MIT Kerberos 1.7/1.8

Luke Howard
lukeh@padl.com
lhoward@mit.edu

Introduction

- Founder, PADL
- RFC 2307
- Novell DSfW (née XAD)
- Consultant, MIT
- Kerberos 1.7
  - Windows interop
  - Developed whilst at Novell July 2006, open sourced December 2008
- Kerberos 1.8
- AES-CCM

1.7

- Aliases and name canonicalisation
- RFC 3244 (set password)
- RFC 4537 (enctype negotiation)
- gss_wrap_iov
- GGF extensions
- GSS_C_DCE_STYLE
- GSS_C_INQ_SSPI_SESSION_KEY
- GSS authdata API
- MS PAC APIs
- Mechglue SPI
- KDC authdata SPI
- KDC mech invoke
- Services4User in KDC

Referrals

- draft-ietf-krb-wg-kerberos-referrals
- KDB backend can return a different principal to that requested
- KDC does not proscribe information model
- Support in LDAP backend (better in 1.8)
- Client library support (better in 1.8)
- Windows interop
  - Canonicalise client if requested in AS-REQ
  - Only canonicalize TGS server name in AS-REQ

RFC 3244 (set password)

- Support password change over TCP
- Support set password
- Subject to same ACLs as kadm5 clients

RFC 4537 (enctype nego)

- Client proposes enctypes in AP-REQ authdata
- If server chooses a different enctype, a subkey with this enctype is returned
- Permits clients and servers to use new enctypes without upgrading KDC

gss_wrap_iov

- #include <gssapi/gssapi_ext.h>
- Modelled on SSPI EncryptMessage
- Principally for Windows RPC interop
- Multiple buffer, in-place encryption
- Associated data buffers (AEAD)
- Flexible arrangement of input buffers
  - HEADER | SIGN_DATA | DATA | PADDING | TRAILER
  - PADDING and TRAILER are optional for DCE
- Unwrap without understanding buffer boundaries
  - STREAM | SIGN_DATA | DATA
- gss_wrap_aead provides a simplified API for a single encrypt, single assoc buffer

GGF extensions

- Buffer sets
- Mechanism-specific glue APIs/SPIs
  - gss_inquire_sec_context_by_oid
  - gss_inquire_cred_by_oid
  - gss_set_sec_context_option
- Mechanism-specific glue SPIs
  - gssspi_set_cred_option
  - gssspi_mech_invoke

GSS_C_DCE_STYLE

- RFC 4757
- Used by Microsoft RPC Kerberos mech
- Avoids replay cache requirement by always requiring client and server to prove session key knowledge
- Varied token format
  - Context tokens omit GSS framing
  - Wrap tokens omit variable length encoding

GSS_C_INQ_SSPI_SESSION_KEY

- Exposes session key for MS interop
  - CIFS
  - DRS
  - Not for general purpose use!
- gss_inquire_sec_context_by_oid (GSS_C_INQ_SSPI_SESSION_KEY)
- Buffer set contains
  - [0] Session key
  - [1] Kerberos encryption type as OID

GSS authdata API

- Based on Heimdal APIs
- Kerberos mechanism specific
- gsskrb5_extract_authz_data_from_sec_context
- gsskrb5_extract_authtime_from_sec_context
- Requires caller to explicitly verify MS PAC (this differs from Heimdal)
- Wait for 1.8 and use naming extensions
  - These do the heavy lifting for you

MS PAC APIs

- Based on Heimdal APIs
- krb5_pac_parse
- krb5_pac_get_types
- krb5_pac_get_buffer
- krb5_pac_add_buffer
- krb5_pac_verify
- krb5int_pac_sign
- krb5_pac_free

Mechglue SPI

- Dynamic loading of GSS mechanisms
  - Export dispatch table
  - Export GSS APIs
- Support for new APIs and SPIs
- Specific NTLM support
- SPNEGO interop with Samba
- Mechanism can implement gss_wrap_iov
  - gss_wrap
  - gss_wrap_aead

KDC authdata V1/V2 SPI

- Extended version of V0 SPI from 1.6
- Supports TGS-REQ as well as AS-REQ
- Built-in methods
  - Copy TGT authdata
  - Invoke DB authdata SPI
  - Invoke V0 SPI plugins
- Interface is unstable: V1 in 1.7, V2 in 1.8
- Plugin called with
  - Client, server, TGS DB entry
  - Encoded and decoded request
  - Services4User information
  - Reply
- KRB5-PADATA-PAC-REQUEST

