BreezeCOM and Floware unite

alvarion
We're on your wavelength.

BreezeACCESS® VL

Security

Technical Paper

Executive Summary

BreezeACCESS VL products offer an extensive set of features to prevent unauthorized access to information or services, whether attempted by means of a similar wireless system, or through other means of interception. By using advanced security measures at several levels to address all types of potential risk, BreezeACCESS VL is the most secure BWA product on the license-exempt market, ensuring its recognition as the best solution for security conscious customers. These security measures include 128-bit WEP and AES data encryption; comprehensive tools for authentication of legitimate users and control of paid-for services; denial of services to "stolen" units and automatic identification of fraudulent configuration change attempts; meticulous control of access for management and configuration of units; numerous filtering and flow control features; and built-in support for virtual private networks.

Introduction

Like any other communication network that serves organizations and individuals who wish to keep their information secure, Broadband Wireless Access (BWA) systems should employ measures to ensure privacy for their end users and prevent unauthorized persons from getting access to sensitive information. Since BWA systems utilize the open air as the medium for transmission, the basic question that begs attention is how to prevent intruders from intercepting sensitive and confidential information transmitted over the airwaves.

Both the customers and the operators themselves should feel confident that the system is private and secure, and that the appropriate measures are available to minimize security risks, including:

➤ Eavesdropping: Intentional interception of information being transmitted

➤ Privacy: Ensure information transmitted is readable only by the intended recipients of the information

➤ MAC Spoofing: Preventing an attacker from copying the MAC address of legitimate CPEs to gain access to the network

➢ Theft of Service: Preventing attackers from gaining access to the Internet or other services using stolen CPEs and preventing legitimate users from getting services for free.

BreezeACCESS VL products offer an extensive set of features to prevent unauthorized access to information or services, whether attempted by means of a similar wireless system, or through other means of interception. BreezeACCESS VL systems use security measures at several levels to address all types of potential risk. The purpose of this document is to present the solutions provided by BreezeACCESS VL products as viable measures for effectively addressing the security issues presented by the use of Broadband Wireless Access systems.

Enforcing Management Access Security

Access to management of BreezeACCESS devices is protected at several levels to prevent any unauthorized changes:

Access Level Protection

Access to all management utilities is password protected, supporting 3 access levels:

➢ User: View-only (status and parameters)

➢ Installer: Configuration of basic parameters (parameters that must be configured during installation) and site-survey tests.

➢ Administrator: Access to all parameters and tests.

Passwords are controlled by the administrator for proper management of passwords provided to installers and users. Depending on specific operator's policy, an administrator can choose to provide the installers with the Installer Password only, limiting the installer access to parameters that are necessary for installation and testing and denying access to parameters that affect chargeable services.

To ensure that unauthorized persons will not be able to change passwords, there is no built-in back-door mechanism for gaining access to the passwords or resetting them to the default values. For cases where for some reason an unknown Administrator Password is

configured in a device, a special application is available for resetting the passwords to default values. This application uses a highly protected device dependent mechanism and is controlled by Alvarion to ensure its use only by properly authorized persons.

Port restrictions for Management Access

Access to management of each unit can be limited by enabling access only via a certain interface port: From the Ethernet port only (which is the default selection for Access Units), from wireless port only (which is the default selection for Subscriber Units), or from both ports. This feature can prevent hackers and other unauthorized persons from being able to access the management utilities of the units.

Address Restrictions for Management Access

Access to each unit for management purposes can be limited using IP Address-based filtering. If management filtering is enabled, the unit can only be managed by stations with IP addresses matching one of the entries in the configurable Management IP Addresses database defined in the unit.

VLAN Restrictions for Management Access

Access to units for management purposes can further be limited using VLAN tagging. By defining Management VLAN, the unit will only accept management frames that have the appropriate Management VLAN ID. All other frames using any management protocol such as Telnet or SNMP will be rejected.

Preventing Tapping of the Wireless Link

Basic Principles of BWA system operation

Broadband Wireless Access systems typically comprise a cell or a group of cells, each of which contain several wireless terminals (also known as subscriber units, or CPEs). Each cell consists of one or more Access Unit devices that are usually connected to the backbone, and which manage all the traffic within the covered area and between the

covered area and the backbone network. Terminals within the coverage area of an access unit connect to the network backbone through the access unit.

All the terminals associated with an access unit are synchronized by both frequency and clock and use a stringent protocol in order to communicate with the access unit. 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 unit.

Can't a potential intruder utilize another Alvarion terminal and attempt to connect to a wireless network and compromise its integrity?

ESSID

The Extended Service Set ID (ESSID) identifies a wireless network, which prevents the unintentional merging of two collocated wireless networks as well as ensuring that units that are not configured with the correct ESSID will not be able to synchronize with the access unit. A subscriber unit can only associate with an access unit that has an identical ESSID. Different ESSIDs are used to enhance security and to segment the wireless access network.

