Fixed-Wireless High-Speed Internet Security

An overview for customers

by PC-TroniX Wireless Division

What is "Fixed-Wireless High-Speed Internet?
It's a wireless method of delivering high-speed Internet access to a home or business. Wireless relies on a small (about 10" square), normally roof-mounted, fixed-position antenna (at your premises), which beams Internet data back and forth between your premises, and a fixed-position PC-TroniX antenna, which connects to the Internet. From your roof-mounted location, normal CAT5 cable is then connected to your computer. A big advantage is the phone and cable company are not needed at all…since wireless is used.

Fixed-Wireless High-Speed Internet is also known as WDSL for short (see p 2).

Virus, spyware, intrusion, monitoring:
Most computer users know that they should use *antivirus* and *spyware* software on their computers, in order to guard against destructive programs that find their way onto their computers from the Internet. Whether your computer has wired or wireless network connectivity, defenses against computer viruses and spyware can be applied at the individual computer level. Good virus and spyware software such as AVG Antivirus, Spybot and Ad-Aware are available for free on-line, for non-commercial use. Spy Sweeper is also a very good spyware defense for a nominal price.

But, computer users may not realize that all networks (wired or wireless), should also have *intrusion* and *monitoring* protection. PC-TroniX applies intrusion and monitoring defenses to our network in order to give all our wireless Internet customers an even higher degree of security to their data.

This white paper lets people know generally what PC-TroniX does to protect its Internet customers.

Public Internet access:
Public Internet access could be at a hotel or coffee shop. You should assume that you have very little security at a public location, since a public venue by its very nature makes it more difficult to apply high levels of security. High levels of security will keep public users out of the system…which is what you do not want. One way around this is to use what is called a VPN connection at a public location. But that's another white paper.

Private Internet access:
Business and residential users are examples of private Internet access users. These types of users are candidates for the application of high security levels, since you do want to keep others out of your network. However, many business and residential users who install their own networks don't know how to properly secure their networks, especially if they are using wireless systems. There are even computer companies that have installed indoor wireless systems that are not very secure. So it's no wonder that people might think wireless systems are not secure.

PC-TroniX outdoor wireless:
PC-TroniX operates an *outdoor* fixed-wireless Internet access system for private use, that delivers high-speed Internet to business & residential customers. We use wireless to deliver the Internet service to your home or business, but **your computers are still connected to a regular wired Ethernet cable**…just like when you have regular cable or dsl Internet service. Wireless can deliver an Internet signal to customers within a neighborhood or county…depending on the design. Page 3 of this paper indicates generally how PC-TroniX handles intrusion and monitoring security on our outdoor wireless system.

Types of connectivity:
Many home and business computers have traditionally received Internet connectivity by way of an outside Internet communications line, which is brought into that home or business, usually by the cable or telephone company. This communications line, which provides a computer connection to the Internet could be a dial up telephone line, DSL (Digital Subscriber Line), cable, T1 or fiber line. There is a lesser known communications medium for delivering Internet connectivity to businesses and homes. And it doesn't rely on a physical "communications line" at all. It's called WDSL.

WDSL:
WDSL stands for Wireless Digital Subscriber Line…a.k.a. Fixed-Wireless High-Speed Internet. It is gaining in popularity due to it being wireless. Many people know about and use indoor wireless routers, but may not know about WDSL.

WDSL uses commercial outdoor wireless equipment to deliver Internet connectivity over a large area…such as neighborhoods and counties. This makes it especially useful in areas where there is no DSL, cable, or fiber such as in rural areas. But it's also gaining in popularity in urban areas, where other forms of connectivity already exist. This is because people are discovering that WDSL can be very cost-effective when compared to other Internet connectivity methods. This wireless signal can be transmitted 10, 15 or even 20 miles with good line of sight conditions, using commercial equipment. And WDSL can deliver Internet connectivity up to 30-40 times faster then dial up modems.

