Faculty Senate Meeting
October 7, 2003

New Business

The FITRC (Faculty Information Technology Review Committee) has voted its approval of a proposed script which will assure that all networked Windows computers on campus have installed the critical updates that are necessary for security purposes. Once implemented, which could be as soon as the end of October, 2003, the script will run every time a Windows computer logs into the network. The script will check the current patch level of the machine. If there is a critical security update that has not yet been applied to the machine, the update will automatically be downloaded and installed. If a reboot is necessary, a message will pop up that says the user will need to reboot the machine for the update to be in effect.

When there are infected Windows computers on the campus network, the potential for disruption of network traffic is great. For example, on Friday afternoon, the 3rd of October, 2003, our network was seriously disrupted by computers infected by the Welchia worm. Over 800 networked computers were infected by this worm, nearly 200 of them being computers in faculty/staff offices or campus labs. This network disruption made it impossible to connect to the Windows Update site to download critical patches, interfered with off-campus access to our servers and our email system, and so on. The patch that could have prevented these computers from being infected by this worm had been available since July of 2003. Clearly, our efforts to teach campus users to update their machines has failed. Sometimes it is much easier to change the technology than to change human behavior.

The FITRC has asked ITCS to provide a "sandbox," an area where users who wish not to be required to keep their machines updated can be networked in such a way that infection of their machines will not have serious impact on the rest of us on the main network. It will, however, take several months to construct such a sandbox, and it is likely that persons who elect to enter the sandbox will not be happy with it – their computers are likely to become compromised or experience network difficulties whenever any of the other computers in the sandbox are infected.

Karl L. Wuensch
Chair, Faculty Information Technology Review Committee