

Wednesday, March 28th
650 Kommas Drive
ITS Boardroom 652
2:00 pm

Attending: Andrew Goble, Tim, David Thurm, Curtis Lawson, Rob, Corey, Dave P, Derick, ?, Isaac, Paul Jeffries, Hang, David from SCL, Wes Tolman, Pieter, Brad, ?, Robert Roll, Demian, Jon Ross, Kevin

Tentative Agenda:

- uconnect.utah.edu PEAP/LEAP

Robert is building a server and we're moving accounts over – within a month, we should have vista-supported wireless. Uconnect will be left as it always was; adding the option for PEAP and MSChat with the same kind of security. TTLS password in the backend would be encrypted. Newer technologies (radiator) allows an r-crypt string (AES encrypted). The last issue to overcome is to take all uNIDs/passwords and create uNID/r-crypt strings. Robert is working on a script. It'll just be turning on PEAP as an acceptable EAP option for users. Some users may have to login to CIS and change their password once. OIT will still support TTLS, WPA2, plus Windows Vista "out of the box" clients. By Friday, we will have some accounts useable and in test mode for a month. By May 1st, it should be in a production state. Pieter: what about other campus Radius servers? Dave P: only implementing it in Aruba APs. The ITS wireless implementation is another department that uses PEAP already. On departmental servers, just enable PEAP. Robert: we've tested it once on passthrough; need to test compatability of old TTLS with PEAP; password stuff. Andrew: the changes on the back-end will allow users to use EAP-TTLS with more inner authentication modes. Up until now, we could only to TTLS with PAP as the inner authentication mode. Now we should be able to use any additional modes (there are several) that use a challenge / response or a hash instead of sending a clear-text password. Thanks for leaving TTLS as an authentication option. Users will still have to have the UofU certificate.

- Vista updates – a rumor going around that the SecureW2 client works with Vista (beta). Isaac: can't use the U cert with the current beta client. Hang: scl.wireless.utah.edu (unofficial vista wireless group). Unchecking the box for the cert means there is no verification that the AP is the right one. Go the the SecureW2 website for the beta client. Insecure.utah.edu doesn't ask for the ActiveX/java plug in. Discussion on the "man in the middle" attack that was insecure's demise . . . The concern was uNID credentials could be captured. The method that ITS used can be used to spoof anything (hotspot, uconnect, WebCT, etc.).
- Hotspot.utah.edu issues – Dave P

ActiveX control is there because of layer 3 hops – no way for the authentication device to know your MAC. ActiveX didn't work in last Cisco version. ISO got some RIAA notices – couldn't kick off the bad users because MACs weren't captured. Upgrade (due to DST) – the bug was fixed in new release. ISO wants the IP/MACs. Users must do ActiveX or Java, if these aren't turned on, the fat client gets installed.

1. Possible redesign of the CleanAccess server for hotspot to work (layer 2) without ActiveX and still get MACs; will allow quarantines, etc. ISO is comfortable with this even though MAC addresses can be changed. This is our "due diligence".
2. Take off ActiveX, let it run like it is right now, users cannot be redirected. ISO would have to use DHCP to see MAC/IP address – then NOC would have to put in an ACL/VLAN (blackhole). Trapeze APs could block these users. Packets get denied and the user doesn't know why. Help Desk wouldn't know, either. Jon: what about giving the user a 10.net address? . . .
3. Turn off activeX/java script, do it just like today (ISO gets nothing that they want).

Hang: need to balance user needs with service and not block all methods for access. Corey: not a lot of legal precedents, but General Counsel wants us to be good citizens (and **not** set precedent). If we

move to a model where ISO can do nothing about “bad” hotspot users, Corey guesses that would speed the demise of hotspot. Isaac: what about taking care of this temporarily? There is not an option in the Cisco software NOT to install the heavy client if ActiveX/java doesn’t work. Brad: how long would it take to get the layer 2 option (#1) in place? Dave P: there is only one server right now for hotspot, but if Option 1 works, we could put this on all Clean Access servers. It will take about a week (if it works). According to Cisco engineers, it can be on the distributed architecture for all of campus. Hang: what can we do right now? Dave P: we can turn off ActiveX/Java until we figure it out (since hotspot is still in test mode). Heavy client requires a login (but has no information as to what it should be) . . very confusing. (Can be whatever the user wants.) Option 1 seems okay with everyone. Also, the scanning takes forever – scans for the Top 10 SANS issues. It’s supposed to scan once every 7 days (puts you in a filter list). Corey: we can have a discussion about scanning. Isaac: what about an option for a scan? Would anybody use it? Corey: I assume that anything a user sends over a public network getting used against them. Scans taking 5 minutes would indicate something is wrong. Layer 2 all the way (no firewall) to Health Sciences APs. Corey’s machine has a firewall, but it took him 20 seconds to get scanned. OIT will take this info back – we’ll turn off scanning right now and try to figure out what the long scans mean. Bottom line: ActiveX/Java and scanning off until the Layer 2 option is tested and in place. We’ll revisit the hotspot issue next month (and Hang will buy pizza).

- OIT Wireless Service Level Agreement

Need the Wireless Committee to okay this, then take it to ITAC. Hang worries about the expectation that the client equipment is no more than 3 years old. Dave P: agrees. Andrew: how about stipulating the client’s capabilities: WPA with TKIP, 802.1b card, etc. Should we put actual protocols in the SLA? How about just a statement of reasonability? Derrick: how about revisiting the SLA each year? Theoretically, just about anything should work on hotspot indefinitely. But, this SLA is overarching for all campus wireless. Some problems are entirely due to the client’s equipment. Just take out the “3 years” – it should indicate the last sentence. Service measurement – doesn’t necessarily work even though it is “on”. This SLA is for OIT wireless (anything we support, we install). What does the outdoor part of the SLA mean? OIT has the task of implementing wireless on campus outdoors. Kevin: the intent is that areas that aren’t managed by a department will be provided wireless coverage by OIT (in most cases). “OIT provides and coordinates with other departments for outdoor wireless coverage.” Andrew: we’ll make these few changes and send the document back to the list (in PDF format!!!). Please respond if you have any major issues. If not, we’ll take the revised document to the next ITAC.

Dave P: Fun thing: applet for a tri-mode phone with wifi – allows him to seamlessly roam between wifi and cellular and lets him talk on his desk phone number. Knows when to switch between wifi and cellular. Very cool, and pretty cheap. Server for 10 phones is only \$2000. Major savings on cellular bills. Software: Davides ? (must have a tri-mode phone). We’ll have Dave send this out.