

Wireless Committee mtg
April 25th, 2007
HSEB Room 1730
12:00 pm - 1:00 pm

Attending: Hang Wong, ?, Steve Adams, Curtis Larsen, Andrew Goble, Jon Ross, ?, Tim Urban, Dave Packham, Eric Ross, ?, Nelson Beebe, Pieter Bowman, Brad Hawkes, Wes Tolman, Isaac Jeppson, Joe Breen, ?

Minutes

uconnect.utah.edu updates (PEAP / Vista) -- OIT Departmental

Dave Packham – everything works today. “Works” means on Radius X which was configured to allow PEAP to pass through. Couldn’t get it to go to LDAP – current encryption was incompatible and unreversible. Systems guys wanted to do a crypt string. Had to store an r-crypt key (for Radiator). PEAP authentication comes in – a match is done on the r-crypt key. Robert Roll has been working on a script. Has about 60,000 uNIDs populated in a database. Waiting to test on an AP that needs to come up in Komas. They would like to test it a little longer in Komas. Rob Wineriter will send an email this afternoon about how long he will test it in Komas. Then will turn Radius to allow PEAP. Steve Adams asked about PeopleSoft Roles passwords – what do they have to do? PSRoles users, gNID holders may have to use TTLS for now. Probably will roll it out in May.

Nelson: do any wireless APs support long packets? Joe Breen: none to his knowledge. Bandwidth and the radios are half-duplex – would impact the wireless network if large frames were put out. 802.11n should help. Andrew: n standard is now in draft form. Getting closer. No one said they’ve seen any n rogues yet. In native or non-compatibility mode, it is invisible (runs over a,b and g stuff and causes havoc). Running an n AP in compatibility mode should allow you to see what’s going on. People are buying pre-n stuff now. Andrew: HSC hardware will be in place once the main mesh can do PEAP.

Hotspot.utah.edu Usage

Andrew: Some of the upper echelons on campus are getting nervous about hotspot (pre-emptive worry). At next month’s meeting, this will be an official agenda item (Dave Huth, probably).

Jon Ross – Business had wired ports up to it, but that didn’t prove to be an issue. Legal is worried about CALEA. It’s an old law but has some applications to wireless stuff. Dave P: allows any officer under the Patriot Act to tap wireless communications. If you are compliant with CALEA, you have to provide an interface to law enforcement to tap VoIP sessions (even over wireless). Andrew says we should filter the SIP ports. (-; The real concern is that hotspot is going to grow so much (the path of least resistance) . . . Hang says that if our users want it, shouldn’t we do it. Why are they using hotspot over uconnect? Reliability? Andrew: once PEAP is enabled on uconnect, headaches should

go way down. Hang: we need to tell the higher-ups that once uconnect is working well (PEAP), hotspot usage should go down. Dave P: kids don't care about encryption. Hang: once we give people the information/education, there's only so much we can do to babysit. Andrew: there are so many things that can happen on an open network (bad). Eric: policy about what cannot go over hotspot (University business)? Dave P: why can't I do Kronos from home? Anyone who does University business over non-encrypted SSL pages is the problem. Andrew: I can get in the middle of the hotspot connection and spoof. Are we going down the easy path? Tim: what do the end users want? Jon: Business students say that uconnect is the set up, but they forget their password. If the password doesn't change, it's completely transparent – good. Nelson: but if the laptop gets stolen, the thief has access to the network. Hang: once users find out that uconnect connects automatically after being set up, they'll want that. Jon: hotspot is very attractive to students right now because of the nuisance that is uconnect. After PEAP is enabled, the only drawback of uconnect would be when the password changes. What about a lower security non-changing password. Steve: certificate after jumping through hoops for a period of time; could be revoked if the machine is stolen. Andrew: that would generate a heavier support burden to maintain the PKI and get the cert on the machine. Will this be user education or something else. Checking Gmail on hotspot isn't a big deal, but logging onto their bank site is something else. Dave P: pick your battles. Train users on checking SSL certs, or something else? Steve: this is about personal responsibility. Tim: a good hacker can set up an AP with an official-looking site asking for usernames/passwords. Andrew: it's just a lot more likely to happen on an open wireless network. Dave P: Google desktop is the future. His kids don't do anything on a heavy client – all through the browser. He tells them any personal information must be encrypted. Students at the U are the same way – will do everything on the Web. ??? - two kinds of users: those who use hotspot and those who know about encryption and use it. If they don't care, why should we? Nelson: when it's University data. Tim: shouldn't University stuff be encrypted? Eric: it isn't clear what services should be encrypted. We have a responsibility to our U data and our users. We don't know what our liability will be until it gets tested. Hang: need a policy. Dave P: banks went to a dual challenge because of sniffers . . . should we talk to ACS about a second challenge for uNID/passwords. Andrew: this is bigger than just hotspot wireless, but there probably should be some direction or policy for hotspot, maybe to the point that we ACL some things away from hotspot IP space. Jon: this is good because if they do it on hotspot, they may do it from any open network. Isaac: wants to see a much more specific breakdown, report, of what is going on at the higher level. Andrew: ITC will tell the Wireless Committee to tell them what we want to do. Dave P: just be careful to give a complete reason to ITC. Jon: would the policy be oriented to protect the student, the data, or to mitigate the liability? You can tell people how to drive, but they won't always do it. However, you still have to build the road the right way. Andrew: due diligence. Dave P: multi-factor authentication for the data we really care about (at the data level, not hotspot). Tim: accountability part. We don't know who is logging in on hotspot. Andrew: CALEA compliance – not in our bailiwick, but technically, does this Wireless Committee see any difficulty in providing that info? Tim: dump a spam port to an FBI guy. Andrew: from a tech standpoint, CALEA isn't an issue.

Other - Brad: Layer 2 bridging on hotspot to track MAC addresses . . . ? Dave P: not doable, testing DHCP to work off the Clean Access Server. Trying to tie an IP address to a MAC address and be able to blacklist it. Brad: are the tests are encouraging? Dave P: Cisco says it's going to work. Just started on the tests. Tim: still working on the blocking. Isaac: hotspot works so much better now that Active X is off.

Curtis: Wireless buildings update: Math, Business Classroom, Kendall Garff bldgs are done, ready for cabling. The campus Wireless AP list is up to about 120. Jon: EHS requires the exact route the cable will follow before they give the approval to run cable (because of asbestos) – but they don't keep maps. It's a Catch 22. Brad: will Physics (JFB and South Physics) get done before Fall? Curtis: trying to do a building every week and a half . . . cable guys are part of the timeline. He listed about 10 buildings before Physics. Dave Kosanke said there were only a couple of those 10 buildings he was worried about. Nelson gave a public compliment to NetCom on what they've done taking over Math wireless. They did a great job. Hang: with the campus VPN, tried to fire it up yesterday before getting on hotspot and it didn't work the way we said it would . Dave said 99% of hotspot users do put in a uNID, but we don't verify them.

Hotpot.utah.edu Scope & Future Usage / Issues

Andrew: for next month, Dave Huth will be here to listen to Wireless Committee concerns about U data (like Kronos). Isaac also wants to have a techie from XMission to talk about how they do their open network. He'll follow up on it.

Next Meeting: Wednesday, May 30th at noon. Room tbd, will try to do pizza next time. Can do it anywhere people want, if they don't want to do the Kommas room. May do it in EBC next time.