Open Access License Notice

Tempting High School Students into Cybersecurity with a Slice of Raspberry Pi

Sandra Gorka
Pennsylvania College of Technology
Williamsport, PA, USA
sgorka@pct.edu;
cyber.pct@gmail.com

Alicia McNett
Pennsylvania College of Technology
Williamsport, PA, USA
amcnett@pct.edu

Jacob R. Miller
Pennsylvania College of Technology
Williamsport, PA, USA
jmiller3@pct.edu

Bradley M. Webb
Pennsylvania College of Technology
Williamsport, PA, USA
bwebb@pct.edu

***Abstract*—Improving the Pipeline is an NSF grant project [1] to extend the Information Assurance and Cybersecurity pipeline into the high school environment by offering an after-school for college credit course to students. This paper discusses the use of an isolated and portable Raspberry Pi network within the course.**

Keywords—computing education, cybersecurity education, K-12 education

I. Introduction

The Raspberry Pi computer has been used within computing to facilitate education in topics such as introductory computer science (CS0), parallel computing, computer security and cluster computing [2-6]. The Raspberry Pi has also been used to teach computing in secondary education [1]. One of the main attractions of the Pi is its low cost. While somewhat limited in speed compared to a more traditional desktop computer, it is generally still sufficient to illustrate the functionality and capabilities necessary to conduct an experiment or teach a particular concept. Where additional processing speed is necessary, the low cost of the Pi platform allows for integrating multiple units to perform a given task. This makes the Pi, or a Pi network, an attractive teaching and proof-of-concept platform. In this paper, we discuss the use of a collection of Raspberry Pis networked together in a "briefcase" providing for a portable and isolated network-in-a-box (NIB). Our NIB was used to create an isolated cybersecurity-lab-in-a-box (CLIB).

II. The Network in a Box

The original NIB, a former student's senior project, had the Pis mounted directly to the case of the box. This gave the entire system a very low profile. However, we envisioned instances where it may be necessary for students to remove and manipulate individual boards and then replace them into the case. As a result, our CLIB mounts the Raspberry Pi units on a rail system installed in the case. See Figure 1.

The Pis are held in place using 3D-printed clips that allow them to be readily removed and reinstalled while holding them securely when mounted. See Figure 2. The Pis are powered by a central USB power hub and networked together via an 8-port switch. With the Pis mounted on the elevated rails, the power supply and switch are mounted under the rails in the bottom of the case. This allows for up to six Pis to be mounted comfortably in the box. Although the operating systems on the Pis can vary, our implementation uses three Linux distributions: Kali Linux [7], Raspian [8] and RaspOwn [9] (a vulnerable Linux distribution for the Pi).

Fig. 1. Photo showing the completed CLIB. The case is an inexpensive aluminum "briefcase" with a foam lining adhered to the inside. Rails are mounted to plywood blocks glued to the inside of the case. Pis are mounted in clips to the tops of the rails. The switch and USB power supply are mounted to the bottom of the rails using screws and zip-ties. This leaves a small amount of space beneath the switch and power supply for network cables, power cords, the switch power supply and the power cord for the USB hub. There is also space for a portable monitor and keyboard (not shown) if desired.

In order to use the lab, it is necessary to connect a monitor and keyboard to at least one of the Pis. Our original vision incorporated an HDMI portable monitor and a small Bluetooth keyboard. This would allow everything to be packed in the box for portability. While these worked, they were not as comfortable to use as simply plugging in a more traditional monitor and keyboard. In addition, our Information Technology Services group has a store of unused monitors and keyboards. It made sense to use the "free" monitors and keyboards rather than purchase additional equipment.

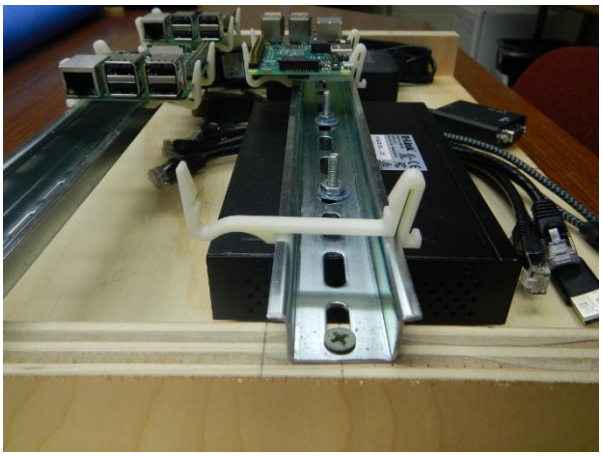

Fig. 2. Photo showing the prototype as well as the clips used to mount the Pis to the rails. The rails are commonly used to mount electrical devices such as controllers and relays to a backer board. A search on the Internet yields several sources for clips and holders that will mount Raspberry Pis to these and similar rails. The clips we chose were selected due to their minimal materials cost and ability to remain clear of all the Pi's ports and connectors. They also lent readily to unmounting and remounting the Pis.

