OSPF Analysis

Sam Hartman
Dacheng Zhang Painless Security, LLC

IETF 80
April 1, 2011

Scope of Draft

- Design guide section 4.1 requires an analysis of each protocol
- Identify current state with reference to requirements
- Gap analysis
- Recommendations
- Work plan

Interesting Requirements

Some requirements from `threats-reqs` stand out for OSPF:

- ➜ Related key attacks: secure usage of preshared keys
- ➜ Inter and intra-connection replay
- ➜ Support for packet prioritization
- ➜ Secure identification of neighbors

Approach to Current State

- Describe OSPF as a routing protocol to security community
- Show how OSPF fails to meet goals proposed for routing security
- Please review; responses needed both from routing and security community
- Did we get it right? Does it make sense?

Gaps to Fix

- Replay of packets provides DOS opportunity
- Significant on LAN and wireless deployments; less significant on SP links
- OSPF does not authenticate source address; uses source address to identify neighbor entry sometimes; DOS opportunity
- Use of IPsec for OSPFv3 is problematic for deployment of OSPFv3 authentication

Gaps to Fix (2)

- The specification of OSPFv2 security does not make it clear how to prioritize some packets; protocol changes not required
- Using the same key in different cryptographic contexts may create problems; OSPF has no key derivation function
- Security depends on how the key is used elsewhere in a deployment, so very hard to evaluate
- If we make changes to OSPF authentication, we should fix this.

Proposed Work

- Fix source address authentication
- Use similar mechanism for OSPFv2 and OSPFv3 security
- Solve the replay problem
- Document packet prioritization
- Possibly fix related key issue

Replay Work

- ➜ Two proposals for handling replay will be discussed later in the meeting
- ➜ Draft only discusses the challenge/response solution.
- ➜ The other (extended sequence space) solution is probably more preferred
- ➜ Desire to update the draft to reflect this.
- ➜ Confirm the security properties of this solution