University of Dubuque

2000 University Ave
Dubuque, IA 52001
563)589-3233
http://www.dbq.edu

Mesh Stalkings – Penetration Testing with Small Networked Devices

By Dr. Philip A. Polstra, Sr.

January 2013

Contents

Introduction

Penetration testing has become a mainstay of many penetration testers. At the same time many organizations have moved toward wireless networks. This paper will describe a penetration testing Linux distribution known as The Deck which runs on the ARM-based BeagleBoard-xM and BeagleBone devices. In particular, an extension to to The Deck that allows multiple devices running The Deck to be connected via 802.15.4 Xbee networks.

Problem Statement

Penetration testing without prolonged physical access can be challenging, especially when organizations are not making use of wireless networking. Even when wireless networks are employed prolonged presence near the target organization can arouse suspicion.

Previous Options

Several drop boxes are available for penetration testers. However, most of these devices require the user to either retrieve them or they must tunnel out of the target network in order to gain results from any hacking done by the devices. This dramatically increases the chances of detection and/or delays reporting of results to the penetration tester.

Penetration testing on wireless networks may be done for a distance by using high gain antennas and high powered wireless transmitters. This does require a prolonged presence in the vicinity of the target, however. Additionally, many wireless attacks are quicker and/or more successful when performed in close proximity of targeted clients and access points.

Proposed Solution

An open source penetration testing Linux distribution for the ARM-based BeagleBoard-xM and BeagleBone devices known as The Deck is presented. The Deck is a full-featured distribution suitable for penetration testing systems and drop boxes alike. Several extensions have been created for The Deck. This paper will focus on the Mesh Deck which allows multiple devices running The Deck to perform attacks which are coordinated using IEEE 802.15.4 networking.

Benefits of Proposed Solution

Low Cost

The BeagleBone which is ideal for drop boxes is available in Europe for €73. The BeagleBoard-xM which is used as the master device and/or control console is available for €133. This is considerably less than the cost for commercial drop boxes such as the Pwnie Plug series which sell for hundreds of Euros.

Improved Functionality

The solution presented here has more functionality than its expensive commercial counterparts. Each device running The Deck has a full-featured penetration testing Linux distribution. This allows much greater flexibility. Devices are easily reconfigured on the fly. Unlike some commercial alternatives, the same device can be used for wired and wireless penetration testing.

Greater Stealth

Because 802.15.4 networking is used for device control and reporting suspicious activity is not introduced into the target network. Drop boxes can run 24/7 (often off of battery power) which permits the penetration tester to be away from the premises for extended periods of time. 802.15.4 Xbee Pro adapters have ranges of up to 1.6 km. Some proprietary adapters from the same manufacture have ranges of up to 14 km. This allows more distance between the target and tester without a degradation in penetration testing performance.

Open Source Solution

Full source code is freely available. Redistribution and modification is permitted in accordance with the GNU GPLv3.

Implementation

Base Device

The BeagleBoard-xM and BeagleBone were selected as a platform to run The Deck. This selection was made because the BeagleBoard family of devices best met the criterion of being small, affordable, mature, low-power, inbuilt networking, and good USB support. The BeagleBoard-xM works well as either a control console or a drone. While the BeagleBone could be used as a command console it is better suited for use as a drone.

Base Operating System

One of the reasons for selecting the BeagleBoard family of devices was good support for Ubuntu. Many existing security-oriented Linux distributions, such as BackTrack, are based on Ubuntu. As a result, many of the common security tools are in repositories or are distributed as DEB packages. The choice of Ubuntu for a starting point greatly reduced the amount of porting of source code when creating The Deck. A tweaked versions of Ubuntu from Robert C. Nelson is used.

Building The Deck

The Beagles store the operating system on a microSD card. Typically the devices ship with a 2 or 4 GB card with Angstrom preinstalled. The Deck image is 6 GB, so at a minimum an 8 GB card is required. A 16 GB or larger card is recommended in order to allow sufficient working

space during a penetration test. Note that this version of The Deck has the Mesh Deck functionality preinstalled.

