Alternative Authentication mechanisms for MN-HA Authentication in Mobile IPv6

draft-patel-mipv6-auth-protocol-01.txt

59th IETF, Seoul, Korea – 1st March, 2004

Alpesh Patel
Kent Leung
Mohamed Khalil
Haseeb Akhtar
Kuntal Chowdhury
Motivation

• AAA servers today identify clients by using the Network Access Identifier (NAI)
• Authentication method supports NAI or IPv6 address used to identify MN
• Authentication method supports mobility session keying capability
• Protocol changes limited to MIPv6, simplifying deployment
• IPSec is not required on clients, possibly eliminating overhead of dual IPSec sessions for remote access to enterprise

WG thoughts?
Solution

• Use a lightweight hash based authentication between MN and HA
• SA’s for authentication can be stored on AAA or derived using AAA
• With introduction of NAI, SA’s need not be tied with IP address (device identifier)
• Control messages are authenticated (with some contents within it protected, for Route Opt.)
• Simplifies MIPv6 deployment
Details …
NAI Extension ... format

+-----------+-----------+-----------+-----------+
| Subtype   |          NAI |
+-----------+-----------+-----------+-----------+
Solution ... details (authenticating BU/BA)

Obtain a CoA

BU with new Mobility Options
(MN Identification option, MN-HA Authentication option)

BA with new Mobility Options
(MN Identification option, MN-HA Authentication option)

Data Session
Solution … details (HoT message)

- HA needs to intercept the HoT message from CN to MN
- HA encrypts the ‘Home KeyGen Token’
Identification Option

Identification option – to prevent replay protection
MN-HA Authentication Option

Authenticator – calculated using mobility data and shared secret