

Implementing Additional Security in the University of Cincinnati's Wireless Network

In the past few years, the University of Cincinnati has implemented an enterprise class wireless network consisting of nearly 700 access points with over 5,000 registered wireless users. As this network grows, it will include more on-campus coverage as well as the campus edge included with the implementation of the Uptown wireless mesh network.

From the original implementation of 802.11b technology which provided wireless speeds of 2mb and then 10mb, to the new standard of 802.11g technology, which provides speeds of 54mb, UCit has been consistent in advancing wireless technologies in the network as these technologies have become universally available.

Initially, the wireless network security relied on a Service Set Identifier (SSID) and a wired equivalent privacy (WEP) key, along with mac address filtering. The SSID makes it easy for users to see the network and associate to an access point. For UC, the SSID is NoWireUC. The mac address is the wireless card's hard-coded identifier. The WEP key is an encryption key that encrypts the data sent over the air. Initially, the WEP key was a 40-bit key, the standard at that time. The standard evolved to a 104-bit key, providing a higher level of security.

The Institute of Electrical and Electronics Engineers developed new standards to enhance wireless security. This new level of security, known as 802.11i or WPA2, breaks away from using SSID's and WEP keys to authenticate onto a network and relies on the wireless client's ability to authenticate onto a network with a username and password and then encrypts the data with a higher Advanced Encryption Standard (AES).

UCit will enable the new WPA2 wireless security standard on all access points beginning January, 2008. WPA2 users will not need to register their wireless mac address as they do now, but will have the option of using the legacy wireless network or using the higher level of security for their wireless connections. Legacy wireless network registration will be available during Winter Quarter so that users without the hardware or OS capable of supporting WPA2 and the AES encryption standard will have ample time to augment their wireless client. Beginning with Spring Quarter, legacy registration will be disabled, new wireless users will need to support the WPA2 standard. UCit will monitor the legacy wireless network to determine the number of users still connected and the feasibility of maintaining dual networks. The legacy network will stay in place until data supports shutting it off.

Users wishing to implement WPA2 must have a supplicant on their wireless device that supports 802.1x. Windows XP and Vista natively support 802.1x authentication, as well as MAC OS X 10.3 and above. Versions of 802.1x are readily available for download for Linux devices. Users will need to follow the detailed directions posted on the UCit web page to configure their 802.1x supplicant for access to the wireless network.

Instructions for new WPA2 can be found at:

http://www.uc.edu/ucit/access/WPA2_INSTRUCTIONS_v2.html