

*This year, make sure that you spend five extra minutes to secure your Internet Connection. If you cannot do it yourself, then please be sure to call someone else to assist you. The connection that you secure can protect your personal information.*

## ***Secure your Wireless Access Point<sup>1</sup>***

If you have an Internet connection with your Cable, Telephone, or local Internet Service Provider (ISP), then you were probably given a Wireless Router (such as a Linksys or D-Link brand), which will permit you to connect to the Internet with your personal laptop computer.

While everyone likes the convenience of the wireless routers to access the Internet, few are aware of the dangers of not using the proper security (or any of the security which is built into the wireless routers).

I recently performed a scan of the Access Points (APs) visible from my Home. Many of the APs I identified could be easily connected to from our home. If you have a wireless connection, you may be inviting visitors that you did not know exists.

While the Wireless Routers have given us the convenience of permitting us to connect our computer together without cables, many of are not aware of the potential for others to gain access to our internet connection without our knowledge.

Suffice it to say that there many websites dedicated to mapping the APs of the world for others to find. This process is called War Driving, and has been the subject of security experts internationally for many years. In the process of returning from a recent business trip which I installed Wireless Security for a company, I decided to review the wireless APs available in my community.

I was amazed at the number of open APs, and the number of APs without any security. If you do nothing more after reading this page, I hope that you improve the security on your AP. After all, would you just place your checkbook on the front door for others to use? Leaving your access point open is practically doing the same thing.

---

<sup>1</sup> The entire report will be available on-line at [www.ABS-CompTech.com](http://www.ABS-CompTech.com). Select the Library, and then select the wireless security report.

## Viewing the Access Points close to you

I produced this scan from one of the rooms in our home. Notice that the strongest signal is listed first.

The AP that I use is labeled **g-MonKEYs** and is also in bold font. (Because we are connected to it)

There are only two APs listed with Security. (**g-MonKEYs** and sssquared)

All of the necessary connection information for the access point is automatically presented to your computer, to permit it to easily connect to the APs.

Stronger signals mean faster connection speeds. Notice that the AP named tom provides a 270MB connection!

