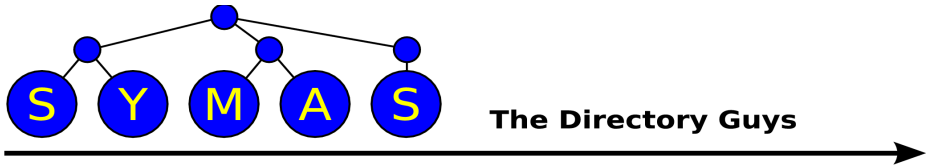
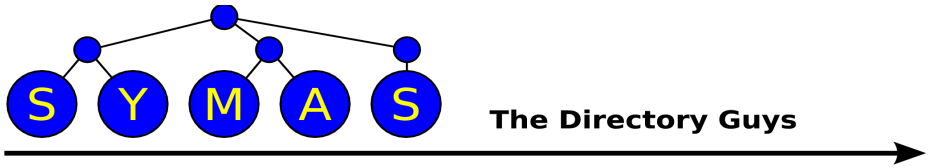


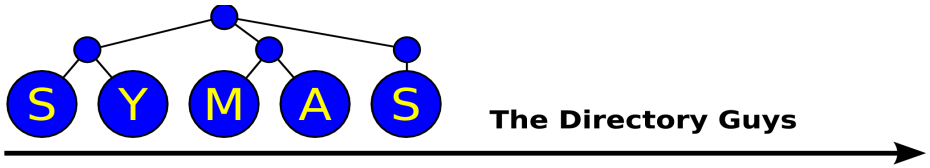
Kerberos and OpenLDAP

Howard Chu
CTO, Symas Corp. hyc@symas.com
Chief Architect, OpenLDAP hyc@openldap.org
October 21, 2009



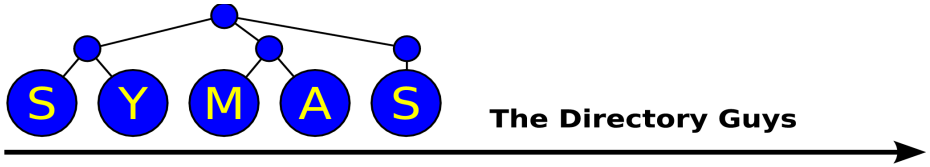
OpenLDAP Project

- Open source code project
- Founded 1998
- Three core team members
- A dozen or so contributors
- Feature releases every 12-18 months
- Maintenance releases roughly monthly



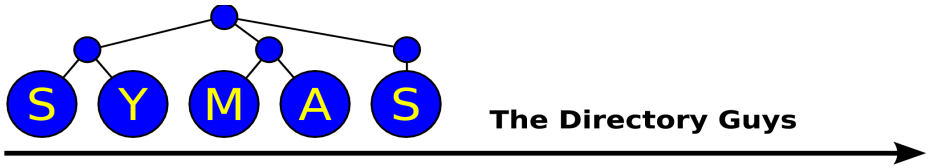
A Word About Symas

- Founded 1999
- Founders from Enterprise Software world
  - *platinum* Technology (Locus Computing)
  - IBM
- Howard joined OpenLDAP in 1999
  - One of the Core Team members
  - Appointed Chief Architect January 2007



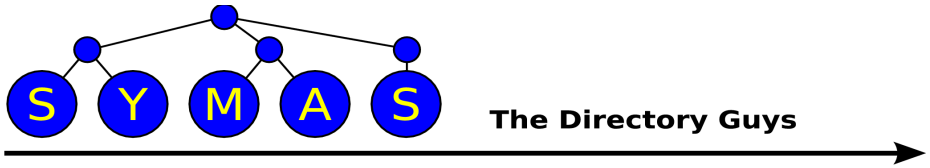
Topics

- Overview
- Current Status
- Related Work
- Future Directions



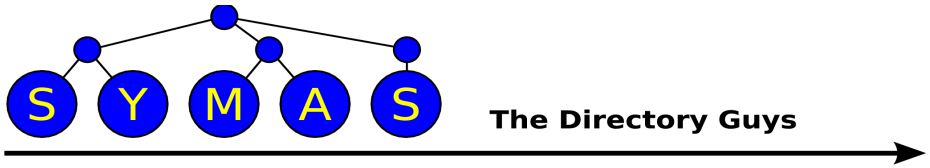
Overview

- Both Kerberos and LDAP are commonly used for authentication in distributed computing systems.
- While there's generally some overlap in the set of entities for whom authentication data is maintained, Kerberos servers and LDAP servers tend to be maintained separately.
- It's desirable to unify the two systems to minimize duplication of data, administrative overhead, and development/design effort.



