Security with LDAP

Andrew Findlay
Skills 1st Ltd

www.skills-1st.co.uk
February 2002

andrew.findlay@skills-1st.co.uk

Security with LDAP

- Applications of LDAP
  - White Pages
  - NIS (Network Information System)
  - Authentication
- Lots of hype
- How much of it works?

andrew.findlay@skills-1st.co.uk

Network Information Service

- Many in service:
  - YP/NIS
  - DNS / Hesiod
  - WINS
  - LDAP
- Maps:
  - passwd, group
  - automount, services, protocols
- Map from a *key* to a *value*
- Give reliable answers

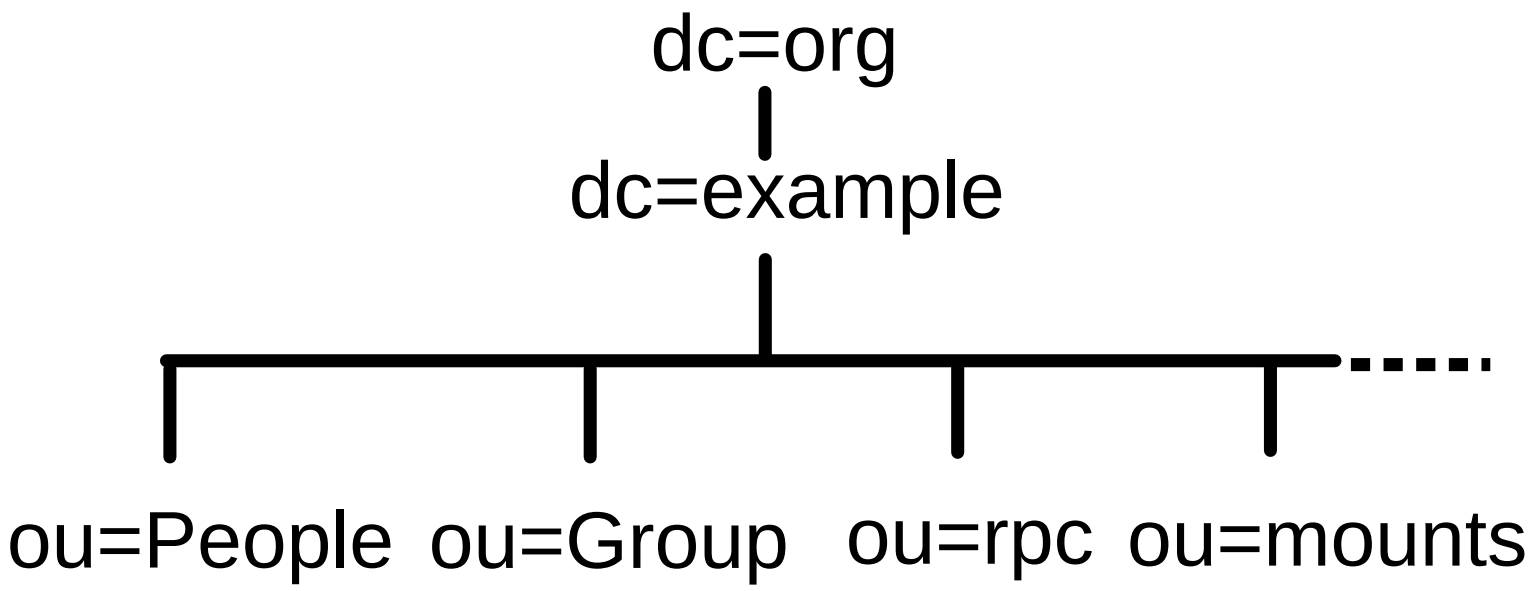
andrew.findlay@skills-1st.co.uk

Authentication Service

- Get password hash from NIS, check locally
- Authentication protocol
  - RADIUS
  - TACACS+
  - Kerberos
  - POP
  - LDAP
- Avoid exposing password in cleartext
- Protect authentication data from rogue clients

andrew.findlay@skills-1st.co.uk

LDAP structure: the tree



andrew.findlay@skills-1st.co.uk

Skills 1st

LDAP structure: person entry

```
dn: uid=andrew,ou=People,dc=example,dc=org
uid: andrew
cn: Andrew Findlay
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/andrew
gecos: Andrew Findlay
userPassword: {crypt}$1$HkYw.fgh$...
```

andrew.findlay@skills-1st.co.uk

Test environment

- Red Hat 7.1 on laptop
- OpenLDAP 2.0.18
- PADL migration tools
- Client OS mostly in VMware virtual machines
  - Red Hat 7.2
  - FreeBSD 4.4
  - SuSE 7.0
  - Mandrake 8.1
  - Solaris 8
- Aim to centralise all user management data

andrew.findlay@skills-1st.co.uk

Name Service Switch

- NSS in Linux and Solaris: dynamic shared libraries
- Linux uses nss_ldap module from PADL
- Solaris has similar module using Netscape LDAP
- Limited support in FreeBSD
- Configure in /etc/nsswitch.conf:

```
passwd: files ldap
group: files ldap
hosts: files dns
```

- Simple config in /etc/ldap.conf:

```
host ldap.example.org
base dc=example,dc=org
```

andrew.findlay@skills-1st.co.uk

Authentication with LDAP

- Search for entry holding username
- Bind to LDAP server as that DN to verify password
- Other forms of credential are possible
- PAM: Pluggable Authentication Modules
- pam_ldap from PADL
- Solaris, FreeBSD and Linux (may be old version)
- Shares /etc/ldap.conf with nss_ldap (Solaris is different)
- PAM config in /etc/pam.d/* or /etc/pam.conf
- Handles password updates too

andrew.findlay@skills-1st.co.uk

Now add Windows...

- Samba will use nss_ldap and pam_ldap
- Can do better: configure with option --with-ldapsam
- Samba PDC now stores all data in LDAP entries
- Add SMB parameters:

  `smbpasswd -a <username>`

  - NT and LANMAN password hashes
  - RID
  - Location of home and profile store
- Experimental code
- Who needs BDCs?

andrew.findlay@skills-1st.co.uk

Tighter Security

- ACLs to protect passwords
- Transport Layer Security (TLS / SSL)
  - Create a Certification Authority key and cert.
  - Sign LDAP server certificate with CA key
  - Server needs key and certificates
  - Client needs CA certificate
  - TLS encrypts traffic and authenticates server
- Can use client certificate in place of password
- Need recent pam_ldap and nss_ldap
- Not yet implemented in automount, AMD etc

andrew.findlay@skills-1st.co.uk

Performance

- NSS and PAM put more load on server than typical browser
- Up to 8 connections and 13 searches just to login
- More recent versions are better
- SLAPD can do 500 searches / second easily
- Watch out for CPU load from TLS
- Add replica servers

andrew.findlay@skills-1st.co.uk

Management tools

- Not much choice yet
- PADL migration tools
- Script using OpenLDAP tools or Perl modules
- GQ
- sourceforge.net/projects/ldaputils

andrew.findlay@skills-1st.co.uk

Summary

- LDAP is a viable Network Information Service
- Current Linux distros easy to set up as clients
- Solaris takes some effort with OpenLDAP server
- FreeBSD has partial support
- Build nss_ldap and pam_ldap from latest source for best security
- Management tools a bit thin
- Security can be very good

andrew.findlay@skills-1st.co.uk

Security with LDAP

Andrew Findlay
Skills 1st Ltd

andrew.findlay@skills-1st.co.uk
www.skills-1st.co.uk