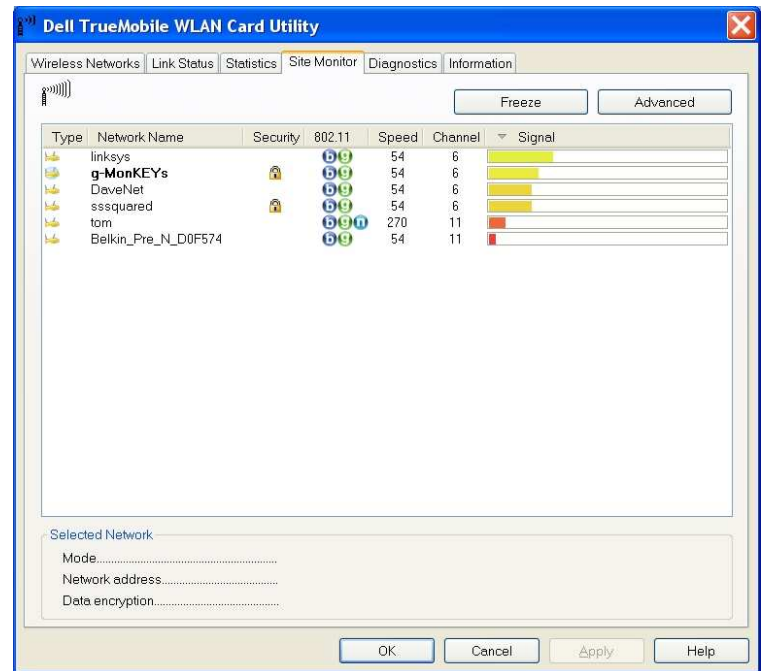


Figure 1 - Access points found in my home

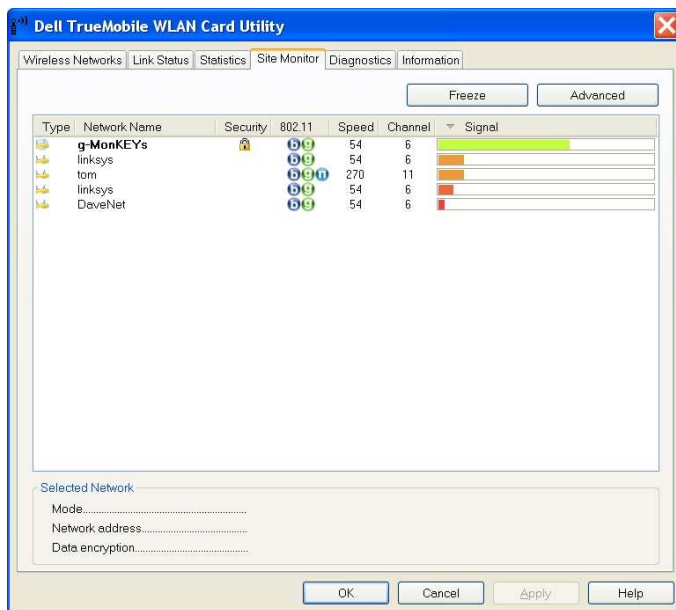


Figure 3- Default configurations detected

Here's a dilemma that we encountered in developing this Newsletter.

Notice that the linksys AP is listed twice. Now if you and your neighbor have the same gear, and have not configured your equipment, you can easily be using each others' internet connection (probably without even knowing!).

You can see that both are fairly close by, and it is probable that they are neighbors.

Maybe you find yourself asking the following question:

*Why is this important?*

## Why is Security Important?

If you know the answer to this question, consider yourself one of the few that understands that security is important. Skip to our next section!

Security has been an issue with mankind since the stone-age. Believe it or not, cavemen have been trying to get what others have, and this has not changed in today's times either.

First of all, if we examine Figure 2, we see the two APs marked linksys. We know that these are the default configurations, and by examining the Site Monitor, we can also see that there is no security on the AP either.

Granting someone access to your Home (or Business) network, is like handing over your password to your computer. Everything on your computer is available for inspection (your personal information, bank accounts ... ), and you are also permitting them access inside whatever protection was originally available with the security of the AP, which was never configured.

OK so you are sharing your home network with a friend, and you think that the security on your PC will protect you, right? Wrong. Security on PCs has been described as being as efficient as a screen door in a submarine. Technically, it's a door, but it will never hold water.

## Recent Scans and Attacks in our Neighborhoods

So what you say, I know my neighbor, and I know that they would never do anything that would hurt me. This may be true, but when you permit open access to you AP, you are permitting anyone access to your network (and also your PC). Not to scare you, but I have given presentations showing how Hackers can use a simple Pringles can as a directional Antenna which they can use up it to 10 miles away!<sup>2</sup>

OK, now how do I stop them you ask? How about setting up the WAP Security that your Wireless AP includes? Anything less than WPA or 128-bit encryption (please note that WEP and LEAP are broken protocols), is easily compromised by tools which are readily available from the Internet.

These types of attacks are normally called script kiddie attacks; because any kid with internet access is easily able to compromise the security.

When in doubt, use WPA and you can improve your security by not broadcasting your SSID.

Instructions for configuring Security on your Wireless router were included in the original box. If you

---

<sup>2</sup> OK, I really am trying to scare you, because until you are scared, you will not do anything to protect yourself.

Please find the entire report on-line at [www.ABS-CompTech.com](http://www.ABS-CompTech.com) , go to the Library, and select the Wireless Security report.

threw away that information, you can contact the support team for your wireless AP via their internet website. Please don't wait, our Security Sensors have already identified malicious activities in our neighborhood, and the War Driving attacks will target the easiest pathways, first!<sup>3</sup>

## Automatic Protection

OK, now we come to the Next Level of Internet Security, which my company promotes under the label of ActiveDefense<sup>SM</sup>, the device I use for Wireless Security is called the SpectraGuard Sentry.

We sell the Sentry to protect the wireless networks of Small Home Office, and Global Businesses. This is the only true device we have found which identifies the attackers, and stops their attacks.

