KARP: OSPF Analysis

Sam Hartman
Dacheng Zhang

IETF 78
July 27, 2010

Goals

- Discuss whether draft-hartman-ospf-analysis is on track for the sorts of issues design teams should cover in their first deliverable.
- Discuss issues design teams may run into with OSPF as an example.

Prior Work

- Draft-ietf-rpsec-ospf-vuln
- Draft-ietf-opsec-routing-protocols-crypto-issues
- RFC 4593

Draft Outline

- Current state
  - OSPFv2
  - OSPFv3
- Replay analysis, Packet prioritization, IP header
- Security requirements
- Gap analysis

Security Requirements

- Integrity protection with cryptographic MAC
- Key rollover support
- Replay protection sufficient to avoid service disruptions

OSPFv2 before Analysis

- Strong MACs
- Good protocol support for key rollover
- Replay protection
- What more could you want?

Not so Easy

- Replay protection leads to DOS
- IP header not covered by integrity
- Packet prioritization difficulty

Analyzing Replay

- Three sequence numbers:
  - Cryptographic authentication
  - Database description
  - LSA level
- Multiple ways to break an adjacency
- Interaction with IP header for source selection
- Cross-session replays

Replay Diagram

T0: A -> DDP(Outer Seq 1, DD Seq 1) -> B

T1: A <- DDP(Outer Seq 500, DD Seq 1) <- B

T2: A -> DDP(Outer Seq 1, DD Seq 2) -> B

T3: Attacker-> DDP(Outer Seq 1, DD Seq 1) -> B

- Time points T1 and T3 are within the same second
- At T3, an attack can reply the packet A sent to B at T0 to break the synchronization already generated between A and B