OPSEC - IETF 76

Joel Jaeggli

Agenda

1) WG status - WG Chair
2) Nanog ISP security BOF report - WG Chair
3) Revised, draft-ietf-opsec-ip-security - Fernando Gont
4) Revised, draft-ietf-opsec-icmp-filtering - Fernando Gont
5) Revised, draft-ietf-opsec-routing-protocols-crypto-issues - WG Chair
6) Others?

WG status

- Since last meeting:
  - Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF) – informational, RFC 5645
- Revised:
  - Draft-ietf-opsec-icmp-filtering-01 2009-10-26
  - Draft-ietf-opsec-ip-security-01 2009-08-20
  - draft-ietf-opsec-routing-protocols-crypto-issues-01   2009-10-20

WG Activities and Outreach

- Philadelphia and Dearborn NANOGs
- KARP BOF
- Draft-bhatia-manral-igp-crypto-requirements-03
  - Rehabilitate
  - Will bring to the WG after the meeting
- Requests from Ron to network operators:
  - 11/04/09 - “Best Common Practices document on ISP Port filtering”
  - 11/04/09 - “I would love to see the IETF OPSEC WG publish a document on the pros and cons of filtering optioned packets.”

Question posed by the Outreach experience?

- Are Industry BCP, regulatory, or, compliance goals working at cross purposes to the health and security of networks?
  - Consider two examples:
  - Stateful inspection
    - Clearly have some liability at any sort of scale
    - http://www.nanog.org/meetings/nanog47/presentations/Monday/Dobbins_ISPSecTrac_N47_Mond.pdf
  - (raised on opsec) SSL inpection
    - When done in the network it typically requires some form of spoofing
    - Like nats reducing the expectations around end-point ideintifiers this plays with the value of SSL certificates and the DNS
- Lack of visibility on the routing table doesn't imply lack of reachability, due to widespread use of default.
  - http://www.potaroo.net/iepg/2009-07-iepg75/090726.iepg-default.pdf