There have been other tools which identified the attacks, but the SpectraGuard Sentry stops the attacks, automatically. The basic use of the Sentry is outside the scope of this document, we just want you to know that there is an affordable tool to protect yourself, and your network. We can make it work.

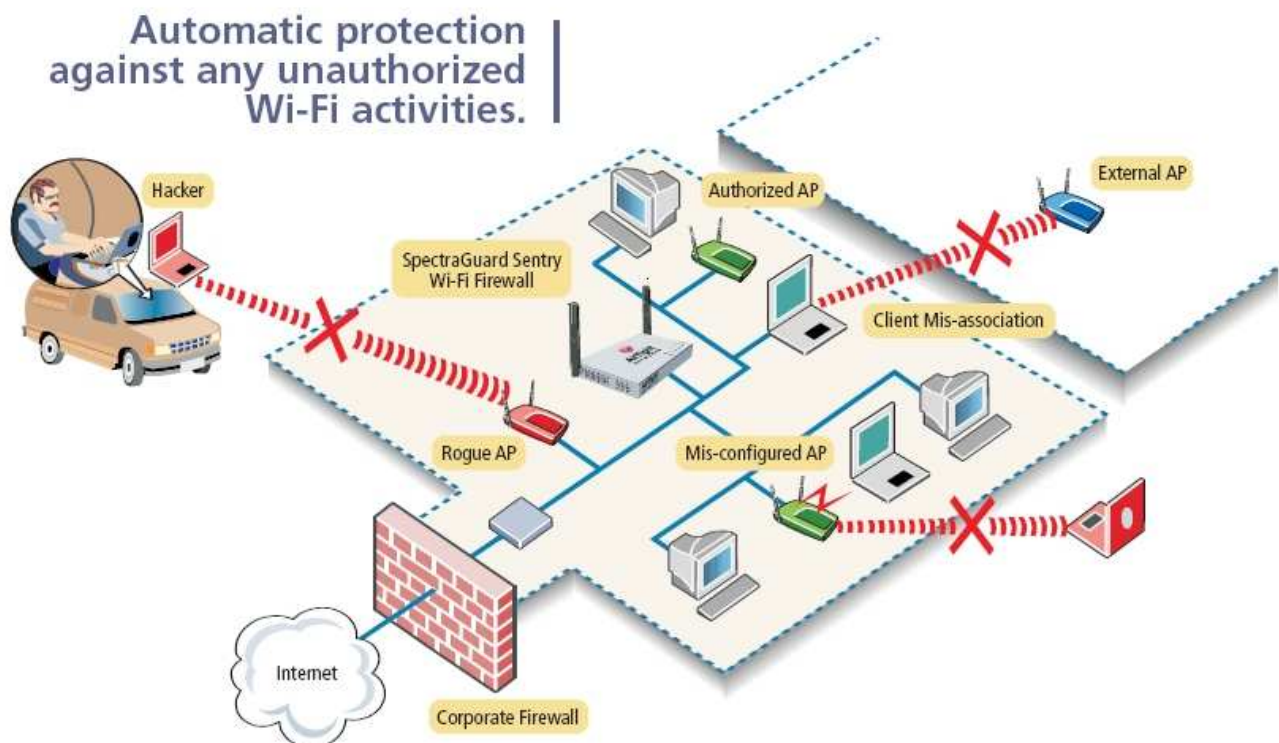


Figure 4 - Example of Protection Scheme for Sentry

<sup>3</sup> After the War Drivers have marked the open gateways, they will then work on breaking the passwords of the gateways which broadcast their SSID information. All of these tools are readily available on the Internet for anyone to download, and use (or abuse).

Please find the entire report on-line at [www.ABS-CompTech.com](http://www.ABS-CompTech.com), go to the Library, and select the Wireless Security report.

The Sentry can categorize APs, and Clients. You identify the friendly assets in the organization and the tool does the rest. If you are large enough for the enterprise system, you will benefit from the ability for all of the devices to communicate together, and block the unwanted access attempts, at all of the sentries in the network.

