# Heimdal status

Love Hörnquist Åstrand, lha@h5l.org
Heimdal

# Heimdal

- Heimdal 1.4 - release status
- Heimdal 1.5 - new features
  - new protocols, networking, kcm, code-size
- What Heimdal version to use
- HDB backends

# Heimdal 1.4

- Released this week
- Native WIN 32 support
  - Thanks Asanka and Secure Endpoints!
- 10 times faster bignum library

# Heimdal 1.5

- new protocols
- networking
- kcm
- code-size

# Heimdal 1.5
# new protocols

- NTLM
- SCRAM-SHA1 (GSS-API and SASL)
- PK-U2U

# Heimdal 1.5
# NTLM

- Legacy protocol to talk to SMB servers
- Don’t use except for that

# Heimdal 1.5 SCRAM-SHA1

- Replacement to DIGEST-MD5
- Users of DIGEST-MD5 should start to migrate theirs servers today
- More secure, sever authentication, support real transport security (same as Kerberos)

# Heimdal 1.5
# PK-U2U

- Certificate based authentication
- Really just Kerberos with PKINIT
- Used to talk to Windows SMB servers running in PK-U2U mode
- Any certificate based system can use this

# Heimdal 1.5 networking

- kpasswdd support for TCP
- Replaced send-to-kdc code
    - Tries other KDC faster
    - Still listens on old replies

# Heimdal 1.5
# kcm

- kcminit - renew and refresh credentials in the background
- Fewer messages for common operations, faster then file caches

# Heimdal 1.5
# code size

- Uses new ASN.1 compiler by default
- New base library, libheimbase
  - objects, collection classes, ipc, signals
  - partly replaces libroken
  - enables more code sharing, smaller code

# Heimdal 1.5

- new protocols
- networking
- kcm
- code-size

# What Heimdal to use

- Many distributions are old (some run Heimdal 0.8, 3 years old)
- There are many bug fixes, you should run the latest major (or the .1 or .2)

# HDB backends

- Available backend today
  - ldap
  - db{1.85,3,4},
  - ndbm
  - sqlite (prototype)
- You should use db4 backend (since the others databases are broken)

# Databases broken

- db1.85 - like to corrupt the database with multiple writes
- ndbm - can’t handle large keys
- sqlite3 - should be default, not complete yet for production

# Questions ?