Windows Administrators Meeting
April 9, 2010 (spelling typos fixed same day)
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- Ongoing security threats (torpig, infected PDF file attachments, etc.): Steve Kunz [ITSYS] and Wayne Hauber [ITSEC] talked about the continued threat of systems being compromised by exploits for Internet Explorer, Adobe Reader, Adobe Flash, Java, and a variety of other third party products. It is critical to keep your Microsoft OS and applications up to date with current patches AND all your third party applications as well. This is difficult to do without using some sort of tool, as not all applications self-update (especially older versions). One tool to look at for personal Windows systems is "Secunia PSI" (http://secunia.com). Make sure you honor Secunia's licensing restrictions. ITS is looking into the cost of the corporate version ("Secunia CSI") for possible site-licensed usage. A similar product exists for Macintosh systems called "AppFresh" (from Metaquark, currently released as a "development preview" product).

- Group Policy Testing Issues/Plea: The Enterprise Admins went through 2-3 difficult days last week trying to diagnose a 100% CPU utilization on all four domain controllers. The issue did NOT cause any outages but caused much intense effort to diagnose the problem (including valuable help from the ITS networking folks). In the end it was a misconfigured group policy for a non-Microsoft product called "PowerMAN" licensed by a unit on campus that was attempting update client software. The "plea" is to please test group policies for non-Microsoft products on a limited number of systems and assure yourself the desired actions are being done correctly before rolling it out to all systems within your unit. [I did not make this clear in the meeting, but we are not telling people to do such testing on normal "Microsoft built-into AD" policy settings, only "custom GP templates" for non-Microsoft products. SLK]

- ITS Possibly Changing "user suppressed" Term in AD: ITS sees the need to change the term that appears when a student desires to suppress their personal information from campus directories (including the main LDAP server "directory.iastate.edu/ldap.iastate.edu") and Active Directory. Currently the first name, last name, address, phone number, etc. have the term "user suppressed" place in each field. ITS needs to change this (for Gmail) to something more unique, so the "first-name mi. last-name" may look like "<net-d> @ iastate.edu". The question was asked if this would adversely affect anyone. In general the comments from people in the meeting were they didn't care or that the change would be an improvement over the current convention.

- Phishers/Spammers have moved to OWA: ITS had internal procedures in the past for dealing with cases where a compromised user account was used to generate large amounts of spam on the WebMail systems. Generally a person gave away

their password to an email spammer as the result of a phishing email. The end result was Iowa State got "blacklisted" on anti-spam RBL lists by off-campus email providers. With the shutdown of WebMail and the move to Exchange the spammers have switched to Outlook Web Access and now phish faculty/staff accounts. ITS is working on adjusting its procedures for rapidly disabling compromised accounts so we can avoid getting blacklisted in the future. Techniques and tools are still being developed.

Kerberos Realm Rationalization [John Hascall - ITSYS]

John Hascall [ITSYS] talked about the ITS plan of shutting down the MIT Kerberos domain which has been used for many years as the core authentication mechanism for "Project Vincent". John diagramed the major ITS services that used authentication such as AFS, the old "net-print" printing system, POP-3 email, VPN, pub-cookie, WebCT, etc. Some services are being shut down or phased out (the old net-print and POP-3). The remaining services are being converted to authenticate against Active Directory. After a transition period (undefined as yet) the MIT Kerberos domain will be shut down. The ITS goal is provide the means and instructions on how departments and individuals can transition services over a period of time.

The end result of this work will be a single Kerberos authentication system with one set of authentication credentials (Kerberos tickets). Logging into an AD domain-member Windows system and accessing an AD domain-member Apache/pub-cookie web server on a RHEL system become seamless to the user (because both systems use the same credential set). In addition, the presence of two realms with the same name has hampered our implementation of a local Private Key Infrastructure ("digital certificates"). There are products coming up that will rely on a PKI infrastructure existing in our environment.

Collaboration with the College of Engineering has already been done on integrating RHEL systems into Active Directory. A document co-authored by Beata Pruski [ITSYS] and John Dickerson [ECSS] called Integrating RHEL5 Systems with Active Directory was presented in a recent CCSG meeting. A second version (with more advanced configuration topics) is being prepared.

Kunz mentioned that one of the issues that will need to be dealt with is Windows Active Directory "bang accounts". The MIT Kerberos system was populated only with NetIDs (registered to a specific individual) and affiliate/sponsored accounts (which are linked to an actual person via a NetID - the sponsor). As a result each account was officially provisioned and was supposedly used for university business. AD "bang-accounts", however, undergo no formal provisioning and generally have no directly-linked responsible party. Some systems (such as the VPN service) currently lack an "authorization" mechanism and say "as long as your account exists in MIT Kerberos you are authorized to use our service". When such systems switch to AD authentication, it may not be acceptable to say "all AD bang-accounts can use the service". Kunz discussed the use of bang-accounts as "non-expiring service accounts" and how the current "sponsored accounts" do not fit well with a critical

service account need (since they expire). Hascall commented that there will be plenty of chances in the future to provide input into the needs of a more encompassing account provisioning (and "authorization") system.

Open Discussion

Most of the open discussion time was spent talking about the future of account provisioning and implications of moving to a single (Active Directory) Kerberos domain.

Meeting Adjourned (10:00)

Next meeting is scheduled for May 14 (provided a sufficient agenda exists).