AAA Registration Keys

Charles E. Perkins/Nokia Research

Pat R. Calhoun/Sun Microsystems

Motivation and context

- Using new AAA security model, mobile node has security only with AAAH
- Mobile IP needs security ass'n between mobile node and home agent
- 3G requirements document specify need for keys also with foreign agent
  - both with mobile node and with home agent

More AAA details

- Mobile node *MAY* use MN-NAI to identify itself
- AAA is separate protocol from Mobile IP
  - Mobile IP extensions for AAA
  - AAA extensions for Mobile IP
- Single Internet Traversal for initial registration

Use of Generalized Key Distribution extensions

- New Unsolicited MN-HA Key Reply subtype
- New Unsolicited MN-FA Key Reply subtype
- HA-FA could be handled within AAA without involvement from Mobile IP

Well-known algorithms 3 & 4

- Mobile IP has a defined range (1-255) for SPIs that indicate well-known algorithms
  - e.g., RADIUS computation from Challenge draft
- It is convenient and accepted today to use MD5 for encoding keys
- AAA keys draft specifies two new MD5 well-known SPIs for simplicity
  - avoids SPI negotiation
  - SPI 3 for MD5 in *prefix+suffix* mode
  - SPI 4 for HMAC MD5 (RFC 2104)