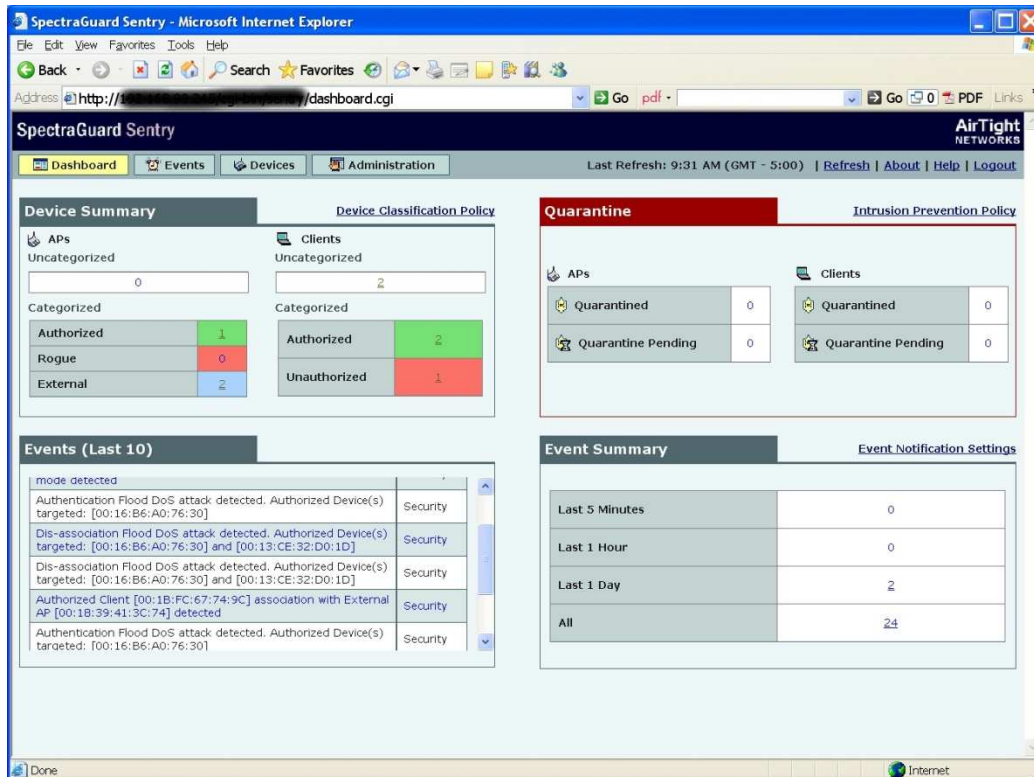


Figure 5 - SpectraGuard Sentry

protection?

Every business that has a wireless access point is mandated by both State and Federal Laws to use the best care to protect their customer's credit card and personal information. Since a single SpectraGuard Sentry is only \$495.00, this is easily in the reach of all Small to Global Businesses.

Configurations for multiple locations and Enterprise editions are also available as well.

If you think that your Network Engineers or Administrators are faster than the script kiddie next door, then you probably don't need the added protection.

As a security consultant with 24+ years of Professional experience, I am confident that I am better protected now, and that the War Driving Hackers will go next door to attempt to penetrate the neighbors network instead.

Please find the entire report on-line at [www.ABS-CompTech.com](http://www.ABS-CompTech.com), go to the Library, and select the Wireless Security report.

Here is picture of the web based control center.

The Spectra Guard Sentry constantly scans the objects which are talking to your network to identify the authorized and the unauthorized devices.

Attacks are immediately mitigated.

Intrusions and denial of service attacks are stopped cold.

So you might ask yourself, who needs this type of

Is your network protected enough? Will the War Driving Hackers be attracted to your Access Point? Is the security in your office effective enough for the Tech Savvy Script Kiddies?

Please call us for an on-site audit or to order the SpectraGuard Sentry today!

If you need more information, or would like to contact the author, please feel free to contact me.

Sincerely,

Albert E. Whale, CHS CISA CISSP  
President

Email: [aewhale@ABS-CompTech.com](mailto:aewhale@ABS-CompTech.com)

Telephone: (412) 635-7488