Windows 2000 Conversion Wrapup

Al Williams (alw@psu.edu)
Penn State Teaching and Learning with Technology
SHARE 98, Nashville, TN
Session 5822
Introduction

• We’ve reorganized (again, and again, and …)
• Teaching and Learning with Technology
• Provides resources and support
  – For teaching
  – For students (labs)
• Do not do PSU Administrative Computing
• Have no authority over Colleges or Departments
  – Part of Computer and Information Systems
    • Oops – that’s now Information Technology Services
    • ITS @ Penn State
My Group

- Classroom and Lab Computing (name changed from Distributed Computing)
  - About 30 full time & 60 hourly employees
  - Student Labs (44)
  - Technology Classrooms (126)
  - Workstations and Servers (2000)
  - Serve up applications (hundreds)
  - 42K Students at University Park campus
  - 80K Students system-wide
Topics of Discussion

- Status last summer
- Completed Windows 2000 Upgrade
- Caused a political firestorm
- Current efforts
- Windows XP for summer 2002
- Lessons Learned
- What next?
You Missed a Good One

- Monday 1:30 Session 5800
- Windows 2000 and .NET Security Solutions and Technologies
- Rand Morimoto
- Look for it in the Proceedings
- Great detail
- This session more introductory in nature
Status Summer 2001

• In middle of W2K upgrade
• Big effort to manage applications
• Replaced older hardware
• Optimistic that we could make it
New GINA

• Graphical Interface for Network Authentication
• Create new PSUGINA
  – Providing an installer
  – Uses stub facility
    • Registry points to PSUGINA
    • We load MSGINA
  – Keeps MSGINA
New GINA

• Logon Interface
  – Capture userid and password
  – Writes security event

• PSUGINA communicates with PALS (encrypted UDP)

• Calls MSGINA for Domain Logon
Print Accounting and Logon Server (PALS)

- Provides proxy server for DCE authentication
- W2K server running Gradient DCE
- DCE (K5) and K4 capable
- Secure, encrypted exchange with PSUGINA
- Enables same service to Mac
- Keeps log of who logs on
Windows 2000 Conversion Completed!

- Up and running for Fall Semester
- One lab renovation not finished
- Considerations for support of other operating systems
- Looked good
  - Systems more stable than NT 4
  - Applications up and running
Supporting Other Operating Systems

- Need to support NTLM (authorization)
  - All Access Account users joined to top Domain
  - Passwords synchronized dynamically

- Users can connect from
  - NT 4
  - W9X, ME

- Added software to Student File Server
  - Apple IP Server
  - Supports Mac file access on a cluster
Access Account Userids?

• In 1991 started project for single userid
  – Called Access Account
  – Everyone gets one when they join Penn State
  – Central authentication service
    • Started as MIT Kerberos V4 KDC and AFS
    • Migrated to DCE and DFS
Userids and Passwords

- All Access Account userids in win domain
  - Nightly update for changes
- PALS server still checking logon authentication
  - Sets W2K password if not the same as DCE
- Added service to our win DC to accept password sets and user joins
- Disabled password change from workstation
- Use a web page to set DCE password
Domain Structure

win.psu.edu

staff.win.psu.edu  labs.win.psu.edu  otc.win.psu.edu
Other Services

• Added AIX Samba Server
  – Provides access to DFS for Windows
• Provide mapping mechanism on desktop
• Added Sun Solaris Netatalk Server
  – Provides DFS access to Mac
• Added Apple IP product to student file server
Political Firestorm

- Thought I had buyoff
- Some viewed synchronizing passwords as stealing passwords
- Some thought this was a security violation
- CIO got involved
- 7 week delay in services
Issues

- Issue of who owns the KDC
- Issue of whether duplicate sets of userids and passwords is a bad thing
- Issue of control point
- Lack of understanding of
  - How Windows 2000 works
  - Services that we deliver
  - What customers want
Why is CLC Doing This?

• Developed expertise to support lots of computers in a distributed environment
• Shared that expertise
• Started delivering support and services
  – Each one blessed
  – No one appreciated the aggregate implication
What Implications?

- Other departments and colleges want what we have
  - Want to authenticate to our Active Directory
  - Want to use our software (when possible)
- PALS has become integral to PSU security
  - Only record of logon / logoff
  - Lots of folks using our GINA code
  - Controlling Karl Bridge router authentication for all of PSU
Strategic Implications

• Should CLC be setting domain strategy for PSU?
• Is this the only way to deliver the services?
• Up till now, no interest in doing Windows Domain planning for PSU.
• Have stirred up interest! (or at least fear)
What Fears?

