Secure Multicast Interest in ChronoSync

Yingdi

UCLA
ChronoSync

- State of a data set is expressed as a digest

<table>
<thead>
<tr>
<th>Digest</th>
<th>State tree modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>00a12...</td>
<td>&lt;update /ucla/alice to SeqNo 4&gt;</td>
</tr>
<tr>
<td>3da49a</td>
<td>&lt;update /arizona/bob to SeqNo 2&gt;</td>
</tr>
<tr>
<td>8f904d</td>
<td>&lt;update /arizona/bob to SeqNo 1&gt;</td>
</tr>
<tr>
<td>c3412e</td>
<td>&lt;update /ucla/alice to SeqNo 3&gt;</td>
</tr>
<tr>
<td>dd79f2</td>
<td>&lt;update /ucla/alice to SeqNo 1&gt;</td>
</tr>
</tbody>
</table>

- Maintain a digest log to identify the state difference
Sync interest multicast

My current state digest is 4de318f...
Identity state digest

What is 4de318f? What is 4de318f?
Recover unknown digest

Unknown digest 4de318f

Start reconcile
If anyone can send multicast interest...
To launch attack

• Attacker needs to
  – get prefix of the sync group
  – generate a large number of sync interests with random digest

• All legitimate users will be forced to
  – do extra lookup
  – do unnecessary reconciliation
  – do extra signing

• No way to distinguish legitimate sync interests from malicious sync interests
Authenticate sync interest

• Signed interest

• Should not prevent interests from being merged in the network
Interest merging

Current state is 4de318f...

Current state is 4de318f...

Current state is 4de318f...

Current state is 4de318f...

Interests representing the same state should be merged
Data multicast

New updates
Authenticate sync interest

• Signed interest

• Should not prevent interests from being merged in the network
  – asymmetric signatures do not work

• Symmetric signatures
  – how to distribute the symmetric key?
Symmetric Key Distribution

- Periodically generate a symmetric key
- Encrypt the symmetric key using the each user’s public key
- Published as a single packet

Who can generate the symmetric key?
- designated user
  - single pointer failure
- any user
  - resolve conflict when more than one user generate keys at the same time

<table>
<thead>
<tr>
<th>Name: /ucla/bob/&lt;sync_group&gt;/SyncKey/SeqNo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content:</td>
</tr>
<tr>
<td>Key encrypted using /ucla/alice's public key</td>
</tr>
<tr>
<td>Key encrypted using /arizona/bob's public key</td>
</tr>
<tr>
<td>Key encrypted using /memphis/cathy's public key</td>
</tr>
</tbody>
</table>

Bob's Signature