



Security Features of the Access5830™ Broadband Access Solution

Introduction

Data security is of paramount interest to the designers, implementers, and users of fixed wireless networks. Much of this concern has arisen due to published technical studies, which highlight the security vulnerabilities in the increasingly popular 802.11b wireless LAN standard. This open, standard architecture permits competing 802.11b equipment manufacturers to co-exist on the same local area network. Unfortunately, this interoperability feature also limits the security of the network employing such technology.

For the purposes of this document it is important to highlight the fact that the Access5830 Broadband Access Solution system does NOT employ the 802.11b RF protocol, and instead employs a proprietary protocol scheme. The very nature of this proprietary protocol, coupled with the advantages of direct sequence spread spectrum, user authentication, and scrambling allows the Access5830 to provide an inherent level of security not found in 802.11b-based systems or other competing, standards based wireless systems.

The proprietary polling and authentication techniques employed by the Access5830 mitigate decryption and unauthorized access. Unlike 802.11b radios, there are no off-the-shelf sniffers, or other such devices that can be employed to “hack” into or eavesdrop on the Access5830 system. The advanced nature of the modulation and data-scrambling techniques ensure that the only method to access the system over-the-air is with another Access5830 radio. And, with the provisions designed for authentication, the network will not recognize an unauthorized Access5830 radio in the proximity of the network.

It is important to point out that the Access5830 does not employ a secondary encryption algorithm (primary encryption is accomplished via spread spectrum by design), and in it of itself does not guarantee a secure network. To guarantee a secure network, whether it is hardwired or wireless, it is recommended that users employ Virtual Private Network (VPN) or other encryption techniques. The inherent security features of the Access5830 system are meant to be a very effective, albeit a first line of defense.

Security Features

There are four distinct features of the Access5830 system, which contribute to an inherent level of security by design and implementation:

1. Proprietary data scrambling of Radio Frequency (RF) data packets
2. Authentication of Subscribers
3. Adaptive Polling protocol
4. Spread Spectrum modulation at 5.8 GHz

Proprietary Data Scrambling

The scrambling technique employed by the Access5830 involves proprietary patterns of sequencing and combining each data byte with one of 256 scrambling bytes. This technique offers a significant level of over-the-air security. The proprietary nature of the scrambling technique permits only authenticated Access5830 radios to intercept and de-scramble the data.

Authentication

An Access5830 wireless system is comprised of one or more co-located Access Points (APs) and one or more Subscriber Units (SUs). In order for information to pass between AP and SU, the AP must authenticate the SU. This is achieved through a password protected database system administered through the AP. Each AP contains a database of SUs that are authorized to communicate with the AP. The SU database, located within non-volatile memory of the AP, must contain the unique MAC identification (ID) of each SU authorized for operation on the network. In addition to the MAC ID, a unique SU number identifies each SU. Similarly, each SU must be set up to associate with a specific AP (referred to as the AP ID) and a specific base location (referred to as the Base ID).

In addition to the above, another layer of authentication is added to each data packet outbound from an AP; a scrambled identifier is encoded with the data packet along with a target SU "address". In other words, only the intended SU can de-scramble and read the data, and recreate the original Ethernet packet.

In short, only authenticated SUs can associate with a specific AP provided the SU's identity resides in the AP's database. In the event an unauthorized or rogue SU is brought into proximity to a wireless Access5830 network, it will not authenticate to the AP and will be impossible for the rogue SU to gain network access.

SMARTPolling™, Trango's Dynamic Polling Protocol

Another feature of the Access5830 system is the SMARTPolling™ protocol that enables highly efficient use of a given AP's 10 Mbps bandwidth in a point-to-multipoint Ethernet system. In addition to providing highly efficient bandwidth efficiency, the SMARTPolling™ feature also provides an additional level of security. SMARTPolling™ is an algorithm executed by the AP that allocates varying timeslots at varying intervals to each SU in order to grant it permission to send data back and forth to the AP. The polling sequence and allocation of timeslots is determined according to various parameters including the amount of data, and the frequency of data needed to be sent by each SU. The polling sequence, and resulting sequence of data transmissions, is dynamic, and not set to a synchronous, predetermined pattern - unlike straight Time Division Multiple Access, or TDMA based systems. As a result Trango's SMARTPolling™ feature provides added protection from outside tampering since the invading party will not be able to predict the polling sequence.

Spread Spectrum 5.8 GHz

The Access5830 employs Spread Spectrum modulation in the unlicensed 5.8 GHz ISM band. Spread Spectrum provides a degree of protection, as there is no simple demodulator, either on the market - or easily constructed, that can receive the signal. The signal and encoded data, is modulated and spread over a band of frequencies. The modulation process employs an 8-bit pseudo noise code, further providing a layer of security and an 8-bit scrambling code.

While the above features represent a good means of addressing security concerns, they are by no means exhaustive. We encourage operators to employ other means of securing their networks via VPN, packet encryption, etc. to even better address security requirements. This paper has presented some features of the Access5830 product line that address the concerns for mitigating security breaches on private networks. Future product releases will continue to build and expand upon what is presented here.