Lorikeet – Integrated Authentication

Who am I?

- 'Student Network Administrator' at Hawker College
- Samba Team
- Authentication in the real world
  - 800 students
  - 170 client computers
    - Win NT, Win2k, WinXP
  - Single sign on, Samba domain

Move along – nothing to see here

- Nothing in this presentation is particularly new
- But nobody seems to be integrating it
  - Except Microsoft
- Directory integration seems particularly lacking

The Holy Grail

- One password
  - Legacy NT passwords in particular
  - Directory storage and Integration
- Secure login systems
- Not acceptable:
  - Custom 'password change' web pages
  - Overnight 'password sync' delays
  - Fixed passwords

Too Many Protocols...

- CIFS
- HTTP
- LDAP
- IMAP
- POP
- SMTP
- TELNET
- RPC
- MAPI
- And these are just the protocols that Microsoft have done single-sign-on for

Starting assumptions

- Hard to get the passwords:
  - Locked up in a Windows PDC
  - NT and LM hashes only
- Still allows:
  - Plain text
  - NTLM
  - MSCHAP (PPP)
- Uses only a **normal** machine trust account in the domain

Plain text Authentication

- If we have the plain text, the game is easy
  - pam_winbind
  - ntlm_auth 'basic' authentication modes.
  - Integrating PAM, SSH etc into windows domains
  - LDAP simple bind -> SASL -> winbindd
- Still 'single source of password'
  - User still uses their windows password
  - Not 'single sign on'
- Exposes passwords on the network

Using pam_winbind

- Killing the 'password sync'
  - Rather than 'sync' your passwords, just always ask the Domain Controller
  - This works, on a DC just as much as a member server
- PAM Module
  - This means POP/IMAP, HTTP (mod_auth_pam), SSH etc
- Possible:
  - 'LDAP authentication' for Linux workstations

NTLMSSP

- Single Sign on
  - Uses the windows password
- Challenge-response authentication
  - No passwords on the wire
- Unprompted authentication
  - About the only good reason to use this abomination...

NTLMSSP in Squid

- 'Transparent' proxy authentication
  - Users are not aware that they are being authenticated
- Supported Browsers:
  - IE
  - Mozilla 1.5 (1.6 all platforms)
- ntlm_auth is an NTLMSSP 'helper' in squid
- Users are 'virtual', do not need to be unix users

ntlm_auth

- The external interface to Samba Authentication
- A number of ways to authenticate
  - Plaintext
  - NTLMSSP
  - MSCHAPv2

VPN integration

- Integrated 'PoPToP' VPNs into Windows domains
  - Allows unmodified windows clients to contact a Linux VPN server.
- pppd modified to call ntlm_auth
  - Previously pppd could not integrate against a windows domain
- Now done:
  - Integrate FreeRadius with ntlm_auth

ntlm_auth in other projects

- ntlm_auth provides a generic interface
  - NTLMSSP client and server
- Cyrus-SASL patch
  - IMAP
  - SMTP
- Midgard

Kerberos is better

- Could be considered the 'original' single sign on
- Microsoft extended it (as usual)
  - NT4 can be upgraded to kerberos, without changing passwords
- Already widely supported on Unix
- Existing work for Kerberos in LDAP

Having the NT and LM passwords

- Allows
  - Plaintext
  - NTLM
  - MSCHAP
  - **Kerberos**
- Still does not allow:
  - Generic Cyrus-SASL
  - Digest-MD5

The Heimdal patch

- Heimdal post 0.6 snapshots includes most of my Samba interoperability patch
- If configured at a Samba LDAP store
  - Uses Samba passwords
  - Honors Samba password expiry
  - Honors Samba account control entries

Single Sign On example

- All these services using one password:
  - Kerberos (Heimdal)
    - Reading the 'samba' password entries
  - LDAP
    - Both Simple and Kerberos SASL binds
  - pam_ldap clients
    - Because LDAP supports the simple bind
  - Samba
    - Reading the Samba passwords

SSO Example – Cyrus SASL

- Cyrus SASL is used by many server applications
- Supports 4 authentication mechanism's:
  - NTLMSSP
  - KERBEROS
  - SPENGO
  - PLAIN

Resources

- My VPN integration paper
  - http://hawkerc.net/staff/abartlet/comp3700
- LDAPv3 HOWTO
  - http://www.bayour.com/LDAPv3-HOWTO.html
- Lorikeet
  - www.samba.org/samba/subversion.html – SVN module 'lorikeet'
  - https://sec.miljovern.no/bin/view/Info/HeimdalKerberosSambaAndOpenLdap