

School's Wireless Networks are a Security Headache

Doug Prouty
dprouty@cccoe.k12.ca.us
Contra Costa County Office of Education
September 2003

A local elementary school asked if the county office could assist with a network survey. They were still not wired to the classrooms and they had a vendor proposal for us to look over. Some areas of the campus were going to be tough to access and the costs would be prohibitive. I suggested that they consider a wireless solution. Wireless Ethernet access points would be easy to setup and we could have teachers and students online in a day or two. Using the non-regulated 2.4 or 5.2 GHz radio frequency, the IEEE standard, 802.11, can bring 11Mbps to 52Mbps connectivity to a computer's wireless network card. When I called the district's IT department to suggest this solution they immediately cancelled the idea and stated security concerns.

The security of wireless networks is an IT Manager's number one obstacle to wireless deployment. Network security is always a concern as schools and districts take the brunt of network attacks and misuse. We are now spending a large percentage of our budgets and efforts installing firewalls, Cisco PIX boxes, virus and content filters, spam control and packet analyzers, in an attempt to block intruders and regain control. With these technologies in place, we are just beginning to feel like the front door is secure. Purchasing a wireless access point at the local computer store and plugging it in out of the box to a jack in the classroom, props the backdoor wide open and even advertises to the neighborhood that the network is here for the taking. A teacher can easily plug a wireless access point into the jack in their classroom and provide extended access to the computers that have a wireless network card. Unfortunately, this includes the neighbors and anyone else that might be in range.

Wireless Popularity on the Rise

Even still, wireless networking is really taking off in our schools. In the Peak Group's report titled, "Wireless Technologies in Education" school districts were predicted to spend \$776 million on wireless technologies in the 2002-2003 school year. A wireless network card is now standard in just about every new laptop. Desktop systems can add wireless access for under \$50. The price of wireless access hubs have dropped below \$40 and they are simple to setup. A novice can plug in an Ethernet cable and be online in seconds. Lots of people are installing them in their homes attached to their modems thus providing roaming access anywhere in their house and yards.

The wireless 802.11 standard is being used to give students and teachers access anywhere on campus and the same technology can be used for a teacher's wireless phones/radios. Handheld-Palm computers can now access the same network. Administrators can check student schedules and information while roaming the hallways. Physical Education teachers can take roll and enter grades on the playing field. Students can access network

resources and the Internet from anywhere on campus without “plugging in.” Unfortunately, an outside hacker has this same ease of connectivity.

Why is Wireless such a Security Risk?

By default a wireless access point (WAP) broadcasts their Service Set Identifier (SSID). This means that anyone in range can see that the network exists and may be able to connect. The SSID is the name of the wireless network and will show up in your computer’s (wireless client) wireless access utility. The WAP’s default name for the SSID and the administrative password is standard for each manufacturer and is easily found. Linksys and Compaq use their company name while Cisco’s Aironet uses “tsunami” and the Apple Airport base station uses “Apple Network” for their SSID’s. If you open up your laptop in range of a WAP that is broadcasting, a user expects to get online.

So Why Should You Secure your Wireless Network?

Since an intruder would come in behind your gateway and firewall, they could access servers, workstations, routers and printers. An uninvited guest with Sniffer technology could acquire email, FTP and server account information including login names and passwords. A school or district could possibly be compromising their student information system as well as other secure databases. At the very least, the intruder can use most of your bandwidth, setting up a download server or other malicious service. If they are involved in an illegal activity such as spam or pornography, their access appears to come from the schools network. Any investigation and legal ramifications would then point to the school district. Your home network is also at risk. Most users don’t bother to take security measures to protect their wireless access point. Your connected desktop may have financial data, tax records and other information that can make you vulnerable to financial and identity theft.

If you do have malicious intent, it does not take much knowledge or high-end technology to identify insecure wireless access points. A common method is to add an antenna to a laptop wireless card to increase its range. Add freeware such as NetStumbler <www.netstumbler.com> and drive your car around until you find an access point. Similar experiments have found a great deal of networks in business and residential areas with over 50% of them insecure and allowing open access. Warchalking is the name given to a practice where people use GPS to mark and post the presence of open wireless networks so that other can enjoy free wireless Internet access.

How Do You Secure a Wireless Network?

There are several measures that should be taken in an attempt to protect a wireless network. These range from simple first line settings to a more advanced approach. Only the last bullet requires extra hardware. The first set is just a matter of configuration. They are listed and explained here by level of simplicity and degree of security.

