order to access their knowledge and reach the working group goal, informal BoFs will be held at relevant operator fora.

Goals and Milestones:

<Milestones may be re-worked. Names of potential authors will be removed from the charter.>

~~**Aug 04 First Working Group Meeting @ IETF 60 in San Diego**~~

Sep 04 First draft of Framework Document as Internet Draft

[Callon, Kaeo, Jones]

Sep 04 First draft of Standards Survey Document as Internet Draft [Lonvick,Spak]

Mar 05 Submit Framework to IESG (info)

Mar 05 Submit Standards Survey to IESG (info)

<First drafts of remaining documents will be added to milestones.>

Aug 05 Submit In-Band management requirements to IESG (BCP) [Budd]

Aug 05 Submit Out-of-Band management requirements to IESG (BCP) [Budd]

Aug 05 Submit Packet Filtering requirements to IESG (BCP) [Callon,Budd]

Aug 05 Submit Event Logging Requirements document to IESG (BCP) [Kaeo]

Nov 05 Submit Configuration and Management Interface Requirements to IESG (BCP) [Kaeo]

Nov 05 Submit **Authentication, Accounting, Authorization (**AAA**)** requirements document to IESG (BCP) [Budd]

Nov 05 Submit Documentation and Assurance requirements document to IESG (BCP)

Nov 05 Submit Miscellaneous requirements document to IESG (BCP)

Mar 06 Submit ISP Operational Security Requirements Profile (informational)

Mar 06 Submit Large Enterprise Operational Security Requirements Profile (informational)

Mar 06 Submit OPSEC Deliberation Summary document

Internet-Drafts (to be written):

See schedule above.

Request For Comments:

None.