



## Wireless Security Review – Concerns and Solutions

By Jane Bloomquist  
and Atif Musa

We know Wi-Fi (wireless fidelity) is not secure, but its use is spreading. In fact, Crain's Chicago Business magazine recently announced the opening of the city's first hot spot, short for open wireless access. The Picasso sculpture in the middle of the Loop marks the best place to pick up the city's first test of a Wi-Fi network, and there are more planned, particularly for lower income neighborhoods where, as Crain's put it, "Internet connections are as rare as Starbucks locations." By combining connectivity with agencies to supply computers and hand-helds, Chicago is building its own bridge over the digital divide.

Chicago Public Schools is a 90% poverty district; we, too, must bridge the digital divide. As the largest school district and largest employer in Illinois with 435,000 students and 50,000 employees, CPS (Chicago Public Schools) manages a huge WAN (Wide Area Network) with hundreds of LANs (Local Area Networks). Our enterprise network contains over 60,000 workstations, 12,000 switches, hubs and wireless APs (Access Points), and 1,200 servers. CPS is embracing wireless to solve connectivity problems in our 650 buildings.

As with most problems, connectivity solutions have been evolving over several years. Through E-Rate and other sources, all schools now have a T1 line, but some schools still have access only in a few rooms. These are the sites that present unique infrastructure challenges. Wireless and hybrid (wireless and hard-wired) networks are providing the solutions.

The use of wireless often avoids the cost of major construction or high voltage electrical upgrades. A wireless solution also avoids the mess and disruption attendant with such infrastructure modifications. Finally, a wireless installation can be completed quickly. The wireless solution is frequently the obvious choice, and wireless popularity has grown quickly. Setting standards, on the other hand, takes time. Further, the first wireless standard was flawed. Many vendors developed their own solutions, but some of the solutions are proprietary and don't talk to each other. Further, none of the solutions provide total security.

Wireless security is almost an oxymoron - it is pretty hard to lock down radio waves. There is a whole movement to open up wireless connectivity, to look for and advertise hot spots for everyone's use. For some individuals, searching for open wireless access is a hobby or a game called war driving or war walking. These individuals spend time walking and driving around with wireless devices. When they find connectivity, they advertise it for others by "war tagging" or writing graffiti (see picture). The Chicago Public Schools got war tagged, and it caused us to re-examine our wireless processes and procedures.



**Graffiti on a building  
advertising a wireless hotspot**

### **Risk Analysis**

When installing wireless access, it is essential to consider the risk. Securing wireless can be very expensive, particularly in an educational environment with limited resources. You need to decide what you are protecting and how much it is worth. The risk analysis that CPS went through included assessing what threats our network might face. In considering who might be trying to access what, we realized that much of our threat might be internal. The "who" could be our own students. The "what" included administrative information which must be protected. In fact, the medical data we must maintain on each



student is subject to federal regulations for strict security. And student identities must be protected for their safety. If you think about the risk factor in terms of protecting children, our information is even more critical than credit card numbers. We have good reasons not to use insecure wireless, and one very compelling reason – access – to use it. Connectivity was the driving force for using wireless. In Chicago, we bit the bullet and budgeted additional funds to try and secure a wireless network.

### **Policy First**

Our wireless security procedures involve several steps. The first, and a required step for everyone, is to establish and maintain policies and procedures. In the past forty years, CPS has passed something like 300 policies; we don't do this lightly. We created our network policy as a dynamic document enforcing standards that can and do change as technology changes. Once we had a network policy, we set up detailed technology documents for vendors and employees providing step-by-step procedures with clearly articulated and swiftly employed consequences for not adhering to the policy.

If you have a policy document in place, it may be possible to simply write the step-by-step procedures to implement wireless security. Users, however, must understand the extra importance of securing wireless connections; otherwise the process will be compromised.

