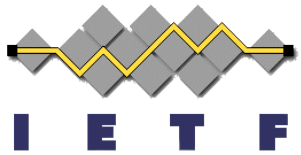
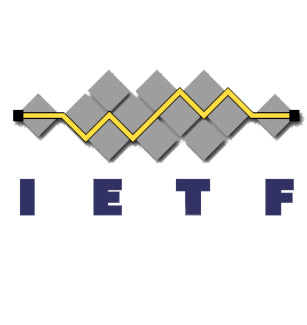
OSPF WG Security Gap Analysis and Response – IETF 86

Acee Lindem, Ericsson

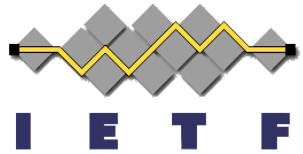


RFC 6863 Requirements



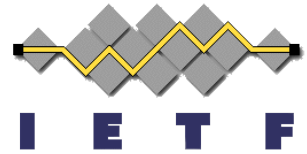
- Simple Secure Pre-Shared Keys (PFKs)
- Non-disruptive Key Rollover
- Mapping to Crypto Key Table Draft
- Stronger Security Algorithms and Algorithm Agility
- Replay Protection
  - Intra-connection
  - Inter-connection (including cross-protocol)
- Secure Neighbor Identification
- Packet Prioritization – OSPF Hello and Ack Packets may be given higher internal queuing and/or QoS than other OSPF packets
- Wide adoption and deployment

OSPF WG General Actions



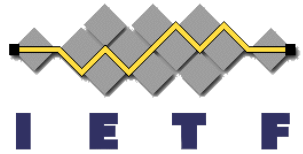
- Generally follow recommendations in RFC 6863.
- Develop a protocol specific (non-IPsec) solution for OSPFv2 meeting all the stated requirements
- Adapt the OSPFv2 solution to OSPFv3 as was done for RFC 6506

OSPF WG Specific Actions 1/2



- Satisfy all requirements for OSPFv2 with draft-ietf-ospf-security-extension-manual-keying-04 [OSPF
- Simple PSKs - RFC 2328
- Key Rollover – RFC 2328 and Crypto Key Table Draft
- Mapping to Crypto Key Table – [OSPF-MANKEY]
- Strong Algorithms and Algorithm Agility – RFC 5709
- Limited Replay Protection – RFC 2328
- Complete Replay Protection – [OSPF-MANKEY]
- Secure Neighbor Identification – RFC 5709
- OSPF Packet Prioritization – [OSPF-MANKEY]
- Wide scale adoption and deployment – [OSPF-MANKEY] Simple Solution meeting requirements.

OSPF WG Specific Actions 2/2



- Additional things to check with draft-ietf-ospf-security-extension-manual-keying-04 [OSPF-MANKEY]
  - Whether the RFC 6506 cross protocol attack protection is sufficient to satisfy the KARP Ops Model section 4.1 requirements.
  - Add cross-protocol protection to [OSPF-MANKEY] in the general sense.
- OSPFv3 specific considerations
  - OSPFv3 always identifies neighbors by Router-ID. However, source address should still be protected.
  - Others – need further analysis