Security Framework for MPLS-TP

draft-mpls-tp-security-framework-02.txt

Editors:

Luyuan Fang	lufang@cisco.com
Ben Niven-Jenkins	ben@niven-jenkins.co.uk
Scott Mansfield	scott.mansfield@ericsson.com
R. Graveman, Ed.	rfg@acm.org

Nov. 17, 2011
82 IETF, Taipei, Taiwan

Contributing Co-authors

- Luyuan Fang lufang@cisco.com
- Ben Niven-Jenkins ben@niven-jenkins.co.uk
- Scott Mansfield scott.mansfield@ericsson.com
- Richard F. Graveman rfg@acm.org
- Raymond Zhang raymond.zhang@bt.com
- Nabil Bitar nabil.bitar@verizon.com
- Masahiro Daikoku ms-daikoku@kddi.com
- Lai Wang Lai.wang@telenor.com
- Henry Yu henry.yu@twtelecom.com

Status and Next Steps

- Current status:
  - Under WG last call
  - Received comments from Gregory Mirsky and Joel M. Halpern
  - Updating the document to address the comments from Gregory and Joel
- Next Step
  - Submit the updated version

Addressing the comments from Gregory

- Section 1.1 “MPLS-TP and MPLS interworking” seems ambiguous. Perhaps “There are also needs for MPLS-TP and non-MPLS-TP interworking”. We meant to say “MPLS-TP and MPLS interworking” at this stage.

  #: We like to stay with MPLS-TP and MPLS interworking within this context.
- Section 1.2 G-ACh might be used to launch attack on the data plane, e.g. trigger protection switchover or lock a connection…… And “Data plane authentication” isn’t it part of G-ACh issues

  #: Agreed.
- Section 3 “…the data plane should continue to forward packets without being impacted”. I think that separation of Control Plane and Data Plane implies that all enabled in the data plane operations, e.g. OAM, protection, will act without impact in case control plane and/or management plane are under attack.

  #: Good point.
- And a couple more of editorial comments.

  #: OK, will fix.

Addressing the comments from Joel

- Major:
  - … Add explanations of the security analysis that goes with the assertion exist somewhere. (This applies to mechanism requirements…) …this is an important part of the framework that users need.

    #: Agreed, will add content for it.
  - Structurally, it seems very odd to have the requirements before the threats. In my experience, the threats drive the requirements.

    # We put threat first in RFC 4111, later received comments that reqs. should be first. Be happy to switch the order same as RFC 4111 – threat first, requirements later.
- Moderate:
  - Clarification in a couple of places should be ‘must’, ‘MUST’, ‘or’… meaning.

    # Will make it explicit in the text.
  - the connection in the second requirement between non-control plane provisioning support and trust boundaries really needs some justification.

    # Will fix.
  - I understand that service providers have a requirement for hiding topology. But is that really a security requirement?

    # This originally came from a SP specific request when we worked MPLS/GMPLS Security Control plane. We would use the wording “to allow”.
  - need to be clear which threats are new with MPLS-TP….

    # Will fix the text
- More comments under minor
  - # Will be addressed

(Back up - the draft overview)

- Content:
  - Identify and address MPLS-TP *specific* security issues.
    - Define MPLS-TP security reference models
    - Provide MPLS-TP security requirements
    - Identify MPLS-TP security threats
    - Provide MPLS-TP security threat mitigation recommendations
- Intended category: Informational
- Scope:
  - Focus on MPLS-TP specific security threats, e.g.
    - GAL/GAch for in-band OAM
    - NMS provisioning model
    - General attached applied in TP operations: DoS attack, ID/Label spoofing
  - Defer to existing RFCs for Internet Best Practice Guidelines, and MPLS/GMPLS Security Framework