Content Management and CIFS:
playing together in Intranet

Alexander Bokovoy
ab@samba.org

Samba Team
The Midgard Project
Agenda

- Overview
- Single sign-on
- NTLMSSP over HTTP for Unix applications
- Midgard Content Management framework
- NTLMSSP support in Midgard
- What's To Do?
- Acknowledgements
Overview

Few facts:

- Most companies do run internal CIFS-enabled networks

- Most companies do have internal Web-based applications

- The same users utilise both CIFS resources and internal Web-based applications

- There is a need for user administration in both cases
Overview: *Microsoft Windows environment*

In Microsoft Windows-based environments:

- MS Internet Explorer can send authorization information based on user's domain logon credentials

- MS Internet Information Services is capable to verify authentication information against domain controller

- Same applies to MS Proxy and some other products
Single Sign-On

By using those products developer can implement a feature called "Single Sign-On" for their Intranet Web-based applications

Pros:
- User is authenticated only once, at logon time
- Once authorized, user doesn't need to enter password multiple times for different applications
- A centralized approach can be used for setting and changing privileges, keeping sensitive information in one place

Cons:
- Highly depends on an availability of a Microsoft products on both client and server side
In a mixed environments (Unix-like servers and Windows clients) on a server side:

- Squid proxy server can be used to authenticate users against domain controller

- A number of modules for Apache provides (incomplete and sometimes broken) support to authenticate against domain controller

- There is a number of Java-based components to provide similar functionality for J2EE applications
Single Sign-On: Mixed environments

In a mixed environments on a Windows client side:

- **MS Internet Explorer 4+** can be used to send authorization information to a server requested NTLM authentication scheme
- **Mozilla 1.4 alpha** can be used to achieve the same goals natively since late March'03
- **Mozilla < 1.4 alpha** can be used with a third-party Python-based module

In a mixed environment on a Unix-like client side:

- **No browser is known to work with NTLM authentication scheme yet**
NTLMSSP over HTTP
Midgard content management framework

What is Midgard?

- Web Application Server
- Content Management System
- PHP Development Environment
- Layout Controlling Tool
Midgard content management framework

Key Benefits

- Integrates seamlessly with Apache
- Uses the PHP scripting language (PHP3 and PHP4 supported)
- WebIWYG Management System
  - Platform independent, works with any Web browser
- Completely free, Open Source
  - Uses the GPL, LGPL and MIT licenses

www.midgard-project.org
Midgard architecture
NTLMSSP support in Midgard

- Uses ntlm_auth from Samba 3.0 to get NTLMSSP server work
- Generalized NTLMSSP processor is in libmidgard
- HTTP-specific part is in mod_midgard
- Allows both NTLMSSP and Basic authentication
- No changes in underlying web site code at all
NTLMSSP support in Midgard

Apache module provides:
- a configurable map between domains and Midgard's site groups (a collection of sites isolated from other sites)
- user privileges mapping for exception cases (how do we live without them?)

Midgard library provides:
- a generalized NTLMSSP processor which communicates with ntlm_auth
- tight integration with Midgard's own authorization facilities
NTLMSSP support in Midgard

When user is authenticated against a domain controller:

- a policy definition process is started:
  - convert domains into site groups
  - raise or low priviledges depending on an account state

- a short-path authorization in Midgard database is performed:
  - no password check (already done during NTLMSSP exchange)
  - user existance check
  - user priviledges are raised or lowered depending on a policy check result
NTLMSSP support in Midgard

When user is failed to authenticate against a domain controller:

- a Basic authentication fallback is provided
- user is asked to enter its conventional Midgard credentials
- a normal Midgard authorization path is performed
Known caveats in NTLMSSP over HTTP support

- Internet Explorer has broken behaviour w.r.t. authentication in some versions

- Cannot be proxed through, direct Keep-Alive connection is required for whole session

- Samba 3.0 winbinddd uses a priviledge separation on a pipe, there is an additional configuration effort for administrators
**ToDo work**

**Short period:**
- support Apache 2
- develop a generic `mod_samba_ntlm_auth` module for Apache:
  - use `ntlm_auth` interface to keep implementation details of Winbind isolated in Samba source tree

- develop (de)multiplexor mode for `ntlm_auth`:
  - handle multiple simultaneous requests on the same pipe
  - support 1:N model of Squid and Apache 2
  - be compatible with existing Squid and Midgard one user at time protocol

- add support for fetching group membership through `ntlm_auth`:
  - deal with INFO3 groups info
  - add a proper generic INFO3 caching
Todo work

Long period:

- create SAML-aware NTLMSSP authentication

- support other Content Management Systems (Zope, RH CMS, ...)

Acknowledgements

Persons:
- Andrew Bartlett / Samba team
- Francesco 'Kinkie' Chemolli / Squid Team

Companies:
- Nemein Oy, Finland
- SaM Solutions Ltd., Belarus