The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

40 Mile Point Lighthouse, Rogers City, MI – Photo: L Folkerth

Out-of-Band Management

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity. It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs.

There are times that I also may discuss areas of the Standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

This is a condensed version of a more detailed article that can be found in full length on the RF website here.

What is Out-of-Band Management?

Out-of-band management is a method of managing computer systems that does not rely on having a physical presence at the computer system. This approach involves a network interface on the computer system that is used outside of the normal network connectivity, hence the term "out-of-band." Since the purpose of out-of-band management is to manage the server remotely, almost all out-of-band management is a form of remote access.

Most data center-class servers have the capability for out-of-band management. For example, Dell offers its "integrated Dell Remote Access Controller (iDRAC)," and Hewlett Packard Enterprise offers the "integrated Lights Out (iLO)" controller. All server vendors I've researched offer some form of this capability.

Out-of-band management is usually implemented by adding a controller with its own network interface to the server. The controller is an additional small computer with extensive monitoring and control capabilities for the server.

Remote Console

A significant feature of a management controller is the ability to access the server's hardware console remotely. This is not the same as using remote access client software to sign in to a Windows or Linux operating system. Once you sign in to the management controller, you can bring up the remote console and see the same display as the hardware video port on the server. The remote keyboard and mouse behave exactly like they are directly connected to the server.

Why is this important? The remote access capability is available even before the system boots its installed operating system. On power up, the remote console sees the boot-up sequence and can enter BIOS and other console-only modes to configure the system, possibly without further authentication.

Web Interface

The management controller has many more capabilities. Many of these can be accessed through a web interface via the management port on the server. The web interface capabilities include:

- Monitoring server temperatures, voltages and power consumption;
- Setting the device that the server will boot from next;
- Power on, power off, or perform a hardware reset to cause a reboot;
- Upload a disk image to the management controller internal storage and then boot from that image;
- Create a blank disk image on the internal storage and make that image accessible to the server; and
- Download an image from the internal storage.

Continued on page 6

Continued from page 5

One of the exercises I've performed involved obtaining administrative access to the server through documented features of the management controller (and a little password cracking). With only default credentials, I was able to obtain files containing encrypted passwords. I then cracked the encrypted passwords on a penetration testing system and was able to remotely sign in to the server's operating system with full administrative privileges.

Are out-of-band management capabilities inherently bad? Of course not. They can be very useful in managing a server at locations such as substations or control centers that do not have local IT staff to manage the IT-type systems. Use of out-of-band management capabilities can improve reliability by shortening downtime and by permitting monitoring of systems so preventive actions can be taken in a timely manner.

Compliance and Security Recommendations

Identification

The best approach I've seen in applying the CIP Standards is to identify the management controller as a Cyber Asset that is part of the hardware of the server. Since it is part of the server, it must be classified the same as the server. For example, if the server is part of a high impact BES Cyber System, then the management controller would be identified as part of the same BES Cyber System. The controller would be tracked in your documentation as a separate Cyber Asset, even though it is actually part of the server.

Whether you use this approach or devise an approach of your own, be sure to identify and document ALL of these management controllers. Audit teams are aware that these capabilities, if not protected, can present a high risk to reliability, and they are actively monitoring for any of these interfaces you might miss.

Networking

Most server vendors recommend connecting the management controller to a network that is separate from the other networks connected to the server, hence the "out-of-band" designation. For servers within an ESP, this separate network must also be within an ESP. Otherwise the management controller would be an EAP, a role it is not suited to adopt.

Access Control

You must control access to the management controller at least as tightly as you control access to the server itself. Interactive Remote Access to a management controller within an ESP must be through an Intermediate System.

Baselines, Patching, Etc.

The management controller should be subject to the same requirements as the server for baselines and change control, patch management, vulnerability assessment, ports and services, and password management.

Conclusion

Be sure to review all of your Cyber Assets within CIP scope and identify the out-of-band management capabilities of each. Document the presence of this capability on each applicable server, identify these devices in your Cyber Asset lists or baselines, and apply the appropriate CIP Standards to each. Be certain you have changed the default passwords.

Requests for Assistance

If you are an entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, can be reached here.