Registration Key Distribution

Charles E. Perkins/Nokia
David B. Johnson/CMU
IETF 47

draft-ietf-mobileip-regkey-02.txt

Ways to get keys

- Security association between FA and HA
- Public Key for FA or mobile node
- Diffie Hellman
  - modular exponentiation group
  - elliptic curve groups
- AAA not considered
  - but Mobile IP and smooth handoff should be able to work in the absence of AAA

Major changes since regkey-01

- use Generalized Key Distribution extensions
- Elliptic Curve algorithm as default
- Diffie-Hellman between FA and HA
  - puts computation where it belongs
- Advertise digestified D-H computed value
  - still many fewer bits than before over the air
- Included *opaque data* handover in algorithm

Request subtypes

- All assuming advertised ‘S’ bit
- Mobile Node Key Request
  - asks foreign agent to “just do it”
- Mobile Node Public Key
- Foreign Agent Public Key
  - sent by FA to HA
  - needs digestified advertisement
- Foreign Agent Request subtype
- Diffie-Hellman subtypes

Reply Subtypes

- Key encoded by HA for MN subtype
- MN public key reply (added by FA)
- FA public key reply (added by HA)
- Single D-H reply, contents depend on request

Issues

- Source code for elliptic key
  - patents?
- Interoperability testing?
- Should HA know the mobile node’s public key?
- Using derived keys
- Non-default D-H parameters?
- Better challenge handling for more m-i-t-m cases?