What this talk is about

- Making Windows Active Directory and Linux work nicely together
  - Why would you want to do that
  - Some tech points about AD

- Different ways of doing it
  - Some free, some cost
  - Pros and cons

- Recommendations and guidelines

- Mainly about OS logon (ssh, telnet, ...)
  - A little bit about web
Assumptions

• #1 you are in an environment that uses AD
  • ~80% of medium to large businesses

• #2 you are not happy with your current Linux/Unix/Mac Auth setup
  • Security, scale, ‘it’s a mess right now’, SOX, HIPAA, PCI, ....
  • You might be happy but others (PHBs, Auditors, ...) are not

• #3 you think AD might be a solution
  • Or it has been strongly ‘suggested’ that you should do it

So now what?
What are we trying to achieve

- Security
  - Strong encryption, no pw hashes on the wire, ...
- Centrally manage users
  - adding new users to machine (no more /etc/passwd editing)
  - Single click disable
  - scalable
- Single Sign on – same user and password everywhere
  - Zero sign on: sign on once and never type user and password again
- Auditable
- Central reporting
- Consistent password policy
You probably have something like this

- AD for Windows
- NIS, /etc/passwd, perhaps LDAP for UNIX
- Who knows what for Web etc
Problems with that mixed environment

- Unix admins spend too much time provisioning users
- Hard to keep of track of – no central reporting
- No password policies – force change after 30 days ...
- Insecure – NIS hashes on the wire for example
- Fragile – home grown scripts to manage it
- Forgotten passwords
- Shared accounts
- No audit
- Computer & DNS trust
How about Meta-Directory / Synchronization

Master directory

Things just got a lot more complex!

Where is the trust?

Windows

Active Directory

Unix

NIS / NIS+ Domain

Linux

LDAP Domain

Mac

Locally Managed

Java/Web

Locally Managed
OpenSSH Host Key Exchange

PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Yes  No  Cancel  Help
OpenSSH Key Distribution

- Force users to memorize host key-pairs
OpenSSH Key Distribution

- Host
  - Automate Public Key Distribution
  - Ignore the problem...

- User
  ```bash
  client$ mkdir ~/.ssh
  client$ chmod 700 ~/.ssh
  client$ ssh-keygen -q -f ~/.ssh/id_rsa -t rsa
  Enter passphrase (empty for no passphrase): ...
  Enter same passphrase again: ...
  client$ chmod go-w ~/
  client$ chmod 700 ~/.ssh
  client$ chmod go-rwx ~/.ssh/*
  client$ scp ~/.ssh/id_rsa.pub server.example.org:
  # next, setup the public key on server
  server$ mkdir ~/.ssh
  server$ chmod 700 ~/.ssh
  server$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
  server$ chmod 600 ~/.ssh/authorized_keys
  server$ rm ~/.ssh/id_rsa.pub
  ```
Or you could just use AD

It sure looks simpler!
Microsoft Active Directory

- Released by Microsoft in 2000
- Derived from DCE
  - LDAP instead of DAP
  - Kerberos V instead of Kerberos IV
  - MS RPC developed from DCE RPC
- Ease of Administration
  - User, group and computer administration
  - Automatic DNS configuration
  - Simple multi-master replica deployment
More AD Features

- Multiple separate trees – a ‘forest’ – that all know about each other.
- Sophisticated Trust configuration
- Secure DNS updates
- Multi-master update and replication
- Global catalog
- Strong password policy (forced change rate, complexity rules, ..)
- Support SASL and SSL security (defaults to SASL/GSS signed data streams)
- Very easy to set up (many users don’t even realize they have LDAP and Kerberos)
- Well designed RBAC API and schema (AzMan)
Yes but …

• Is it really LDAP?
  • Fully compliant with LDAP V3 wire protocol RFC2251 etc. For an LDAP client it looks just like any other LDAP server
  • Note that it really wants to talk SASL
  • Its not slapd. Doesn’t support well known replication systems (slurpd,…)

• Is it really Kerberos?
  • Full RFC1510 implementation. MSFT’s own code base
  • Added vendor extensions with varying degrees of publication
    • PAC, no , then yes.
    • S4U, no
    • PKINIT, implements old draft
    • RC4-HMAC, published
    • Admin Password Change - published
What the solution needs to deliver

- Secure Authentication (Kerberos or LDAP)
- Secure User lookup (Encrypted LDAP)
  - User exists, UID, shell, gid, group memberships, ...

