Windows Administrators Meeting

October 8, 2004
Notes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

None

GDIPLUS.DLL Security Issues

Kunz briefly reviewed the GDIPLUS.DLL security issue as raised in the WinAdmin and CCSG mailing lists (Oct 5, Subject “what are steps to protect against the MS jpeg security breach?”). Kunz indicated he was personally aware of four products in use at Iowa State that carried along GDIPLUS.DLL. These are JMP, Oracle Calendar, WSFTP, and MacroMedia. For Windows XP, JMP recommends you delete the copy in the JMP program folder (so the package uses the updated system copy). For all other versions of Windows running JMP they recommend replacing the JMP local copy with an updated one from Microsoft. Oracle Calendar and WSFTP should probably have the program-local copies updated with the version in the system folder. MacroMedia indicates (on their web site) the issue does not affect their product. There are certainly other products affected by this security issue. It is always best to check the manufacturer’s web-site to see what to do about security updates to GDIPLUS.DLL.

Security Center Group Policy on Domain-Member Systems

Beata Pruski (AIT) provided info on enabling via Group Policy the Windows XP SP2 “Security Center” on systems that are members of a domain. Microsoft treats the enabling of the Security Center differently based on whether or not the system is a member of a domain. Non-members have the security center “enabled” (and it cannot be disabled). Domain-members have the Security Center “disabled” (unless Group Policy changes the default behavior). See the end of this document for detailed information. Enabling the Security Center allows it to check for important items like current antivirus data files, and enabled firewall, etc.

Effects of Department Name Changes on Windows Systems

Jim Wellman (AE EM -> AER E) raised the issue of departmental name changes and their effect on Windows systems. Specifically, Jim found that some Kerberos functions (PCLPR, for example) ceased to work when the IP subnet name changed (in his case, from “aeem.iastate.edu” to “aere.iastate.edu”). Pruski and Kunz indicated this is because there is a control file (used by all Kerberos implementations – UNIX, Linux, Windows, etc) that maps subnets to a kerberos realm. If this file is not updated with the current list of subnets the realm is not correct and the authentication fails. On Windows this file is typically in the C:\KERB folder called “krbrealm.con” (it can be opened with Notepad). Kunz indicated this file should be updated regularly but often lags. AIT will look into getting a current version out on a more timely basis to Windows systems (it currently only gets updated with new versions of the Kerberos client package).

Kunz indicated there is another aspect to this issue associated with OU names. When the department changes names, new faculty/staff members are automatically tagged with the NEW "official short department name". This name is the name of the OU where the user object is dropped automatically. If the departmental OU name is the still the old name, then the Account-Synch process does not find an OU match and the new user is dropped in the general "Users" container (for more details on this process see http://tech.ait.iastate.edu/win2000/admin/OUUserLogic.pdf). Until the OU is renamed correctly, all faculty/staff user objects have to be moved manually (not desired). The Windows Enterprise Domain Administration will NEVER rename an OU automatically to match the new name. This is only done at the request of the OU administrator and with coordination with the Enterprise Admins. The renaming is a simple process at the Enterprise level, however it CAN affect scripts written by OU admins that have the OU name hard-coded into them. The best practice for scripts is that they be written to detect the current OU dynamically upon startup. Second-best would be to use a variable at the beginning of the script (so you only have to change one line in each script). If you have no scripts in use that reply on your OU name then the OU name change is simple and transparent.

Open Discussion

Jim Wellman (AER E) asked about a problem he was having with Kerberos credentials on new laptops. After a restart, when the first user logs in they have Kerberos credentials for a short time (< 10 secs) and then they "disappear" (as indicated by SideCar having a "gold key" indicating "valid tickets" and then the "not-overlay" on the "gold key" indicating "no valid tickets"). This seems to happen only on some newer laptops. It only occurs on the wireless interface (the wired interface is disabled, so it is not a "multiple interfaces active" issue). If users log off and back on or a new user logs in (without a reboot) the problem does not recur until the next reboot. These systems have OpenAFS installed on them.

A long discussion offered a couple suggestions. First, Bill Hart (AIT) and Jacob Dekkenga (AIT) suggested trying to uninstall the OpenAFS "loopback" adapter and see if the problem went away. This fix may help some systems (if they don't need the loopback adapter – with allows NetBIOS name maps like \\afs\iastate.edu\...). Second, it was suggested it may be because the IP address of the adapter changed after the tickets were acquired (DHCP issues, for example). Since the tickets are tied to a specific IP address any change will invalidate them.

Jim will experiment with these ideas and continue to work with AIT staff.

