PSP Maintenance Laptop
Configuration and Operation

By
Matt Bordelon
matt.bordelon@cleco.com

Thanks to Phillip Miller for his help
So what’s a PSP Maintenance Laptop?

- Laptop used to perform maintenance on your cyber assets within your PSPs even those connected to your ESP
- Connected via the external maintenance port on your critical devices
- Configured so that the cyber attack surface is as small as possible
- Following your procedures, it can be transported from one PSP to another
- Costs for this setup are relatively low
  - An old redeployed laptop
  - Open-source operating system (LiveCD)
What’s the takeaway from this presentation?

• Learn how Cleco setup its PSP Maintenance Laptop.
  • What hardware adjustments you have to make
  • How to provide a read-only operating system
  • Limiting the connection capability
  • Show which operating system Cleco went with and how it’s used
  • Guidance on how to connect to a device using the laptop via a serial connection
Cleco’s PSP Maintenance Laptop
Hardware

• Started with a used laptop
  • Didn’t have to worry much about its capabilities (e.g. hard drive size, RAM, etc.)

• Removed the hard drive
  • Forces the unit to use an operating system other than the HD
    • Cleco uses a CD for the operating system (read-only)
    • Have one less place to store anything malicious

  • Your Bios boot sequence will try to boot off the Hard Drive first
    • You can alter the boot sequence to boot off of the CD first
    • Can Password protect the Bios (battery removal will reset though)

• Removed the wireless card
  • If you can’t, then you could disable it from the Bios screen
  • Reduces the number of external connections
Hardware – Removing HD and wireless card

Screws
Hardware – Removing HD and wireless card

Wireless Card

Hard Drive
Hardware – Removing HD and wireless card

- Hard Drive
- Wireless Card

Note the tape over connections
Software - Operating System

- Cleco used a Linux Live CD to boot off of
  - By using a CD-R nothing can write to it

- You can either leave the CD in the laptop or secure it somewhere

- Using System Rescue CD (www.sysresccd.org)
  - Based on Gentoo Linux
  - Download the iso image from the download page
  - Use an application to burn the image to the CD
  - Has the “minicom” serial communication application with it

- You can preconfigure the Live CD ahead of time before burning
  - User accounts
  - Password
  - Setting up minicom
  - Can remove wireless drivers (in case you still have the card installed)
  - Tutorials on-line (Google: personalize system rescue cd)
Procedure

- USB Serial cable
Procedure

- Device Serial connection
Procedure

- Stick the CD in the laptop and turn on machine
- Boot up on Linux Gentoo
- Disable the Ethernet port (if not disabled in the BIOS)
- Plug in the USB to serial adaptor
  - Operating System will automatically create a device, usb tty file in the /dev folder. (/dev folder is where the device files are located)
Procedure – (continued)

• Use the Minicom application to connect serially to device
  • Texted based modem control & terminal emulation program
  • Configure the Serial settings (Baud rate, stop bits, etc.)
  • Modem initialization warning:
    • Minicom sends out a modem initialization string which might cause unexpected actions on the connected device
    • Allow the initialization to complete before connecting the laptop to the management port
    • (could be disabled or removed when personalizing the LiveCD)
Procedure

- Will have to consider documentation of laptop usage in your security procedure.
- Document usage on a log sheet which stays with the laptop.
Procedure

• Cleco placed a sticker on the Laptop for awareness.
  • Prevents someone from mistakenly using the laptop
Considerations

• **What’s the future of serial communications**
  - Some firmware updates are so large now that doing it serially will be very difficult
  - Will devices continue offering serial communication ports due to the speed and throughput?
  - One alternative would be to use the Ethernet port
    • How about configuring the Ethernet port with a Time-To-Live (TTL) of 1?
      • You can plug into an Ethernet maintenance port and the packets can only go to the device connected. Packets would not be able to be routed to a different network.
      • You can potentially still connect to the local subnet though
    • Setting the management port to a different subnet to prevent routing
Questions?