Current Status

- An OpenLDAP backend has been available in Heimdal since 1999.
  - Written by Luke Howard @ PADL.
  - Adds KDC data to LDAP account entries, allowing unified administration of accounts.
  - Keys are distinct attributes, not used in LDAP authentication.
  - Uses IPC to connect to local slapd (ldapi:// scheme) thus avoiding chicken'n'egg credential problem.

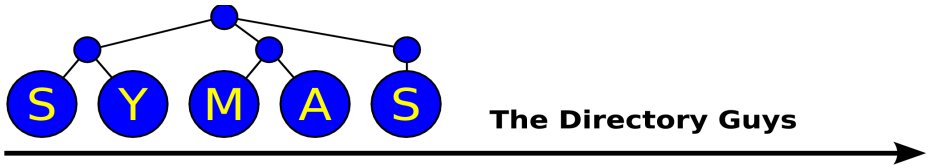


Current Status

- Additional module to unify LDAP, Samba, and Kerberos authentication added to OpenLDAP in 2004.
  - Written by Howard Chu @ Symas.
  - SLAPI version contributed to Red Hat, May 2006.
  - Can directly authenticate LDAP users against the KDC keys.
  - Generates Samba3 NTLM and Heimdal keys when LDAP password is changed.
  - Also supports Samba3 password expiration.
  - No other support for password policies.

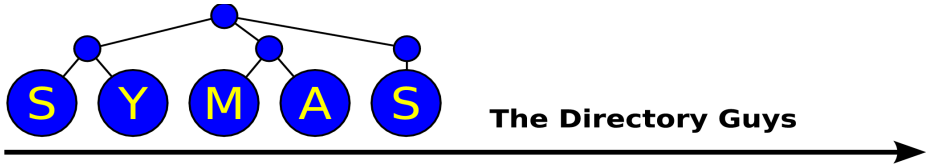
Related Work

- Password Policy
  - Draft-behera-ldap-password-policy-09 currently implemented
  - Supports password aging, reuse control, lockouts, mandatory resets, pluggable quality checks, grace logins, etc.
  - The spec was written to accommodate use from other systems such as SASL and Kerberos, but this is not currently implemented.



Related Work

- Password Policy...
  - Draft-behera-ldap-password-policy-10 currently being edited by Howard Chu and Ludovic Poitou.
  - Adds failure rate controls, plus additional policy and state variables to support the Kerberos KDC Information Model et al.
  - Requirements are also being fed back to the ISO X.500 Standards Body to maintain parity with X.500.

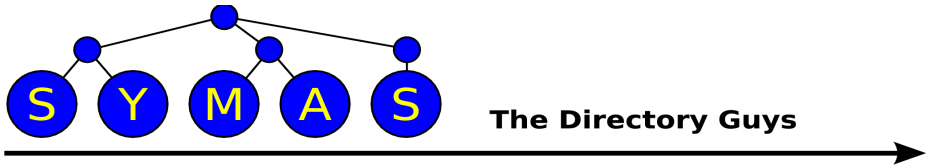


Related Work

- Standard KDC Schema
  - Draft-chu-ldap-kdc-schema-00 just published.
  - Based on KDC Information Model.
  - Leverages LDAP Password Policy spec.
  - Aimed to allow interoperability between Heimdal and MIT KDCs at the LDAP database level.