- **Update Firmware:** Security on older access points have been improved within newer firmware upgrades. Download and install the latest for your wireless access points.
- **Change the default passwords:** The admin interface is password protected but the default password is always the same. The manufacturer of the device is also broadcasted so a intruder can get a manual from the website easily find the default password.
- **Disable Remote Management:** This is prevents configuration of the access point through the Internet.
- **Disable SSID Broadcast:** The SSID is must be known in for a user to connect. Hiding the name by disabling SSID broadcast will make the network hard to find.
- **Change the default SSID:** Now that it is not broadcasted, you need to change it so an intruder doesn't just guess the default. Just like passwords, make it hard to guess.
- **Enable Wired Equivalence Privacy (WEP) encryption:** Also enable the broadcast key rotation feature. There are lots of articles about the insecurity of WEP encryption. This is built in and at least provides a little protection. Use 128bit or higher encryption and be sure it is required for increased security. Check that your wireless clients have the latest drivers for the WLAN cards. Some old cards may not support WEP.
- **Disable DHCP (*Dynamic Host Configuration Protocol*):** This is a pain, but if possible assign IP addresses to your wireless devices. This will force an intruder to guess viable IP and Gateway numbers.
- **Filter by MAC address (access control list):** All network cards come with a unique 12 digit hexadecimal number that is assigned by the manufacturer. You can configure the access point to only allow specified addresses. This will block other computers form accessing the network. Some hackers however can "sniff" legitimate MAC addresses from the data packets in the air and reconfigure their network card to match. The amount of effort to update changing and new MAC addresses might not outweigh the benefits.
- **Don't Boost your Signal:** It is better to increase the number of access points as opposed to adding an antenna to push your range. This will help keep the range to within your site so there is less of a chance for neighbors to "hear" your signal.
- **Separate the Wireless LAN (WLAN):** It is most secure to have the wireless network attached to a separate wire run. This can then be segmented at the router for increased security. If your switches can use VLANs, configure a separate one for the wireless hubs. You will need to decide which services you will want to provide. The more limited your wireless users are, the more secure.
- **Stop Rogue Access Points:** Impress upon users the security issues of setting up their own wireless hub and have a strict policy against anyone adding a wireless connection to the network. Use software to try and monitor the network and keep an eye out for these hubs.
- **RADIUS (*Remote Authentication Dial-In User Service*) Server:** Companies are beginning to include capabilities for RADIUS authentication. This provides an authentication for the wireless client to the access point and the access point to the client. It also can include authorization, preventing breaches and provide

accounting which can help in detecting rogue access-points attached to your LAN. The **IEEE 802.1X** standard was ratified in April 2003 to address layer 2 (MAC address layer) security. When a client requests connection to the wireless access point, it must provide credentials. The access point then forwards these credentials to the RADIUS server for authorization and authentication. The main security measure in 802.1X is EAP (Extensible Authentication Protocol). This allows manufacturers to create their own method of passing credentials. Currently, there are four common methods: EAP-MD5, EAP-Cisco Wireless (LEAP), EAP-TLS, and EAP-TTLS

If you do nothing else, the basics such as changing default passwords, turning off SSID broadcasting and enabling WEP is a good start. Whatever configurations that you make to your wireless LAN, be sure to write them down (and keep them in a safe place.) If your access point ever crashes causing it to lose all of your settings, you'll be glad you have a record.

Bibliography

WLAN Security on the Rise

2/4/2002 - Dave Molta

<http://www.networkcomputing.com>

Your 802.11 Wireless Network has No Clothes

3/20/2001 – Arbaugh, Shankar, Wan

Dept of Computer Science, University of Maryland

Wireless LAN (WLAN) Security

Dr. Peter J. Welcher – Chesapeake Netcraftsmen

<http://www.netcraftsmen.net/welcher/papers>

Exploiting and Protecting 802.11b Wireless Networks

9/4/2001 - Craig Ellison – PC Magazine

http://www.extremetech.com/print_article/0,3998,a=13880,00.asp

How to Use Wireless Security

CNET

<http://www.cnet.com/internet/0-3767-8-21067832-1.html>

Cutting the Cord: Wireless Computing Comes of Age

Kristen Hammond and Judy Salpeter

<http://www.cosn.org/initiatives/compendium.html>

Wireless Technology in Education: Moving from Pilots to Mainstream

<http://www.peakgroup.net>

Wireless Networking in Schools: A Decision Making Guide for School Leaders

British Educational Communications

http://www.becta.org.uk/news/wireless_networks

Wireless Networking in Schools

<http://members.ozemail.com.au/%7Ecumulus/wireless.htm>

Keith Lightbody

Wireless Security Blackpaper

<http://arstechnica.com/paedia/w/wireless/security-4.html>