Securing Mobile IPv6 with AAA protocols

Julien Bournelle
Maryline Laurent-Maknavicius

INT-Evry
Network Software Department (LOR)
9, rue Charles Fourier
91011 Evry
Outline

i. Mobility and IP
ii. AAA concepts and Diameter
iii. Our proposal: Diameter for Mobile IPv6
IP and Mobility

– Routing: based on network prefix of IP address
– TCP connections: identified by the quadruplet
  ( @IP source, Source Port, @IP destination, Destination Port )
– Conclusion: IP doesn’t permit mobility!

– Solutions:
  – Mobile IPv4 (RFC 3220)
  – Mobile IPv6 (<draft-ietf-mobileip-ipv6-18.txt>)
Mobile IPv6 Architecture

- Mobile Node (MN) has 2 associated addresses:
  - home address: on home link; fixed
  - care-of address: current location; variable
- Home Agent (HA) forwards packets sent to mobile node’s home address to its care-of address
- Binding Update (BU): used to inform the HA and other IPv6 nodes about mobile node’s care-of address
Limitations of Mobile IPv6

- Mobile IPv6 is “just” a routing protocol

- Mobile users need to be authenticated, authorized and correctly billed!

=> We need AAA protocols
What is AAA?

- **Authentication**: act of verifying the identity of a claimed entity (e.g. OTP, hashed secret key or Encryption Techniques)
- **Authorization**: act of determining if a requestor can be granted a right (e.g. QoS, Bandwidth...)
- **Accounting**: collecting information on resource usage (e.g. billing purposes)

- examples of AAA protocols:
  RADIUS, TACACS, COPS, Diameter
Diameter

- AAA protocol being designed by the AAA WG at IETF

- Documents: base protocol + 3 extensions:
  1. NASreq (Dial-up/PPP environment)
  2. CMS (security at the Diameter level)
  3. Mobile IPv4 (Mobile IPv4 environment)

- but **nothing** for Mobile IPv6!

- our IETF submissions:
  1. draft-dupont-mipv6-aaa-01.txt
  2. draft-le-aaa-mipv6-requirements-00.txt
Our proposal

visited domain : mno.net

Local Diameter server

INTERNET

Home Domain : xyz.com

Home Diameter Server

Home Agent

Mobile
NAI: Julien@xyz.com

ASWN’2002  Julien.Bournelle@int-evry.fr  INT
Proposed Exchanges

**AS :** Attendant Solicit

**AA :** Attendant Answer with LC

**Areq :** LC, NAI, RPI, [H@]

[H@], {aaa_key},

{attendant_key}

{SecuParam_I}

Credentials

**AMR :** same content than Areq

but Diameter packet

**HAR :** [H@], SecuParam_I

**HAA :** SecuParam_R

**AMA :** RC (Result), attendant_key

RPI, [H@], [HA@] and {SecuParam_R}

**Arep :** Final answer

**BU :** Binding Update
Advantages

Permits the deployment of Mobile IPv6 in a commercial environment

- Mobility inter and intra domain
- Users are identified by their NAI (user@realm)
- Dynamic assignment of the Home Agent (load balancing)
- Dynamic creation of an SA (IPsec ESP) between the MN and his HA
Implementation

- FreeBSD 4.5 (OpenSSL library)
- Use of EAPoL (802.1x) between the MN and the Attendant
- Use of IKEv2
- Sources will be freely available at: www-lor.int-evry.fr/~bournell
Any questions?

www-lor.int-evry.fr/~bournell