Benefits of WDSL
1. WDSL can be very cost effective when compared to other Internet connectivity methods.
2. Great for anyone that needs quick Internet connectivity deployed.
3. Cable and phone companies cannot deploy Internet connectivity as fast as WDSL providers.
4. You don't need to pay for a cable or phone line to get Internet connectivity.
5. Cable and phone providers make you sign a year contract (or longer). PC-TroniX doesn't.
6. A WDSL antenna is smaller then a satellite dish. Some are just 10" square.
7. You can quickly upgrade to higher available speeds…sometimes on the same day.
7. No physical line to be degraded by weather, since most all its path is by radio waves.
8. WDSL can offer attractive pricing plans, not available with cable or phone companies.

Security:
Wireless security concerns are valid, but it's interesting that many people don't express the same level of concern with wired systems. One of the most unsecured Internet access systems that this writer knows of is a *wired* Internet access system, at a hotel in Hagerstown, MD. There are plenty of other unsecured wired systems…just as there are also unsecured wireless systems. The truth is that both wired and wireless systems should utilize proper security methods…since both wired and wireless are vulnerable, if not properly protected.

An under-secured wired system can be more of a security risk then a secured wireless system. That's because there are many times more hackers on the Internet worldwide, that can reach a wired computer, as compared to anyone that might be able to directly "hack" a wireless signal. Fortunately there are now relatively secure encryption techniques that can be applied to a wireless signal.

PC-TroniX uses various methods to secure your wireless data transmissions and our network from hackers.

Intrusion and monitoring defenses. Some or all of these methods can be used.

1. **Access broadcasts turned off.** "Access Points" are the names of devices that we usually place outdoors at high locations that PC-TroniX uses to wirelessly connect our Internet access network to a customers home or business. We can turn off our access point broadcast ID. That way a hacker won't know the "broadcast name" of our access point, thus making it more difficult for a hacker to gain entry.

2. **Up to three authentication methods**. We use up to three checks to determine that the correct person is accessing our network before allowing a customer to gain access to our wireless network. a.k.a. "authentication".

3. **No automatic wireless connection**. We do not allow would-be wireless users to automatically connect to our access points. This makes it difficult for a hacker to know the necessary configuration information for gaining access to our network.

4. **"Client-to-client" blocking**. This puts a firewall between all clients so they are not able to "look" at another client's computer, even though they are connected to the same network.

5. **DSSS sounds like noise.** If you are using a broadband telephone (VoIP) on our system, no one can hear what you are saying, even if they did use a receiver to tune into your frequency. That's because we use a modulation scheme called Direct Sequence Spread Spectrum (DSSS). No one can hear what you are saying on your VoIP phone, since the signal sounds like noise.

6. **Advanced Encryption Standard.** Even if a hacker was to receive your computer data over the air waves, we use an encryption method for all data on our network called AES (Advanced Encryption Standard). AES is a Federal Information Processing Standard (FIPS) that specifies a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information.

7. **Hardware firewall.** We have a hardware firewall between the Internet and our network. This helps keep Internet hackers from being able to enter our network from the Internet.

8. **A second hardware firewall.** We have a second firewall on our receiving equipment located at the customer's premises. This further protects the customer from Internet hackers.

9. **Software firewall.** And to top things off, our clients are urged to use a nationally recognized, Free software firewall package called Zone Alarm on their computer. This is a third firewall method that can keep hackers out of your computer…and it's free.

Conclusion:
Wired and wireless networks can have very good security if proper security steps are taken. However, there is no perfect security for Internet users, whether you are a wired or wireless Internet user.
PC-TroniX has access to the above security methods for our wireless network to protect our customers to a very high degree. Wireless networks can take advantage of all the security measures that are available to wire-line networks, and then add additional security features not available in the wire-line world. As a result, wireless networks can be as secure as wire-line networks, if not more secure.

For more information call:
Bob Young – 717-648-8431
PC-TroniX Inc.
5130 E. Trindle Rd.
Mechanicsburg, PA 17050