III. Activities using the CLIB

This section provides an overview of several of Raspberry Pi activities completed by the students. Readers interested in the full details of the activities can request them from the authors.

A. Connecting the CLIB

The first activity using the CLIB was targeted more at creating a network. Student were grouped in teams of 2 – 3 students and given a CLIB box, keyboard, mouse and monitor. The CLIB box contained all of the components of the CLIB and the necessary cables, but none of the cables were connected. Students were required to connect the Pis to both the USB power hub and the switch. Students were also required to connect the monitor, keyboard and mouse to a Raspberry Pi designated as the primary Pi. Students could then power the CLIB to determine if the primary Pi was properly connected to the keyboard, mouse and monitor. Students then tested the network functionality of the CLIB using the next activity.

B. Network Addressing

The starting point of this activity typically follows the previous activity. However, this activity can be completed after giving the students a CLIB with all of the cables properly connected.

This activity was completed after a class discussion on MAC and IP addresses, subnet masks and default gateways. Students experimented with several Linux commands as follows:

- `ifconfig` to determine the MAC and IP addresses of the primary Pi.
- `route` to determine the default gateway.
- `ping` to determine whether or not an IP addresses was in use.
- `arp` to see the IP address to MAC address mapping in the ARP lookup table.

C. Networks and Programming

In this activity students used the CLIB to code two Python scripts. Students were previously introduced to Python programming and this provided an opportunity to combine networking and programming concepts in a pair of activities.

The first script was a Python script that performed a ping sweep of IP addresses. The script pinged a total of ten IP addresses, some of which were not connected to a Pi and some of which were connected to a Pi. Students were given the code to implement and were asked questions about what the script accomplished. They were also asked questions about what the output tells them about the network and the computers on the network.

The second script was also a Python script that determined the MD5Sum of a file. Students were previously exposed to the concept of hashing and how it could be used to verify the integrity of a file. The student executed the program with a file to determine its MD5Sum. The file was then modified and the program executed again. To determine its new MD5Sum. Students were asked to address how such a program can be used to identify when a file has been modified. It should be noted that at this activity does not make use of the networked aspect of the CLIB as the activity was restricted to a single Pi.

D. Future Activity – Using nmap

This activity is currently accomplished using virtual machines (VMs). We had planned on using the CLIB, however extenuating circumstances such as inclement weather and COVID-19 prevented the use of the CLIB for this activity.

In the VM version of this activity, students use a Kali Linux VM to execute a nmap scan another Linux VM. In the CLIB version, students will use the Raspberry Pi with Kali installation to execute a nmap scan on the Pi with the RaspOwn installation. After the scan is complete, the students would review the output to determine the name of the computer scanned, its IP address, its operating system, which ports are open and what services are associated with the ports.

IV. Benefits

One of the primary benefits of the CLIB is its isolated environment. This is important as students just beginning study in cybersecurity can be both intimidated and careless. Students may be reluctant to experiment for fear of breaking things. Other students are often anxious to "just get started" and don't always follow the complete instructions when setting up an experiment. Of course, on an open network, this can be disastrous. With the CLIB being a self-contained environment, students can experiment without worrying about anything getting "loose" and wreaking havoc. For the

most part, if anything does cause a catastrophic failure (e.g. launching a DoS attack or fork bomb) you simply reboot the affected systems and all is as it was.

The CLIB can be quickly reconfigured to use different OSs simply by replacing the SD card in each Pi. This can prove beneficial if a student unintentionally damages an installation - a fresh SD card can be inserted into the Pi and have it back to "normal" in minutes. We made several copies of each SD card for this reason. During teaching/lab sessions when something went wrong, it was simple to start over with a fresh card and diagnose the problem later. Additionally, OSs can be configured to create a particular scenario and then easily replaced for a subsequent activity. While not a focus in this course, scenarios for diagnosing configuration and network problems can be easily built and swapped out for lab or testing purposes.

