



The Wireless Security Experts

CASE STUDY

Code Red Systems Ltd.
21 HaVaad HaLeumi
POB 16120, Jerusalem, Israel
T +972-2-642-3401, F +972-2-642-3402
Email: info@code-red.biz
Web: <http://www.code-red.biz>

Sep 1, 2003

AirBlock Wireless Security for Retail and Industrial Applications

By,
Drew Tick, CEO

(Jerusalem, Israel) Many people believe that wireless LANs burst onto the technology scene as part of the new millennium. They may not realize, however, that wireless devices could be found a decade earlier in both retail and industrial applications. At that time, very few security measures were taken as the threat of a wireless attack was very low. Today, due to advances in mobile computing and the availability of wireless connectivity, these networks have become extremely vulnerable. Unfortunately, many of the latest enterprise-based 802.11 security measures are not applicable for these legacy environments.

This document explores the difficulties associated with providing wireless security for these non-enterprise environments, and how Code Red's AirBlock technology can be used to secure retail and industrial wireless networks.

Overview

The IEEE 802.11b standard was ratified in 1999, but the roots of wireless LAN can actually be traced to over a decade earlier in proprietary systems running in the 900 MHz range at then impressive speeds of 1 Mbps. These products could largely be found in vertical markets, particularly in the retail and industrial market segments.

Early wireless devices included bar code readers, cash registers and forklifts in both retail outlets, warehouses and the factory floor. At that time, wireless PC cards were expensive and difficult to find outside of these vertical applications. Therefore, security was not a major concern of customers or integrators, as the probability of a person with a laptop and wireless PCMCIA card breaking into the wireless network was virtually zero.

With specification of the 802.11b standard, it was only natural that these wireless users migrate to the new standard which offered significantly higher data rates and great multi-vendor interoperability.



The Wireless Security Experts

Fast forward to 2003, and suddenly there are literally millions of users with wireless cards within ample reach of most retail and industrial wireless networks.

In retail environments this may result in exposing confidential information such as credit cards, stock numbers, price lists, sale quantities and more. At the warehouse, a professional intruder can sit in the parking lot, equipped with just a laptop and a \$60 wireless PC Card, and easily penetrate a backdoor to central corporate servers .

The Problem

Since there is no security in place, many of these companies are looking for immediate solutions to plug the security holes in their wireless networks. As opposed to enterprise implementations, there are a number of limitations regarding the type of wireless security solutions which are applicable to retail / industrial environments. These may include:

- Support for legacy hardware
- Support for legacy Windows systems
- Support for DOS based devices
- Limited memory
- Limited disk space
- No 802.1x support
- No firmware upgrade
- Multi-vendor environments
- Short timeframes
- Large rollouts

According to industrial priorities, this must all be done in an application which does not hinder work-flow or cause down-time. As one technology manager at a large food manufacturer put it: “Even if your security solution fails, it cannot effect ongoing operations.” In other words, if there are problems, they want to be able to turn off security and continue operations. Production is the primary concern and wireless security can be implemented as long as it does not interfere.

These limitations preclude most VPN-style and standard 802.1x wireless security solutions. For example, implementation of 802.1x requires client-side software which may not be supported by legacy hardware and operating systems. In terms of VPN solutions, many mobile devices do not have the disk space or memory to support software based encryption.

Industrial and retail environments require a solution which is flexible enough to support legacy hardware and software, robust enough to minimize down-time, but simple enough to allow for a quick rollout.

The Solution

The AirBlock product was originally designed to secure home and small business networks. This requires a product which is simple to install and does not require ongoing maintenance. The key features identified for this product are:

- Automation
- Transparency
- Redundancy



The Wireless Security Experts

Automation is used to automatically configure access points and wireless cards. Transparency means that the software operates in the background and does not interfere with foreground transactions. Redundancy ensures that if the management server goes down for any reason, a second server will automatically take over encryption key management operations.

Code Red Systems was approached by large retailers and industrial companies who were interested in the benefits of the AirBlock solution. Unfortunately, the off-the-shelf AirBlock product currently supports single access point networks and is limited to the Windows XP and 2000 operating systems.

To overcome these obstacles, the parties agreed to a custom project where Code Red could use the underlying AirBlock technology to provide security, while new code would be written to provide additional features according to the customer's requirements. For example, a specific retail customer required changing WEP keys on DOS based devices, while an industrial customer needed support for Windows '98 based industrial computers.

In terms of management, the AirBlock product was initially designed for the SOHO market, and therefore combines both client and server functionality in a single piece of software. For retail and industrial applications it was necessary to separate the server and client components. The server component was then moved to the wired side of the network, while the client component was installed on each machine.

The AirBlock software supports access points and wireless interface cards from multiple vendors. For each project it is necessary to verify which access points, cards and operating systems need to be supported. If not currently supported by AirBlock it takes approximately 2-3 weeks to adapt the software to most Wi-Fi compatible cards and access points.

