Iowa State University
Information Technology Services

Windows Administrators Meeting
October 12, 2007
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- NetID suspensions happened Monday evening, Oct 8. This is the normal process to suspend accounts for 1) students no longer enrolled 2) staff no longer employed 3) sponsored accounts that did not renew. See section 7 of "The Care and Feeding of Iowa State Net-IDs" at http://www.ait.iastate.edu/pubs/ggs317/ggs317.pdf
- SpyBot Search & Destroy 1.5.1 is available as an "Advanced" Scout-Kit (or directly from http://www.spybot.info/en/index.html).
- Networking and Communications has begun work on supporting IPv6 at Iowa State University. Some systems in Durham are already using IPv6 addresses for testing. More information will be coming as ITS supports the "next generation" of Internet IP addressing.

Prepare for Kerberos-4 Authentication Demise [Kunz]

Kerberos-4 is an older version of the Kerberos authentication protocol (and has been present at ISU since the late 1990's with the advent of "Project Vincent"). Kerberos-5 is the current Kerberos protocol and has been supported for several years by ITS. Support for Kerberos-4 (for security modifications, bug-fixes, etc.) by the MIT authors is being discontinued. ITS feels it is prudent to remove the Kerberos-4 KDCs (Kerberos "key distribution center" servers") since any future security vulnerabilities cannot be addressed.

Many services and clients have already been converted to Kerberos-5 for authentication. In the Windows area Eudora Pro has used native Kerberos-5 authentication for quite some time. Recent versions of OpenAFS use Kerberos-5 for credentials. However, there are still a few ITS services that are "Kerberos-4 only" and need to be upgraded. Two examples of ITS servers that need to have Kerberos-5 authentication added are the "print servers" and the "zephyr servers". There is a two-phase plan to upgrade these and other services and finally shut down Kerberos-4.

Phase 1: By the end of the current semester ITS will modify the remaining ITS servers doing "Kerberos-4 only" to also do Kerberos-5 authentication. Such servers will then talk to old Kerberos-4 clients (during the transition period) and updated/modern Kerberos-5 clients. Following these upgrades new clients (for example new versions of PCLPR and WinZephyr for Windows systems) will be prepared and released.

Phase 2: By the end of the spring 2008 semester (at the earliest) the ISU community should have had sufficient time to upgrade their clients (which will use the new Kerberos-5 authentication method). At that point, sometime during the summer of 2008 – but certainly prior to the start of fall 2008 classes – the Kerberos-4 KDCs will be shut down.

In most cases the modification of clients to support Kerberos-5 will not result in a change in the way the client works. Everything is "under the covers". One Windows product previously supported by ITS will be discontinued. "SideCar" will not be ported to Kerberos-5. SideCar is the "POP3 authentication product" that allows email clients that only do "standard POP3 authentication" (i.e. "clear text passwords") to authenticate to our KPOP (Kerberized POP3) email servers. People have been using SideCar for such products as "Outlook", "Outlook Express", "Thunderbird", and any other "POP3 standards based" email clients. As a replacement product for SideCar, an ITS written product called "kpoprelay" will be supplied. As with SideCar, this product will "sit in-between" the email client and our KPOP servers and automatically supply Kerberos-5 credentials when a normal POP3 authentication attempt is made. Watch for more announcements on "kpoprelay" as this ITS conversion project progresses.

Jim Wellman [AER E] commented it is becoming increasingly difficult to deal with "pocket devices" (such as "Windows Mobile", "Blackberry", "Palm", etc.) and use of ISU email services. He asked if there are any ITS plans to better support these devices in the future. Vince Oliver [ITS] announced that he is actively working on an "Exchange Blackberry Enterprise Server" for enhanced Blackberry support for ITS Exchange usage. He also announced the availability of "Secure IMAP" on the ITS Exchange system (watch for more info on this coming out soon).

Enterprise Domain [Kunz]

Steve Kunz [ITS] talked about abuse metrics being watched on the Enterprise Windows Active Directory domain controllers. The existing IDS system for excessive "authentication failures" has been in place for several years. ITS is now monitoring additional activities such as "expensive LDAP searches" and "heavy successful authentications". "Expensive LDAP searches" are LDAP queries to the domain controllers that search a large number of objects and return few (if any) results. These searches produce a considerable load on a domain controller if repeated on a regular basis. "Heavy successful authentications" are simply a large number of successful authentications from one host. An average user desktop will perform 30-50 authentications per hour. In one recent example ITS detected one system doing 50-70 thousand logins per hour on each domain controller over a period of several days. Both of these "abusive behaviors" can deny (or severely slow down) all other authentications and domain controller activity. The new metrics (and individual followup by the Security Team) will help ITS continue reliable service from the Enterprise Domain controllers.

Kunz also talked about shutting down LDAP "simple binds" on the Enterprise Active Directory domain controllers. This was discussed in the August 10, 2007 "Windows Administrator" meeting. The solution is to install digital certificates on the domain

controllers so they can do "LDAPS". ITS will be installing a digital certificate on one domain controller in the near future (probably WINDC4) and proceed with departmental testing with a couple applications. Full rollout will follow. More information will be released as continue on this important security measure. For more details see:
http://tech.ait.iastate.edu/win2000/admin/WinAdmin.08.10.07.pdf

Open Discussion

Steve Spencer [ECSS] asked if anyone else was seeing "Unknown authentication error 63" from OpenAFS on systems configured to "Obtain AFS tokens when logging into Windows". After the failure at login time you can manually get tickets successfully. Nobody else in the room had ever experienced the same error. ITS will try to pursue the issue with the OpenAFS developers.

Meeting Adjourned (10:55)

Next meeting is scheduled for November 9, 2007.