But, wouldn’t it be nice to also have..

- Access control
  - Joe exists, knows his password, but which machines can he use?

- Privileged Command Control
  - Centrally managed sudo

- Token based single sign on (Kerberos)
  - Trusted SSH Key-exchange!
  - Eliminate embedded passwords

- Secure Dynamic DNS
Ways to achieve AD integration

• Microsoft’s SFU

• Open source
  • Build your own
  • PADL / nss_ldap / pam_ldap

• Vendor supplied (OS, server, App)

• SAMBA

• Commercial products
Services For UNIX

Free
NIS server with password sync
(Microsoft code running on Unix!)
Not secure!
Also includes:
• NFS server
• Unix subsystem for windows
Open Source building blocks and challenges

- Build your own with Kerberos and LDAP
  - You have to really understand all the bits and AD
  - See Centrify’s Paul Moore on MSFT’s port25 site (port25.technet.com)
  - It can be done, but not very easy
- Common modules in most distros
  - pam_krb5 – WARNING, not secure unless you have computer account in AD
  - pam_ldap (PADL)
  - nss_ldap (PADL)
- Unix Vendor tools
  - Usually a combination of the above
  - Hard to setup
  - Not consistent between platforms
  - Mac very strong Kerberos support (Add OpenDirectory -> Golden Triangle)
SAMBA

- Primary job is as Windows file server
- Winbind can do AD authentication
- Works but limited functionality (group policy, central management tools, ....)
- Unix Profile
  - Random UID generation
  - RFC 2307 (W2K3 R2)
- No support, poorly documented, tough to deploy on a large scale, not available for all platforms
- Used successfully at workgroup scale
The hard parts...

- Disconnected operation
- Cross-forest, one-way trust
  - Lab trusts Production, Production does not trust the Lab...
- Group Membership
  - Universal, Global and Local Domain Groups
  - Kerberos PAC Parsing (S4U)
  - Mixed Mode vs W2K vs W2K3 vs W2K8 vs RODC
- User Migration from NT->W2K->W2K3
- Active Directory Site awareness and fail over
- Active Directory configuration errors
Commercial Products

- Makes your non-windows machines integrate with AD just as though they were Windows
- Support of AD features
  - Password policies
  - Seamless SSO
  - Group Policy
  - Central management of access and privilege (RBAC)
- Supports base platform, servers and applications
- Tested, supported and documented
Sidebar: What's PAM

- PAM – pluggable mechanism for doing authentication
- Core sequences through modules till somebody says ‘OK’
Sidebar: What’s NSS

- Name service switch: pluggable framework for looking things up (users, groups, ...)
- Answers API calls such as getpwnam, getgrid,...
Sidebar: what is Group Policy?

- AD mechanism for bulk configuration of systems
- Based on machine and or user identity
- Desktop
  - Control desktop lockdown
  - Installed applications
- Server
  - Product configuration
  - General file copy
  - Login scripts
What about web

- We want
  - User authentication via password
  - SSO - SPNEGO
  - Authorization

- Apache
  - Mod_pam – punts to the OS
  - Mod_auth_gss - tough to setup

- J2EE
  - Weblogic and websphere do user/password auth via plugins
  - Tomcat has open source SPNEGO support
Sidebar: what is SPNEGO

- Actually a mechanism for negotiating GSS mechanism
- But usually used to refer to IE -> IIS silent Auth – aka Windows Integrated Authentication
Things to look for

- Central reporting, management and access control
  - Windows, web, Unix CLI

- Delegated management
  - You must still be in charge
  - Joe AD admin should not be

- Rationalization of UIDs
  - You don’t want to be forced to choose 1 per user

- Auditing

- Uniform support of many platforms
More things to look for

- Sophisticated Forest and Trust Support
- Non invasive to AD
  - They trust you as much as you trust them
- Migration
  - Tools
  - Clean up what’s there – what the heck is this user account from 5 years ago?
- Root Access Control (ldap sudo)
- Web and Application support
  - Apache, J2EE, Database, ERP, etc..
Questions

• Battery Life?