

University of Utah Wireless Network Committee
June 7, 2006 ~ 10:30 AM – 12:00 PM
650 Komas Drive, Board Room

I. Task Force Funding Update – Bryan Morris

Document handed out – spells out the relationships between ITC, ITAC, Wireless Committee; ubiquitous definition, and the campus wireless funding model. Wireless funding comes from one of two sources: centrally funded or departmentally funded. Stipulations for campus wireless networks that are centrally-funded (either OIT or from Task Force funds):

- Must be compliant with campus wireless standards
- No hardware changes required unless upgrade is necessary; then, OIT will repair/replace & maintain new equipment
- no new central funding will be used to maintain or replace existing infrastructure that isn't in keeping with the new campus standards that this body is defining*
- any new implementations will be funded & maintained by OIT (not ITS)

Stipulations for campus wireless networks that are departmentally-funded:

- good neighbor policy (comply with the standards being decided by this committee)

- departments with their own networks will get some OIT support, but not at the same level

Derrick: if we have a wireless network funded by Task Force, is OIT just going to come in and take over?

Dave Huth: ITC sets the direction; every department has an ITC representative. OIT follows those directions. ITC has set the direction for campus wireless. ITAC helps with the technical solution; the Wireless Committee is to advise ITAC on this. The ubiquitous (roamable) campus wireless network is not expected to replace the research wireless or department wireless networks. The difference between HSC and OIT is a little cloudy right now – must define how the roaming is going to happen. Task Force requests ended up becoming a prioritization list of buildings needing wireless. What that results in needs to be based on the consensus of this group. Standards, ubiquity requirements, how campus must meet these.

Andrew: to clarify – will the systems be side by side, redundant, or will the old be ripped out and replaced? How will they be managed?

Bryan: the HSC/OIT infrastructures hinge on the roaming question and its logical conclusion. He wants to begin heavy discussions on that asap. As far as what to do tomorrow – same as it is today.

Question: an example would be requesting Task Force funds for a server for my department. Why am I putting in something that OIT is going to manage?

Kevin: ITC said “ubiquitous must be secure, authenticated, encrypted service ubiquitous across campus with persistent connections.” That component has to be addressed, but not

at the expense of the individual departments. ITC basically said that OIT should make that happen. If this isn't the best way, this body should go back to ITC to say so. The roaming issue is a big technical discussion. ITC wants roaming; thus, departmental cooperation will be necessary.

Question: confusion – do I do this or does OIT? Do I have to go to ITC every time I need or want to tweak my system that was purchased with SCAC funds? Answer: not today, as long as the (current) campus standards are being met.

Derrick: Does ITC set security definitions for wireless? Bryan: yes, but ISO does specifics. Derrick: does that include VPN? Kevin: this body is to advise exactly what security means.

Nancy: in HSC, they make proposals for funds each year through SCAC (may or may not get them). Why would we make a request in a Task Force proposal for any wireless funds if OIT will pay for them.

Kevin: SCAC is one component of Instructional Computing funding (which is much bigger). ITC oversees how that money is spent. ITC is possibly choosing to use a big chunk for campus wireless.

Dave P: would HSC be okay with Trapeze being put in the Pharmacy network? Bo: no.

Derrick: elemental problem that needs to be solved: OIT/ITS collaboration. Isaac: why do we have to discuss funding in this committee at all? Andrew: because many of our technical decisions are hinged on how the funding occurs.

Corey: to be clear – if the equipment is funding centrally, then OIT would manage it. If the department funds it, they run it. The problem comes with roaming – required by ITC.

Kevin: we may have to go back to ITC saying we can't do roaming. Pierre Pincetl advanced a proposal to ITC with a ubiquitous computing environment for campus – this was a while ago (1.5 yrs ago). ITC agreed unanimously, as did Loris Betz and Dave Pershing. OIT doesn't dictate anything – we get our marching orders from ITC.

II. Hotspot Initiative

- Web Page Design – Rob Wineriter, Mindy Tueller
any policy about using a false email address? No – just need a unique identifier.
Nelson – why can't it generate that behind the scenes? Dave P: Clean Access doesn't have that capability.

Suggestions: put “**Unencrypted** traffic sent . . .” ; add the port list restrictions when it's finalized. Dave P: Xmission doesn't have any outbound port restrictions. No solid answers from Legal yet; but they haven't shot us down. Dave Huth: Legal is for the project and will help with anything that advances the business of the University. Liability – are we more legally liable than a typical ISP? Kevin: we are the same. Corey: we limit some things that a typical ISP doesn't on the campus network to be good networks.