KDC mech invoke

- #include <kdb_ext.h>
- KDC to KDB backend private interface
  - Add new methods to KDB SPI without changing vtable
  - Avoids updating every backend, kadm5, etc
- Sign authdata
  - Similar to V1 SPI, for KDB backends that issue authdata
- Check transited realms
- Check policy before processing request
- Audit after processing request
- Check constrained delegation policy

Services4User in KDC

- Protocol transition (S4U2Self)
  - Service can get a ticket to itself on behalf of any principal
  - May use ticket for constrained delegation subject to policy
  - W2K3 variant only (W2K8 in 1.8)
- Constrained delegation (S4U2Proxy)
  - S1 wishes to authenticate to S2 on behalf of C
  - TGS-REQ { S1, S2, STkt(C, S1) }
  - TGS-REP { STkt(C, S2) }
  - Requires AD-like (DSfW) backend
- KDC-side support only
  - 1.8 has client library (service) support

1.8

- Services4User GSS API
- Naming extensions
- Principal lockout
- HDB shim

Services4User GSS API

- gss_acquire_cred_impersonate_name
  - Protocol transition
  - Returns a credential handle given a name
- gss_accept_sec_context
  - Constrained delegation
  - Always returns a delegated cred handle if
    - deleg_cred_handle != NULL
    - verifier_cred_handle has GSS_C_BOTH usage
  - No application changes required
  - Actual S4U2Proxy request done at context init
- krb5 API is not exposed
- No certificate protocol transition support yet

Naming extensions

- draft-ietf-kitten-naming-exts
- Attribute-based API for interrogating and setting authorization information
  - gss_inquire_name
  - gss_get_name_attribute
  - gss_set_name_attribute
  - …
- Attribute names are URIs (eg. urn:mspac:logon-info)
- Known authdata elements are always verified, however:
- Caller should check authenticated flag on returned attribute
- Builtin support for MS PAC
- krb5 SPI layer for new authdata types
- Sample code for AD-KDCIssued krb5 and KDC plugins for positive authdata
- Attributes set on initiator cred handle are sent in AP-REQ

Principal lockout

- Lock principal out after a certain number of preauthentication failures
- Roughly follow Windows / LDAP password policy model
- DB2 and LDAP support
  - DB2 lockout attributes are non-replicated
- Reuses existing KDB attributes
  - last_success
  - last_failed
  - fail_auth_count
- Extensions for lockout policy
  - pw_max_fail
  - pw_failcnt_interval (period after which fail_auth_count reset)
  - pw_lockout_duration (period after which account unlocked)
- Uses policy/audit hooks introduced in 1.7
- Changes to kadm5 and replication protocols

HDB bridge

- Load Heimdal database backends
- Also loads Heimdal windc plugins
  - windc_pac_generate
  - windc_pac_verify
  - windc_client_access
- Read/write support
- Samba4 with MIT KDC
- Test migrations
- kdb5_util dump –mkey_convert

Post-1.8: AES-CCM

- RFC 5116 section 5.3 / NIST 800-38
  - ENCTYPE_AES128_CCM_128
  - ENCTYPE_AES256_CCM_128
- Key derivation
  - Kc = DK(base-key, usage | 0xCC)
- AEAD
- Nonce/payload length is parameterized
- CCM implementation is cipher agnostic
  - src/lib/crypto/krb/dk/dk_ccm.c
  - New ciphers need only implement counter mode
- Tested with DCE RPC GSS mechanism
- users/lhoward/aes-ccm branch

1.7 references

- http://k5wiki.kerberos.org/wiki/Projects/DBAliases
- http://k5wiki.kerberos.org/wiki/Projects/Aliases
- http://k5wiki.kerberos.org/wiki/Projects/RFC_3244
- http://k5wiki.kerberos.org/wiki/Projects/RFC_4537
- http://k5wiki.kerberos.org/wiki/Projects/AEAD_encryption_API
- http://k5wiki.kerberos.org/wiki/Projects/GSSAPI_DCE
- http://k5wiki.kerberos.org/wiki/Projects/PAC_and_principal_APIs
- http://k5wiki.kerberos.org/wiki/Projects/GSS-API_mechanism_plug-in_support

1.8 references

- http://k5wiki.kerberos.org/wiki/Projects/Services4User
- http://k5wiki.kerberos.org/wiki/Projects/VerifyAuthData
- http://k5wiki.kerberos.org/wiki/Projects/Lockout
- http://k5wiki.kerberos.org/wiki/Projects/HDBBridge

Questions