



Communication Devices Inc.  
85 Fulton Street  
Boonton, NJ 07005  
PH: 973.334.1980  
FX: 973.334.0545  
<http://www.commdevices.com>

## Urban Legends of Secure Out of Band Management

Secure Out of Band Management is a niche market that has attracted several “fringe” players recently. Their understanding of what is required for true Out of Band Management is suspect, and, in fact, can mislead a client into purchasing a product that does not perform as required.

Products sets that do not belong in this arena are being touted as having Secure Out of Band Management capabilities. These features include:

- Secure keys
- Two factor authentication
- On board databases

However, these products are just standard network based devices masquerading as something else. In some of the worst cases, they are completely misleading the prospective buyer about their capabilities.

### **Terminal Server Vendors**

Most of these misapprehensions revolve around Terminal Server vendors. It should be clearly understood that a terminal server is an IN BAND device. It has a network port and multiple serial ports which rely completely on the network for access and security. By definition, “Out of Band Management” uses a separate path to the managed equipment. Therefore, if you use the same network as your managed device – you are IN BAND.

This simple fact does not prevent many terminal server vendors from marketing their products as “Out of Band Management” devices.

Some Terminal Server vendors offer an external modem port or even an internal modem for out of band access. While this now makes it an out of band management device, it is still not secure. The device still relies on the network for its security such as RADIUS or TACACS. As has been explained in another of our white papers, such security measures are inadequate for Secure Out Of Band access. If these devices include on board passwords, they are static ones which, because they can be guessed, are not secure.



Communication Devices Inc.  
85 Fulton Street  
Boonton, NJ 07005  
PH: 973.334.1980  
FX: 973.334.0545  
<http://www.commdevices.com>

### **Secure Key Access & Encryption**

Other vendors promote their products through a series of “buzzwords” that indicate they use a secure key for access – when, in fact, they use a static and unsecure numeric password. This is misleading and potentially fraudulent.

To understand why, you need to understand something about encryption, which is a complex field. Products can utilize AES Encryption (Advanced Encryption Standard) in several different “modes.” These different modes strengthen a device’s security exponentially.

The simplest mode is “Electronic Code Book (ECB),” a one-for-one encryption method that is the least secure of the modes. It works by one byte into the algorithm, one byte out. Because of its simplicity, ECB is the fastest method, using the least amount of processor power. So most (if not all) of those who claim that their products utilize encryption in the Secure Out of Band market are using ECB in their software. These vendors usually include ECB in software, which slows down the processor.

On the other end of the spectrum, CDI uses Cypher Feedback, the strongest mode of encryption. Cypher Feedback uses the previous eight encrypted characters to encrypt the current character: eight characters into the algorithm, one character out. Therefore each encrypted character depends on the previous eight rounds.

Because this method is processor intensive, CDI embedded its own AES encryption engine in silicon, which processes the encryption algorithm without loading down the main CPU. This is the only way to obtain CFB encryption on an embedded device as otherwise it will create too much strain on the CPU.

### **FIPS Certification**

At least one vendor has gone to the extent of obtaining FIPS certification on their terminal server (for one model only). While this is perceived as highly beneficial for a terminal server, they are still lacking **end-to-end encryption on the modem access**.

Potential buyers need to understand that this server would fail any audit for secure out of band access because it is just a secure terminal server based on network protocols and security. We are making this claim due to our first-hand experience having to resolve the issue purchasing this product created for one of our clients. CDI’s product set was subsequently ordered by a U.S. government agency to provide the Secure Out of Band Access to these terminal servers after the agency failed audit. These “certified” servers did not encrypt access via the dial port, which is the only true out of band access to the device.

As we often tell our clients, you can receive FIPS certification on a “web browser” – this does not make it an out of band management device.