

Windows Administrators Meeting

October 14, 2005

Notes (taken by Steve Kunz)

Updated 10/18/05

Meeting Started (9:00)

Announcements

- There continue to be security issues with Symantec BackupExec. It is VERY IMPORTANT for anyone using BackupExec to follow the advisories issued by Symantec. Scan the CCSG mailing list for recent items with “Symantec Technical Advisory” in the subject line. Just because you patched a few weeks ago does not mean you are covered for the latest vulnerabilities.
- Port 6106 was blocked at the campus border at about 4:10 p.m. on Oct 13, 2005 to address the latest BackupExec exploit issue.
- A recently released patch from Microsoft - MS05-051 - has caused problems at some other sites. Reports of “DCOM errors associated with some web applications on Windows 2000 SP4 hosts” and “Windows XP desktops display a variety of problems post patching - including Windows Update not functioning, inability to uninstall the patch, and problems rolling back to a restore point” exist. If you are experiencing these problems recently this may be one thing to investigate.
- ITS has started a new “SIG” (Special Interest Group) on security issues in general (non-OS-specific). This meeting is held monthly on the “2nd Tuesday” from 2:00-3:00PM in Durham 144. There is a mailing list (secsig@iastate.edu) established. Send requests for membership on the mail list (or further information on the meeting) to Wayne Hauber at wjhauber@iastate.edu.

Thin Clients and Terminal Services

Steve Kunz [ITS] talked about the general increased interest on campus in “thin clients” (on a variety of operating systems) and “Windows Terminal Services” in particular.

There is a presentation on “Thin Client Technology Overview” by R&D Industries, Inc. on Oct 20 at 3:00 PM in Parks Library 031. No cost – no pre-registration. More details in the CCSG/WinAdmin/MacOSX-Admin mailing with the subject “Do you manage a lab? Read this msg about an Upcoming tech session”.

ITS is interested in learning how many people are currently using Windows Terminal Server or intend to use it in the future. Over half the people in the room indicated they were currently using Windows Terminal Server.

The question of CALs required to run Windows Terminal Server has been raised. There is some confusion on CALs under Windows Server 2003 and how they apply under our current campus agreement (“MCA”). Kunz will ask the person who deals with the MCA for clarification and will post the response to the WinAdmin mailing list.

Software and Windows XP x64 (Beata Pruski [ITS])

Beata Pruski [ITS] talked about software issues that arise when you try to install current 32-bit software on 64-bit OS platforms (such as a Dell Optiplex GX620 running Windows XP x64). People should be aware that many ITS supported software products will not currently install or run correctly! Beata presented a list of currently known issues as follows:

- OpenAFS – Won't install
- PCAFS – Won't install
- Kerb (current) – Won't work
- KFW (upcoming) – Installs, “mostly” works
- KerbLogon – Won't work
- WinZephyr – Installs, won't work
- PCLPR – Installs and works
- HostExplorer – Installs and works
- FileZilla – Installs and works
- JMP – Installs, won't work (seems to be a simple license-key issue)
- VirusScan – Installs and works (but Windows Security Center doesn't see it)
- Eudora Pro – Installs and works

In general, any process written to hook into the login process will not unless updated. Device drivers not converted to the new OS will not work.

People are strongly cautioned to experiment with a test system before assuming applications will work. Work with your software vendors. ITS will work on locally authored packages (such as Scout and KerbLogon).

Open Discussion

- Chris Thach [CIRAS] asked if there was some sort of “timeout” built into a Cisco VPN connection. An off-campus user seems to be regularly disconnected after a period of time. General consensus in the room was “No”. Kunz will ask the question of ITS staff person who maintains the VPN server.

[Information since the meeting – 10/18/05]

Steve Schallehn [ITS] says: “The VPN server timeout is 72 hours. This was a compromise between keeping connections up long enough to be useful and making sure we have fair utilization of a resource shared among the entire ISU community.”

- Chris Thach [CIRAS] asked if there were any restrictions on editing alternate phone numbers within Active Directory user objects under departmental control. Kunz responded that unless the attributes were explicitly stated as being “mastered” from official university data (see <http://tech.ait.iastate.edu/win2000/admin/UserMgmtInOUs.pdf>) there are no restrictions.
- Steve Kunz [ITS] talked briefly about key issues he and Wayne Hauber [ITS] learned at a 6-day SANS training session on Windows security. Highlights were:

- 1) Move to 15+ character “pass phrases” (this eliminates the need for multi-character-set expiring “passwords”).
- 2) Establish a PKI (digital certificate) infrastructure
- 3) Remove LANMAN, NTLMv1, and “anonymous” access from your Active Directory structure.

Kunz and Hauber intend on providing a summary presentation on this training to the ISU Windows community at the future date (possibly in the “Security SIG” meeting venue).

- Web Wilke [RES H] asked what could be done to eliminate multiple complex passwords across several systems on campus (Active Directory, AccessPlus, ADIN, etc). A general discussion followed about “single signon” and security issues of a “one-key-fits-all world”.

Meeting Adjourned (about 10:05)

Next meeting is scheduled November 11