

Network Security in a Wireless LAN

by



First Draft (7/7/97)

Breeze Wireless Communications, Inc.
2195 Faraday Avenue, Suite A
Carlsbad, CA 92008
Phone: (760) 431-9880
Fax: (760) 431-2595
<http://www.breezecom.com>

July 1997

INTRODUCTION3

LAN SECURITY ISSUES – WIRED VS. WIRELESS3

FRIENDLY FOES? – SITE CONTROL3

KEEP OUT! – AUTHORIZED USERS ONLY4

THE SPIES HAVE IT? – EAVESDROPPERS4

WIRELESS SECURITY CONSIDERATIONS.....4

BREEZECOM’S WIRELESS NETWORK5

SPREAD SPECTRUM TECHNOLOGY5

STATION AUTHENTICATION – ESS ID6

USER AUTHENTICATION – PASSWORD CONTROL.....6

DATA ENCRYPTION7

OTHER WIRELESS CONSIDERATIONS7

WEP – WIRED EQUIVALENCY PRIVACY.....7

CONCLUSION.....8

INTRODUCTION

One of the most frequently asked questions put to Wireless local-area network vendors is, “What about security?” In this day and age, it is wise for network administrators to be concerned about security, given all the attention it’s getting in the press. Unfortunately, disgruntled employees, hackers, viruses, industrial espionage, and other forms of destruction are not uncommon in today’s networks. What we will discuss in this white paper are the threats to the security of *any* network, how they specifically relate to the *wireless* aspect of the LAN, and what is uniquely embedded in wireless LAN technology or available as an add-on to combat these potential threats.

LAN SECURITY ISSUES – WIRED VS. WIRELESS

People might be complacent about security when using a wired LAN but as soon as the data packets begin traveling through “the air”, they become concerned. After all, they reason, the wired LAN is inside the company’s building – as if the wired network has some intrinsic “security” built into it. In fact, any network, including a wired LAN, is subject to substantial security risks and issues, namely:

- Attacks from within the network’s user community
- Unauthorized users gaining access
- Eavesdropping from outside the company or work group

The good news is that there are ways to combat these security threats for both wired *and* wireless LANs and, in fact, the *wireless* LAN segments come with some built-in security features you might not have considered.

FRIENDLY FOES? – SITE CONTROL

By far, the biggest threat to a company’s network comes from within the company itself. Without the proper security measures in place, any registered user of the network can access data that he or she has no business accessing. Disgruntled current and ex-employees have been known to read, distribute, and even alter, valuable company data files.

Network administrators, regardless of whether or not they have *wireless* segments on their LANs, need to have the right security products for their environments, the proper security levels set for their users, and an on-going way to audit the effectiveness of the security process.

KEEP OUT! – AUTHORIZED USERS ONLY

Another area of concern for security conscious network administrators is the growing use of the Internet. If users from inside can get *out* to the Internet, then users from outside can get *into* your network if you haven't taken the proper precautions. And this applies not only to the Internet, but to any capabilities you might have that allow users to come in from the outside. Remote access products that allow your traveling sales and marketing people to dial in for their email, remote offices connected via dial-up lines, on-site Web sites, and "Extranets" that connect your vendors and customers to your network all can leave your network vulnerable to hackers, viruses, and other intruders.

Many products are available to help network administrators secure their networks from the above threats. User authentication and authorization is provided by most network operating systems, and can be enhanced by adding third party products. Firewall products offering packet filtering, proxy servers, and user-to-session aware filtering add additional protection.

THE SPIES HAVE IT? – EAVESDROPPERS

Perhaps the most difficult threat to detect is someone just looking at the data packets. Actually, *wired* nets are quite vulnerable to eavesdropping. Most Ethernet adapters on the market today offer a "promiscuous mode" that, with off-the-shelf software, enables them to capture every packet on the network. What network administrator doesn't have some kind of "Sniffer" or datscope for trouble-shooting the network? For about \$1,000 anyone can buy a copy of FTP Software's LANWatch or AG Group's EtherPeek and run it on virtually any PC on the net. These programs let you read, capture, and display any type of packet data on the net.

