secureendpoints

# Heimdal on Windows

Jeffrey Altman
Asanka Herath

# *Why Heimdal on Windows?*

- MIT has abdicated its role as promoter of GSS and KRB5 as cross-platform APIs
- No official MIT support for Win7/2008-R2 nor any 64-bit environments
- OpenAFS requires GSS PRF for rxgk
- It is much easier to get changes accepted to Heimdal than MIT

# What will be supported?

- GSS, KRB5 and com_err libraries
- No Kerberos v4 or 524
- Credential Cache Interface is pluggable
  - MSLSA and MIT API cache implementations from Secure Endpoints
- KDC to follow

# *High Performance Cryptographic Operations*

- Heimdal Crypto layer implemented on top of the Windows CryptoAPI
- Access to hardware devices
  - Smartcards
  - Hardware Secure Modules
  - Hardware Acceleration

# Distribution Model

- MIT deployed as a loose collection of DLLs discovered via the PATH
  - No support for multiple versions on the same system let alone the same process
- Heimdal distributed as an Assembly
  - Support for multiple versions on the same system
  - If Python and Perl are built against different versions, and both are loaded into IIS, that is ok.

# *Migration Strategy*

- GSS applications will just work
- For new KRB5 apps, SEI will provide a Heimdal compatibility SDK for application development
  - NetIdMgr and OpenAFS will build against the compatibility SDK
  - Use Heimdal assembly if available, otherwise failover to either MIT 3.2.x or 2.6.x if in the PATH
- For existing apps, SEI will provide a translation from MIT KRB5 ABI to Heimdal

# How Heimdal Compat SDK works

- Heimdal 1.4 API has been expanded to include many missing functions from MIT API
- Compat SDK is a pass-through to Heimdal KRB5
- For MIT, data structure and memory allocation conversion functions are provided
- Delayed loading of Heimdal assembly permits redirection to MIT libs on failure
- Requires recompilation of applications

# MIT Compatibility Library

- MIT krb5_32.dll/krb5_64.dll compatibility libraries will be provided
- The most commonly used functions will be implemented in first revision
  - Full export list to be supported
  - KRB5 errors returned if not implemented
- Most functions are pass-through to Heimdal

# *Availability*

- Windows support in Heimdal 1.4
- Secure Endpoints Installation Packages
  - Waiting on updates to OpenAFS, NetIdMgr
  - NetIdMgr 2.1 credential providers built against Heimdal Compat library
- Beta later this month
- Production releases in October

secureendpoints

secureendpoints

# All-in-One Installers and an Automatic Update Service

Reducing Complexity for End Users

# Too many dependencies

- On a 64-bit Windows system, end users require NetIdMgr, two OpenAFS installers, and two Kerberos installers in order to support both 64-bit and 32-bit applications
  - Additional NetIdMgr credential provider installers may also be required
- Different orgs develop different pieces
- Too complex for the end user

# All-in-One Installers and Update Services

- Secure Endpoints will begin shipping next month all-in-one installers that bundle open source and proprietary components
- An update service will provide automatic updates of all components based upon the subscribed policy
  - Nightly builds, beta release, official release, known stable release

secureendpoints

# Platform Detection

- The installation service automatically detects 64-bit and 32-bit Windows variants
- The appropriate version of software is offered to the end user

# Security

- The update client authenticates the update server
- Trusted tokens are used by the server to identify the client
- All installers are securely verified by server provided SHA-1 hashes
  - Install packages may be distributed from untrusted paths (web and afs)

# *Licensing*

- Update Services are licensed annually on a individual or organization basis
- Organizational licenses can include:
  - Site specific configuration for all products
  - Site branding for end users
  - Update publication for non-SEI distributed software packages
  - Software Support for SEI distributed software packages
  - Site specific update policies

secureendpoints

# Availability

- Closed beta in progress
- Send mail to update-support@secure-endpoints.com if you wish to join
- Public availability in the 4th Quarter 2010

secureendpoints

# Contact Information

Jeffrey Altman
jaltman@secure-endpoints.com