Kerberos Working Group Update

Jeffrey
Co-Chair, IETF
Kerberos Working Group
Past Work

- 2005: Kerberos - RFC 4120
- 2005: Crypto Framework - RFC 3961, 3962
- 2005: GSS-API Mechanism - RFC 4121
- 2006: Enctype Negotiation - RFC 4537
- 2006: PKINIT - RFC 4556, 4557, 5349
- 2007: TCP Extensions - RFC 5021
Kerberos Working Group
Recent Work - Completed

- May 2010: Cross-Realm Problem Statement - RFC 5868
- Jun 2010: Preauth/FAST - RFC Editor Queue
- Aug 2010: STARTTLS - APPROVED; in AD wait
- Oct 2010: Naming/Anonymous - APPROVED; AD wait
Kerberos Working Group
Recent Work - Post WGLC

- Jul 2009: IAKERB
- Aug 2010: KDC Data Model
- Sep 2010: OTP
- Oct 2010: DES DIE DIE DIE DIE
- Oct 2010: DHCP Option
Kerberos Working Group
Stalled Work - Help Wanted

- GSS, PKINIT hash agility
- Referrals
- Set/Change Password
- Hardware Tokens
- Ticket Extensions
- IANA Considerations
Kerberos Working Group
Proposed Work

- KX509
  - draft-hotz-kx509-00.txt

- Camellia-CCM
  - draft-kanno-krbwg-camellia-ccm-03.txt

- PAC - generic-PAC probably not in krb-wg, but
  - draft-sorce-krbwg-generic-pac-00.txt
Kerberos Working Group
Proposed Work

- Wireless Mesh Networks
  - draft-moustafa-krb-wg-mesh-nw-00.txt

- Unencrypted KRB-CRED
  - (not yet published)

- KSM - proposed in ISMS
  - draft-pejaver-isms-kerberos-01.txt
Kerberos efforts in OASIS

2010 Kerberos Conference
26-27 October, 2010
Security Service TC (SSTC)

• Three (3) specifications in Oasis have completed 60-day Public Review
  – SAML2.0 Kerberos Web Browser SSO Profile
  – SAML2.0 Kerberos Attribute Profile
  – SAML2.0 Kerberos Subject Confirmation profile

• New use-case received from CMU
  – Updates to be made to Attribute Profile
WS-Security Maintenance (WSS-M)

• The WSS-M TC:
  – TC has been re-started to perform maintenance on WS-Security specifications.
  – Opportunity to update the WS-S Kerberos Token Profile 1.1 (2005)