Secure Shell (secsh) Working Group

IETF62, 10 March 2005

Chair: Bill Sommerfeld <sommerfeld@sun.com>

Agenda

- IV/agenda bashing/bluesheets 5 minutes
- WG/Draft status 5 minutes
- Core draft nits 10 minutes
- filexfer draft 10 minutes
- milestones 10 minutes

Administrivia

- MP3 audiocast
- Jabber Scribe/Notetaker?
- Blue Sheets

WG Status

- Core Drafts waiting for IPR WG
- Other drafts languishing
- New IETF IPR process docs
  - replace 2026 with 3667, 3668
  - replace 3667/8 with 3978, 3979
- New Issues(tm)

New Issues(tm)

- Process was unclear regarding TM reference.
  - Inconsistency between past IESG ruling and new process
  - WG chair referred to IESG; IESG referred to IPR WG
- RFC3667 required mention of trademarks
  - "All trademarks, trade names, service marks and other proprietary names used in the Contribution that are reasonably and personally known to the Contributor are clearly designated as such where reasonable."
  - Author of 3667 says this is a bug.
- RFC3667 also commits IETF to retain trademark references made by contributors
  - This is not regarded as a bug

- draft-ietf-ipr-trademarks-00.txt written
- Observed apparent smooth consensus in IPR-WG room on:
  - "X is a trademark" ok
  - "X is a trademark of Y" not ok
  - Former appears to be sufficient to preserve rights of tm holders without appearing to have IETF endorse claim.

Issue Tracking: Reminder

- Picked RT as run by Randy Bush/Rob Austein
- https://rt.psg.com
  - log in as "ietf", password "ietf" for anonymous access
  - ask WG chair for write access.
- Want more participation from document authors!

General Nits For All Drafts

- New site at http://tools.ietf.org/
- Automated draft nits checking.
- Security considerations section
  - Looks really lame if SEC area forgets this!
- IANA considerations section.

draft-ietf-secsh-dns

- In RFC editor queue, waiting for core drafts

Core Drafts Status

- Almost all IESG issues believed dealt with
- Fixing nits while waiting for IPR-WG

Fun with UTF8

- Unprocessed UTF8 username, password
- recommend saslprep on server side
- Convergence with sasl, kerberos, ...

Miscellaneous confusing bits & wordsmithing

- References to arcfour/RC4
  - no change made
- arcfour variable length cipher
- "n-bit" vs "n bits"
- missing constants for
  - SSH_MSG_KEXDH_INIT
  - SSH_MSG_KEXDH_REPLY

Misc Drafts

- draft-ietf-secsh-auth-kbdinteract
- draft-ietf-secsh-dh-group-exchange
  - nits only; wg chair has still been lame about followup
- draft-ietf-secsh-newmodes
  - expired. was pretty close. wg chair has been lame
- draft-ietf-secsh-gsskeyex
  - author has been lame
- draft-ietf-secsh-filexfer
  - Active discussion, call for comments

http://tools.ietf.org/wg/secsh/

Expired:

- draft-ietf-secsh-break-02
- draft-ietf-secsh-gsskeyex-08
- draft-ietf-secsh-newmodes-02
- draft-ietf-secsh-publickey-subsystem-01
- draft-ietf-secsh-publickeyfile-05
- draft-ietf-secsh-agent-02
- draft-ietf-secsh-fingerprint-01
- draft-ietf-secsh-scp-sftp-ssh-uri-01

Milestones Are Really Stale

Done Submit Internet-Draft on SSH-2.0 protocol
Done Decide on Transport Layer protocol at Memphis IETF.
Done Post revised core secsh drafts
Done Submit core drafts to IESG for publication as proposed standard
Done Post extensions drafts for review
Done Start sending extensions drafts to Last Call
Apr 02 GSSAPI draft ready for last call
Apr 02 Publish draft on new crypto modes
May 02 Agent draft ready for last call
May 02 Publish draft on X.509v3/pkix support (or subsume into gssapi draft)
May 02 Publish draft on terminal server support
Dec 02 File transfer draft ready for last call

Milestone strawman

Apr 05 GSSAPI draft ready for last call
Apr 05 Last-call newmodes
Drop Agent draft ready for last call
Drop Publish draft on X.509v3/pkix support (or subsume into gssapi draft)
Apr 05 Resurrect and last-call secsh-break
Apr 05 File transfer draft ready for last call
Dec 07 IESG approval of core drafts :-)

Anything else?