Meeting Adjourned (about 9:45)

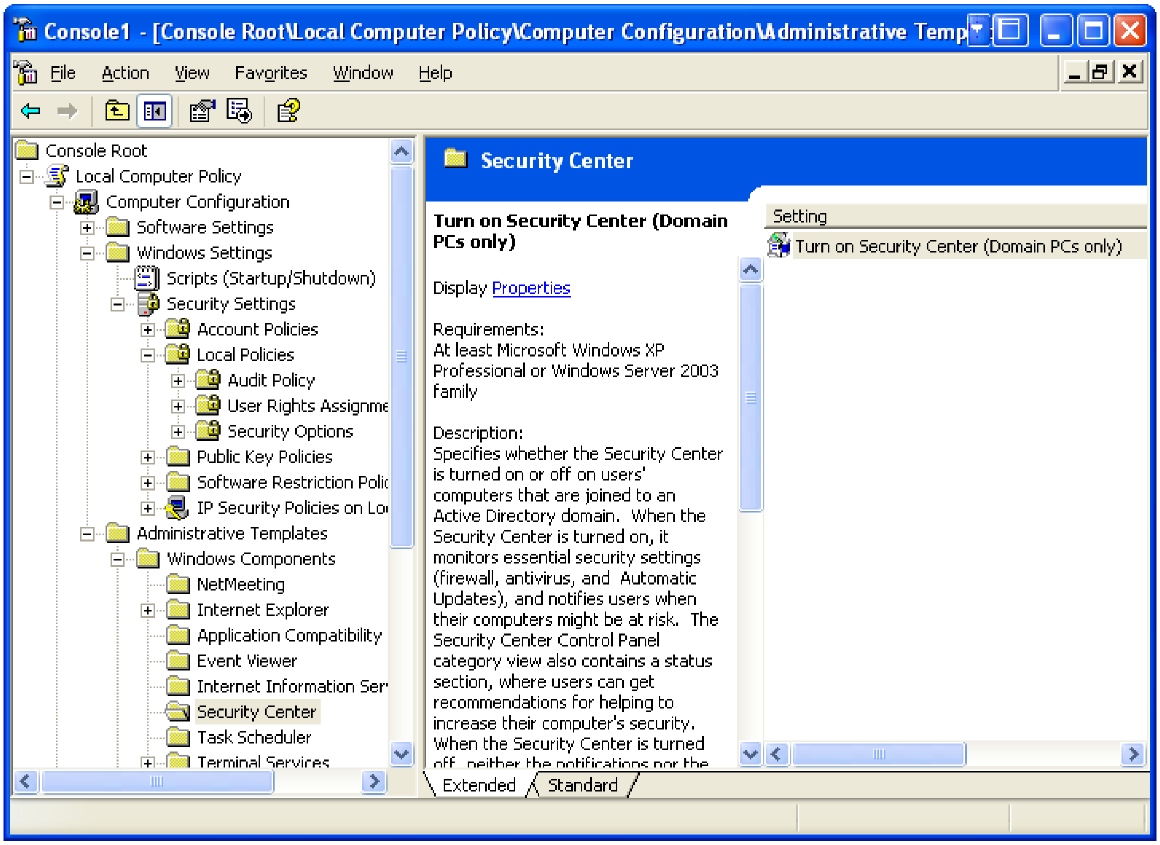
Next meeting is scheduled November 12.

Details -- Security Center Group Policy on Domain-Member Systems

[Thanks to Beata Pruski (AIT) for this information]

How to enable the full Security Center functionality in Windows XP SP2 for machines that are members of a domain

The full functionality of the Security Center in Windows XP SP2 can be changed through Group Policy. Open the group policy editor or GPMC from a workstation that has SP2 installed. This will allow you to edit the new group policy extensions for SP2. The setting can be found in the following location:



Turn on Security Center (Domain PCs only)

Display Properties

Requirements:
At least Microsoft Windows XP Professional or Windows Server 2003 family

Description:
Specifies whether the Security Center is turned on or off on users' computers that are joined to an Active Directory domain. When the Security Center is turned on, it monitors essential security settings (firewall, antivirus, and Automatic Updates), and notifies users when their computers might be at risk. The Security Center Control Panel category view also contains a status section, where users can get recommendations for helping to increase their computer's security. When the Security Center is turned off, neither the notifications nor the

Setting this policy[1] to “enabled” should allow the Security Center service to start on domain machines.

[1] “Turn on Security Center (Domain PCs only)” policy specifies whether the Security Center is turned on or off on users' computers that are joined to an Active Directory domain. When the Security Center is turned on, it monitors essential security settings (firewall, antivirus, and Automatic Updates), and notifies users when their computers might be at risk. The Security Center Control Panel category view also contains a status section, where users can get recommendations for helping to increase their computer's security. When the Security Center is turned off, neither the notifications nor the Security Center status section are displayed.

Note that the Security Center cannot be turned off for computers that are NOT joined to a Windows domain, and this policy setting will have no effect in that case.

If this setting is Not Configured, the Security Center is turned off for domain members.

When this policy setting is Enabled, the Security Center is turned on for all users. Note that the Security Center will not become available following a change to this policy setting until after a computer is restarted.

When this policy is Disabled, the Security Center is turned off for domain members.