Extensions of Host Identity Protocol (HIP) with Hierarchical Information

draft-zhang-hip-hierarchical-parameter-00

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

2009-7-28

Hierarchy

“Hierarchy, I shall argue, is one of the central structural schemes that the architect of complexity uses.”

--Herbert A. Simon, in “The Architecture of Complexity”

“Hierarchy is a fundamental method for accommodating growth and isolating faults”

--B. Lampson, in “Designing a global name service”

Benefits Introduced by Hierarchy in HIP

- Hierarchical information is essential for the combination of HIP with hierarchical overlays (e.g., hierarchical resolution mechanisms).
- Hierarchical information can be used to address the uniqueness verification issues with HITs in current HIP solutions.
- Hierarchical information can be employed in authorization systems
- Hierarchical information may associate HIP with better HIT administrating and auditing capabilities

Transporting Hierarchical Information (1)

- Generally, there are 4 solutions of embedding hierarchical information in HIP Headers
- The first two solutions are:
  - To embed hierarchical information into HITs directly
  - To modify the common part of HIP header to transport hierarchical information
- The two solutions introduce relatively big modifications to HIP, and show their limits in privacy protection

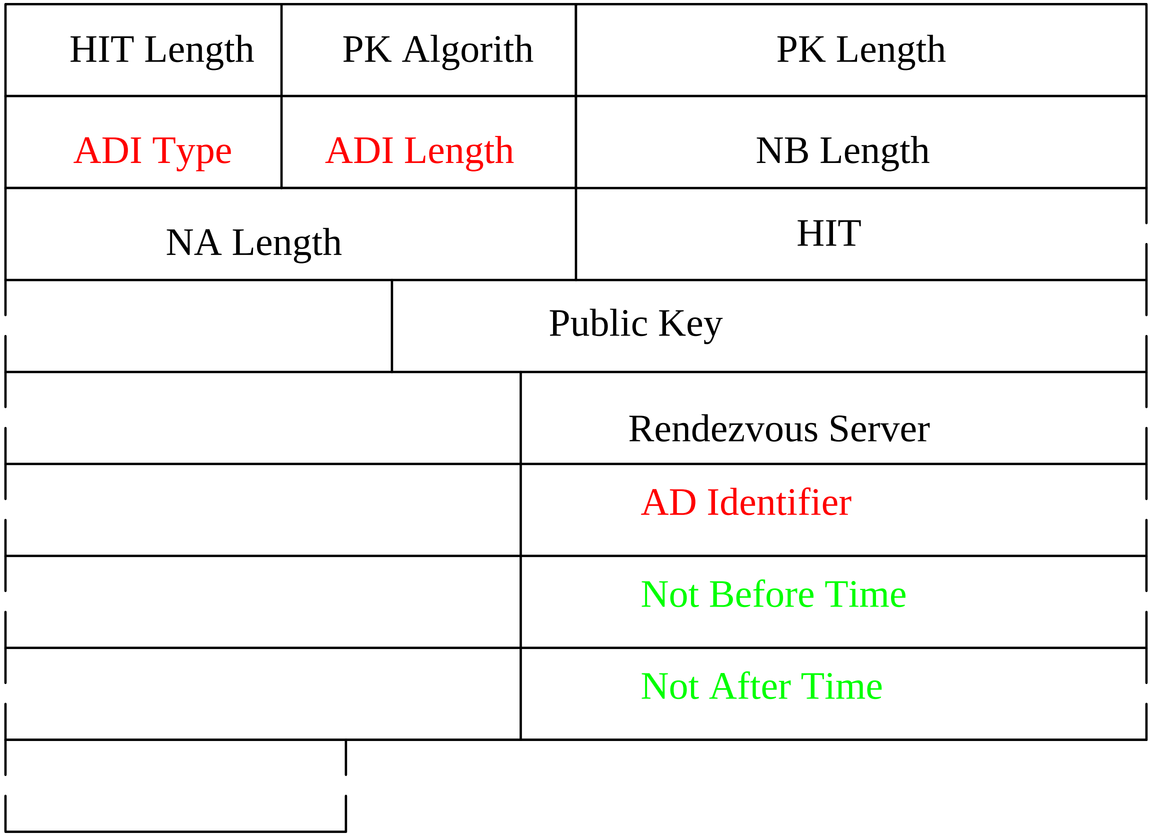
Transporting Hierarchical Information (2)

- The third solution is:
  - To encapsulate hierarchical information in a certificate and transport the certificate within the CERT parameter of the HIT header.
  - This solution transports redundant information in some cases
- The forth solution is:
  - To transport hierarchical information in a parameter.
- The third and forth solutions introduce little modification and enable privacy protection

Hierarchical_HIT Parameter

<table>
<tr><td colspan="4">Type</td><td>Length</td></tr>
<tr><td colspan="2">ADI Type</td><td colspan="2">ADI Length</td><td>NB Length</td></tr>
<tr><td colspan="4">NA Length</td><td>Sig Length</td></tr>
<tr><td>SIG alg</td><td colspan="4">AD Identifie</td></tr>
<tr><td colspan="3"></td><td colspan="2">Not Before Time</td></tr>
<tr><td colspan="3"></td><td colspan="2">Not After Time</td></tr>
<tr><td colspan="3"></td><td colspan="2">Signature</td></tr>
<tr><td colspan="3"></td><td colspan="2">Padding</td></tr>
</table>

Domain Name System (DNS) Extension



HIT Length

PK Algorith

PK Length

ADI Type

ADI Length

NB Length

NA Length

HIT

Public Key

Rendezvous Server

AD Identifier

Not Before Time

Not After Time

Next Step

Any Comments?