Lemonade
IETF 62

Eric Burger

eburger@brooktrout.com

Glenn Parsons

gparsons@nortel.com

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- **the IETF plenary session,**
- **any IETF working group or portion thereof,**
- **the IESG or any member thereof on behalf of the IESG,**
- **the IAB or any member thereof on behalf of the IAB,**
- **any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,**
- **the RFC Editor or the Internet-Drafts function**

All IETF Contributions are subject to the rules of BCP 78 and BCP 79.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult BCP 78 for details.

Scribes and Transcribes

?? for Wednesday

?? For Thursday

JABBER details

Room: lemonade **Server**: ietf.xmpp.org

Logs: http://www.xmpp.org/ietf-logs/lemonade@ietf.xmpp.org/

mp3 details

Wednesday: http://videolab.uoregon.edu/events/ietf/ietf628.m3u

Thursday: http://videolab.uoregon.edu/events/ietf/ietf627.m3u

Chair’s Agenda

Wednesday

- Status review
  - Goals, S2S Notification, MMS, Future Delivery,
  - Pull Trio (cooked and updated)
- Profile (phase 1)
- Security
- Media Conversion
- Deployment Challenges (L3/L7 Interaction)

Thursday

- Goals (phase 2)

Status Update

Chairs

Lemonade Charter Review

- LEMONADE Goals
- IMAP4 extensions for VM playback
- IMAP4/SUBMIT extensions for forwarding
- IMAP4 extensions & profile for diverse endpoints
- Server-to-Server Notification Protocol
- Translation to and from other messaging systems

WG Deliverables

- LEMONADE Goals

  draft-ietf-lemonade-goals-05.txt

- IMAP4 extensions for VM playback

  draft-ietf-lemonade-imap-channel-02.txt

- IMAP4 extensions for forwarding

  draft-ietf-lemonade-burl-00.txt

  draft-ietf-lemonade-urlauth-05.txt

  draft-ietf-lemonade-catenate-04.txt

- IMAP4 extensions & profile for diverse endpoints

  draft-ietf-lemonade-reconnect-02.txt

  draft-ietf-lemonade-futuredelivery-01.txt

  draft-ietf-lemonade-profile-01.txt

- Server-to-Server Notification Protocol

  draft-ietf-lemonade-notify-s2s-00.txt

- Translation to and from other messaging systems

  draft-ietf-lemonade-mms-mapping-02.txt

WGLC Status

- Goals
  - RFC Editor Queue
- Server-to-Server Notification Requirements
  - IETF Last Call Closed, Should be Informational, Needs Chair Write-Up
- MMS Mapping
  - IETF Last Call Closed, No Comments, Needs Chair Write-Up
- Future Delivery
  - WGLC Closed, Nits Review Needed
- Catenate
  - WGLC Happened; Enough Comments to Need New WGLC After Next Draft
  - WGLC Should Be Closed, But Enough Will Change to Keep Open
- URLauth
  - WGLC Closed (will send note to list), Need New Draft
- BURL
  - WGLC Closed, Nits Review Needed

Lemonade Profile

Stéphane Maes

Alexey Melnikov

Security Models

Glenn Parsons

Eric Burger

Pete Resnick

Security AD Comments

- State recovery at apps layer
  - Persistent session layer instead
- Security model
  - e2e, access all keys, per message key
  - This needs protocol work with S/MIME or PGP WGs
- Security credentials for streaming
  - Negogiate keys, use TLS/SASL or SDP

Reconnect

- Principles
  - Cannot Reduce IMAP Security
  - Cannot Break IMAP Security Model
- Acceptable Approach
  - Network-side Server
  - Proxies Full IMAP Authentication Handshake
  - Holds IMAP Session, Passing Cookie towards Client
  - Client May Use Cookie to Authenticate on Reconnect

Reconnect Properties

- Since Network-side Server Holds IMAP State, No Need for Re-Sync on Reconnect
- Theory, Want Scheme for All Related Protocols (e.g., http, sip)
- Practice: Unnecessary
  - Retrieval protocols have concept of “Start at block/time X”
  - Retrieval protocols do not have re-sync problem
- Although Proposed as a Proxy Model, Should We Build-In to Server? Decomposition a Local Matter / Implementation Detail?

Transcoding

- Turns Out e2e Security is Possible
  - S/MIME and PGP Take Body, Generate Session Key, and Encrypt Session Key with Public Key
  - Recipient Uses Private Key to Decrypt Session Key, not Body
- Process
  - Server Hands Encrypted Session Key to Client
  - Client Decrypts Session Key
  - Client Hands Key to Server for Document Processing
- Requires New Protocol Mechanism for Passing Keys

Streaming

- Streaming Has More Complex Trust Relationships
  - IMAP Server <-> IMAP Client
  - IMAP Client <-> Streaming Server
  - Streaming Server <-> IMAP Server
- Do Not Want to Impose Additional Requirements on Client
  - E.g., If Client Infrastructure is all SASL, Don’t Want to Impose X.509 TLS on Client <-> Streaming Server Connection
- Passing Session Keys in SDP OK Approach

Deployment Challenges

Media conversion
Intermediaries
Transport optimization
S2C notifications

Media Conversion

Michael Wener

Intermediaries

Stéphane Maes

Transport Optimization

Needs Work

Next Steps

- Volunteers for Nits
- Volunteers for WG Write-Ups
- Media Conversion Strategy

Charter Dates

Goals and Milestones:

Oct 04	Submit LEMONADE goals and use-cases specification to the IESG
Oct 04	Submit server to server notification requirements to the IESG
Nov 04	Submit translation to other messaging systems to the IESG
Nov 04	Submit IMAP/SUBMIT extensions for forward without download to IESG
Jan 05	Submit IMAP4 extensions for streaming multimedia to the IESG
Feb 05	Submit IMAP4 profile for mobile devices to the IESG
Mar 05	Submit server to server notification protocol to the IESG

Thanks!

- Mail List:
  - General Discussion: lemonade@ietf.org
  - To Subscribe: lemonade-request@ietf.org
  - In Body: in body 'subscribe'
  - Archive: ftp://ftp.ietf.org/ietf-mail-archive/lemonade/
- Supplemental Work Group Page
  - http://flyingfox.snowshore.com/i-d/lemonade/