MDPCS – TECH NOTE

WIRELESS SECURITY

The Miami-Dade County Public Schools (MDCPS) Network Security Policy states that "Network installations with wireless components must maintain the highest level of security possible" and "…the installation's security features must be turned on". Wireless systems without security are easily penetrated and provide hackers with the same access they would get by plugging into one of the schools' hardwired network drops. Unauthorized modification and/or theft of information, denial of service (DoS) and theft of Internet bandwidth are among the possible unpleasant side effects.

Wired Equivalent Privacy (WEP)

The WEP format of encryption, based on the original Institute of Electrical and Electronic Engineers (IEEE) 802.11b standard and used in much of the recent wireless equipment is seriously flawed. It uses a low bit encryption method combined with a single key. Freeware like "AirSnort" can break this encryption in as little as 15 minutes. After that the hacker has access to the network. Many of the manufacturers have anticipated a revised IEEE standard by introducing higher bit encryption and "per user, per session" keys (meaning that even if a hacker breaks the encryption on a current session, they will still have to break the encryption on all other sessions individually). At this writing (07/2002) many of their newer products include this revision with names like WEP Plus, Advanced WEP, Enhanced WEP, etc. There are software upgrades in many cases that will also add this higher security to older installations. The new IEEE standard is expected later in 2002.

In the meantime, most of the "net stumblers" and "war drivers" (hackers who drive around and locate wireless networks by using a very simple setup that includes a laptop with an access point, a directional antenna and free software) are ignoring wireless networks with security turned on because it is so easy to find wireless installations with no security at all. This is why the security should be turned no matter how weak.

Older Wireless Installations

Older wireless installations (3 or more years old) may have minimal or no security available. This equipment should be replaced as soon as possible because of the risks described above.

Wireless Security Settings

In general, there are 5 possible security mechanisms that can be enabled in a wireless system.

1. **MAC Address Access Control**
   Settings may be available that require a closed system and limit which computers may join the network by MAC id. The MAC ids of only those computers to be joined to the network are entered and no other computers will be allowed to join. Note that any time you add or remove computers from the network, you must modify the MAC id list in the wireless setup.

2. **Enable Closed Wireless System by Requiring Network Name**
   There are also settings available that require all computers joining the network to have the network name in their profile. Each member station must then have this same network name entered into its profile. This prevents computers not having

that network name from joining the network. The network name is hidden from outside hackers either by a separate setting or automatically when the setting requiring network name is marked.

3. **Radius Server**

   If the network includes a Radius server, some wireless systems can connect to it to authenticate users. This way, even if hackers get past the other wireless device security mechanisms limiting computers, they are still prevented from getting past the wireless component by user authentication.

4. **Encryption**

   Encryption should be turned on if available. Although some system performance degradation may occur, degradation will be the least of the problems if hackers get in. The setting to enable encryption depends on the wireless card and the access point being used. For instance, Orinoco wireless systems have the following possible types:

   - Silver wireless cards have 40 bit encryption and the profile allows up to 4 encryption keys, each 5 characters long and using upper case and numeric characters.
   - Gold wireless cards have 128 bit encryption and the profile allows up to 5 encryption keys, each 13 characters long and using upper case, lower case, special, and numeric characters.

   Of course the encryption is limited by the maximum encryption allowed by the access point. Check your wireless components' online help, manual, web site or vendor to locate this information.

5. **Default SNMP Password**

   When installing the wireless system, be sure to change the default SNMP password. This is the first password hackers guess.