WIRELESS NETWORK SECURITY

David Papp, (780) 951-4869, david@remote.net, Mar/04

** Be very careful when working with wireless technology and understand the vulnerabilities.

Select appropriate hardware – Ensure wireless device supports more than 40-bit WEP, has upgradeable firmware. Also single vendor hardware facilities compatibility, especially with large WEP keys.

Manage SSIDs – Default SSIDs should be changed immediately and periodically. Broadcast SSIDs should be disabled where possible. While this requires users to manually enter the SSID on their system, it helps deter unauthorized connections.

Change default usernames and passwords of access points – Passwords should be at least 8 characters and a combination of alphanumeric and non-alphanumeric symbols. Must be different than SSID.

Use large WEP keys – 128-bit or greater.

Provide VPN service – Added layer of security with stronger encryption.

Require user authentication – Corporate used access points should support LEAP, WPA or 802.11i for user authentication for wireless access

Filter by MAC address and/or IP address – This makes it extremely difficult for your wireless network to be compromised. DHCP services should also be disabled when filtering by IP address.

Secure the wireless clients – Like wired systems, wireless devices should be outfitted with firewall and antivirus software to prevent them from being compromised and also preventing malicious cost from impacting the device as well as the network.