

SECURITY OF SOLECTEK RADIO LINK

HOW IT PREVENTS HACKING AND EAVESDROPPING

Current Situation of 802.11b Security

Consider the following scenario; A hacker casually rolls into your company's parking lot, equipped with a laptop, an 802.11b client card, and a commercial available 802.11b analyzer software. He will find the signal from your access point and quickly overcome your 128bit WEP encryption and Voila... He is cruising on the Internet using your T1 line and while he is on it, he thinks he may as well check out what goodies are available on your LAN. Far fetched? Not at all, as this type of occurrence has been documented in the media, often with the actual case studies. Technologies exploited by the hackers were originally developed as LAN analysis tools for IT managers and recently extended to 802.11b WLAN purposes. Commonly referred to as "sniffers", these tools are normally uninteresting to hackers in wired LAN (due to the need for a physical connection), but present interesting possibilities for hackers who could easily penetrate a network from the outside.

Even for outdoor bridges, the results are the same as long as your wireless bridges use the same 802.11b media access control (MAC) protocol, i.e. all wireless bridges in the market that are compatible with 802.11b CSMA/CA are susceptible to hacking efforts. Unfortunately, the open standard could enhance the market acceptance of new technology and products as we have witnessed the success of the 802.11b indoor WLAN, but the by-product of such openness is the wide availability of analysis tools that could be used to breach the security of your network as explained above. With such standards-based architecture open for widespread use, such hacking tools get even more sophisticated and dangerous for your network as the 802.11 market matures.

The question then is:

How can you prevent such security breaches with Solectek's wireless bridges? The answer lies in many security measures implemented in Solectek products, which are describes below:

Proprietary protocols

Solectek's proprietary and patented polling access protocol is fundamentally different in how packets are encapsulated from the standard 802.11b. Not only is it a performance improvement over 802.11 in terms of efficiency and better throughput, but is also equally effective in fighting hackers who would have no way of knowing the protocol differences.

Baseband Processor

Solectek's bridges some elements of the 802.11b architecture such as the baseband processor in the radio. However, we have modified the usage of the processor away from 802.11b in many ways. Finding out what changes are possible will take an intimate knowledge of the processor design and Solectek's confidential design process.

Strict Network Access Control

The SkyWay base station maintains a list of authorized subscriber units. The base station gives a chance for communication to only those that are on the list and opens its receiver to such subscriber units only one at a time. All other incoming connection requests, either from unauthorized subscriber units are discarded by the base station. Likewise, subscriber units are designed to receive traffic from the base station it is associated to. This prevents cross-talk and unauthorized access among the subscriber units.

MAC address Authentication

Part of the base station filtering process is performed with the private MAC addresses that are confined to the wireless network, separate from the Ethernet MAC addresses that are related to the network at each subscriber location. Unlike the Ethernet MAC addresses, these MAC addresses for the wireless network are private and are not exposed to the outside networks.

Routing

When the wireless network is deployed by an ISP or to multiple location or a multi-tenant building, each subscriber unit will be deployed at different organizations and thus will need to be logically separated as separate networks. Most of the 802.11b-based outdoor networks are configured as bridges, which in effect form a single LAN among all subscribers. Such bridged networks expose each subscriber network to all others and pose a great security risk. Solectek's wireless networks can be easily configured as fully functional routers so as to securely deploy each subscriber unit, without additional cost to the ISP or the subscriber for separate hardware.

Solectek Corporation, headquartered in San Diego, California, designs, manufactures and markets a full line of wireless interconnectivity products. Through technical innovation and steady revenue growth, Solectek has become a recognized leader in the wireless LAN/WAN connectivity market and the industry market leader in wireless bridges. Founded in 1989, Solectek has over 15,000 installations worldwide. The Solectek product line of wireless bridges and routers is the most flexible, reliable and secure in the industry. For more information visit www.solectek.com.

SOLECTEK
Wireless Networking Solutions