IETF 58 (Minneapolis) Report: multi6, hip and nfsv4

Nevil Brownlee
CAIDA, SDSC, UC San Diego *and*
The University of Auckland
nevil@caida.org

CAIDA, November 2003

Overview

- IETF 58 (Minneapolis, November 03) was both busy and interesting
- IPFIX: The Requirements and evaluation drafts are now ready to submit to IESG, work continues the protocol and information model drafts.
- This meeting there were three Working Groups with interesting new technical material
  - multi6: IPv6 multihoming proposals
  - hip: Host Identity Protocol
  - nfsv4: Channel Bindings

RFC 3582: IPv6 Site-Multihoming Requirements

- v4 multihoming: announce more-specific routes via several providers $\Rightarrow$ big routing tables, won't scale to v6 address space
- v6 gives us a chance to do it better, or at least different
- v6 *hosts* can multihome, since they need a new (v6) IP stack, site multihoming may be harder

IPv6 Multihoming: the idea

- Need a *host ID*, and a list of *locators* for it
- When setting up a connection, each end:
  - looks up target host using DNS to resolve FQDN
  - gets locator list from DNS
  - decides which locator will be *best* for now
  - opens connection
- SCTP already handles lists of IP Addresses at each end of a connection

multi6 WG: two proposals

- two proposals, drafts:
  - `draft-nordmark-multi6-noid-01.txt`
  - `draft-nordmark-multi6-sim-01.txt`
- Erik Nordmark's drafts asses how well noid and sim handle redirection attacks and other security concerns
- Much of the detail comes from mobileip-v6 drafts
- noid and sim both use a multi6 shim in the IP stack between IP and Upper Layer Protocols (ULPs)
  - Keeping AH and ESP above the shim means that IPsec can be unaware of locator changes, just as transport protocols can be unaware
  - security associations remain stable even though locators change

noid: Multihoming without IP Identifiers

- addresses *site* multihoming
- uses DNS to maintain list of site locator prefixes
- routers can rewrite locator for a connection
- locators can change with time (renumbering), need a ‘rewrite-ok’ bit
- shim uses bits in IPv6 header, no extra bytes in packet
- use flowid field as a ’compression tag’ to carry AIDs
  - application identifier (AID) $\Rightarrow$ *IP locator which has been selected for communication with a peer to be used by the ULP*
  - different connections to a host might use different AIDs in order to enable load spreading

sim: Strong Identity Multihoming using 128 bit Identifiers

- uses 126 bit identifiers which are hashes of public keys
- when a connection needs to use a new locator, verify that locator using a public-key based challenge-response
- uses an extension header for the multi6 shim, at least 8 bytes

hip: Host Identity Protocol Architecture

- drafts:
  - `draft-moskowitz-hip-arch-05.txt`
  - `draft-moskowitz-hip-08.txt`
- Internet namespaces
  - IP addresses and DNS names
  - we overload these too much!
- a new namespace, Host Identity, would be useful

nfsv4: Channel Bindings

- draft: `draft-ietf-nfsv4-channel-bindings-00.tx`
- aim is to prove that endpoints at application layer are the same as at another, secure, layer
- an old idea, concept comes from GSS-API (RFC 2743)
- want to use crypto h/w at one layer, recognise and use it at other layers
- question: what's an IPsec channel?
  remember that IP is connectionless!