From Code Red's experience, a typical project may require the following support:

<u>Access Points</u>	<u>Cards</u>	<u>Operating Systems</u>
Symbol 4121	Aironet 4800	DOS
Cisco 350	Intel	Windows '98
Cisco 1100	Orinoco Gold	Windows XP

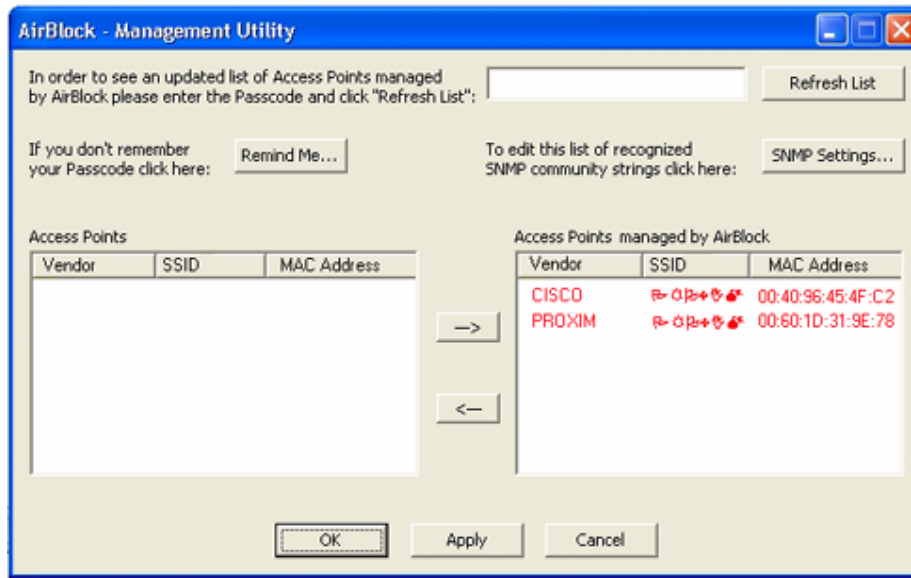
The key challenges in such configurations are:

- Enabling centralized security management for multi-vendor AP/wireless networks
- Supporting multiple operating systems including old legacy Win '98 and DOS and Win98 systems
- Implementing wireless security for low-end, low-memory hand-held devices with limited memory and storage.

One of the benefits of the AirBlock solution is that it can be adapted for most leading access points and wireless cards, regardless of vendor or model number.

Operations

As opposed to 802.1x, configuration on both the server and client are minimal. On the server side, a simple interface is used to identify all access points in the network and define on which ones the encryption will be enabled. The administrator is also prompted for a pre-shared key (PSK) which is an administrator-defined ASCII string 6-25 characters long.



The access points are also set to Accept Encrypted Data Only which means that unless a client device has the correct keys, it cannot even talk to the access point. This further prevents wireless attacks on the network and prevents unauthorized sharing of broadband internet access.

On the client side, AirBlock must be installed on each client device. Upon installation the software prompts for a pre-shared key (PSK) which must be the same for all devices in the network.

Once the PSK has been entered on the devices and the management console, AirBlock automatically creates, distributes and changes encryption keys for all access points and wireless cards in the system. The default value for key rollover is every 10 minutes, or more depending on the limitations of the hardware and operating system.

The AirBlock Management Console is also installed on a second machine on the wired side of the network. If for any reason, the initial server goes down, the secondary server can automatically assume responsibility for management of encryption keys. On the client side, adding a new device to the wireless network is quite simple. The only requirement is installation of the AirBlock software on the new device, entering the pre-shared key, and the new device can communicate securely with the rest of the wireless network.



The Wireless Security Experts

As one can see, the AirBlock software is highly automated for simple configuration and maintenance, runs transparently in the background, and provides redundancy in case the main server has failed.

Conclusion

Emerging 802.11i security standards and its 802.1x subset, certainly improve wireless security for enterprise customers, but it is not always possible to implement this solution in non-corporate environments such as retail, industrial, SMB and SOHO applications. The reason for this is mainly the need for new or upgraded hardware, complexity of operation, and price performance requirements.

AirBlock provides a simple solution for automated encryption key rollover which provides enhanced wireless security by overcoming most of the WEP deficiencies as cited in leading academic and professional research.

The software-only solution, features automation, transparency and redundancy to provide a wireless security solution which can be installed on legacy systems, does not require complicated configuration and maintenance, and has a backup system in place in case of failure.

While the AirBlock 802.11 Security Software can be purchased as an off-the-shelf product, the AirBlock Industrial Edition, utilizes underlying AirBlock technology to implement a custom industrial wireless security solution according to customer requirements.

About Code Red Systems:

Code Red (www.code-red.biz) is a software developer specializing in security solution for the 802.11 wireless networks. The company is headquartered in Jerusalem, Israel, and has a staff of software engineers with hands-on military and civilian data security experience. The company has released its AirBlock product for the SOHO market, and also provides custom wireless security solutions for retail, industrial and enterprise environments.