71st IETF

Kerberos Working Group
Kerberos Working Group

Introduction


- Mailing List: ietf-krb-wg@anl.gov
  - To Subscribe: https://lists.anl.gov/mailman/listinfo/ietf-krb-wg
Please Use The Mic!
Kerberos Working Group
Agenda

- Preliminaries (5 min)
- Document Status (10 min)
- Last Call (30 min)
- Technical Discussion (60 min)
  - Preauth Framework
  - OTP
  - Cross-Realm Directions
- Review and Milestones (10 min)
- Open Mic
Kerberos Working Group
Document Status

- **Set/Change Password**
  - draft-ietf-krb-wg-kerberos-set-passwd-07.txt
  - Needs new revision, then on to IESG

- **GSS Agility**
  - draft-ietf-krb-wg-gss-cb-hash-agility-03.txt
  - WGLC done; writeup in progress

- **Cross-Realm Problems**
  - draft-ietf-krb-wg-cross-problem-statement-02.txt
  - Lame chairs will finish review soon
Kerberos Working Group
Last Call

- ECC for PKINIT
  - draft-zhu-pkinit-ecc-04.txt

- Naming
  - draft-ietf-krb-wg-naming-04.txt

- Anonymous
  - draft-ietf-krb-wg-anon-05.txt

- Data Model
  - draft-johansson-kerberos-model-04.txt
Security Considerations

- How can unintended access be granted if authentication is allowed to succeed with an unsupported well-known name?

- Why is it permissible for the TGS to allow authentication to succeed even if the client and/or server principal name is an unsupported well-known name?
Kerberos Working Group
Technical Discussion

- Preauth Framework
  - draft-ietf-krb-wg-preauth-framework-06.txt

- One-Time Passwords
  - draft-ietf-krb-wg-otp-preauth-03.txt

- Cross-Realm Directions
  - Client-Friendly Cross-Realm - Kamada Ken’ichi
Recent Changes

Open Issues
Mandatory Mechanism
- RFC2289 (OTP)
- RFC4226 (OATH)
- Do we need one at all?
<table>
<thead>
<tr>
<th>Date</th>
<th>Milestone Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 2007</td>
<td>Hash agility for PKINIT to IESG</td>
</tr>
<tr>
<td>Sep 2007</td>
<td>WGLC on preauth framework</td>
</tr>
<tr>
<td>Nov 2007</td>
<td>WGLC on OTP</td>
</tr>
<tr>
<td>Nov 2007</td>
<td>WGLC on hardware preauth</td>
</tr>
<tr>
<td>Dec 2007</td>
<td>WGLC on data model</td>
</tr>
<tr>
<td>Jan 2008</td>
<td>WGLC on STARTTLS</td>
</tr>
<tr>
<td>Jan 2008</td>
<td>WGLC on Referrals</td>
</tr>
<tr>
<td>Mar 2008</td>
<td>WGLC on Kerberos v5.3</td>
</tr>
<tr>
<td>Mar 2008</td>
<td>WGLC on IAKERB</td>
</tr>
<tr>
<td>Mar 2008</td>
<td>WGLC on LDAP schema</td>
</tr>
</tbody>
</table>
Kerberos Working Group

Open Mic