In addition to using the CLIB for cybersecurity coursework, it can be used for projects/lessons within many other areas of IT. One of the labs we conducted had the students build the network and demonstrate its functionality. This was a precursor to demonstrating networking scanning and reconnaissance techniques. We divided the class into groups of two or three students. We supplied each group with the CLIB components and instructions on how to configure the various OS installations. They assembled the hardware, configured the network and then demonstrated the functionality by writing a small application to exchange data among the various computers in the network. After verifying the networks operated correctly, we began looking at tools for scanning and reconnaissance.

The other main benefit of the CLIB is the cost. The college supports an isolated security lab for our cybersecurity classes. This lab is significantly more sophisticated than a box full of Raspberry Pis, but the cost is also significantly higher. The security lab is capable of supporting several hundred simultaneous VMs and virtual networks; however, the price tag ran in the tens of thousands of dollars for that functionality. By contrast, the CLIB, sans monitor, keyboard and mouse, can be built for about $230 (2017 prices). It will not support hundreds of VMs, but that functionality is not necessary. In addition, the students responded very positively to the "visceral" knowledge they acquired by being able to see and touch the machines they were working with. It was much more engaging than an icon of a VM on a screen.

Another benefit of the low cost is that high schools could fund one of these CLIBs to use in teaching a similar security class. In addition, they can get extra mileage out of the expenditure through using it to support networking and programming classes as well. It would be helpful in any instance where having access and control over the server and/or network along with the client is desirable. Moreover, the cost is such that even individual students could afford to construct a NIB/CLIB for about the price of a cheap laptop.

Another significant benefit of the CLIB stems from its portability and low cost. One difficulty of our on-campus security lab is access control. In order for the students to do assignments in the lab, they would have to be physically on campus. While we did use the lab for on-campus events [10], most students would not have been able to access the lab in general. One intended mission of the CLIB was to accompany the students back to the high school where they could use it during the school week when not on the college campus. While there were concerns that the CLIBs could be damaged or compromised, again the overall feeling was that financially, there was very little at risk. Additionally, this would be less risky and preferable to trying to manage off-campus access to our isolated security lab.

While taking the CLIB to the high school was an intended part of the project, feedback from the students raised two issues. None of them felt there would be time enough in their regular school days for them to use the CLIB at the high school. Most, if not all, of the students who participated were very active in extra-curricular activities, so things like study halls were simply not available in their schedules. Additionally, the students felt they would get more mileage out of the CLIBs in the classroom and by coming to campus. Several students arranged their after-school schedules in order to come to campus early to do work with the CLIBs. As a result, the CLIBs were never deployed to the high schools but were utilized to support in-class lab activities.

V. Results

Prior to the exercise outlined above, several students in the class had never built a physically connected network before. Many had never installed and configured servers before. Most had attached wireless devices on home networks, but had never really taken the time to understand the subtleties of network addressing, subnetting and the like. Moreover, other than creating access passwords, they had never considered the exposure of their data while in transit over the network. Assembling the network, configuring the services, scanning the servers and later monitoring the traffic gave them all an appreciation (wakeup call!) of what happens to their data and the sometimes difficult task of protecting it.

In spring 2019, sixteen students completed the activity and 14 of them indicated that the activities were interesting. Several commented during the exercise that they had never done anything like this before and found it very enlightening. Some of the more experienced students, having helped assemble physical networks before, found the build part of the exercise only "kind of" interesting. Generally, all the students felt the exercise was worthwhile and were very engaged with the subsequent cybersecurity parts of the labs.

Visual observation indicated that several students were initially timid about physically interacting with the hardware. We encouraged more experienced students to work with inexperienced students. While the instructors were encouraging with everyone, getting encouragement from their peers vastly helped some students overcome their fears. Once engaged, the students enjoyed the activity and appeared to be confident about dealing with the hardware.

While these results may seem limited and relatively unsurprising, the value of the confidence gained by some of

the students was immeasurable. Students who just an hour earlier were leery of even opening the briefcase, were now willing to assemble a network, jump into configuring and troubleshooting network services, and monitoring the network and servers for illicit behavior. While all of these activities had been discussed in class over the prior few weeks, nothing brought the concepts home like these little networks.

In addition, many students expressed that they had a much better feel for what was going on with their data. Security concerns over things like cloud storage, smart home appliances, online banking, and having their entire life on their phone suddenly seemed to snap into a sharper focus now that they had experienced managing a network first-hand. Based on their comments, it seems unlikely they would have received the same experience from virtual networks in our security lab.

VI. Student Feedback

At the end of the experiment, we asked the students to provide feedback on the Raspberry Pi activities. In particular, we asked them what they learned and for any general comments they had on the exercises.

