

BreezeCOM and Floware unite



**Secure Broadband Wireless Network
With BreezeACCESS & BreezeNET PRO.11**

Introduction

The purpose of this document is to present the security issues affecting Broadband Wireless systems and to introduce the BreezeACCESS & BreezeNET PRO.11 products as viable solutions for effectively addressing these concerns. Since Broadband Wireless systems utilize the open air as the medium for data transmission, the obvious basic question that begs attention is how to prevent intruders from intercepting sensitive and confidential data transmitted over the airwaves. This document will analyze this issue and other security oriented concerns that demand consideration when Broadband Wireless systems are employed as a network alternative by a service provider or in an organization that deals with mission critical information.

Principles of Operation

Broadband Wireless systems typically comprise a cell or a group of cells, each of which contain several wireless terminals (also known as station adapters, subscriber units, or CPEs). Each cell consists of one or more Access Points (also known as Access Units), devices that are usually connected to an existing backbone (in this instance, an IP backbone with an Ethernet interface), and which manage all the traffic within the covered area. Terminals within the coverage area of an access point connect to the network backbone through the access point. All the terminals associated with an access point are synchronized by both frequency and clock, in order to transmit and receive data to and from the access point. The same rule applies for an interception device. In order for data to be intercepted, a wireless device must be employed and synchronized within the covered area of the access point.

How can the interception be prevented? Can't a potential intruder utilize another Alvarion terminal and attempt to connect to a wireless network and compromise its integrity?

The BreezeACCESS & BreezeNET PRO.11 products offer an extensive set of features that prevent tapping, whether attempted by means of a similar wireless system, or through other means of interception.

Alvarion: Securing Wireless Access Over the Airwaves

1. Frequency Hopping vs. Direct Sequence

Direct Sequence Broadband Wireless systems (as well as narrow band systems) work in a predefined constant frequency, i.e. when an access point or a terminal is installed, it is set for working in a certain constant frequency. In this instance it is easier to detect the frequency of the carrier wave and to synchronize with it. With Frequency Hopping systems, the frequency of the carrier wave is continuously changing. It is therefore considerably more difficult to detect the current frequency of transmission. In the event that the frequency is detected, it is ultimately of little significance; it changes within milliseconds, rendering any attempt at steady synchronization a virtual impossibility. Alvarion's BreezeACCESS and BreezeNET PRO.11 products utilize the inherently security-oriented Frequency Hopping technology.

2. The ESSID

The ESSID (Extended Service Set ID) is a password that is configured in the Access Point or Access Unit. Only terminals configured with the same ESSID can synchronize with the access point and join the network. This means that an intruder attempting to join a network with an Alvarion station adapter cannot do so unless the correct ESSID is entered.

Let us assume that someone successfully steals one of the terminals and uses it to connect to the network. When any terminal joins the network, an SNMP alarm is sent by the Access Point to the management station with the MAC address of the joining station. In the event that an unauthorized terminal is detected, the ESSID of the network's Access Points and Station Adapters can be simply changed so that the network is once again secured (management platform scripts can be written to fully automate this process).

Changing the ESSID can be done either through the local craft interface (monitor port) of each unit or remotely by SNMP. With the BreezeACCESS & BreezeNET PRO.11 products, the wireless configuration of ESSIDs can be performed by using SNMP management. In this manner, network managers need not worry about configuring remote wireless station adapters as the entire process can be activated via the SNMP manager (all the SNMP settings are protected by SET and GET communities).

3. RC4 Authentication

The BreezeACCESS & BreezeNET PRO.11 products support a shared, key-encrypted authentication algorithm, which is activated upon the joining of a terminal to an Access Point.

The process proceeds as follows:

- The joining terminal sends an authentication request
- The Access Point returns a randomly generated challenge text
- The joining terminal encrypts the random text according to its own configured encryption key and an RC4 encryption algorithm and sends it back to the access point
- The Access Point decrypts the text according to its own key and checks whether it is identical to the original text
- Following verification, the terminal is authenticated and can join the network; lack of verification leads to automatic rejection.

This authentication algorithm differs from the 802.11 WEP data encryption process, which has been found to contain security flaws. The Alvarion authentication transaction is very brief, and as the generated text is random, wireless sniffer devices cannot collect enough data in order to break the key.

4. Local Monitor Access Rights Levels

BreezeACCESS & BreezeNET PRO.11 units can be configured through either SNMP or by connecting a terminal with an RS-232 cable to the local craft interface of a unit (monitor port). Monitor access has three different access levels protected by a changeable password. The different levels prevent intruders from changing certain parameters by physically connecting to the unit or even from seeing the configured parameters.



5. Proprietary Hopping Patterns

A unique and outstanding security feature of the BreezeACCESS & BreezeNET PRO.11 products is the ability to set proprietary hopping patterns. In Frequency Hopping systems, when a station adapter joins an access point (assuming it is configured with the same ESSID), the access point tells it the number of hopping pattern used, so it can tune itself to the same one and synchronize with the AP. The Hopping Pattern is a list containing the frequencies (channels) of operation in the specific order of hopping.

