Windows Administrators Meeting
July 8, 2005
Notes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- Forest and Domain Functional Mode switch completed. See: http://tech.ait.iastate.edu/win2000/admin/Announce.07.05.05.pdf

- Eudora Pro for Windows version 6.2.3 has been released to the "Advanced" Scout-Kit list and www.sitelicensed.iastate.edu . This version will move to the "Current" list within a week or two if no significant problems are reported.

- A new version of the Kerberos support libraries and OpenAFS are being prepared. These versions allow OpenAFS to use Kerberos 5 authentication (rather than back-level-converted Kerberos 4 credentials).

- IT Services will be performing a schema update to the Enterprise domain to support SMS. We anticipate this happening within 2-3 weeks. We will announce to the WinAdmin mailing list when we have a solid date (and again, when the update is completed).

Status Reports

- IT Services will be installing Service Pack 1 to the Windows Server 2003 operating systems on the Enterprise domain controllers over the coming weeks. This involves firmware upgrades on the Dell systems.

Class List Status

Kunz gave a status report on the "Class-List" project (pushing official university lists down as Windows Global Security Groups). This project is close to being complete. For the past month official university college, department, major, and class lists have been pushed down and synchronized. Few problems have been found with the process so far. IT Services anticipates a "safe for production use" status announcement well before the fall semester starts. OU managers are encouraged to examine the lists (in the "AutoLists" container within "Active Directory Users and Computers") and email Kunz with any questions (skunz@iastate.edu).

Kunz discussed a few aspects of the list-based "Global Security Groups" that OU Administrators should be aware of.

First, this is a direct synch of official university lists, therefore will be no "manual adds/deletes". The entire process is automated and as students enroll in (or leave) classes the class list data will automatically be updated (on a daily basis). If departments want to include other "non-official" members in a class group they can follow the Unix practice of creating a private group, adding the "official class list group" and any other members, and use the private group for access control.

Second, viewing the membership of a class list means you must be an "instructor of

record". This means someone (your departmental secretary or whoever maintains instructor status for the university) must approve this instructor status. The automated process will automatically add such people to the "instructor" group for the class (and instructors are allowed to view the membership).

Third, OU managers are strongly advised to place a "!" in front of group names they create. This is covered in section 8 of the "Enforced Conventions for User and Group Names" document at:

http://tech.ait.iastate.edu/win2000/admin/enforced.conventions.pdf

If you create a conflict with one of the official class list names you will break the synchronization process and we will be contacting you to change the name of your group. If we cannot contact you we will probably place a "!" in front of the group for you (to let the automatic synch process continue). Duplicate names should not be much of a problem as the official names are long and ugly enough discourage this mistake. Avoid the naming convention used for the official lists in all cases (and always use a proceeding "!" in your group names).

Fourth, OU managers are STRONGLY urged to NEVER delete a NetID-based user object (those whose login name does not start with a "!"). This will remove the user object AND remove it from all security groups it is a member of (including the official college, major, department, and class groups). Having the user recreate the user object (by changing the password in ASW) WILL NOT repopulate all the group memberships! Staff often leave departments and come back as students (or employees in other areas). Repopulating official groups is a manual process and there may be considerable delay until the official groups are repopulated. Private list membership is never recovered (unless each group owner adds the individual user back to each group). Follow the guidelines in the "Managing Users Within a College/Departmental Organizational Unit" document at:

http://tech.ait.iastate.edu/win2000/admin/UserMgmtInOUs.pdf

Security

Mike Bowman (ITS) and Wayne Hauber (ITS) discussed the importance of "good security practices" in light of recent exploits seen on campus. The "BackupExec" exploit announced in the CCSG mailing list in the past couple weeks has caused several server-class systems to be compromised. Patching your systems with latest Microsoft critical hotfixes AND watching for the latest versions of third-party software (such as network backup clients, RAID remote management, power and system remote management) are the best way to protect your systems. Another critical piece is current antivirus software checking for virus signatures daily. System admins are cautioned that firewalls are NOT considered good protection in this day and age. Firewalls are "another good layer" but should never be considered a replacement for keeping software up to date.

Wayne outlined the steps you might want to follow if you suspect your Windows system has been compromised (via the BackupExec exploit or other means). This is the same advice Wayne gave in a post to the CCSG and WinAdmin mailing lists on June 30:

If you use Backup Exec, it would be prudent to run an on-demand scan with your antivirus program and a rootkit detection program such as rootkit revealer from www.sysinternals.com or F-Secure Blacklight (beta copy can be downloaded from http://www.f-secure.com/blacklight/).

For more information about the CERT advisory, see:
http://www.us-cert.gov/cas/techalerts/TA05-180A.html

The Veritas patch link is:
http://seer.support.veritas.com/docs/277429.htm

Please let ITS Security know if you have questions or concerns about either this action or the Backup Exec exploit.

Wayne Hauber (515) 294-9890
Information Technology Services -- IT Security and Policies
109 Durham Center, ISU, Ames, Iowa 50011
wjhauber@iastate.edu

ITS Security would like to encourage anyone who becomes aware of a security-related update for software that may be in common use at Iowa State (such as BackupExec) to post notification to the CCSG, WinAdmin, and ExchAdmin mailing lists. For example, Mike Long [CARD] posted a warning to the CCSG mailing list on June 24 with the subject "Veritas Backup Exec patches". This post contained the following link to information on how to obtain the patch:

http://seer.support.veritas.com/docs/277429.htm

Follow Mike's example if you find a "patch warning" that might be valuable to others (Thanks, Mike!)

Open Discussion

Dave Orman [CNDE] asked about the status of the request for departmental IT admins to offer roaming profiles, home directory, Exchange, and logon scripts for students.

Kunz announced he had taken the concerns (from Vet Med, Engineering, and others) to a CIO-level meeting in May and that approval had been given to proceed with an "experimental project" with Vet Med. This project would utilize a "compromise approach", granting control of the "service oriented fields" (for Exchange, roaming profiles, etc) to departmental IT admins via "access control lists" applied to a container holding a college's students. The departmental OU admins for the college would only be able to control the service oriented fields specified – account suspension, password reset, etc. would remain under control of central IT Services for students. The intent is that should this experiment be a success, the provision would be extended to other colleges. No timeline is promised (though we recognize others are anxiously waiting for this capability). Much depends on the outcome of the "experiment".

Kunz explained that the technical component of this "experiment" is fairly minor. However, the IT Services "enterprise support" issues for the student Windows resources are great. A large part of this "experiment" will be developing policies and procedures for what happens when a student leaves one departmental IT support area and moves to another (with different or "no departmental support"). What happens when a student leaves "College A" where they have two years of Exchange mail, files in a home directory, and documents stored on a roaming profile desktop and shows up at "College B"? How can the student be assured the files and mail can safely follow them to the new department (especially when the current OU admin is anxiously wanting to recover space on their systems)? Who exports the Exchange mail and imports it into the new Exchange server (or WebMail)? Who exports the files from departmental servers and coordinates transfer to AFS (or a new department's servers)? What are the Solution Center help desk support issues when a student shows up at the Solution Center with a corrupt roaming profile? All these questions are greatly compounded with the numbers of people who change majors during the average school year. This will be a challenging experiment.

Meeting Adjourned (about 10:00)

Next meeting is scheduled August 12