It is always a good idea to keep the policy short and concise. A high-level policy will then point to procedures that can be easily updated. Using policy as guidance, decide how and by whom you wish your wireless network to be used. Also make a firm decision about providing your surrounding community with a public Internet access point. While verboten from the security standpoint, many organizations and individuals wish to offer this service to their neighbors. Policy must at all times guide such decisions.

### **Basic Wireless Configurations**

Our second wireless security measure is to employ the basic security features that are built into all wireless APs. These configuration tools can help secure the network, but the trick is to change the configurations from their factory defaults which are readily available on the Internet. Changing SSID (Service Set Identifier or network name) and WEP (Wired Equivalent Privacy or encryption) settings provides minimal security, but the settings are easily configured and are essential steps. While changing these settings will not keep out a determined hacker, they will block casual and inadvertent intrusions. These and other configurations are available on the manufacturer's CD shipped with wireless products.

To change the SSID, open the AP Manager application on the manufacturer's CD. Don't use an easily identified SSID such as the name of your school or district. If possible, turn off broadcasting of the SSID. If you do that, though, all users of the AP will need to know its network name to attach.

WEP is the original encryption protocol for wireless networks built into APs, but most APs ship with WEP disabled. Enabling and configuring WEP is fairly easy. End-users are able to configure their own settings with basic documentation, reducing the management overhead for administrators. Unfortunately this protocol suffers from critical weaknesses that limit its effectiveness. WEP encrypted networks can be broken into with concerted effort on the part of an attacker. WEP has the advantage, however, of having the broadest range of support among wireless vendors (including support for PDA and other lightweight devices), and WEP was the first cross-platform security solution. However, it is important to understand that if your WEP key is broken by an attacker, your wireless network will be completely open to attack.

When configuring WEP, use the strongest encryption available. It is also helpful to change the encryption key as often as possible, but, as a manual process required on all wireless devices, changing WEP keys does not scale well.

**VPN Provides Security for Wireless Connections**

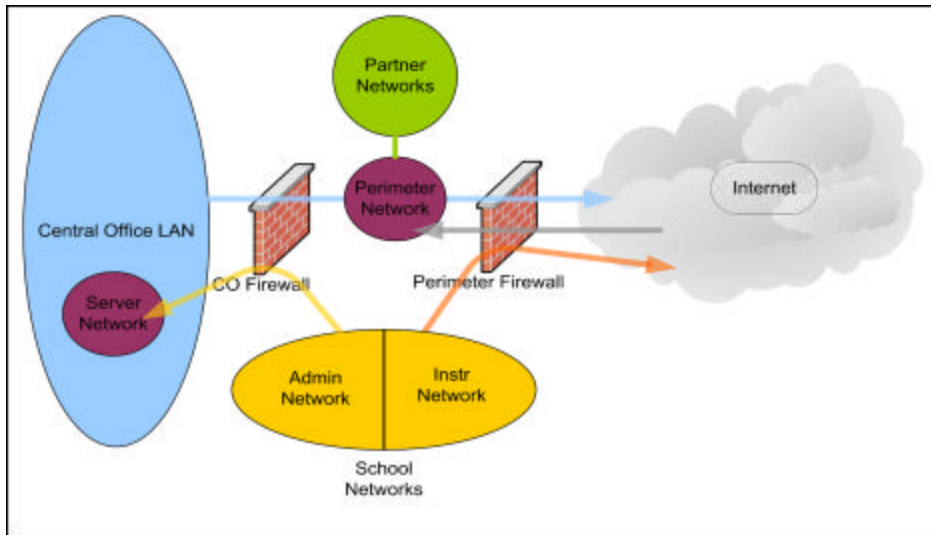
A third wireless security measure is VPN (Virtual Private Network). VPN has a history of securing Internet connections, and it is not equipment dependent, making it a good choice in an eclectic environment such as CPS. Since we have been using VPN for several years as a secure solution for remote clients, it was a natural extension to secure our wireless network. It is not the best solution, particularly in instructional settings where valuable class time needs to be spent training users and authenticating to VPN.

