Account Management

Nathan Rini
National Center for Atmospheric Research (NCAR)

Jenett Tillotson
Senior Cluster System Administrator
Research Technologies / University Information Technology Services
Indiana University

May 25, 2017
Access Control

- Authentication
- Authorization
Authorization or
Who Can Access What?
Unix (Posix) Accounts

- User account
  - User identification (uid or username)
  - uidnumber
  - Default group identification number (gidnumber)
  - Password, Gecos, Home directory, Default shell

- Group entry
  - Group name
  - Group identification number (gidnumber)
  - Password, Uid list
Storing Authorization Information

1. Flat files
   - `/etc/passwd`
     
     `jsmith:*:510:101:John Smith:/home/jsmith:/bin/bash`
     
   - `/etc/group`
     
     `users:x:101:jdoe`
     
     `gid:password:gidnumber:userlist`
Centralized Authorization Info

- Lightweight Directory Access Protocol (LDAP)
  - Can be used to store any directory information
    - telephone book, address book, network information, etc.
  - Based on x.500
- Microsoft ADS (LDAP-based)
- NIS (not really used anymore)
LDAP Structure

dc=example,dc=com

ou=people
  - uid=mike
  - uid=jane
  - uid=dave

ou=groups
  - cn=Users
  - cn=shipping
  - cn=accounts

cn=admin
Berkeley LDAP Utilities

- ldapadd
- ldapmodify
- ldapdelete
- ldapsearch
- slapcat
LDAP Server Config

- /etc/openldap/slapd.conf
- slapd.conf is now stored in the LDAP directory tree
- slapttest
LDAP Client Config

- /etc/openldap/ldap.conf

base dc=YourCompany,dc=com
Using Authorization Information

- Name Service Switch
  - /etc/nsswitch.conf

  passwd: files ldap
  shadow: files
  group: files ldap
Using Authorization Information

- Pluggable Authentication Modules (PAM)

Uses plugins (libraries) to make authentication and authorization decisions.

Standardized configuration files in /etc/pam.d/
Resources

- File systems
  - Home directory - /home/jsmith
  - Other directories/files

```
drwxr-x--- 14 jsmith adm 4096 Jun 23 17:42 mydir
```

- Logins
  - /etc/security/access.conf
    - : ALL EXCEPT (adm) jdoe root : ALL

- Printers, Tape drives, Queues, QOS, etc.
Authentication or
How Do I Know Who You Are?
Identity Methods

- Passwords
  - Encryption (DES, MD5, SHA)
- One-time password (OTP)
- ssh keys
  - ssh-keygen
  - id_rsa.pub --> /home/jdoe/.ssh/authorized_keys
  - Requires shared home directory file system
  - ssh host-based authentication
Identity Methods (cont.)

- Cert-based
  - Public Key Infrastructure (PKI)
  - Certificate Authorities (CA)
- One-Time Passwords (OTP)
Storing Authentication Information

- Flat files
  - /etc/shadow

  
  
  jsmith:$1$xyRJYA$kX$k5wv3HHv73uI$SzcU$Akq1q:.15842:0:99999:7::
  
  uid:password:last changed:may be changed:must be changed:
  expire warning:disable after expired:disabled:reserved

- LDAP (only use SSL wrapped LDAP)

- Kerbereros
  - Returns a tickets you can use for future authentications
Using Authentication Methods

- Service specific
  - Configure each service to use the authentication system
  - GSISSH
- Pluggable Authentication Modules (PAM)

```plaintext
auth    required       pam_env.so
auth    sufficient      pam_unix2.so
auth    sufficient      pam_krb5.so  use_first_pass
auth    required       pam_deny.so
```
Specific Example

- ssh
  - /etc/ssh/sshd_config

  PubkeyAuthentication yes
  PasswordAuthentication yes
  KerberosAuthentication yes
  UsePam yes
Security

- Passwords or passphrases
  - Picking good passwords
    - 14 characters is the minimum
    - Minimum 4 word long passphrase
    - Misspell one of the words to be extra secure
  - Changing passphrases
    - Forcing users to change their passphrase too often is insecure
    - At a minimum, change your passphrase yearly
- Cracking passphrases
  - John the ripper (GPU enabled now)
Security (cont)

- Keep private keys and certificates safe and protect them with a passphrase
- Two-factor authentication
  - Something you have (OTP, credit card, phone)
  - Something you know (passphrase, PIN)
  - Something you are (fingerprint, retinal scan)