Heimdal + Samba 4

=

True

Love Hörnquist Åstrand
Stockholm University, Samba Team

Heimdal

- Kerberos 5 implementation from Sweden
- Been in the works for over 10 years now
- Last major work has been PK-INIT support

History

- Samba 3 uses external Kerberos
- Samba 4 needs closer integration with both the Kerberos library and KDC
- Andrews Bartlett (with some help) did the first integration

Samba 4 needs

- Need its own KDC
- Kerberos library that system independent
- Work with someone that understands the Kerberos protocol

The Merge

- From the beginning the diff was LARGE
- Now we are down to about 200 lines
- Working on the merge for over 2 years now
- Describe the components that we modified

PAC

- Request no pac in AS-REQ
- KDC support - windc plugin to the KDC
  - The KDC handles keys, do the verifition and signs the request
  - The plugin only provides the PAC-data
- Server verifies the PAC (krb5_rd_req)

hdb backend

- Abstraction of the Kerberos database
- Supports: Berkeley DB (1.85, 3, 4), ndbm, gdbm, ldap
- Extended to allow database to save state inbetween operations

GSS-API

- DCE-STYLE GSS-API
  - Messages w/o ASN.1 pseudo header
- Message size confusion
- Work in progress, SSPI EncryptMessage with multibuffer/extra signed data

Referral support

- Two flavors, initial and service
- Allows email like login names
- Windows uses GC to find the user/service
- Windows clients always uses it cross realm
- Have been partly supported since forever in Heimdal for the cross realm case

SPNEGO

- Support the update SPNEGO, RFC 4178
- Inter-op tested with Microsoft and MIT
- Not currently used by Samba

AES for Vista ?

- Vista to vista in a 2003 domain uses AES ?

AES for Vista ?

- Vista to vista in a 2003 domain uses AES ?
- Yes, sends a ETYPE-NEG in ap-req(ap-data)

AES for Vista ?

- Vista to vista in a 2003 domain uses AES ?
- Yes, sends a ETYPE-NEG in ap-req(ap-data)
- Field is called EtypeList, list of enctypes

AES for Vista ?

- Vista to vista in a 2003 domain uses AES ?
- Yes, sends a ETYPE-NEG in ap-req(ap-data)
- Field is called EtypeList, list of enctypes
- Client announces supported enctypes in ap-req

AES for Vista ?

- Vista to vista in a 2003 domain uses AES ?
- Yes, sends a ETYPE-NEG in ap-req(ap-data)
- Field is called EtypeList, list of enctypes
- Client announces supported enctypes in ap-req
- Server generates a subkeys of selected type and since GSS-API uses acceptor subkey that subkey is selected

PK-INIT

- smartcard, usb dongles or files
- X.509 - raw RSA key supported by protocol
- heimdal includes a bignum and X.509 library
- Integrated into Samba4, is a samba4kinit distributed with samba

ntlm library

- GSS-API mechanism
- Delegates NTLM operation to KDC
- Not currently used by Samba
- Will add support for winbind

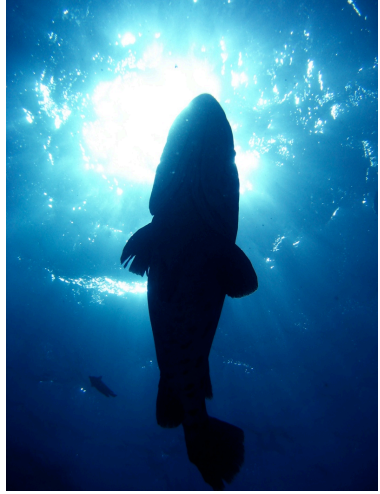
kx509

- Allows the KDC to issue X.509 certificates
- Certificates have a long lifetime as the tickets used to fetch the certificate
- pkcs11 clients that takes to the kca/kx509 and fetches certificates when they are needed

digest service

- Service forwards digest the request to KDC
- KDC verifies the request and returns the correct response
- Returns Kerberos tickets (if needed) in the reply, think WEB-DAV + AFS
- Uses Kerberos to secure the communications
- chap-md5, ms-chap-v2, ms-chap-v2, and sasl-digest

Future



- Complete referrals support, tgs-req missing
- SSPI support, EncryptMessage and friends
- Support different crypto back-ends (nss, evp)
- Test AES in Samba
- More integration with Samba4

Questions?