W2k Security At FNAL

Jack Schmidt

FNAL W2K Migration Working Group Chair

April 16

Background

- W2K Migration working group
  - Existing NT4 Domain Admins and Division/Section representatives
  - Initially chartered to propose domain design only - but presently implementing design
  - Pressure to migrate but also to do things right!

Background

- win.fnal.gov
  - Top level domain. Apply site wide security policies
  - Limited number of Administrators
  - Contains no users or resources.
- fermi.win.fnal.gov
  - Child domain. Contains all users and most resources.
  - Limited number of Domain Administrators.
- ‘resource’.win.fnal.gov
  - Child domain(s). Controls systems, members of other critical systems.
  - No user accounts allowed.

Lab Policy

- Kerberos authentication
- Domain Controllers are ‘critical systems’
- Centralized accounts/ou administration
- No shared accounts

Authentication

- Kerberos and NTLMv2
  - 95/98/NT and non-domain w2k systems use NTLM
  - No ‘kerberos-only’ setting
- 2 central kerberos servers
  - MIT
    - Can’t change password
    - Long incorrect password timeout
  - Active Directory
  - 2 way trust

Critical System

Definition

“Computer security incidents involving certain systems could seriously impact the laboratory’s science programmatic operations. Such systems may be designated “critical systems” and may be subject to additional computer security policies and procedures”

Plan

- Identify systems
- Identify possible weaknesses and solutions

Critical System Plan

- 4 Domain Admins for win and fermi domains appointed by Computing Division and CSExec
- DCs in locked cabinets
- Remote administration using IPSEC and terminal server
- Services monitored for state change and additions
- Backup policy and domain disaster recovery
- One password policy
- Identification of OU Admin Rights
- Define W2K Policy Committee

Centralized Accounts

- Single user account
  - One per realm. Same username.
- create/disable
  - Security able to flip a ‘switch’
  - Admins not allowed to create accounts
- User accounts only in 1 domain

win.fnal.gov

fermi.win.fnal.gov controls.win.fnal.gov

- NT4 Domain Admins -> OU Admins

OU Administration

- Requirements:
  - Reset passwords
  - Define print/disk shares in AD
  - Change allowed user account information
  - Add/Delete/Move machine accounts
  - Add/Delete/Modify global groups
  - Enable/Disable user accounts
  - Move user accounts to ‘terminated’ OU
  - Retrieve user accounts from New-User OU

OU Administration

- Requirements (cont)
  - Set and Define policy for the OU
  - Create sub-OUs
  - Delegate control of sub-OUs

OU Administration

Implementation Issues

Admins can:

- Reset passwords
- Define printers/shares
- Change allowed user account settings
- Add/Delete/Move machine accounts
- Add/Delete/Modify global groups
- Enable/Disable User accounts

OU Administration

Implementation Issues

Admins CAN'T:

- Create/Delete OUs below their top OU
- Move users within their OU structure
- Delegate control of sub-OUs

Why?

AD does not provide a 'move' permission - only create/delete!

AD does not provide a basic security setting to prevent Admins for changing subOU permissions

OU Administration

Possible Solutions

- Domain Admins perform function
  - Not acceptable to group
- Explore commercial products
  - None that fit our security requirements
- Write a service program
  - Time consuming
- Combination GPO and Audit Policy
  - Implementable now

OU Administration

GPO Implementation:

OU Creator Group

- Domain Admins control membership

  username-Creator-OU
- Full Control over OU
- Only found in top-level OU
- Limited membership (3 per OU)

OU Admin Group

- Domain Admins or OU creators control membership

  username-Admin-OU
- Limited control over OU/sub-OU

OU Administration

OU Creator Rights:

- **This object and all child objects-**
  - **Full control**
- **This object only-**
  - **Deny Delete**
  - **Deny Modify Permissions**
  - **Deny Modify Owner**

The Creator group provides all requested admin rights – but also can create/delete users

OU Administration

OU Admin Rights:

- This object and all child objects-
  - Full Control
  - Deny Modify Permissions
  - Deny Modify Owner
  - Deny Create OU Objects
  - Deny Create User Objects
  - Deny Delete User Objects
- This object only-
  - Deny Delete

OU Administration

OU Admin Rights: (cont)

- **User Objects-**
  - **Deny Write Division, Last Name, Logon Name, etc.. 18 total**

The OU Admins group have basic rights but cannot create sub-OUs or move users

OU Administration

Audit Policy

- Monitor DC event logs for violations in security policy
  - Create/delete users
- Notify appropriate personnel
- Auditing done on external computer(s)
  - Harder for hackers to cover tracks

OU Administration

Audit Policy Implementation:

- Configure DCs to log proper events
- Install software on DCs to forward events to unix syslog server
  - Event Reporter ($49)
  - ELM (price varies)
  - Ntsyslog (free)
- Central syslog unix server
  - Uses syslog-ng and swatch
- Violation notification
  - Sends email to archived list

OU Administration

- Present status
  - Testing design
  - Needs Computer Security Review

No Shared Accounts

- Existing NT4 Shared accounts:
  - Administrative accounts
  - Test accounts
  - Console/Demo accounts
  - Data logging accounts
  - Monitoring Accounts
  - Service Accounts

No Shared Accounts

- Progress so far:
  - No shared admin or test accounts.
  - Service Accounts:
    - Examples: tape backup, anti-virus management, web server anonymous account
    - Waiver request form
      - Approval by Policy committee and computer security
    - Requires annual review

Future

- **Shared accounts**
- **Terminal servers**
- **Home Users**