An Extension of HIP Base Exchange to Support Identity Privacy

draft-zhang-hip-privacy-protection-00

Dacheng Zhang
<zhangdacheng@huawei.com>
Miika Komu
<miika@iki.fi>

Motivation

- HIP leaks identity-related information even though ESP protects the confidentiality of the data-plane
- In the current version of base exchange (BEX), the identities (HITs and HIs) of communicating partners are transported in plain text
- An active or passive attacker can eavesdrop a base exchange and track the identities and movement of communicating end-hosts
- As a consequence, privacy is hindered because the connectivity of a host can be traced securely
- Anonymity vs. identity protection

Solutions for Identity Privacy

- Ephemeral identities
  - Thrown away when used once
  - More overhead to generate new keys
  - Anonymous authentication
- Encrypted certificates and public keys
  - Non-anonymous authentication with delegation
  - Sent over BEX using emphemeral identities
  - Requires presharing of public keys
- Scrambled identities (aka “blind”)
  - Optimization of the previous approach and no certificates
  - Only HITs are preshared

The BLIND Extension

- The proposed solution is based on the BLIND extension from Ylitalo et al
- The solution attempts to address the privacy issue by scrambling HI(T)s with nonces and exposing the real HI(T)s in the encrypted parts of HIP packets
- The unscrambled HITs have to be known in advance (for full identity protection)
- Scrambling of an identity is denoted by a flag

Generation of Scrambled HITs

- Before sending out an I1 packet, an initiator first selects a random number nonce N
- The initiator generates a scrambled HIT for it by SHA-1 hashing the concatenation of N and its HIT (HIT-I), that is, SHA-1(N, HIT-I)
- If the identity privacy of the responder has to be protected, the initiator generates a scrambled HIT for the initiator in the same way

Next Revision of the Draft

- Is this work interesting?
- Should we have a specific use scenario?
- Location privacy using HIP/ESP Relay?
- HICCUPS compatibility
- Analyze BLIND dependency to algo agility
- BLIND-based mobility
- Encrypted pub keys + certs a better than BLIND?
  - HIP-capable middleboxes can authenticate at least the ephemeral identities
  - Midbox throttles throughput or drops the connection

Thank you

www.huawei.com