Windows Administrators Meeting
June 13, 2003
Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

Kunz announced that there are plans in progress to change the Kerberos authentication service provided by AIT. There are two versions of the Kerberos protocol – version 4 and version 5. Our Kerberos servers were version 4 until the past year or two, when they were converted to version 5 with "version 4 compatibility" (meaning our Kerberos servers will give out both versions 4 and 5 "Ticket-Getting-Tickets" – "TGTs"). Deliberations by the OASIS committee and other security needs indicate we should shut down the version 4 authentication mechanism and only provide Kerberos 5 authentication. A preliminary target date for this change has been self-imposed by AIT for January, 2004 (no formal plans have been set by OASIS or any other administrative body as of yet).

Most of our client software only supports getting Kerberos 4 TGTs. This means a lot of software must be changed. One path to do this involves modifying the client authentication software to get a Kerberos 5 TGT and convert it to a version 4 TGT locally, which can then be used by the client to get "service tickets". Using this technique means you don't have to modify ALL the server software at the same time. This is the approach being taken by the ISU AIT Windows software developers.

A new version of Scout (currently in beta-testing) will install new Kerberos libraries that get version 5 TGTs and convert them to version 4 TGTs locally (so both sets are available). This software should be tested and become the "Current" Scout in a few weeks. For lab managers and other who don't use Scout for installations, a separate "Kerberos library installation package" will be available.

This change will not likely affect departmental IT managers UNLESS you have custom written software that only gets Kerberos 4 TGTs. When the Kerberos 4 protocol is turned off this software will cease to work. AIT has identified one class of software already that cannot be fixed – Macintosh OS 9 (and below). This version of MacOS uses a version of KClient (the Kerberos package) and SideCar that the authors have indicated will NOT be ported to Kerberos 5. The only answer for MacOS 9 (and below) owners will be to convert to Mac OS X. Mac users should note that Mac OS X will only run on a Mac "G3" or above.

Wayne Dowling (ECSS) asked if the Mac OS 9 systems could have a similar "Kerberos 5 to 4" conversion written for them. Bill Frazier (AIT) replied that it could be written but not installed into the packages that were asking for the version 4 TGTs (since we do not have the source or compile the software).

Open Discussion

Chris Thach (CIRAS) asked about VirusScan 7.0 and the scanning of email delivered from POP-servers. It appears that the email-scan configuration settings in version 7.0 only relate to Exchange email and no provision is available for scanning POP-mail. The discussion that followed centered on the idea that the "on-access" scan feature of the new version probably handled files deposited from any source (including POP mail). Kunz indicated he would get a formal response from Jeff Balvanz (AIT – antivirus support).
[**Information since meeting**: Mike Long posted some information from the VirusScan 7.0 "Release Guide" that supports the "on-access covers all" supposition. The text is reproduced at the end of this document. Thanks Mike! - SLK]

Dave Orman (CNDE) asked a related question about VirusScan version 7.0 and usage with Eudora Pro. Eudora Pro downloads mail into a "spool area" before moving it to the inbox or a folder. Dave indicated that if a user received a piece of infected mail with Eudora Pro and it was infected, VirusScan's "on-access" detection would move the item from the spool area to a VirusScan "quarantine" area and Eudora would not believe the item was received from the server. On the next POP-mail check it would then re-requested the item, repeating the whole process. A comment was made from the audience that this may not be "new behavior". Kunz indicated he would get formal response from Jeff Balvanz (AIT – antivirus support).

Dave Orman (CNDE) asked about converting ftp.sitelicensed.iastate.edu to a "secure FTP server" (possibly Kerberos, where the password does not go over the network in "clear text"). Kunz (AIT) and Frazier (AIT) both commented this issue had been raised in the past and that the "right mix" of server and client software that did not break other FTP clients had not been found. Kunz noted that the Scout client's use of ftp.sitelicensed is currently Kerberos-authenticated via locally-written software. However, this cannot be retrofitted into FTP clients we do not have the source for. A near-term fix may be on the way, however, since it may be possible for AIT to add an Apache web-server front-end to the software on ftp.sitelicensed, enabling secure SSL file transfers from that server.

Russ Hoffman (STATL) asked about traveling staff and secure access back to systems and servers at ISU. Kunz indicated the solution most often used by other universities seems to be "VPN" (Virtual Private Network). This provides an authenticated and encrypted connection from clients anywhere on the internet back to the campus network, making the client system appear to be "on campus" (in the network sense). Most modern operating systems have VPN client software available. The preferable solution would be a "campus wide" one. Telecommunications is currently researching vendors and costs to provide such an offering (no promises of any such service yet).

Kunz asked for comments on enhancements/changes that could be made to the ISU enterprise Windows support that would be most important to college/department IT managers. The top two items were "folder redirection" and "departmental Exchange email support" for students. A good discussion followed which covered the benefits of folder redirection (your files and settings follow you around) and pitfalls (longer login times if quotas are not applied). Kunz asked "If folder redirection could be applied to redirect to the existing AFS home directory, would this at least solve some problems?" A resounding "Yes" was considered enough to research this further as time/priorities permit. Having this, additional departmental file-space mapping could be done with login scripts and "loop back processing". Kunz will try to find time to research more. [Anyone having any additional ideas is encouraged to email skunz@iastate.edu - SLK] The Exchange mail support is a bit more complicated, since only one Exchange mailbox is supported per user object and multi-departmental use would not be possible. However, it MAY be possible allow the student to coordinate a switch between departments using ACLs on the Exchange attributes. Again, more research/experimentation needed.

Meeting Adjourned (about 10:00)

Next meeting is July 11.

Excerpt from NAI VirusScan Enterprise "Release Guide"

42 VirusScan® Enterprise software version 7.0

Scanners and updates

The following scanner and update features have been removed from VirusScan Enterprise 7.0:

Internet Filter on page 42

- *Download Scan* on page 43
- *Exclude action* on page 43
- *On-Demand Scan wizard* on page 44
- *AutoUpgrade* on page 44

Internet Filter

Previous release: The Internet Filter was based on an outdated model. The Internet Filter blocked Java applets, ActiveX scripts, URLs, and IP addresses.

Current release: VirusScan Enterprise 7.0 does not block Java applets or ActiveX scripts, but its on-access scanning provides equivalent scanning protection against these threats. URL and IP address blocking functionality is not replaced.

Benefits: Removing the Internet Filter provides better performance and more efficient use of system resources.

Removed Features

Download Scan

Previous release: Through Download Scan, the user could select a different set of scan options for a collection of programs (for example, browsers, or POP3 clients) that are capable of introducing new infections to a protected system. The administrator did not have the ability to set different scanning options for different processes.

Current release: The scanning engine has been extended to allow users to set different scan options for three classes of processes:

- **Default**
- **Low-Risk**
- **High-Risk**

NOTE

For more information on using these features, see *Scan options for low-risk and high-risk processes* on page 21.

Benefits

- Fewer components to manage and configure.
- Greater administrative control.
- More control when scanning different processes.