Feedback was generally positive in nature. Students indicated that they enjoyed the activity and that it was a fun way to learn about the Raspberry Pi. Informally, when we asked if we should continue with the Pi labs, the response was a resounding yes. Several students offered advice that we should try to incorporate them more.

VII. Postmortem

For every up there is a down. When we first planned the incorporation of the CLIBs into our class, they seemed very necessary. Several of the activities we had planned could not be carried out safely on an open network; some still cannot. However, during the two years between the time we wrote the proposal and began the work, virtualization got better, new resources became available and a lot of material was published to do many of the planned activities on-line in a safe manner. While we cannot do everything on-line, many of our planned activities became a lot easier to do via various websites targeting cybersecurity training. Other activities became much more doable via VMs than they had before. This was mostly a function of better performance in the VM software making VMs a lot less cumbersome and a lot more responsive.

We believe the CLIB still represents a valuable asset. No amount of VM magic will replace the learning that happens when students can see, touch and manipulate the physical objects. The thrill a student gets when he or she powers up a complex collection of devices and sees it function is immeasurable. But do you need a CLIB? We think it depends. If you can securely configure a virtual network so that nothing hostile being played with by a novice can ever escape, then there are some consultants that would like to hire you. There is no way to make every activity that you might want to do in cybersecurity training and research absolutely safe. The CLIB gives you adequate protection at a very low price.

But whether or not you need a CLIB for safety is somewhat peripheral to the point of the activity. If you want to engage, inspire and retain students, then we think the CLIB performs in a way that VMs just cannot do. For the cost, we can think of no better way to give students the sense of learning and accomplishment that these boxes accomplished.

It seems that Raspberry Pi is excellent bait.

Acknowledgments

This material is based on work supported by the National Science Foundation under Grant No. 1623525. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

The authors would also like to acknowledge and thank Sebastian Peipher for the inspiration of his network in a box project and his advice as we began creating ours.

References

[1] Improving the Pipeline: After-School Program for Preparing Information Assurance and Cyber Defense Professionals. In *Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17)*. ACM, New York, NY, USA, 167–167. https://doi.org/10.1145/3125659.3125665

[2] Francesco Cuomo, Eric Mibuari, Komminist Weldemariam, and Osamuyimen Stewart. 2013. Leveraging Raspberry Pi for Interactive Education. In *Proceedings of the 4th Annual Symposium on Computing for Development (ACM DEV-4 '13)*. ACM, New York, NY, USA, Article 16, 2 pages. https://doi.org/10.1145/2537052.2537068

[3] Kevin Doucet and Jian Zhang. 2019. The Creation of a Low-cost Raspberry Pi Cluster for Teaching. In *Proceedings of the Western Canadian Conference on Computing Education (WCCCE '19)*. ACM, New York, NY, USA, Article 7, 5 pages. https://doi.org/10.1145/3314994.3325088

[4] Brian Krupp and Andrew Watkins. 2019. CS0: Introducing Computing with Raspberry Pis. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19)*. ACM, New York, NY, USA, 832–838. https://doi.org/10.1145/3287324.3287488

[5] Suzanne J. Matthews, Joel C. Adams, Richard A. Brown, and Elizabeth Shoop. 2018. Portable Parallel Computing with the Raspberry Pi. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. ACM, New York, NY, USA, 92–97. https://doi.org/10.1145/3159450.3159558

[6] Adam H. Villa. 2016. Hands-on Computer Security with a Raspberry Pi. *J. Comput. Sci. Coll*. 31, 6 (June 2016), 4–10. http://dl.acm.org/citation.cfm?id=2904446.2904447

[7] Kali 2019. Kali Linux - Raspberry Pi. Retrieved June 12, 2019 from https://docs.kali.org/kali-on-arm/install-kali-linux-arm-raspberry-pi

[8] RASP [n. d.]. Raspberry Pi Downloads. Retrieved June 12, 2019 from https://www.raspberrypi.org/downloads/

[9] RasPwn 2016. RasPwn OS. Retrieved June 12, 2019 from http://raspwn.org/

[10] Allison Chapman and Margot Rinehart. 2019. Capture the Flag as a Testing Platform. Online. Retrieved June 16, 2019 from http://ccscne.org/wp-content/uploads/2018/09/StudentPostersDocument-2019-Final.pdf CCSCNE 2019, Student Poster Abstracts, April 12 - 13, 2019, West Haven, Connecticut, 37.