And if you think that because your wires are inside your building, you are safe from outside eavesdropping – think again. Ethernet 10Base-T cabling acts as a remarkable antenna. Anyone with a strong motivation and a good antenna can sit in the parking lot and pick up your wired Ethernet data packets!

Data encryption is the only line of defense against this kind of threat.

WIRELESS SECURITY CONSIDERATIONS

As you can see from the above discussion, data security considerations impact the entire network architecture. If security is a concern to you, then you must consider solutions for *both* your wired and wireless users.

BREEZECOM®'S WIRELESS NETWORK

In fact, as we will explain below, the wireless technology itself and, in particular, today's available LAN implementations, offer some inherent features that add to the overall security of wireless LAN products.

Breeze Wireless Communications Inc. (BreezeCOM) offers a line of radio frequency (RF) LAN products designed to offer wireless services to wired Ethernet users. BreezeNET® products consist of Access Points (AP-10 PRO) that act as a "bridge" or "hub" from the wireless to the wired network and Station Adapters (SA-10 PRO and SA-40 PRO) that connect desktop and notebook users wirelessly to the LAN through the AP-10 PRO.

The security of BreezeNET's technology is defined at four levels:

- The frequency hopping, spread spectrum (FHSS) wireless technology itself
- The Extended Service Set Identifier (ESS ID)
- A user password
- The addition of a third party data encryption product

SPREAD SPECTRUM TECHNOLOGY

Spread spectrum technology was first introduced about 50 years ago by the military as a way of sending secure communications. From the beginning it was designed to be resistant to noise, interference, jamming, and unauthorized detection. Spread spectrum transmitters send their signals out over a multiple range of frequencies at very low power, in contrast to narrow band radios that concentrate all of their power into a single frequency. There are several ways to implement spread spectrum transmission, the two most common being direct sequence and frequency hopping.

BreezeCOM products use the frequency hopping method of spreading their signals, whereby the range of available frequencies in the ISM (Industrial Scientific Medical) band of 2.400 - 2.483 GHz is divided into a series of up to 79 separate and distinct channels. Transmissions are sent over each of these channels in what appears to be a random sequence (called a "pseudo-random sequence") such as channel 1, channel 32, channel 3, channel 56, etc. The radio switches frequencies many times a second, transmitting on each channel for a fixed amount of time, then proceeding on to the next channel in its sequence, covering all of the channels before repeating the sequence. Without knowing how long to stay on each channel (the "dwell time") and what the hopping pattern is,

it is impossible for a non-participating station to receive and decipher the data.

The use of different hopping patterns, dwell times, and/or number of channels is what allows two disjoint wireless LANs to exist nearby one-another without causing interference and without fear of data from one network being seen by the other.

STATION AUTHENTICATION – ESS ID

For any station to be able to access BreezeNET Access Points, the AP-10 PRO first determines if that station belongs to its network, or Extended Service Set (ESS). The AP-10 PRO looks to see if the station's 32-character ESS Identifier (ESS ID) matches its own. Non-members, even with another set of BreezeNET products, can neither participate in the network nor learn the hopping sequence and timing needed to eavesdrop. The ESS ID is programmed into the SA-10 PRO and SA-40 PRO station adapters and the AP-10 PROs, under the control of an Installer password, and can only be accessed or changed while directly connected to the AP-10 PRO itself, never remotely.

If there is a need to have separate wireless LAN segments on one network, such as to segment the accounting department from the rest of the company, then you can program the ESS IDs to be different. If you need to have several AP-10 PROs near one another, for example, to increase overall bandwidth or to support roaming notebook users, then the Access Point's ESS IDs would be programmed to the same value but the hop sequences would be programmed to different values, always under the control of an Installer password, at the AP-10 PRO.