Encrypted Authentication Process

Unauthorized wireless connection is prevented using encryption during the authentication process. Each subscriber unit must be authenticated before enabling it to associate with the access unit. This is based on interchange of information between the two units, where the subscriber unit proves the knowledge of a given key by using it to encrypt a challenge text sent by the access unit. Both WEP 128 or AES 128 encryption algorithm are supported by BreezeACCESS VL products and can be used for the authentication process. For more details on these algorithms and the applicable encryption keys refer to Data Encryption on page 10.

The following authentication options are available:

➢ Open System: A subscriber unit configured to Open System mode can only associate with an access unit that is also configured to Open System. In this case, the authentication encryption algorithm is not used.

5

➤ Shared Key: The authentication messages are encrypted. A subscriber unit configured to use a Shared Key can only be authenticated by an access unit configured to use a Shared Key, provided the applicable key (which means both the key number and its content) in the access unit is identical to the key selected as the Default Key in the subscriber unit.

➤ Promiscuous (Support All) Mode: Regardless of the above, the Promiscuous Authentication mode enables new subscriber units to join an active cell where Shared Key operation and/or Data Encryption is used, even if this subscriber unit does not have the correct security parameters. After the subscriber unit joins the cell it should be remotely configured with the proper parameters. Once the subscriber unit is configured properly, the Promiscuous Mode should be disabled in both the access unit and the subscriber units.

Denying Services to Stolen or Units

Authentication Prevention

The Promiscuous "Support All" mode in the access unit can be used to authenticate all subscriber units, regardless of their configured authentication encryption parameters. This is intended primarily for installations with possible stolen subscriber units, as well as in situations where according to the operator's security policy encryption parameters' values are not provided to installers. In such cases, initial authentication will be in this mode enabling all units to be authenticated. The operation mode will be changed to encryption-based authentication after remotely configuring appropriate encryption parameters only in "legitimate" subscriber units, thus causing de-authentication of all other units.

Service Denial to Subscriber Units

The MAC Address Deny List feature enables to define units that are not authorized to receive services. The access unit will not provide services to a unit whose MAC Address is included in the deny list. This feature enables to disconnect units from the services in cases such as when the unit is suspected to be stolen as well as when the user had fraudulently succeeded to configure the unit to values different than his subscription plan.

Provisioning Services to Specific Users Only

The User Filtering option incorporated in the subscriber unit enables to configure selected addresses of devices connected to the unit, permitting IP traffic only to/from these addresses. Any attempt to gain access to services from any unauthorized terminal connected to local network will be blocked.

Identifying Fraudulent Service Configurations

In addition to all access control measures taken to prevent unauthorized changes to parameters that define chargeable services, there are additional features that enable identification of unauthorized configuration changes. Once such changes have been identified, the administrator can choose whether to just correct the configuration or to completely deny services to the unit.

Any change to a parameter included in a special list will automatically initiate transmission of a trap message indicating the nature of the change. The list of such parameters includes all parameters that can affect chargeable services.

Moreover, Network Management Systems such as AlvariSTAR or others can automatically identify any change to service affecting parameters through routine periodical enquiries, overriding any attempt at trying to prevent trap sending by making configuration changes off-line.

Maintaining Privacy Within the BWA System

Several measured at different levels are available to ensure that traffic within the wireless network will reach only the intended recipients:

Virtual LAN Support

Virtual LAN (VLAN) technology addresses the need to control traffic flow across the network. VLAN is a network topology in which the network is divided to logical "sub networks" (VLANs). Each VLAN includes stations that can communicate between themselves acting together as a separate, independent LAN, but cannot communicate

with stations from other VLANs. VLAN technology also provides the ability to set traffic priority for transmitted frames.

The VLAN feature implementation in BreezeACCESS VL units is based on IEEE standard 802.1Q. The implementation enables the access unit and the subscriber units it serves to function as a VLAN-Aware Distributed Wireless Switch. VLAN is implemented through adding to each frame a special VLAN Header Tag, which includes the VLAN-ID as well as the VLAN Priority. A VLAN-aware switch supports tagging/un-tagging and filtering of frames based on the information in the tag.

The ports in the distributed wireless switch can be defined to support different link types, according to the devices connected to them. Access units can function as either a Trunk link or a Hybrid link. Subscriber units can function as an Access link, a Trunk link or a Hybrid link

A link is defined as an Access link if all devices connected to it are VLAN-unaware. Therefore, an Access link cannot transport tagged frames, and the BreezeACCESS VL unit performs the required tagging of frames transmitted to the wireless media and untagging of frames before transmission to the Ethernet. The BreezeACCESS VL unit will accept from the wireless media only data frames whose VLAN ID matches its configured Data VLAN ID.

All the devices connected to a Trunk link should be VLAN-aware. Therefore, a Trunk link can transport only tagged frames. The BreezeACCESS VL unit accepts only tagged frames and does not perform any tagging/un-tagging. A Forwarding filtering feature incorporated in BreezeACCESS VL unit enables to optionally filter the received frames and to forward only frames who's VLAN ID is included in a forwarding list. The Relaying filtering feature incorporated in Access Units enables to optionally filter the frames received from Subscriber Units and intended for relaying back to the wireless media, by relaying only frames whose VLAN ID is included in the relaying table.

