Preconfigured Kbm

Charles E. Perkins

draft-ietf-mip6-precfgKbm-00.txt

August 3, 2004

Not Confidential

Preconfigured Kbm between Mobile and CN

- “Preconfigured Binding Management Keys for Mobile IPv6”
- A mobile node and a correspondent node may preconfigure a Binding Management Key for authorizing Binding Updates.
- For use when the mobile node and the correspondent node are able to configure such a key, and when the correspondent node has reason to be confident that mobile node will never act maliciously
- Binding Update sequence number amply protects against replay
- Geared towards use of the Binding Authentication Data option

Not Confidential

Testing Care-of Addresses

- Requires new specification subsection, or else new document
- Would depend on flag in preconfigured security association
- Proposal: each new care-of address requires mobile to send CoTI and await reception of CoT message from correspondent node before sending Binding Update
- Then, mobile can create new Kbm, using care-of keygen token, as specified in RFC 3775
- Value of home keygen token is the value that is preconfigured between mobile node and correspondent node
- Value of home nonce index is arbitrary, randomly chosen for each Binding Update, and ignored by correspondent node
- Value of care-of nonce index is as given in CoT message
- Preconfigured security association is presumed to imply confidence that mobile will not send (e.g. millions of) malicious CoTI messages

Not Confidential

Questions and consequences

- Should the preconfigured Kbm draft be expanded to allow the correspondent node to demand care-of address test?
- Kbm then becomes a preconfigured home keygen token, so that teminology in draft should be changed
- For consistent external behavior, should all Binding Updates should contain the Nonce Indices option, even if the indices aren't used?
- When care-of test is not required by correspondent node, the preconfigured data could still be treated as a preconfigured home keygen token, with the new care-of address itself being used as the new care-of keygen token.
    - In this way, the actual Kbm would change at every new care-of address, and processing would be more consistent whether or not the care-of test was demanded by the correspondent node
    - Has the effect of further improving the effectiveness of the sequence number in the Binding Update for replay protection

Not Confidential