• Everything that we visited before is back
  – DNS
    • Why does my machine have that DNS name?
    • Why do you want to run DNS?
    • Why is it integrated with AD?
  – File service
    • Why are you doing file service?
  – AD Accounts
    • Why do you have Access Accounts in AD?
    • Why do you need the real passwords?
Communications Breakdown

• Developed services strategy a year ago
• Communicated to my management
• It was largely ignored
• Perhaps no one thought we could do all that
• Not being ignored now
Current Efforts

• Educate
  – Bridge the understanding gap
  – Market the services strategy
  – Build consensus

• Placate
  – Try a one-way relationship with DCE
    • Building and testing a separate AD Domain
    • See what works and doesn’t
Meanwhile Windows XP

• Target conversion this summer
• Roll out even more services
  – Terminal server for software access
  – Roaming profiles
• Services dependant on both authentication and authorization
Why Windows XP?

- Only way to get Windows 2000 maintenance
- Improvements in handling MSI packages
- Some nice new features
- Annual window of opportunity
  - Only do major changes in summer
- Prepare for .Net
What XP Features?

• Built in terminal server on Workstation
  – This might be real useful for help desk
• Application Compatibility Mode
  – Allows us to run some applications that don’t run on Windows 2000
• Native CD write capability
• Reliability improvement
  – Seems even better than Windows 2000
What XP Features?

- Better plug and play
  - Recognizes and uses more devices
  - Not universal plug and play
- Digital media?
  - New media player, movie maker, photo support
- Better power management (for laptops)
- 64-bit itanium support
- More policies
Windows XP Plan

• Prototype lab next month
• Only do XP equipment upgrades
• Migrate our way through all labs and classrooms this summer
• Improve servers to support
  – Roaming profiles
  – User file space upgrade
  – Terminal server
Lessons Learned

• Sometimes it’s better to be a planner than a doer
• Last reorganization diverted attention away from windows strategies
• Need to formalize our windows strategy
• Need to market the strategy and obtain senior management buy in
• We aren’t just supporting PCs any more
Lessons Learned

• Active Directory really works
• Our objectives seem quite attainable
  – Services for both DFS and NTFS
  – Ubiquitous Access Account
  – Ultimately – Single Signon
• Lots of Windows applications are not Kerberized
• Still need NTLM
Lessons Learned

- Authorization is much more difficult than authentication
- They don’t understand what I’m saying
  - Need to provide more basic windows education
    - For peers
    - For management
What Next?

• When in doubt – reorganize!
• I have new job
  – Develop strategy
  – Recommend policy
  – Market the ideas
  – Build consensus
What Next

• Continue with XP conversion
• Also happen to be doing Mac OS X
• Build test bed for Active Directory integration into Kerberos / DCE realm
• Document everything in open forum
• Spend lots of time doing presentations
Objective

- Teach about services and capabilities of Windows
- Focus on services for customers
- Reach senior management
- Propose policy
- Build a Penn State Domain Strategy
What are Our Alternatives for Authentication?

- Continue with current
- Develop K5 interoperability with AD
- Extend the current process
- Deploy CyberSafe Active Trust style solution
- Drop back to NT4 approach
Continue With Current

• No changes to accounts process
• No changes to DCE password change web page
• All synchronization done by CLC
  – Will add web service for password change management
• Works OK but
  – Prefer central management of userid/password
  – Prefer central management of password change
K5 Interoperable AD

- Need MIT Kerberos 5
- Establish Trust between AD and K5 (DCE)
- All users joined to AD
- No passwords in AD
- Use K5 for Authentication
- Breaks NTLM and other services
  - No services for older Windows (NT4 or older)
- Authorization synchronization is problematic
**Extend Current Process**

- Institutionalize control by
  - Accounts sets passwords at user join
  - www.work does password change for windows
  - Accounts does immediate suspend
- Users and passwords in the root domain
- Authorizations work natively
- Single Sign On much easier
- All native services work
CyberSafe Active Trust Solution

- Third KDC mitigates and populates both
  - K5 KDC
  - Active Directory
- Works well
- Expensive
- Complicated
- No advantage over our synchronized approach
Return to NT4 Model

- No users in Active Directory
- No Authorization capability
- Use our own MSGINA
- Use PALS to do all authentication to DCE
- No capability to offer services for the rest of PSU
- Retains single point of control
- Roll back all new services
And the Winner Is?

• Watch this space for future developments!
References

• Lots available through Microsoft web pages
• New detailed information about AD authorization
• Look at what other Universities are doing
• Web references tend to move
• Building my own collection
  – http://dsg.cac.psu.edu/support/domains/domstrat
Questions?