Horizon Solutions Offer Best in Class Security

DragonWave

www.dragonwaveinc.com

Horizon Solutions Offer Best in Class Security

DragonWave's Horizon systems are highly resistant to data intercept and decoding. These solutions include a number of imbedded security characteristics including:

- Narrow beamwidth, directional point-to-point communications
- Bit-level data stream with Horizon synchronization and framing
- Horizon authentication
- Proven interoperability with 3rd party 256-bit AES encryption
- Leading network management security

Before addressing these security features, it should be noted that the Horizon systems are inherently secure from common intrusion schemes for signal intercept and decoding. Any intruder even attempting to extract the wireless signal would have to execute a very elaborate plan involving all of the following:

- Direct access to the LAN/WAN data stream via network equipment at the customer premises
- Access to appropriate user names and passwords
- Physical access to the Horizon units
- Direct inline access to the narrow-beam signal using a DragonWave Horizon system as the receiver. If Horizon authentication is enabled, even a 3rd Horizon system would not be able to communicate with the secure link. Any other non-DragonWave receivers would not be able to decode the Horizon synchronization and framing information.

If data security over the physical LAN connection by way of tapping into Ethernet cable or a LAN device is a concern, DragonWave recommends the use of a Virtual Private Network (VPN) between Horizon endpoints.

Narrow Beamwidth

One of the most significant security attributes of the Horizon systems is the narrow-beam signal (<2°) which is transmitted as a series of bits with Horizon synchronization, requiring a Horizon unit located within the signal beam in order to capture any data. The receiving unit must be located directly in line with the narrow-beam signal. Even with no other security mechanism enabled, an intruder would be hard pressed to place a Horizon unit directly in the 2° signal path. The narrow, directional radio beam itself is thus a formidable impediment to eavesdropping. For example, using a 24" antenna attached to a 23 GHz radio, the beamwidth of at the end of a 1 km link is only 29 meters. This means a receiving radio must be located within 14.5 meters on either side of the target receiving radio. Additionally, the signal rolls off rapidly beyond the target radio location meaning that signal interception would require a receiver sensitivity of –75 dBm in order to obtain a clear signal at a distance of 2 km. This type of receiver would be an extremely high-performance device.

Scrambled Bit-Level Data Stream

The signal contained in the Horizon data stream is encoded in such as manner as to present a seemingly random string of data bits. The user data is taken as a series of individual data bits and the Horizon framing and synchronization bits are interleaved in a proprietary manner. The receiving

Horizon system extracts the framing and decodes the user data; only a Horizon system is able to extract the information. Idle time is filled with Horizon generated random patterns (stuffing) which further mask the user data. This, combined with a lack of standard framing or start/stop indicators, makes it impossible for a sniffer to decode the data.

Authentication

Horizon authentication restricts a Horizon modem from communicating with other Horizon modems unless both units have matching authentication rings. Even if a Horizon system were placed inline with the signal, it would not be able to authenticate if another Horizon system were already in place and authenticated. The two modes of authentication are *Unique* and *Group* authentication. Unique authentication is used in a point-to-point configuration where two Horizon systems wish to communicate with each other and no other system. Group authentication is used where a network of Horizon systems is in place. The system uses out of band authentication to validate its peer every 5 minutes.

256-bit AES Encryption

DragonWave's solutions have undergone comprehensive interoperability testing with 3rd party 256-bit AES encryption – the highest level of encryption in use today. Being a fully layer-2 platform, Horizon eliminates the possibility of any potential conflicts with 3rd party security solutions.

Network Management Security

Support for SNMPv3 means that all management traffic can also be secured with AES encryption. In addition, support is provided for both SSL and SSH.

Summary

Horizon's imbedded and inherent security characteristics result in extremely secure transmission. To recap, these security features include:

- Directional point-to-point communications with <2° beamwidth
- Indecipherable bit-level data stream with proprietary scrambling, stuffing, and synchronization
- Horizon unique authentication mechanisms
- Proven interoperability with 3rd party 256-bit AES encryption
- Powerful network management security options