



*Wireless Security Management*

# CASE STUDY

Code Red Systems Ltd.  
21 HaVaad HaLeumi  
POB 16120, Jerusalem, Israel  
T +972-2-642-3401, F +972-2-678-3403  
Email: [info@code-red.biz](mailto:info@code-red.biz)  
Web: <http://www.code-red.biz>

(Jerusalem, Israel) There has been much written about 802.11 wireless security. Most of the articles are good at describing the bits and bytes related to the underlying security problems, but few address the really painful issues concerning soaring tech support costs and increasing return rates which are currently facing the 802.11 industry.

Bug Computers is the leading retailer of computer software in Israel. They currently have over 30 stores which cover the entire country. Their current offerings include Symantec's security products, wireless home networking products and subscriptions to leading broadband Internet providers.

The company's marketing department understood the inherent problems of security in wireless home networks and did not have a solution. Believing in this market opportunity, Bug is now offering Code Red's AirBlock Wireless Security Software to its customers.

## ***Overview***

Doing an Internet search on "802.11 wireless security", one may find a large number of documents explaining why WEP –Wired Equivalent Privacy is not really secure in the first place. In the simplest terms this can be attributed to a static encryption key and the length of the Initialization Vector (IV). The static key can be explained by using the example of a large office building where all the offices have locks – which are opened by the same key. Clearly this office building cannot be considered secure since it is very simple to copy the key and use it to gain access to someone else's office.

It is more difficult to explain the Initialization Vector which can best be described as a 24 bit sequence which is sent in clear text for every data packet. Using standard equipment, a potential hacker can eavesdrop on wireless communications and by utilizing the knowledge of the IV values, may use a known mathematical formula to determine the identity of the static encryption key.

These weaknesses have not been ignored by the IEEE 802.11 standards committee, or the Wi-Fi vendor organization who is responsible for 802.11 compatibility testing. WiFi has responded by introducing the WPA standard, while the IEEE committee has passed 802.11i standard.

While these standards are good for underlying security, they also increase user confusion and result in more tech support calls.



## *Wireless Security Management*

### ***The Problem***

The market is demanding a solution which improves usability, not just underlying security.

Few people are finding answers to the real problems facing the 802.11 industry, namely an inordinate amount of tech support and high equipment return rates. WPA solves previous security inadequacies which reduces consumer fear and opens the market for additional customers, who may have previously delayed a purchase decision due to security concerns. It does not, however, address the major problems plaguing the industry.

After all, 90% of current users do not enable WEP due to their deep concerns regarding static keys and initialization vectors. Most users do not enable WEP simply because it is too complicated!

The bottom line is that users want security made simple. They are not really interested in the various committees or memorizing the myriad of current, interim and future standards. The major problem for the SOHO market goes far beyond understanding, it is really about usability.

The companies most active on the standards committee serve the large enterprise market. Therefore, their solutions usually reflect the price point, complexity and maintenance requirements which are standard fare for the IT staffs of large companies.

Therefore we find ourselves in a predicament where not only are the 802.11 security solutions difficult to implement, but they are simply not applicable to the SOHO environment.

### ***The Solution***

Everyone agrees that users want security, the question is how difficult it will be to implement that security. The first problem is the two-step process required for first configuring the wireless card and then a separate interface for configuring the access point. Exacerbating this process is the inevitable mixed environments where users will try to implement security between WEP and WPA enabled equipment. Thus the question is not one of security, but rather of the user's determination to complete the process and overcome the incompatibilities in order to implement the security.

The question thus arises of what should be done in terms of 802.11 security solutions for the home and small business (SOHO) market. It is precisely in these markets that RADIUS based solutions do not apply and users are left to their own resources.

One solution is to develop a product specifically for 802.11 wireless networks in the SOHO market. This solution should emphasize the following features: Transparency and automation.

In this scenario, the user should be prompted for a secret code known in security terms as a shared secret or pre-shared key (PSK). Using automation technology, the software should have the simultaneously configures both the wireless card and access point from a single user interface, with no further involvement required.

If both the card and access point are WPA enabled, then the software should automatically configure network security using WPA Home Mode. If both the card and access point are



### *Wireless Security Management*

WEP enabled, then the software should enhance the standard WEP implementation by automatically rotating the encryption keys at regular intervals. By rotating the encryption keys at regular intervals, the software can overcome the main security weaknesses described in the University of California at Berkeley and the University of Maryland wireless LAN security reports.

For mixed WPA/WEP environments, the software should automatically implement dynamic WEP and can even advise the user if a firmware upgrade for WPA is available for a particular piece of hardware.

The advantages of an automated security solution specifically for the SOHO market includes: Better security, less tech support and seamless implementation in mixed security environments.

### *The Market*

Bug computers are now in the process of introducing the AirBlock solution to managers of stores in key regions. In parallel, the marketing department together with Code Red and leading importers of wireless equipment are cooperating on a marketing and sales plan including: PR, advertising, posters and in-store promotions.

The public is becoming more aware of the problems associated with unauthorized use of wireless networks. This includes recent criminal cases brought in the US and users complaining about narrow bandwidth and slow performance. Therefore both Bug and Code Red are confident that AirBlock will succeed both in providing secure wireless networks and meeting business objectives.

### *Conclusion*

Current, interim and future security standards certainly improve wireless security. They also, however, increase confusion amongst endusers, especially in environments with legacy WEP equipment and no RADIUS server such as homes and small businesses.

Users are looking for a secure and simple “out-of-the-box” solution. Automated 802.11 security software, can accomplish this goal by automating configuration of both the wireless card and access point in a single simple process. This includes implementation of the best possible security regardless of which standards are supported in a given environment.

---

### *About Code Red Systems:*

Code Red is a software developer specializing in security solution for 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 recently released its AirBlock product for the SOHO market, and also offers specialized wireless security solutions for large corporations, WLAN vendors, PC vendors, chip makers, and broadband internet providers. For more information please visit our web site at: <http://www.code-red.biz>