Requirements Draft


IETF 67 – Wednesday November 8 2006

Jean-François Mulé - jfm@cablelabs.com, Editor

IETF Speermint Working Group
Changes since draft-00 (1)

- Integrated wg comments received on the mailing list and at the interim meeting
- Clarified the intent and scope of the ID
  - When protocol mechanisms are used, provide guidelines or best current practices on how they should be implemented to facilitate session peering
  - the "must implement" rather than "must use"
- Generalized some requirements beyond just VoIP
- Aligned terminology with draft-speermint-terminology
- Addressed various editorial comments
  - E.g. Separated requirements from motivations/justifications
Changes since draft-00 (2)

- Clarified a few technical requirements (RFC 2119 language)
- Added a requirement on the variability of Call Addressing Data per mailing list thread based on input from Daryl, Otmar, Penn and others
- Captured mailing list ‘chats’ about things that should be considered as part of a session peering policy
  - Definition, Static vs. Dynamic, relationship with SIPPING policy
  - List of Parameters for policy description (new annex A)
- Updated requirements to reflect wg consensus on Media & Codecs
- Started to develop text on Security
  - Added input we got from various participants at the interim on the fact that some VSPs rely on network-layer and lower layer security mechanisms for VoIP exchanges
  - Added pointers to rtpsec bof for media related security requirements and new IDs on media security requirements
  - Replaced the basic TLS requirement with more detailed paragraphs per the wg recommendations at the interim
Session Peering Policies and Draft’s Annex A

Goals:
• Describe the types of policy information that needs to be discovered or exchanged between peers
• Position the discussion on “what” information is needed rather than focusing on the “how”
• Identify the things that can break calls due to lack of protocol interoperability

Content of Annex A
• IP Network Connectivity
• Media session parameters
  – Codecs for audio, video, real time text, instant messaging media sessions
  – Modes of communications for audio - IM
  – Media transport
• SIP
  – SIP RFCs, methods and error responses
  – headers and header values
  – possibly, list of SIP RFCs supported by groups (e.g. by call feature)
• Accounting
• Performance Metrics
• Security
  – Call admission control, call authorization
  – Network and transport layer security parameters
  – Media security parameters

Is this a good direction for the ID? Should we continue and provide more details on some of these?
TLS Considerations for session peering

Goals
• Provide details on how TLS could be deployed and used between 2 VSPs/ASPs to secure SIP exchanges
• Capture what two VSPs/ASPs should discuss and agree on in order to establish TLS connections for SIP session peering

Content of Section 4.4.2.
1. Peers SHOULD agree on one or more Certificate Authorities (CAs) to trust for securing session peering exchanges
2. Peers SHOULD indicate whether their domain policies require proxy servers to inspect and verify the identity provided in SIP requests
3. SIP servers involved in the secure session establishment over TLS MUST have valid X.509 certificates and MUST be able to receive a TLS connection on a well-known port.
4. List some TLS/SIP Protocol parameters SHOULD be agreed upon
5. Validation of TLS client certificates
6. All of this should be part of session policy discussions

Adapt this section & security requirements based on threat analysis and recommended solutions?
Comments on TLS considerations for speermint?

IETF Speermint Working Group
Thanks.
Other Feedback?

mailto:speermint@ietf.org