

IETF 77 opsec WG

Joel Jaeggli – Nokia
Joe Abley - ICANN

Agenda

- Achievements since IETF 76
- Document status
- New work
- Any additional agenda items

Achievements

- Security Assessment of the Internet Protocol version 4
 - draft-ietf-opsec-ip-security
 - WGLC in December
 - Comments favorable
 - Feedback from Alfred Hoenes is being incorporated into draft prior to IESG submission.
- Issues with existing Cryptographic Protection Methods for Routing Protocols
 - draft-ietf-opsec-routing-protocols-crypto-issues
 - WGLC in January
 - Submitted to AD
 - Now in expert review

Achievements continued

- Cryptographic Authentication Algorithm Implementation Best Practices for Routing Protocols
 - Draft-ietf-opsec-igp-crypto-requirements
 - Accepted as a WG document now added to the stable.
 - Next steps prior to last-call?

Document status

<u>Draft name</u>	Rev.	<u>Dated</u>	<u>Status</u>	Comments, Issues
<i>Active:</i>				
draft-ietf-opsec-efforts	-11	2009-11-15	Active	
draft-ietf-opsec-icmp-filtering	-01	2009-10-26	Active	
draft-ietf-opsec-igp-crypto-requirements	-00	2010-01-29	Active	
draft-ietf-opsec-ip-security	-02	2010-02-20	Active	

IESG Processing:

draft-ietf-opsec-routing-protocols-crypto-issues	-03	2010-01-21	Expert Review	
------------------------------------------------------------------	---------------------	------------	-------------------------------	--

Published:

Draft name	Rev.	Dated	Status	Obsoleted by/(Updated by)
draft-ietf-opsec-blackhole-urpf	-04	2009-06-05	RFC 5635	
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-logging-caps	-04	2007-08-24	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	

Document Status Continued

- Draft-ietf-opsec-icmp-filtering
 - Updated, still incomplete, authors hope to finish shortly
 - Will probably solicit reviews based on finished docs

Work with other groups

- draft-ietf-tcpm-tcp-security-01
 - Socialized on opsec.
 - discussion is continuing in TCPM
- KARP
 - draft-lebovitz-karp-roadmap
 - draft-ietf-karp-framework
 - draft-ietf-karp-threats-reqs
 - draft-ietf-karp-design-guide

New Work

- IP Options Filtering Recommendations
 - Draft-gont-opsec-ip-options-filtering-00
 - Steven Fount and Fernando Gont
 - In the style of ICMP filtering, for better or worse.

Example

4.	Advice on handling of specific IP Options	6
4.1.	End of Option List (Type = 0)	6
4.1.1.	Uses	6
4.1.2.	Option specification	7
4.1.3.	Threats	7
4.1.4.	Operational/interoperability impact if blocked	7
4.1.5.	Advice	7
4.2.	No Operation (Type = 1)	7
4.2.1.	Uses	7
4.2.2.	Option specification	7
4.2.3.	Threats	7
4.2.4.	Operational/interoperability impact if blocked	7
4.2.5.	Advice	7
4.3.	Loose Source and Record Route (LSRR) (Type = 131)	7
4.3.1.	Uses	8
4.3.2.	Option specification	8
4.3.3.	Threats	8
4.3.4.	Operational/interoperability impact if blocked	9
4.3.5.	Advice	9
4.4.	Strict Source and Record Route (SSRR) (Type = 137)	9
4.4.1.	Uses	9
4.4.2.	Option specification	9
4.4.3.	Threats	9
4.4.4.	Operational/interoperability impact if blocked	9
4.4.5.	Advice	9
4.5.	Record Route (Type = 7)	10
4.5.1.	Uses	10
4.5.2.	Option specification	10
4.5.3.	Threats	10
4.5.4.	Operational/interoperability impact if blocked	10
4.5.5.	Advice	10

New Work

- Protecting The Router Control Plane
 - draft-dugal-opsec-protect-control-plane-02
 - David Dugal
 - Carlos Pignataro
 - Rodney Dunn

DONE
Thanks!