Host Identifier Revocation in HIP

draft-zhang-hip-hi-revocation-00

Dacheng Zhang
<zhangdacheng@huawei.com>
Xiaohu Xu
<xuxh@huawei.com>
Background

• The security strength of cryptographic keys is a critical factor affecting the capability of a security mechanism (e.g., HIP) in tolerating attacks.

• After HIP has been in use for a certain period, the strength of keys will be reduced.

• Key revocation mechanisms are then needed for HIP.
Key Revocation in HIP

• Essential objectives of key revocation includes:
  – Discarding obsolete keys
  – Using newly generated keys to take place of obsolete ones
  – Prevent attackers from taking advantages of revoked keys

• Transient key revocation has been achieved in HIP basic exchange. However, many issues with HI revocation are left for further exploration
HI Revocation in HIP

- An HI revocation mechanism for HIP needs to:
  - deal with the lack of trust between communicating HIP hosts
  - support Large amount of HIP hosts
  - be efficient
  - consider HIP-aware middle boxes which are transparent to the HIP-aware systems by design
Motivation

• Analyze different key revocation solutions and find out their advantages and limits when they are used in HI revocation

• Inspire discussion on the issues with HI revocation
Implicit HI Revocation

• Implicit key revocation does not need any additional operations to revoke a cryptographic key
  – Associate an HI with a life period, the HI is discarded when the period expires

• Candidate Solutions:
  – Self-signing certificates — only work when communicating hosts trust each other
  – PGP style solutions — low efficient
  – PKI style solutions — lack successful examples of global deployment before
Explicit HI Revocation

• Explicit HI Revocation without Third Parties
  – It is efficient, if a host only has a small group of collaborating partners and the relationship between the host and its partners is stable

• Explicit HI Revocation with Third Parties
  – Delegate revoking operations to trusted third parties
  – Enable both the “pull” and “push” modes
  – DNS, RVS, PKI can be candidates
Conclusion

• An HI revocation mechanism should enable both implicit and explicit key revocation
• There is no silver bullet in HI revocation
• We need to find a tradeoff between security and performance
Next Step

• Analyzing issues introduced by middle-boxes which are transparent to HIP hosts
• Analyzing security requirements to resolution systems introduced by HI revocation
• Looking for co-authors
Any Comments?