

## Wireless Networking Security Tips

Cris DeWitt, CISSP

Although not as secure as its wired equivalent, in some cases wireless networking is justified. It's these cases where an out of the box implementation can really "lower the shields" of your security posture. If you choose to implement wireless, plan on a little more administrative effort than its wired cousin. The good news is that the 802.11 TGi group is working to replace most of the insecurities in the current implementation of wireless standards with much more robust protocols and encryption schemes. Until then, here are some tips from the field:

- Always change the default administrative password on the device
- Change the SSID to something that makes sense to you, but not plain English (I prefer all numbers)
- Disable SSID broadcasting altogether
- Enable end-to-end encryption
- Logically place the access point outside your firewall and require a VPN to gain access to the "inside"
- Insure your VPN's authentication mechanism is robust and integrated with your overall IT administrative framework (like RADIUS, TACACS...)
- Tune your antennas and transmitters to only broadcast where needed (this is the most overlooked implementation item in the wireless space)
- Test your implementation on a regular basis (wireless attacks are quite popular these days)