With a 32-character ESS ID and a 3-character hop sequence, you can see how difficult it would be for someone to figure out the exact ESS ID and hop sequence in order to gain access to the LAN via one of its wireless segments.

USER AUTHENTICATION – PASSWORD CONTROL

While not specific to wireless networks, we feel that we much encourage the use of network password controls in wireless network stations. Network operating systems and servers, such as Novell NetWare and Microsoft NT, provide built-in levels of security, including password management. Passwords should be under tight control and changed frequently. Since wireless LANs can accommodate mobile users who tend to move their notebooks from location to location, a strict password

policy adds a level of security that helps to ensure that the station is being used by the person for whom it is intended.

DATA ENCRYPTION

If your data needs to be kept ultra-secure, such as on a financial or military network, then you might need extra measures. The last and highest level of security is achieved by the addition of an encryption product on the network as a whole. Either by hardware or software, the data in the packets is scrambled before it is sent over the LAN. Only stations that have the correct decryption key can unscramble and read the data.

If total security is a necessity, encryption is the best solution. Encryption capabilities can be found in some network operating systems. Low cost third party products are available on a per-seat or per-server basis. For about \$50 per seat, products such as McAfee Associates' NetCrypto or Capital Resource's Snare can ensure that only authorized users can access the network and read the data. BreezeCOM endorses the use of third party encryption software since companies that develop such software have a focused effort on this type of business and can provide the best features and highest level of quality, service, and support for their customers.

OTHER WIRELESS CONSIDERATIONS

Wireless LANs have certain other characteristics that make them less of a security concern. First, the AP-10 PRO Access Point filters all network traffic which is not meant for the associated wireless stations. This means that most of the wired network traffic never appears on the airwaves at all. Furthermore, wireless network nodes and access points have a transmission range limit, usually of several hundred feet, depending on the environment. This means an eavesdropper must be nearby. And last, wireless users can be mobile, moving from one Access Point to another during the same session. In so doing, their network traffic will no longer be transmitted using the same hopping sequence as before, making eavesdropping nearly impossible.

WEP – WIRED EQUIVALENCY PRIVACY

The IEEE 802.11 committee is responsible for setting the standards for wireless LANs and BreezeNET wireless LAN products were designed to be compatible with this important standard from their inception. This standards organization has addressed network security issues by

creating and defining Wired Equivalency Privacy. Users are primarily concerned that an intruder should not be able to:

- Access the network by using similar wireless LAN equipment
- Capture wireless LAN traffic, i.e. eavesdropping

In 802.11 networks, access to network resources is denied any user who does not prove knowledge of the current key. This is analogous to a user having a key to the building to access the wired network. BreezeNET products will offer this extra level of security by the addition of an Authentication Password, whereby the user of the station hardware needs to provide the current key before the station will be given access to the Access Point and the wired network.

Eavesdropping is prevented by using the WEP algorithm whereby a pseudo-random number generator is initialized by a shared secret key. Based on RSA's RC4, this simple algorithm has the following properties:

- *Reasonably strong* – A brute-force attack to this algorithm is difficult because every frame is sent with an initialization vector which restarts the PRNG for each frame.
- *Self-synchronizing* – Because just like in any LAN, the wireless LAN stations work in a connection-less environment where packets may get lost, the WEP algorithm re-synchronizes at each message.

As this white paper goes to print, the IEEE 802.11 standard has been ratified and BreezeCOM has reconfirmed its total commitment to the standard by promising a software upgrade path to the final 802.11 standard for all of its BreezeNET PRO products.

CONCLUSION

A certain level of security is a must in most local area networks, regardless of whether or not there are wireless segments. Even wired networks are vulnerable to insider curiosity, outsider attack, and wire-tapping. No one wants to risk having the LAN data exposed to the casual observer or open to malicious mischief. But if the data is very confidential, such as that found on banking and military networks, then extra measures must be taken to ensure privacy. From this discussion, we hope you will see the importance of security to your entire network and realize that your wireless segments can offer you at least the same, if not more, protection as your wired ones.