Security Extension for OSPFv2 Using Manual Key Management

Manav Bhatia, Alcatel Lucent
Sam Hartman, Painless Security
Dacheng Zhang, Huawei Technologies
Acee Lindem, Ericsson

Draft Overview

- Defines new OSPFv2 AuthType for backward compatibility – Value of 3 suggested to IANA.
- Extends OSPFv2 sequence number from 32 bits to 64 bits and partitions the sequence number space.
- Defines keys selection rules with respect to draft-ietf-karp-crypto-key-table-00.txt.
- Protects IP source address with cryptographic hash.

Sequence Number Extension (1/3)

- Current sequence number weaknesses
  - Monotonically increasing
  - Only 32 bits – no provision for router restart
- New AuthType Sequence Number
  - Strictly increasing
  - 64 bits – 32 bits of boot count and 32 bits of sequence number
  - Moved out of OSPFv2 header auth data

Sequence Number Extension (2/3)

- Boot Count
  - Maintained in non-volatile storage for the life of the deployed router.
  - Incremented each time OSPF router loses its state.
  - Can also be incremented if low order sequence number wraps
- Sequence Number is incremented for every OSPFv2 packet sent

Sequence Number Extension (3/3)

- Receiver drops packet if received packet’s sequence number is not greater than previously received OSPF packet of same type – handles prioritization of hellos and acks.
- 64 bit sequence number follows OSPF packet but before authentication data
  - Doesn’t fit in OSPFv2 header
  - Not in OSPFv2 length
  - Included in IP packet length

Key Selection Rules Mapping Key Database

- Mapping to Database of Long-Lived Symmetric Cryptographic Keys <draft-ietf-karp-crypto-key-table-01.txt>
- Key Mapping for Unicast transmission
  - Currently problem with virtual links
- Key Mapping for Multicast transmission
- Key Mapping for Reception
- Discussion on usefulness of this section or normative reference to key database draft.

IP Source Address Protection

- Currently unprotected – Source IP address used by OSPFv2 for OSPF router identification on broadcast and NBMA networks
- IP Source Address replaces Apad in cryptographic authentication as described in RFC 5709, section 3.3.
- Apad is a hexadecimal constant value 0x878FE1F3 repeated (L/4) times, where L is the length of the hash in bytes.

Next Steps

- Revision Forthcoming
- Determine if Key Selection useful in the context of this draft
- Review and discussion on the OSPF list

Review of Proposed Changes

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Version #  |     Type    |        Packet length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Router ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Area ID                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Checksum             |            AuType (3)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               0               | Auth Data Len |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Key ID                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                   OSPF Protocol Packet                        |
~                                                               ~
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Sequence Number (Boot Count)                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Sequence Number (Strictly Increasing Packet Counter)      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                    Authentication Data                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```