- ISO Port Restriction Policy – Steve Scott: we have a responsibility with this. In a wired environment, we know what is happening. In this wireless environment, we can't track what is happening. We want to be good neighbors. If you want more access, get a gNID and use the full network. Corey: there is accountability with the gNID system. On this hotspot system, no accountability. Dave P: hotspot will run on the Clean Access system. We can add a login box to allow the insecure network (authenticated and accountable). Dave Huth: we are supposed to determine how to implement hotspot – insecure can be a second step. ???: seems as though we have good three options: hotspot – enter any old goobledygook and get access. With a gNID – use the UConnect network. With a uNID & password – insecure or UConnect. Kevin: Council of Academic Deans told Steve Hess that guests to campus (researchers, guest lecturers, etc.) don't have the access they need at the U. The uNID thing – they don't want to be held to gNIDs because everyone was using the same one to log in. They just want broadly available access for basic stuff (email). Derrick: what is the difference between putting in a fake email address vs a MAC address. From a user's standpoint, it's one less step and we're kind of hiding what we are doing. Jon: it's just a work-around for the Clean Access system. Andrew: the uNID is kind of sensitive on this campus. Rob W: but you can pick which network you want to use (hotspot, insecure, uconnect). Nancy: this login page encourages putting in a clear text uNID. Isaac: why are we trying to provide security on an inherently insecure network. Steve Scott: to be good neighbors; to avoid problems arising from traffic leaving this network. Dave P: Clean Access can put people in different roles with completely different capabilities. Shouldn't we be just killing the people who accept a uNID on campus without enforcing security on the server side rather than on the client side (this discussion). It can be spoofed, but we're taking one piece of straw out of their haystack. Steve: we are allowing basic access. Nancy: just want guests to have access to legitimate public resources (including streaming). Andrew: we're trying to accommodate everyone on this network. Bryan: Starbucks analogy: filters on the front door to keep the bad guys out and to keep us good neighbors. Isaac: shouldn't restrict the outgoing ports. Dave P: this hotspot network goes through the front door firewall. Corey: but if someone using this network attacks Google, ISO gets called. Hang: can't we come up a list we don't want. Derrick: should we set up a subcommittee to determine the port list and the full committee can vote? Corey: can we set it up so most hack tools, viruses are stopped, best effort. Steve: we'll have every kid in the valley up here sending out attacks. Derrick: let's do a test. Steve: leave it open and see how many complaints we get? Certain restrictions are necessary, maybe the things we block at the front door. Now ISO has a new task. ISO gets calls weekly as things are; this will be a big can of worms. XMission hasn't gotten any calls. Maybe a test will be okay. Corey: maybe XMission just doesn't return any calls.

Andrew: what unauthenticated services do people need or want on Hotspot (outbound)?

Good:		Bad:
Web	(80, 443)	
VPN	(IPsec)	

Joe Breen: other comparable universities have made their unencrypted networks completely open outside the firewall. Their results: a few users did annoying things, but they didn't get a large amount. They just turned off those MAC

addresses. They did put in the antivirus and blocked the known bad ports. Joe recommends we try running it open but block all main virus ports, Microsoft ports, etc., for 3 – 6 months. Then, see what we've learned. If it's really bad in a shorter time frame, then it's obviously not a good idea and we back off. It's a balancing act. We can take a stepped approach with a defined timeline. Give feedback to this group and ITAC, ITC at that time.

Dave Hoisve: most users won't understand why they can't do certain things – this is a huge support issue. John Stratton: haven't had any complaints on their "open" network.

Andrew: motion – to open this up with the default port restrictions (on the ISO blocked list) and bandwidth restrictions – outbound only. No inbound. ISO will forward that blocked list to the Wireless Committee. Treat this like all outside networks. Derrick seconded. Unanimous in the affirmative.

Pieter: what should the domain name be, since it's IP space outside the U? Should it be _____.utah.edu? any answer??

- Report of Legal Research / Policy – Dave Huth (Tentative)
- Timeline Development:
 - June 15th ITAC meeting
 - MPLS tunnel will be turned on first outage window in June per Tim Urban. This should be running by the end of June. (July 1st)
 - Shake out period prior to production: 30 days (testing in some key buildings like EBC, Libraries, Union)
 - Production: July 15th, 2006
 - Turn off insecure.utah.edu? Disable the login functionality with information on what is happening (based on where it is available on campus) around August 15th. Hang: motion to kill insecure. Let ITC know. Early off date: _after school begins___? ITC August meeting to get approval. Add an exception if departments need it longer.
 - ISO review on port restrictions: October 15th.
 - Final insecure SSID off date: October 31st.
- Motion to Approve / Disapprove hotspot.utah.edu for Recommendation to ITAC at June Meeting – unanimous vote of approval.

Next meeting – roaming issues. Will schedule an outside meeting for funding stickiness. Andrew will have proposals for ITAC at next week's meeting.