**Additional Monitoring for Wireless Security**

We have always monitored our network, but with the advent of wireless we had to expand monitoring to include rouge APs and inappropriately configured devices. When we got war tagged, it brought home the need to expand monitoring even more. Walking and driving around with a wireless laptop helps ensure we don't miss anything. If you have newer APs, they can be configured to sniff for rouge devices and save you the walk. In a large school system, it is a sure bet that someone is trying to look around at any given moment, even if only out of curiosity. Consequently, our monitoring schedule is very aggressive and robust.

**Firewalls and Virtual LANs**

Most of us now use some kind of firewall. At CPS we have two – one around the Central Office and one around the perimeter (see the following graphic). Of course, wireless doesn't have a perimeter the way a wired network does. When we first got aggressive about wireless security, we did consider more firewalls - many more even down to specific devices. While that provides good security, it is impossible to deploy with ease in our diverse environment. Our basic firewall setup allows us to keep wireless on the instructional network and away from sensitive data.



**Visualization of Chicago Public Schools Firewalls**



VLANs (Virtual Local Area Networks) help us separate wireless from the rest of the network. They allow segmenting a LAN based on something other than location, for instance usage or access. VLANs provide good security and are particularly helpful in a mixed wired and wireless environment. From a network design perspective, a wireless network should reside in its own VLAN (virtual Layer 2 network). Think of VLANs as intersecting highways where control signals are needed. Adding more VLAN zones is like adding more highways, and your network will require more traffic control. If your traffic filtering requirements are basic, a router may be configured with access lists to control traffic. Otherwise, a firewall with several physical ports may be needed.

### **LEAP – a Vendor Solution**

Our most aggressive and most expensive wireless security solution is to try and move to a single platform environment based on Cisco products. There are a couple of reasons why we went with Cisco. First, we are primarily a Cisco house on the hard-wired side. We run Cisco routers and at least one Cisco switch at each school. The second reason is that Cisco jumped the gun on the forth-coming IEEE 802.11i standard and has a successful history with LEAP (Lightweight Extensible Authentication Protocol), also known as the Cisco EAP solution. LEAP provides multiple authentication levels and supports VLAN port restrictions. It also integrates with our existing Active Directory and LDAP.

Most importantly, LEAP supports dynamic WEP keys. Part of the 802.1x, a large network authentication standard that defines port-based access control for both wired and wireless networks, EAP automatically rotates encryption keys at set intervals faster than hackers can intercept and crack them. While LEAP has its own set of challenges (user accounts required for all wireless users, LEAP software needed on all client machines, how-to documentation difficult, cost), it seems to provide more benefits for us than other solutions we considered.

Wireless provides needed connectivity, but it does create security challenges. We have to meet those challenges to continue to provide simple and rewarding educational technology experiences to all students.

### **Some Vendor Solutions to Note**

Hewlett Packard - ProCurve switches provide traffic monitoring, VLAN capabilities and port based access control for wireless networks

Newbury Networks - WiFi Watchdog provides wireless monitoring and security capabilities by creating a virtual location-based firewall around facilities, preventing internal or external unauthorized wireless access

SonicWALL - SOHO TZW, a firewall appliance which integrates secure wireless and Virtual Private Networking technologies in one solution

Wavelink - Mobile Manager Enterprise allows centralized setting and enforcing of all network and security configurations, including SSID, WEP, and LEAP

### **Internet and Print Sources for More Information**

<http://grouper.ieee.org/groups/802/11/>

<http://searchsecurity.techtarget.com/>



Strategies, Solutions and Innovations for Technology  
Leaders

<http://wifinetnews.com/>

Reid, Neil and Seide, Ron. 802.11 (Wi-Fi) Networking Handbook. McGraw-Hill/Osbourne, Berkeley, 2003.

Ross, John. The Book of Wi-Fi. No Starch Press, San Francisco, 2003.

Wang, Wallace. Steal This Computer Book 3. No Starch Press, San Francisco, 2003.

Produced

TECHNOLOGY  
& LEARNING