Diameter Security

DIME WG
IETF 86
March, 2013
Which Scenarios do we want to cover?

Possible Examples:
- Client<->Server
- Proxy<->Proxy
- Proxy<->Server
Requirements

- Crypto Agility
- Data origin authentication, integrity and confidentiality.
- Backwards compatibility with existing Diameter Applications
- Replay protection (based on timestamps)
- Selectively apply protection to certain AVPs (assuming some out-of-band agreement?)
- Mandatory to implement cryptographic algorithms
- Symmetric keys and/or asymmetric key support?
- Requirements regarding automatic key management (assumptions about PKI?)
- Support for statically provisioned keys
- How to provision long term keying material and other parameters?
Keying Database

draft-tschofenig-dime-keying-database-00.txt

• Describes a conceptual model for a keying database
  • Sending side: what AVPs to protect, and what keys / algorithms to use.
  • Receiving side: select the appropriate security association for verifying the protected AVPs.
• Idea inspired by draft-ietf-karp-crypto-key-table and IPsec
• Diameter uses a number of databases already, e.g., realm based routing table.
Examples

client.example.com  proxy.example.com  server.example.com

Diameter Client  Diameter Proxy  Diameter Server
Example #1: Symmetric Key

Entry from the keying database at the Diameter client.

KeyName: abc123
DestinationHost: server.example.com
ApplicationID: *
AVPCodeList: *
AlgID: HMAC-SHA1-96
KeyType: SymmetricKey
Key: 617CAA833BEF64D88E45
Direction: out
SendNotAfter: 201302142000Z
## Example #1: Symmetric Key

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Dst Host</th>
<th>ApplID</th>
<th>AVP Code List</th>
<th>KeyType</th>
<th>Key</th>
<th>Dir</th>
<th>Send Not After</th>
<th>AlgID</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc123</td>
<td>server.example.com</td>
<td>*</td>
<td>*</td>
<td>Symm. Key</td>
<td>617C…8E45</td>
<td>out</td>
<td>201302142000Z</td>
<td>HMAC SHA196</td>
</tr>
</tbody>
</table>
## Example #2: Asymmetric Key

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Dst Host</th>
<th>ApplD</th>
<th>AVP Code List</th>
<th>Key Type</th>
<th>Key</th>
<th>Dir</th>
<th>Send Not After</th>
<th>AlgID</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc123</td>
<td>server.example.com</td>
<td>*</td>
<td>*</td>
<td>Asymm. Key</td>
<td>61…45</td>
<td>out</td>
<td>201302142000Z</td>
<td>RS256</td>
</tr>
</tbody>
</table>
Feedback?