A Hybrid link can contain both VLAN-aware and VLAN-unaware devices. Therefore, a Hybrid link can transfer both tagged and un-tagged frames. The BreezeACCESS VL unit accepts both tagged and un-tagged data frames and does not perform any tagging/un-tagging.

An access unit may connect to either a Hybrid link or a Trunk link. A subscriber unit may connect to a Hybrid link, a Trunk link or an Access link.

BreezeACCESS VL units handle management frames in a different manner: If the Management VLAN ID is configured as No VLAN, it will accept all un-tagged management frames. If it is configured to a specific VLAN ID value, it will accept only management frames with a matching VLAN ID, and will tag management frames generated by it with the same VLAN ID as well as with the value of the configured VLAN Priority-Management. This applies to all management applications using protocols such as SNMP, TFTP, ICMP (ping), DHCP and Telnet. All servers/stations using these protocols must tag the management frames sent to the unit with the appropriate value of the VLAN ID - Management parameter.

Filtering Ethernet Broadcasts

The Ethernet Broadcast Filtering feature enables defining the layer 2 (Ethernet) broadcast and multicast filtering capabilities for each subscriber unit. Filtering the Ethernet broadcasts enhances the security of the system and saves bandwidth on the wireless media by blocking protocols that are typically used in the end-user's LAN but are not relevant for other end-users, such as Net-Bios. The implementation of the Ethernet broadcast filtering feature in BreezeACCESS VL units enables to filter broadcast received on the Ethernet port, the wireless port or both ports.

The implementation enables to exclude specific protocol frames from being filtered when Ethernet filtering is used. Thus, it is possible to filter all Ethernet broadcasts while still allowing DHCP and/or PPPoE and/or ARP broadcasts.

Wireless Relay Filtering

Normally, broadcast messages originating from devices on the wireless link are transmitted by the access unit back to the wireless link devices, as well as to the wired LAN. The multicast relay filtering feature allows to filter these transmissions and to send broadcasts only to the wired LAN without sending them back to the wireless link. If all

broadcast messages from subscriber units are not intended to other devices served by the access unit, broadcasts relaying can be disabled.

Similarly, it is possible to disable relaying of unicast messages back to the wireless link when all such messages should be directed to the wired LAN port of the access unit.

Controlling Information Flow in Access Units

Using the inherent bridging functionality, the access unit can be configured to control the flow of information from the Ethernet Backbone to the wireless media in either one of two methods. When configured to reject unknown addresses, the access unit transmits frames only to those addresses that the unit knows to exist on the wireless link side. When configured to forward unknown addresses, the access unit transmits all frames, except those sent to addresses that the access unit recognizes as being on its wired Ethernet side.

Data Encryption

BreezeACCESS VL products enable to use either WEP 128 or AES 128 for encrypting the data transmitted over the air and/or the authentication protocol:

Wired Equivalent Privacy (WEP)

In 1999, the IEEE 802.11 Working Group proposed an optional security mechanism called the WEP protocol. WEP seeks to provide a level of wireless networks security similar to that of wired LANs by encrypting data transmissions and preventing unauthorized users from connecting. WEP is not a mandatory part of the IEEE 802.11 specification, though, and most 802.11b products do not have the computing power to run WEP encryption without significant performance degradation. Thus, many 802.11b users have turned off WEP security in their networks. Over time, however, more users have recognized the importance of wireless network security and started to enable WEP encryption.

Regrettably, WEP has proven inadequate for securing wireless networks. Many security

experts in both academia and private industry have identified holes in the underlying WEP specification. In light of these deficiencies, many vendors increased the WEP key length in their products from 40 to 112 bits and marketed this capability as "stronger" WEP encryption. Note, however, that a longer encryption key is only beneficial if the underlying encryption cipher is secure. Because WEP is inherently not secure, increasing the WEP key length simply increases the amount of time it takes for a hacker to break into the network.

Advanced Encryption Standard (AES)

In the wake of WEP's flows, the IEEE 802.11i task group has adopted the AES algorithm for encrypting data in wireless networks. The Advanced Encryption Standard is a secure encryption cipher that is resistant to all currently known techniques of cryptanalysis. The United States National Institute of Standards (NIST) has selected AES to replace the Data Encryption Standard (DES and 3DES) commonly used in Virtual Private Network (VPN) solutions.

Encryption Keys

Four different encryption keys can be defined for each access unit. The encryption key is used for initializing the pseudo - random number generator that forms a part of the encryption/decryption process. Each Key is comprised of 32 hexadecimal numbers.

At the subscriber unit one of the four available keys is selected for encrypting/decrypting the authentication messages (Shared Key mode) and/or data frames (Data Encryption). The access unit automatically learns the key used by each subscriber unit, and it may use different keys when authenticating and/or communicating with different subscriber units. When encrypting data, the selection of the key to be used for encrypting multicasts is performed at the access unit.