Related Work

- Integrated PAM/NSS support
  - Nssov module services PAM and NSS requests using a client stub and an IPC listener
  - Avoids namespace collision issues of existing pam_ldap/nss_ldap solutions
  - Supports fine-grained authorization using slapd ACL engine
  - Can be combined with replication or proxycaching to provide immunity to network outages / support disconnected operation



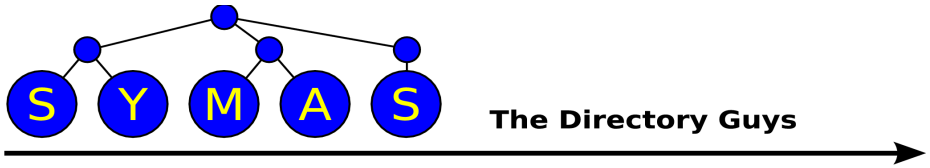
PAM Authorization

- Example host entry

```
dn: cn=hostX,ou=hosts,dc=example,dc=com
objectClass: ipHost
objectClass: authorizedServiceObject
cn: hostX
ipHostNumber: 192.168.1.127
authorizedService: sshd
authorizedService: ftp
```

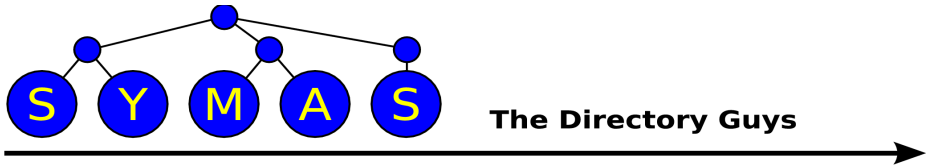
- Sample Access Control rule

```
access to dn.subtree=ou=hosts,dc=example,dc=com
  attrs=authorizedService val.exact=sshd
  by group.exact="cn=admins,ou=groups,dc=example,dc=com" write
  by peername.ip=198.207.56.0%255.255.255.0 read
  by * none
```



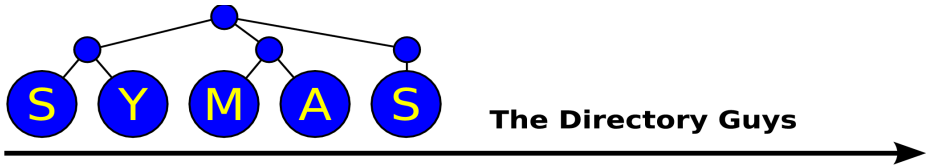
Certificate Authority

- Simplified, automated certificate generation
  - Automatically issued to the currently bound user's DN and stored in their entry - no need for certificate request objects
  - Certs can be generated with short lifetimes for single-use or short-time usage - analogous to Kerberos tickets
  - Implemented in an overlay, triggered by a search request on the user's entry and userCertificate attribute with magic filter parameters



Certificate Authority

```
ldapsearch -x -H ldap://my-server -ZZ
 -D cn=someone,dc=example,dc=com
 -w goodpassword
 -b cn=someone,dc=example,dc=com
 -s base
 (&(startDate=200909212245Z)
     (endDate=200909212300Z))
  userCertificate userKey
```



Certificate Authority

```
ldapsearch -x -H ldap://my-server -ZZ
 -D cn=manager,dc=example,dc=com
 -w secretpassword
 -e authzid=cn=hostX,ou=hosts,dc=example,dc=com
 -b cn=hostX,ou=hosts,dc=example,dc=com
 -s base
(&(startDate=200909211800Z)
  (endDate=201109211800Z)
  (subjectAltName=DNS:bighost))
  userCertificate userKey
```

Future Directions

- Further integration work with MIT and Heimdal Kerberos projects
- Implement Password Policy checking for Kerberos and SASL authentication
- (Notice that a lot of future work is peripheral to OpenLDAP. We've succeeded in building our core functionality and are bugging other projects now while still managing to avoid writing an OpenLDAP GUI...)

ProxyCache Enhancements

- "Offline" mode - suspends cache expiration while the remote server is unreachable
- Time To Refresh - cached entries that have been referenced and aren't expired are automatically re-fetched after a certain age
- Bind caching - credentials used in a Simple Bind are hashed and stored for satisfying subsequent Bind requests
- Cached credentials have a separately configured Refresh period

ProxyCache + nssov

- Seamless authentication + authorization
- Configuration managed centrally, only a stub is exposed
  - actual configuration can be distributed via syncrepl, for painless automatic maintenance
- Multiple options for availability / disconnected operation, using syncrepl or proxy + cache
- Natural integration with LDAP Password Policy