In 2.4 GHz systems, for example, the hopping pattern 4,32,26,18...45 means that the units should commence working in 2.404 GHz, then hop to 2.432 GHz, then to 2.426 GHz and so on, until the end of the pattern is reached and the cycle commences again. In all other Broadband Wireless systems, the AP must be configured to one of the predefined hopping patterns, which is hardware-coded into both access points and terminals. Those patterns are standard and appear in the standard tables, so it is possible, even though it is very complex, for someone to build a device that will hop in those patterns and intercept the data.

With the BreezeACCESS & BreezeNET PRO.11 series, it is possible to download proprietary hopping patterns to the Access Point and to all other BreezeACCESS & BreezeNET PRO.11 terminals. After configuring the Access Point to work with the proprietary hopping pattern, only terminals downloaded with the same hopping pattern can join it. Building a device that will synchronize with a specific network's transmission becomes virtually impossible, since the transmitted pattern is not listed anywhere, and can be changed as often as desired.

The download is executed with a standard TFTP application, and can even be initiated via wireless (i.e. from the wired LAN to the wireless station adapters). The units can store up to three different sets of proprietary hopping patterns.

This powerful feature is intended for use in very sensitive applications (such as military use, financial establishments, etc.), and it provides the best existing solution against tapping.

If a unit downloaded with a proprietary hopping pattern is stolen, simply download different patterns and continue to work. The available number of possible patterns is almost infinite.

6. Sniffer Devices for 802.11 systems

As the 802.11b standard became increasingly popular, more and more Sniffer devices were being introduced into the market. These devices contain the inherent flaws in the 802.11 WEP data encryption protocol that allow hackers to penetrate into 802.11-based systems. It is noteworthy that most of those sniffer devices can operate only in 802.11b direct sequence networks, and are designed to break the WEP data encryption protocol.

In contrast, the BreezeACCESS and BreezeNET PRO.11 do not employ the WEP data encryption protocol and therefore are not sensitive to its flaws. Sniffer devices are less common for the Frequency Hopping technology, as this technology is much more complex and less common. Moreover, using the proprietary hopping patterns feature protects a network against frequency-hopping sniffer devices, since those devices are not capable of scanning non-standard hopping patterns.

Conclusion

Whether employing copper, cable or wireless infrastructures, the integrity of any network may be compromised by creative hackers. This document has shown that the security issues common to networks based on Broadband Wireless systems can be addressed confidently and successfully by the BreezeACCESS & BreezeNET PRO.11 products. By applying the enhanced security features of these solutions wisely, network operators can look forward to offering access and networking services to their customer base with significantly limited risk of intrusion, making the already strong business case for BWA deployments even more attractive.



www.alvarion.com



International Corporate Headquarters

Alvarion Ltd.
21a HaBarzel Street
Tel Aviv 69710, Israel
Tel: +972 3 645 6262
Fax: +972 3 645 6222
Email: corporate-sales@alvarion.com

Alvarion Worldwide offices:

Latin America & Caribbean

7497 W. Oakland Park Blvd.
Suite 304
Lauderhill, FL 33319 USA
Tel: +1 954 746 7420
Fax: +1 954 746 9332
Email: lasales@alvarion.com

Asia Pacific

Room 2603, 26/F
Laws Commercial Plaza
788 Cheung Sha Wan Road
Kowloon Hong Kong
Tel: +852 2786 9996
Fax: +852 2310 0062
Email: far.east-sales@alvarion.com

China

R. 803, Tower 1,
Bright China Chang An Building, No. 7
Jianguomen Nei Avenue
Beijing 100005 China
Tel: +86 10 6510 2800
Fax: +86 10 6510 2803
Email: china-sales@alvarion.com

North America Headquarters

Alvarion Inc.
1890 Rutherford Road, Suite 100
Carlsbad, CA 92008
Tel: (760) 517 3100
Fax: (760) 517 3210
Email: n.america-sales@alvarion.com

France

Le Saint James, 3 Chemin de la Dime
95700, Roissy en France
Tel: +33 1 34 38 54 30
Fax: +33 1 34 38 54 39
Email: france-sales@alvarion.com

Germany

Weltenburger Str. 70
Munich
Tel: +49 89 92 404 212
Fax: +49 89 92 404 200
Email: germany-sales@alvarion.com

U.K. & Ireland

15 Liberty House
New Greenham Park, Newbury
Berkshire, RG19 6HW England
Tel: +44 845 450 1414
Fax: +44 845 450 1455
Email: uk-sales@alvarion.com

Czech Republic

Detsky Dum
Na Prikope 15
110 00 Praha 1 Czech Republic
Tel: +420 222 191 233
Fax: +420 222 191 200
Email: czech-sales@alvarion.com

Brazil

Av. Brigadeiro Faria Lima, 1685
1st Fl., room 1C
Sao Paulo 01452-001 Brazil
Tel: +55 11 3813 0467
Fax: +55 11 813 467
Email: brazil-sales@alvarion.com

Uruguay

Br. Espana, 2586
Montevideo 11300 Uruguay
Tel: +598 2 712 3210
Fax: +508 2 712 3211
Email: s.america-sales@alvarion.com