Here are the steps to load your microSD card:

1. Create a directory to work in on your Linux computer "mkdir thedeck".
2. Change to the directory "cd thedeck".
3. Download the archive to your Linux computer using "wget http://www.udcis.org/TheDeck/thedeck-v1.0.1-bheu13-ed.tar.gz".
4. Uncompress the archive with "tar xzvf thedeck*.tar.gz"
5. You need to determine the device for your microSD card. If you haven't already done so, insert your microSD card. You can use the setup script to figure out the right device using "sudo ./setup_sdcard.sh --probe-mmc". Make a note of the device letter.
6. Now you can load the card. If you are loading a card for a system with the ULCD7 the command is
"sudo ./setup_sdcard.sh --mmc /dev/sdX --uboot beagle_xm --addon ulcd" Where X is your drive letter (don't add any numbers!)
If you do not have the ULCD7 just leave off the last part and use "sudo ./setup_sdcard.sh --mmc /dev/sdX --uboot beagle_xm"
or if you are installing on a BeagleBone
"sudo ./setup_sdcard.sh --mmc /dev/sdX --uboot bone"
7. Go do something else for a while! Installing to a class 4 card takes about 1.5 hours. If you have a faster card it will take less time, maybe as little as 20 minutes for a class 10 card.

Now you are ready to boot up the system for the first time:

1. Install the microSD card into the BB-xm (or BBone).
2. Attach any peripherals before you power it up. This is especially important for any monitors.
3. Power it up.
4. It should boot. Note that the first boot may take a little longer than normal.
5. The "Demo User" with user name ubuntu has a password of "temppwd" which you will need to login.
6. Once you are logged in go exploring. You should have all the fun tools installed. You may wish to update your copy of Metasploit and possibly the OS itself.
7. At a terminal change to the Metasploit directory "cd msf". Then update your exploits "sudo ./msfupdate".
8. To update the OS "sudo apt-get update && sudo apt-get upgrade".

Create a Small Battery Power Supply (if desired)

The Beagles require 5 Volts at up to 2 Amperes of power. The device itself easily runs with less than 1 Ampere of current, but peripherals might require more current. The simple supply described here is not recommended for devices with attached touchscreens as they draw a considerable amount of power. The supply described uses 9V batteries, but any combination of batteries providing more than 5V should be suitable. You will need a 7805 power regulator, 2.1 x 5.5 mm barrel plug adapter, battery adapters, and a small capacitor to build this supply.

Put the 7805 flat on the table. The leftmost pin is the positive for your battery (6-14 volts), the middle pin is ground, and the right pin is +5V. If you are using 9V batteries attach the red wires to the left pin and the black wires to the middle pin. Attach the outer connector for your 2.1 by 5.5 mm barrel plug to the middle pin and the inner conductor to the right pin. Connect your optional capacitor to the middle and right pins. If you use an electrolytic capacitor be careful since they are polarized, so make sure the + side is connected to the right pin. For a heat sink most any small piece of metal will work. I used 3 pennies with a hole drilled in them bolted and soldered to the 7805 heat sink. There are variations on this supply. Note that the higher your voltage is over 5V the more heat (and waste) you will have. If your supply voltage is too high you might consider something better than the 7805. The biggest pluses for the 7805 is that it is cheap and small. As previously noted, do not use this supply with the touchscreen. The touchscreen uses a lot of power and you might start a fire. At a minimum you will burn through batteries pretty quickly.

802.15.4 Networking Adapters

An adapter is required to connect the 802.15.4 Xbee adapters to the Beagles. Adapters are available from several vendors and come in UART (serial) and USB varieties. For the BeagleBoard-xM a USB adapter is recommended because there are 4 USB ports available and the a level-shifter circuit would be required when using a UART adapter thanks to the use of a non-standard 1.8V logic level. A UART adapter is recommended for the BeagleBone because it has a single USB port which might be needed for something else such as a WiFi adapter.

Appropriate pins and modes for the BeagleBone can be found in the manual. For BeagleBone UART2 the pinouts are as follows:

- 3.3V & Ground P9 pin 3 & 1, respectively
- TX P9 pin 21 (to Xbee Din)
- RX P9 pin 22 (to Xbee Dout)

The BeagleBone multiplexer must be configured for the correct mode of operation using the following commands:

- “echo 1 > /sys/kernel/debug/omap_mux/spi0_d0”
- “echo 21 > /sys/kernel/debug/omap_mux/spi0_sclk”

Test connection by connecting terminal program to /dev/ttyO2 (not a zero).

