Windows Administrators Meeting
February 12, 2010
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements
(None)

Heightened Windows Security Threats [Wayne Hauber - ITSEC]

Wayne Hauber [ITSEC] talked about the heightened security threats present on the internet today. Among the issues Wayne addressed were:

- Very large numbers of viruses and compromised web servers are out there (in the millions). The numbers are increasing all the time.
- Most notable among the viruses are torpig and mebroot (a master boot record rewriter). There are very sophisticated keyloggers and virus delivery systems.
- Current anti-virus programs will generally not detect or remove the latest generation of viruses. It does no good to simply format the system drives – you need a low level format. Killdisk and dban (Derricks's Boot and Nuke, http://www.dban.org) are good low-level formatters.
- There are some very ordinary, popular, and formerly believe to be "safe" web sites that can compromise your system.
- Recent versions of Adobe Reader/Flash and IE8 (prior to 2008.02.08 patch) have large security holes). Make sure you are always running the latest patched up versions.

Jim Wellman [AER E] asked if Secunia (http://secunia.com/products) was still considered a good tool to check for up-to-date Windows patches and third-party software versions. Wayne indicated it was still a good choice. It was noted that Secunia PSI licensing indicates it is only free for "personal use". Secunia CSI is available for corporate use, but no cost information is known (to our knowledge nobody is using a corporate license at ISU). A similar product (still in beta) is available for Macintosh systems called AppFresh (http://metaquark.de/appfresh).

David Orman [CNDE] said virtualization may be the only answer (using a fresh copy of a virtualized image each time).

Open Discussion

Chris Thach [CIRAS] asked about the appearance of a new section on the TechCyte's Dell page that has "ISU ITS Standards (w/image loaded)". Darrin Fischer [ITSYS] indicated that ITS has worked with Dell to provide pre-imaged systems built to ISU standard specifications. Chris would be interested in hearing more about this in future meetings.

Steve Kunz [ITSYS] asked about the value of the Windows Administrators meeting and whether or not people preferred to have the items discussed be presented only at the CCSG meeting (and WinAdmin meetings discontinued). Steve indicated that only one meeting had been held since September 2009 and that most topics addressed in the WinAdmin meeting were also addressed in the CCSG meeting. All comments received in the meeting indicated people preferred to continue the WinAdmin meetings with the desire for more "technical information and techniques" in the future. Kunz indicated he was fine with that but requested attending members to consider providing some of the technical content to share with others. The WinAdmin meeting will continue to be held the 2nd Friday of each month (same place/time) when an agenda warrants it. If no significant agenda exists for given month the meeting will be cancelled (with an email notice to the WinAdmin mailing list).

Meeting Adjourned (09:55)

Next meeting is scheduled for March 12.