



*The Wireless Security Experts*

# SECURITY ANALYSIS

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](mailto:info@code-red.biz)  
Web: <http://www.code-red.biz>

April 2003

## WPA for the SOHO Market: More Security means More Tech Support

By,  
Drew Tick  
CEO, Code Red Systems

(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.

### *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. They have responded by initiating the IEEE 802.11i committee responsible for defining a more robust and secure standard. This standard for better security is due to be ratified by the end of 2003.



*The Wireless Security Experts*

The Wi-Fi vendor organization felt that waiting until the end of 2003 was too long and therefore decided to declare an interim security standard known as WPA (Wi-Fi Protected Access). WPA is meant to include many of the improvements in the draft version of 802.11i, but is meant to work with the existing RC4 WEP encryption algorithm which is built into current wireless LAN hardware. The hope is that WPA will be backwards compatible with most existing 802.11 equipment, provided that the user performs a firmware upgrade. It is also designed to be forward compatible with AES, which will eventually replace RC4 as the standard 802.11 encryption algorithm.

WPA will inevitably bring more security, more user confusion and more tech support calls.

***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 average user reading this article will not complain about the technical weaknesses of underlying security, but rather about too many acronyms with no meaning, and no understanding of how these standards are applicable in the real world anyway. That is without even mentioning 802.1x, which has been co-opted as part of 802.11i or Cisco's proprietary LEAP solution based on 802.1x which they are currently offering free to wireless LAN card vendors. There is also really no need to mention them, since these RADIUS based solutions are not even applicable to the vast majority of home and small business customers.

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 reference here is mainly to home and small business (SOHO) users who now make up a whopping 50% of the wireless LAN market. It is beyond the scope of this article to debate whether this also applies to medium and large enterprises, who may have an IT staff and possibly thrive on understanding and implementing complex security solutions.

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.

The best example of this is the 802.1x standard. It is based on having an authentication server (preferably a RADIUS server) and certification server, in order to authenticate wireless users



### *The Wireless Security Experts*

and provide per session encryption keys. Again, no one denies that this improves security -- but one must also ask when is the last time they saw a small business purchase, install and maintain RADIUS and certification servers? Asking the same question about a home user is even more absurd.

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 Complicated Solution*

Despite the emphasis on the enterprise, both the IEEE committee and Wi-Fi understand that a solution must be offered for the SOHO market and have therefore defined the WPA Home Mode solution which is based on a pre-shared key (PSK).

While this is good for the SOHO market because it does not require a RADIUS server, it is still confusing for the typical user. When WPA is commercially available, WEP will not disappear. With an existing installed base of millions of WEP enabled devices, there will be at least two years where users will have to choose between Open Mode, WEP, WPA Home Mode and WPA Enterprise Mode. Even if users can figure out how to set up their wireless card in WPA Home Mode, they will inevitably run into a dead end, or make multiple tech support calls, when they find that there can be no communications between a wireless card operating in WPA Home Mode and an access point which has been set with a WEP encryption key.

If the user is truly robust, and won't grow too old waiting for tech support to answer, perhaps they will do a firmware upgrade on the access point – if it is available. More likely, the user will forget about security entirely, or worse yet, contribute their card to the growing return rate for wireless LAN equipment.

### *The Simple 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.

Code Red Systems, specializes in 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.

AirBlock™, is a software-only solution specifically for 802.11 wireless networks in the SOHO market. This solution has two basic features: Transparency and automation.

Using AirBlock, any user who knows how to install a Windows software application is capable of configuring wireless LAN security. The first step is for the user to get the wireless



*The Wireless Security Experts*

network operating in its default mode with no security. The user then installs the AirBlock software on their PC, and is prompted for a secret code known in security terms as a shared secret or pre-shared key (PSK) and then presses enter. The software then 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 AirBlock will automatically configure network security using WPA Home Mode. If both the card and access point are WEP enabled, then the software will enhance the standard WEP implementation by automatically rotating the encryption keys every 10 minutes. This improved WEP, available only in AirBlock, overcomes the main security weaknesses described in the University of California, Berkeley and University of Maryland wireless LAN security reports.

For mixed WPA/WEP environments, the software will automatically implement improved WEP and may advise the user to see if a firmware upgrade for WPA is available for further enhancement of network security.

The advantages of the AirBlock solution include: Better security, less tech support and seamless implementation in mixed security environments.

***Conclusion***

Current, interim and future security standards certainly improve wireless security. They also, however, increase confusion amongst endusers, especially in markets where they are difficult to apply such as homes and small businesses.

Users are looking for a secure and simple “out-of-the-box” solution. Code Red’s AirBlock 802.11 Security Software, does this 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.

The AirBlock software is currently being licensed to wireless LAN vendors under OEM agreements and should be commercially available to endusers towards the end of 2003.

---

*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>