Heimdal Status Report

Jeffrey Altman

26 March 2014

State of the Project

- 34 contributors in last 12 months
  - Most in history of the project
- 127% year over year increase in commits
- Average age of the committers is increasing

Heimdal 1.5

- Last release 1.5.3; tagged Dec 2012
- 42 patches applied to heimdal-1-5-branch since
- Most important for this audience
  - DES exception for AFS service principals
  - Session key selection changes necessary for rxkad-k5 to work

1.6 is a Major Release

- New Features
- Improvements
- Bug Fixes
- Security Fixes
- Windows Updates

Features

- FAST (RFC 6113)
- HDB password history
- Cross-realm key rollover safety
- LDAP StartTLS
- DIR cred cache
- MIT/Heimdal KDB/HDB migration functionality

Improvements

- FILE cred cache improvements
- interop bugs (gss_pseudo_random())
- New plugin interface model
- kinit improvements
- Kx509 configuration options

Bug Fixes

- KDC 1DES session key selection
  - AFS rxkad-k5 compatibility
- Keytab file descriptor / lock leaks
- FILE cred cache corruption bugs
- GSS PRF+ interop bug
- TGS client requests failed to ask for renewable, forwardable, proxiable
- KDC handling of enterprise principals

Security Fixes

- kx509 realm-chopping security bug

Windows

- Redesign of Side by Side Assembly
  - Plugins must be part of the assembly
  - Otherwise, internal DLL Version conflicts
- Public SDK
  - Merge Modules available for third party integration
- kadmin client provided
- MIT KFW 3.2 shim libraries

What is Missing?

- libkafs supports neither rxkad-k5 nor rxkad-prf
- No FAST OTP implementation

HEIMDAL STATUS REPORT
2014 EAKC