

PARITY CHECK

**OVER THE PAST YEAR I'VE WRITTEN ABOUT SERIOUS security risks in using IEEE 802.11—a k a Wireless Ethernet or Wi-Fi—on the plant floor. With all my ranting, you'd think I was against using wireless networks in process control, but I actually like and use Wi-Fi a lot. It is simply too useful to be dismissed and I believe industry can use it for control, but only if it is deployed with awareness. There are a few important steps that can**

Regardless, the original WEP encryption can be cracked, so I recommend doing more than just the basics. We have two primary possibilities: implement either an overlay Virtual Private Network (VPN) or Wi-Fi Protected Access (WPA) security. The VPN technique assumes that the wireless network is as insecure as the Internet and then superimposes a more proven encryption scheme such as IPSec. Traffic is encrypted

# Lock Down Your Wireless Ethernet

make the difference between a secure wireless system and a hackable insecure one.

The first step is to make sure all employees understand that any Wi-Fi deployment has potential security risks and these need to be handled carefully. As pointed out in Cisco's excellent white paper, "Cisco SAFE: Wireless LAN Security in Depth" ([http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm)), wireless networks have become one of the most appealing targets for hackers today. Hackers don't care what you make. If they realize you have an unsecured Wi-Fi they will go after it.

At the same time, develop a clear policy on how wireless is going to be deployed by your company. For example, what wireless technologies are allowed on the plant floor? IEEE 802.11 or Bluetooth? Wireless Keyboards and PDAs? These technologies are so pervasive it is easy for an employee to bring them from home and not realize the danger to the company.

Also, identify who has overall responsibility for managing wireless systems on the plant floor. Then set minimum security requirements for all wireless equipment. To do these things well, you'll need to really understand the general security issues and solutions regarding Wi-Fi. There are excellent resources available on the web that will help. Besides the Cisco paper, other favorites include the NIST Special Publication 800-48 (<http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>) and the Wi-Fi Alliance web site ([http://www.weca.net/OpenSection/Protected\\_Access.asp](http://www.weca.net/OpenSection/Protected_Access.asp)).

Next, use the security features available in your wireless equipment. Some 60-70% of all wireless systems are deployed without any security features enabled. Enabling WEP encryption will scare away the average hacker, making your site more secure.

before it reaches the wireless system by either desktop software or dedicated encryption gateways. If your company already uses VPNs for securing corporate traffic on the Internet, this can be a reasonable solution. However, it is not my favorite for the plant floor, as VPNs tend to be complex, often need reconnection, and there is limited VPN client software for anything but Windows and Linux-based systems.

A more effective solution is to deploy wireless hardware that supports the new WPA security. Realizing they had created a mess, the IEEE formed the 802.11i working group to develop security enhancements to the original standard. This is taking some time, so the Wi-Fi Alliance released a subset of IEEE 802.11i last year (called Wi-Fi Protected Access or WPA), so users and manufacturers have something to work with until 802.11i is ratified.

WPA addresses WEP's data encryption problems through a set of improvements called the Temporal Key Integrity Protocol (TKIP). To strengthen authentication, WPA implements both IEEE 802.1x and the Extensible Authentication Protocol (EAP). This combination utilizes a central authentication server such as RADIUS to authenticate each user before they join the network, and also employs "mutual authentication" so the wireless user doesn't accidentally join a rogue network sitting in the company parking lot.

For the plant floor TKIP and MIC are easy to deploy, but 802.1x, EAP, and RADIUS can be complex and difficult, especially with devices such as PLCs that use non-standard operating systems. For small facilities there are ways to simplify WPA a bit such as using an option called WPA-PSK (Pre-Shared Key). As long as you don't have too many wireless devices to set up, this works pretty well. ●

HACKERS DON'T CARE

WHAT YOU MAKE.

IF THEY REALIZE YOU



HAVE UNSECURED

WI-FI THEY WILL

GO AFTER IT.

ERIC BYRES, P. ENG.

...is manager of the British Columbia Institute of Technology's Internet Engineering Laboratory. He also holds the Advanced Systems Institute research fellowship for industrial network security. E-mail him at [ebyres@bcit.ca](mailto:ebyres@bcit.ca).