Configuring Xbee Devices

Before they can be used each Xbee device must be configured by placing it in an adapter connected to a PC running either the Digi X-CTU or Moltosenso Network Manager IRON software. Here are the configuration steps:

- Place Xbee module in USB adapter and connect to PC running X-CTU or IRON
- Select correct USB port and set baud rate (default is 9600)
- From Modem Configuration tab select Read to get current configuration
- Ensure modem is XB24 and Function Set is XBEE 802.15.4
- Set the channel and PAN ID (1337?) noting the settings which must be the same for all modems
- Set the Destination Low and Destination High address for the drone adapters to whatever you have chosen to use for the console adapter (say 1, and 0), it doesn't matter what you set this to for the console adapter
- Set the My Address to a unique 16-bit value
- Click Write to stored the new config on the Xbee
- Repeat this process on the second Xbee but reverse the addresses
- The modules should now talk to each other just fine

Updates and Support

Updates and any fixes will be published on the author's blog at http://ppolstra.blogspot.com. You may contact the author via Twitter @ppolstra as well.

Summary

The devices described here permit some serious penetration testing to be performed at a low cost. They also allow penetration testers to execute effective attacks without the need for prolonged proximity to the target systems. Other add-on modules for The Deck are also in the works which should provide even greater possibilities.

About the Author

Phil cleaned out his savings at age 8 in order to buy a TI99-4A computer for the sum of $450. Two years later he learned 6502 assembly and has been hacking computers and electronics ever since.

Phil currently works as a professor at the University of Dubuque in Dubuque, Iowa. He teaches computer security and forensics. His current research focus involves use of microcontrollers and small embedded computers for forensics and pentesting. Prior to entering academia, Phil held several high level positions at well-known US companies. He holds a couple of the usual certs one might expect for someone in his position.

Phil is also an accomplished aviator with several thousand hours of flight time. He holds 12 ratings including instructor, commercial pilot, mechanic, inspector, and avionics tech. When not

working, he likes to spend time with his family, fly, hack electronics, and has been known to build airplanes.

Phil has a Baccalaureate degree in Physics/Math from Calvin College (the number one physics undergraduate institution in its class during Phil's tenure there), a Master's degree in low-temperature condensed matter physics from Purdue University (ABD PhD), and a PhD in business administration with a concentration in computer and information security from Northcentral University.

In addition to teaching his normal classes, Phil serves as an advisor to the University of Dubuque Computer and Technology Club. Under his leadership, the club has attended several information security conferences around the USA, constructed a 3-d printer (RepRap Mendel), built a number of computers, been introduced to the wonderful world of Linux and open source software, and has helped numerous people in the community through PC tuneup events. Phil has also developed some new and exciting classes at University of Dubuque including cyber-forensics, microcontrollers, and ethical hacking. Phil has also been instrumental in developing online training offerings at the university.
Phil is no stranger to conference presenting having spoken at BlackHat, DEFCON, 44Con, and several other conferences over the last few years. Phil is currently developing a new Digital Forensics program which is scheduled to launch Fall 2013 at University of Dubuque. A second new program in Ethical Hacking and Countermeasures is also in the works for a Fall 2014 launch.

Phil may be contacted via e-mail at ppolstra@gmail.com or ppolstra@dbq.edu. You can also follow him on Twitter at @ppolstra. His blog lives at http://ppolstra.blogspot.com.

About University of Dubuque

The University of Dubuque is a small, private university affiliated with the Presbyterian Church (U.S.A.) offering undergraduate, graduate, and theological seminary programs. The University is comprised of individuals from the region, the nation, and the world.

As a community, the University practices its Christian faith by educating students and pursuing excellence in scholarship. Therefore, the University of Dubuque is committed to:

- The Presbyterian tradition;
- Excellence in academic inquiry and professional preparation;
- Relationships which encourage intellectual, spiritual, and moral development;
- Community where diversity is appreciated and Christian love is practiced;
- Stewardship of all God's human and natural resources;
- Zeal for life-long learning and service.

References

1. General BeagleBoard xM/BeagleBone http://beagleboard.org
2. Installing Ubuntu on Beagles http://elinux.org/BeagleBoardUbuntu
3. Cross-compiling for Beagles by Jan Axelson http://www.lvr.com/eclipse1.htm
4. Instructions on how to build The Deck http://www.instructables.com/id/The-Deck-Portable-Penetration-Testing-and-Forens/
5. My blog where updates will be posted http://ppolstra.blogspot.com/2012/09/introducing-deck-complete-pentesting.html
6. Download link for The Deck (warning 6 GB) http://www.udcis.org/TheDeck/thedeck-v1.0.1-bheu13-ed.tar.gz
7. Getting Started with Xbee by Parallax http://www.parallax.com/portals/0/downloads/docs/prod/book/122-32450-XBeeTutorial-v1.0.1.pdf
8. General information on Xbee modules from the manufacturer http://digi.com
9. Download Moltosenso Network Manager IRON software http://www.moltosenso.com/#/pc==/client/fe/download.php