GIST – The NSIS Transport Layer

`draft-ietf-nsis-ntlp-12.txt`

Robert Hancock, Henning Schulzrinne
(editors)

IETF#68 – Prague

March 2007

Overview

- What’s Changed in v12
- Status

What’s Changed in v12

- Short story: read section E.1
  - ‘Protocol change’: you must update your implementation
    - [PC#*n*] in these slides; all covered
  - ‘Technical clarification’: you might have to update your implementation if you ‘misunderstood’ an earlier version
    - [TC#*n*] in these slides; few covered
  - ‘Editorial’: everything else
    - Includes non-trivial text on conceptual aspects
    - Not covered in these slides

Highlights

- Some specific, detailed protocol fixes
- Text on Legacy NAT interactions
- Q-mode encapsulation changes
- State machine modifications for restarts & reset attacks
- Routing state authorisation and identity checking
- RAO clarifications and deployment issues
- Changed text on MTU thresholds and congestion control
- New text on handling path splitting and route flapping

Detailed Protocol Fixes

- [PC1] Modified processing rules for the Hop Count
- [PC2] Endpoint Found is now a fatal error
- [PC3] MA-Hello enhanced to correlate request/reply
- [PC5] Error messages have a TLV format
  - As previously discussed on the mailing list
- [PC11] NLI is now present in all Response messages

Legacy NAT Handling

- [PC4] New section 7.2.1 on overall procedure
- Scope & limit of ambition:
  - Base specification says ‘this is how a node detects that messages are crossing a NAT’
  - Base specification says ‘give up promptly at this stage’
  - Open to extension specifications to define better handling
- Cf. old draft: was silent on what happened (i.e. fail in an undefined way)
- Detailed consequences:
  - 7.2.1 brings together the analysis and requirements for Q/R processing
  - Main additional details are changes to S-flag processing in 5.2.2, 5.3.1, 5.3.2

Q-mode Encapsulation

- [PC6] Avoid intercepting messages with UDP-dest = GIST when they are not really GIST packets by adding a magic number
  - Still open: need to fix that magic number is for packets → GIST port, not Q-mode packets
- Also [TC13] discusses what has to be done with IP options

State Machine Updates

- [PC7] Better handling of “no routing state” error messages to handle node restarts but avoid blind reset attacks
- New dedicated section 4.4.6
- Simplified discussion in 5.3.3 (‘Lost Confirm’ section)
- Corrections in 4.3.2, 6

Routing State Authorisation and Identity Checking

- [PC8/9] Current non-cryptographic checks (return routability check) unchanged, but
- Role of MA security in protection against upstream/on-path attacks formalised
- New section 4.4.2 says "these are the rules a person should use in deciding whether a peer should be an authorised participant in an MA"
  - Applies regardless of security mechanism; phrased in terms of an 'Authorised Peer Database', who should be in it, when to check it
- New section 5.7.3.1 defines how to implement these rules when using TLS
  - Essentially a set of name matching rules

RAO Handling

- [PC10] Made more explicit the text in 4.3.1/9 about how the GIST specification should be used to satisfy the IANA requirements for RAO value allocation
- Association absolute prohibition on Q-mode fragmentation
- New informative Appendix C on “what might happen if RAOs are handled unfavourably and what implementations or specification extensions could be used to handle it”

Transport Properties

- [TC1] Clarifications on in-order delivery over multiple MAs
- [TC2] More precise definition of D-mode message size threshold
  - Will be updated again in v13
- Change ‘MAY’ use C-mode to ‘SHOULD’ unless capacity is engineered
  - Will be introduced in v13 (tut tut…)

Path Splitting and Route Flapping

- [TC19] Added new section 7.1.4 modifying the relationship between GIST and NSLPs for handling route changes
  - Route change is decomposed as Add/Delete rather than Change
  - NSLPs can remember as many routes as they like and keep state on all of them
  - This GIST doesn't try to understand the set of active routes, just the current one
  - GIST extensions to do more precise route set management would fit within this framework
    - But it's a ******* hard problem in general

Status

- Version -13 should be released shortly
  - Resolving open issues in the tracker
  - http://nsis.srmr.co.uk/cgi-bin/roundup.cgi/nsis-ntlp-issues/
  - Check the issues against v13!
    - Issues against v12 have been left open just to be visible
  - Plan WGCL to start 2nd April