Developing Plug-ins for Network Identity Manager

Asanka Herath
Agenda

- What's NetIDMgr?
- Role of plug-ins in NetIDMgr
- Resources available for developing plug-ins
- Requirements
- Walk-through
- Q and A
What is NetIDMgr?

- Introduced as Khimaira at the BPW 2005
- A unified user-interface for Kerberos and AFS credentials management on Microsoft Windows
<table>
<thead>
<tr>
<th>Identity</th>
<th>Type</th>
<th>Service Name</th>
<th>Time Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>asanka@ATHENA/MIT.EDU (Default)</td>
<td>Kerberos 5 tickets</td>
<td>afs/sipb.mit.edu@ATHENA/MIT.EDU</td>
<td>9 hours 54 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>afs/athena.mit.edu@ATHENA/MIT.EDU</td>
<td>9 hours 54 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>kbtgt/ATHENA/MIT.EDU@ATHENA/MIT.EDU</td>
<td>9 hours 54 minutes</td>
</tr>
<tr>
<td></td>
<td>AFS tokens</td>
<td>afs/sipb.mit.edu</td>
<td>9 hours 54 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>afs/athena.mit.edu</td>
<td>9 hours 54 minutes</td>
</tr>
<tr>
<td></td>
<td>Kerberos 4 tickets</td>
<td>kbtgt/ATHENA/MIT.EDU@ATHENA/MIT.EDU</td>
<td>9 hours 54 minutes</td>
</tr>
<tr>
<td>nobody@TEST.HEIMDAL-0.6</td>
<td>Kerberos 5 tickets</td>
<td>kbtgt/TEST-HEIMDAL-0.6@TEST-HEIMDAL-0.6@TEST-HEIMDAL-0.6</td>
<td>9 hours 59 minutes</td>
</tr>
<tr>
<td>nobody/instance@TEST-KERBEROS-1.3.1</td>
<td>Kerberos 5 tickets</td>
<td>kbtgt/TEST-KERBEROS-1.3.1@TEST-KERBEROS-1.3.1@TEST-KERBEROS-1.3.1</td>
<td>9 hours 59 minutes</td>
</tr>
<tr>
<td>nobody@TEST-KERBEROS-1.3.1</td>
<td>Kerberos 5 tickets</td>
<td>kbtgt/TEST-KERBEROS-1.3.1@TEST-KERBEROS-1.3.1@TEST-KERBEROS-1.3.1</td>
<td>9 hours 59 minutes</td>
</tr>
</tbody>
</table>
asanka@ATHENA.MIT.EDU - New credentials

Username: asanka
Realm: ATHENA.MIT.EDU
Password for asanka@ATHENA.MIT.EDU

Credentials:
Selected identity: asanka@ATHENA.MIT.EDU
This identity is the default
Krb5: Creds for realm ATHENA.MIT.EDU
AFS: Tokens for cells athena.mit.edu, sipb.mit.edu
Krb4: Tickets for realm ATHENA.MIT.EDU

Identity  Kerberos 5  AFS  Kerberos 4

Ok  Cancel
NetIDMgr Design Goals

• Provide the functionality of AFSCreds and Leash
  – User friendly
  – Minimize required knowledge
  – Intuitive

• Extensible
  – Plug-in based
  – Easy to add support for new credential types and new functionality

• Easy to maintain
NetIDMgr Plug-ins

- NetIDMgr doesn't have any knowledge of any type of credentials or identities
- All support for credentials types and identities are provided by plug-ins
- The application provides a framework on which the plug-ins function
Architecture Overview

- User Interface
  - Configuration Provider
  - Credentials Database
  - Error reporting/Alerts
  - Plug-in manager
  - Kerberos 5
  - Kerberos 4
  - AFS
  - ...

Message Queue
Message Queue

• NetIDMgr is message based
• Per thread message queues
  – (also, per plug-in)
• Manages all the communication between NetIDMgr and plug-ins
• Sync, async, scatter-gather, broadcast, multicast, unicast
Configuration Provider

- Layered configuration stores
  - User, machine, schema
- Overlapping configuration spaces
  - Overlapped parameters for different levels of scope
- Backed by Windows Registry
  - Allows settings to be deployed via Group Policy
Configuration Provider

- User configuration store (per user)
- Machine configuration store (per machine)
- Schema store (defaults and schema defs)
- Shadowed configuration space
- Abstract configuration space
Error Reporting

• Collects event information including debugging information from multiple threads
• Automatically handles reporting of error conditions to the user
Plug-in Manager

- Manages
  - Loading and unloading of plug-ins
  - Localization
  - Registration of plug-ins
  - Plug-in execution threads
User Interface

• NetlIDMgr is a “tray application”
  – Conservative about UI

• Plug-ins provide delegates for handling UI
  – Specific operations require special delegates (E.g.: acquiring new credentials)

• Plug-ins can request user interaction, if necessary
Types of Plug-ins

- Credentials Providers
  - Registers credentials types
  - Provides a list of credentials that currently exist
  - Respond to credentials messages
    - Refresh the credentials list
    - Obtain new credentials
    - Renew credentials
    - Etc...
Types of Plug-ins

• Identity Providers
  – Provide and manage identities on behalf of NetIDMgr
Types of Plug-ins

• Other
  – No inherent constraint on plug-in type
    • (Assigning a type allows NetIDMgr to manage message subscriptions. Exception: Identity providers)
  – A plug-in can listen for specific messages it is interested in and respond accordingly
Available Resources

• The KfW 3.1 SDK Developer Documentation (distributed as part of the SDK)
• A set of samples and templates for developing NetIDMgr plug-ins
• Source for the Kerberos 5, Kerberos 4 plug-ins (available with the KfW source)
• Source for the OpenAFS plug-in (available soon)
Development and Build Requirements

- NetlDMgr SDK (part of KfW 3.x SDK)
- Microsoft Platform SDK (Windows Server 2003 SP1 or later)
- Microsoft Visual C++ Compiler (version 13 or later)
Walkthrough of Plug-in Development

• Provide module entry points
  – Setup localized resources
  – Register plug-ins
Walkthrough of Plug-in Development

• Provide message handlers
  – Handle system messages
    • Register credentials types, data types, properties, configuration panels, schema, etc...
Walkthrough of Plug-in Development

- Provide message handlers
  - Handle credentials messages
    - Refresh, change notifications, new credentials acquisition, credential renewals, destroying credentials, etc...
Walkthrough of Plug-in Development

• Provide UI delegates
  – Credentials operations
  – Configuration
Walkthrough of Plug-in Development

• Provide message handlers
  – For any other messages as required by the plug-in
Questions

Asanka Herath
asanka@secure-endpoints.com