IETF 63
GSS-API Next Generation WG

Chair: Jeffrey Altman

Preliminaries

- Introduction
- Blue Sheets
- Scribe, Jabber
  - http://www.xmpp.org/ietf-chat.html
- Audio Streaming
  - http://videolab.uoregon.edu/events/ietf/ietf63.html
- Testing of new Proceeding Submission Tool
  - https://datatracker.ietf.org/public/proceeding_onsite.cgi?meeting_num=63
- Agenda Bashing

Agenda

- Document Status - Jeffrey Altman (5 min)
  - A PRF API extension for the GSS-API
    draft-ietf-kitten-gssapi-prf-05.txt
  - A PRF for the Kerberos V GSS-API Mechanism
    draft-ietf-kitten-krb5-gssapi-prf-04.txt
  - Corrections and Updates of GSS-API Java Bindings
    draft-ietf-kitten-rfc2853bis-00.txt
  - C# Bindings
    draft-ietf-kitten-gssapi-rfc2853-update-for-csharp
  - Desired Enhancements to GSS Naming
    draft-ietf-kitten-gss-naming-02.txt
  - GSS Naming Extensions
    draft-ietf-kitten-gssapi-naming-exts-00.txt
  - Clarifications to GSS API v2 update 1

Agenda

- **Technical Discussion (90 min)**
  - GSS-API Naming Extensions - Nico Williams draft-ietf-kitten-gssapi-naming-exts-00.txt
  - Moving RFC2743 and RFC2744 to Draft
  - Review CAT and KRB-WG mailing list archives to determine contents of 'Clarifications to GSSAPIv2' as Informational
- **Update Milestones (10 min)**

Document Status

A PRF API extension for the GSS-API

- Draft -05 submitted
- Addresses issues raised during the most recent WGLC
- Will be submitted for a short WGLC next week

A PRF for the Kerberos V GSS-API Mechanism

- Passed Working Group Last Call (WGLC)
- Being held until "A PRF extension for the GSS-API Mechanism" passes WGLC

Corrections and Updates of GSS-API Java Bindings

- The current draft contains just a list of proposed changes to RFC 2853 to bring it into compliance with the Java GSS implementation produced via the Java Community Process

- A new XML master is being created for RFC 2853 into which the proposed changes are being merged

- A new draft will be submitted soon for review and submission to WGLC

- Future drafts for GSS v3 will be submitted through the JCP to obtain feedback for use by this WG.

C# Bindings

- Since IETF62 consensus was reached to split the C# Bindings from the Java Bindings

- A new draft providing a complete C# binding for GSS-API v2 update 1 to be submitted to the working group in the next couple of weeks

Desired Enhancements to GSS Naming

- -02 draft submitted at the beginning of June
- It is ready for WGLC which will run for two weeks starting Monday

GSS Naming Extensions

- Draft -00 was submitted in May but has yet to receive any feedback on the list
- We will discuss this draft further during the technical discussion

Clarifications to GSS API v2 update 1

- No draft has yet to be submitted
- The WG has missed a milestone
- Previous volunteers to work on this draft have withdrawn
- We will discuss this draft during the technical discussion

Technical Discussion

GSS-API Naming Extensions

Nico Williams

Moving RFC2743 and RFC2744 to Draft

Sam Hartman

Outstanding issues

- Would the RFCs need to be republished before they could be submitted to Draft Standard?
  - Are there items for which there are no interoperable implementations?
- What do we use for interoperability tests for an API?
- Martin Rex (SAP) has performed certification tests for compatibility
  - The results of these tests are confidential
  - Martin is willing to contact implementers to see if they will take part but we must first have a testing plan

'Clarifications to GSSAPIv2' as Informational

Chair

GSS v2 Clarifications

- Character-set issues
  - 2744 refers to Latin-1
- Thread safety issues
- Use of Channel Bindings
- C language utilization clarifications and recommendations
  - type utilization
  - name spaces
- Guidelines for GSS-API mechanism designers
- Guidelines for GSS-API application protocol designers

Mailing List Archives

- Kitten
  - http://www1.ietf.org/mail-archive/web/kitten/current/index.html
- CAT
  - http://www.mail-archive.com/ietf-cat-wg%40lists.stanford.edu/index.html
- Kerberos
  - ftp://ftp.ietf.org/ietf-mail-archive/krb-wg/

Goals

- Obtain a volunteer to Edit this draft
- Produce an Outline
- Begin to Propose Text
- Search Archives of CAT and Kerberos for related e-mail messages from which draft text can be pulled
- Continue on the mailing list

Milestone Review

Chair

Closing Notes

- Where are the Blue Sheets?

- Kerberos WG today at 1400 room 362
- SecMech BOF Tuesday at 1030 room 342