Problems with the UT Guest wireless network:

* Security by pop-up? The wireless authentication system for the UT Guest network uses pop-ups to "maintain" your login. Most people at this point in history have pop-ups blocked in their web browser. You have to enable pop-ups to get in. See "security certs" below, for other unintended bad security consequences that are the result of the way the UT Guest network implements its security system.

* Bandwidth limitations: You have a limitation of bandwidth external to campus, but you're not actually told that fact anywhere when you log on (unless you decide to investigate the cheerful message on the login pop-up that tells you have "first-class bandwidth" and go read the help documentation). Even in the help docs, you're not told what your bandwidth limit actually is. In any case, though, in a room full of people running computers that are trying to use the network, you get dropped for *inactivity* as well, when other users consume the available wireless bandwidth: that's because we seem to be on an 802.11g wireless access point, which has pretty low limits for number of concurrent connections, and tends to have short lease times, on the order of 10 minutes (which might explain the dropping of VPN, below). There are newer wireless access point technologies (802.11n, high-performance wifi from vendors like Xirrus and Cisco) that can accommodate many more simultaneous connections and don't have the limit on connection time, but those don't seem to be in use here. So you can get dropped for using too much external to campus bandwidth or for using not enough internal wireless bandwidth. Then you run into the next problem, described below:

* Sensitivity to number of attempts to connect to the UT authentication system: If you get kicked off the wireless for reasons above, and you have running applications that try to reconnect to networked servers (e.g., twitter, ichat, email, etc.) the wireless system decides that you are infected with a bot, and shuts your access down for five minutes. If you continue, during that five minutes, to connect, you probably extend your banishment. In fact, you really have to turn wireless off altogether--for five minutes--in order to regain your wireless access. But nothing tells you that: you have to deduce it from the help documentation on the UT wireless authentication site.

* Periodic ditching of VPN: You might think you could get around some of these problems by running VPN, which would shield at least some of your activity from the brain-dead scrutiny of the UT security apparatus, but it turns out that the UT wireless just periodically ditches your VPN connection, probably because your lease has expired. The fact that VPN is periodically dropped is even documented in the wireless help documentation--documented, but not explained.

* Security certs: Bad implementation of security cert on the authentication service, such that it masquerades as the cert of any other secure site you try to reach through it, which results in frequent messages telling you that site X has a bad security cert, which turns out to be the cert for the UT authentication service. If you

get tired of responding to these messages and then not getting to the secure site you wanted to get to, you have to tell your browser to ignore security certs altogether--great!  That's secure.

* Needless windows bias: when the authentication system decides that you are infected with a bot (because, for example, your twitter client is trying to connect to the twitter server too frequently after you've been dropped from the network) the solution UT offers you is to go to Microsoft.com and download a fix for rootkit infection.