OSPF Authentication

Randall Atkinson
(Presented by Steven Blake)

IETF OSPF WG

November 2008

Long Long Ago

- Originally, OSPF only had clear-text authentication
  - a simple password, highly vulnerable to passive attacks
  - RFC-1704 discusses passive attacks in more detail
- In mid-1990s, US DoD wanted to eliminate use of clear-text authentication.
  - Murphy developed OSPF with Digital Signatures (RFC-2154), which is still the strongest approach.
  - Atkinson+Baker developed OSPF Keyed-MD5 (RFC-2178)
- Commercial router vendors shipped Keyed-MD5
- Some users, mostly US DoD, deployed Keyed-MD5

Keyed-MD5 for OSPF

- OSPF Auth Data = MD5(OSPF Packet, Key, Trailer)
- MD5 was commonly used in IETF authentication protocols at that time (e.g. SNMP, RIPv2, IPsec)

About MD5

- The key property of MD5 in this use is that it is non-invertible. So knowing the MD5 output does not let one learn the value of the Key that was used.
- Concerns about MD5 as a compression function date back at least to a paper by Hans Dobbertin in 1996.
- However, as of now, no published attack exists on MD5 -- when used in the mode on previous page.
  - So MD5 (as used above) has not been “broken”.
- Many users are still deploying OSPF with clear-text passwords. They believe this is sufficient for them.

More Recently

- US DoD policy says that to only use USG algorithms.
- SHA-2 is a USG algorithm; MD5 is not.
- So US DoD would like to have an open specification for routing protocol authentication using SHA-2.
- So far, only governmental users seem to have any interest in this.
- Commercial users seem quite happy with either Keyed-MD5 or clear-text passwords.

Current Proposed Mode

- There is a current OSPF I-D proposing to add SHA-2 as an optional authentication method.
- OSPF Auth Data = SHA-2 (Key xor OPAD, SHA-2(Key XOR IPAD, OSPF Packet))
- Constants:
  - B = byte length of block size of SHA-2.
  - IPAD = 0x36 repeated B times
  - OPAD = 0x5c repeated B times.

Alternative Mode

- 1) Put APAD into OSPF Authentication Data field of OSPF packet.
- 2) OSPF Auth Data = SHA-2(Key XOR OPAD, SHA-2(Key XOR IPAD, OSPF Packet))
- Constants:
  - B = byte length of block size of SHA-2.
  - L = length of hash output in bytes
  - IPAD = 0x36 repeated B times
  - OPAD = 0x5c repeated B times.
  - APAD = 0x878FE1F3 repeated L times

Why the Alternative

- This is already standard for RIPv2 (RFC-4822)
  - Credit: Maths are from Matt Fanto, who was then at NIST
- Also adopted by IETF IS-IS WG for IS-IS with SHA-2
- No good reason for OSPF WG to do something different than IETF has adopted for RIPv2 or IS-IS, since the threat model is identical for all 3 IGPs.
- US DoD has asked for this mode instead of the one currently in the OSPF SHA-2 I-D
  - US DoD are the only known customer for this !

Proposal

OSPF WG should adopt the same cryptographic mode for SHA-2 authentication that has already been standardised for RIPv2 SHA-2 and adopted by the IS-IS WG for IS-IS SHA-2.

Thank You