MIT Kerberos Enhancements for Samba

Vinayak Hegde,
Engineer, Novell, Inc.

Premalatha,
Senior Manager, Novell, Inc.

Michelle Escalante,
Product Manager, Novell, Inc.
Outline

• Samba - Kerberos integration

• Status of Samba requirements for MIT

• Design of Data Base Abstraction Layer

• Dependency on Specific Kerberos distribution

• Novell's work with MIT KDC

• Conclusion
Samba - Kerberos integration

- Samba3
  - Own implementation of Kerberos and GSSAPI
- Samba4
  - Not viable to recreate the development effort of Kerberos and GSS API implementation
  - Proposes to have explicit dependency on Heimdal libraries and installation
Some Kerberos improvements from Samba 3 to Samba 4

**KDC**
- KDC to query the Samba user DB
- Integrate PAC support
- Handle password changes

**Kerberos Client / Server**
- GSSAPI enhancements from Samba 3
- Changes in SPNEGO
- Threading issues with kerberos libraries
- Support for AES encryption type

**Installation & Build**
- Build samba libraries against the Kerberos libraries installed at a specified location / prefix

**Working Relationships with Kerberos team**
# Status of Some Samba requirements with MIT KDC

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Status</th>
<th>Contributed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSS API Changes</td>
<td>In progress</td>
<td>MIT</td>
</tr>
<tr>
<td>SPNEGO</td>
<td>Contributed</td>
<td>SUN</td>
</tr>
<tr>
<td>Thread safe Kerberos Libraries</td>
<td>Included in 1.4</td>
<td>MIT</td>
</tr>
<tr>
<td>Database Abstraction Layer</td>
<td>Contributed</td>
<td>Novell</td>
</tr>
</tbody>
</table>
This release builds on work introduced in Kerberos 1.4 and focuses on better active directory interoperability and support for the needs of enterprise operating systems.

Support for the SPNEGO mechanism will be added, allowing better Microsoft interoperability, support for evolving security protocols and dynamic selection of security mechanisms.

Support for multiple KDC backends including LDAP will be added. This provides for integration of Kerberos into enterprise account management and identity management solutions as well as supporting Novell's plans to base their authentication solution on MIT Kerberos.

This release depends on cooperation and code contributions from Sun, Novell and Apple.
Objective

- Support for Database plug-ability allowing use of external back-end stores

Helps Samba because ..

- Through DAL, Samba's database (LDB) can be plugged into MIT Kerberos easily
- Small learning curve as it is similar to hdb
Samba with MIT Kerberos

- Samba Client
- Samba Server as AD DC
- MIT KDC
- DAL
- DB2
- LDAP
- LDB
- LDAP Server
Database Abstraction Layer (cont'd)

DAL facilitates the following

- Load and Initialization of a DB module
- Flexibility for DB module configuration
- Set up and tear-down of DB connection
- Defines what are the Mandatory functions
- Provides interface for Optional functions
Database Abstraction Layer (cont'd)

Mandatory functions for module

- DB connection management
- Realm creation and destruction
- DB lock/unlock
- Principal management

Optional Functions

- Realm master key management
- Policy management
Example of an Enterprise deployment of Samba with Kerberos

Applications

MIT Kerberos

Heimdal

Samba

Identity store

LDAP Server

eDirectory, A/D etc.

RDBMS

Oracle, DB/2, etc.
Dependency on Specific Kerberos distribution

• Less freedom to choose the Kerberos that fits
  • Administrative nightmares
    - Two sets of Administration utilities
    - Multiple user databases
    - Co-existence issues
    - Complicating the Kerberos story further
Novell's work with MIT KDC so far …

Novell's association with MIT Kerberos

- Novell is integrating Kerberos with eDirectory based on MIT Kerberos
- We made a switch from a proprietary distribution to MIT
- SuSE also made a switch from Heimdal to MIT Kerberos from SuSE 9.3

Novell's contributions to MIT Kerberos

- DAL (Database Abstraction Layer) design and implementation
  - Design reviewed by members from MIT, SUN & PADL
  - The code is being contributed to MIT Kerberos
- Multi threading for KDC Server (in progress)
- A crypto layer for pluggable crypto functions
- LDAP backend for replacing DB2
- Standardization of Kerberos LDAP Schema (in progress)
Conclusion

Next steps

• More discussions to fill in the gaps in requirements
• Interactions / communications mechanisms(#samba-technical, krbdev@mit.edu)
• Convenient time for real time discussions
Questions ?