BUILDING A CYBERSECURITY LAB WITH LEGACY EQUIPMENT

Magdy Ellabidy, Chen-Hsiang Yu, Mira Yun

Department of Computer Science and Networking, Wentworth Institute of Technology (UNITED STATES)

Abstract

According to the Electronics TakeBack Coalition report in 2013, we not only generate more electrical or electronic waste, but we also recycle more in recent years. Recycling legacy electronic equipment is a long-term effort. On the other hand, experiential learning in cybersecurity is crucial to enhance the learning experience for computer science and networking undergraduates. However, limited budgets to support teaching in cybersecurity and outdated configurations of legacy equipment have been challenging institutions. In order to address above issues, we developed a cybersecurity lab, *CyberLab*, that uses legacy hardware and open source software to provide an experimental environment for undergraduates. The infrastructure of the environment includes a Virtual Private Network (VPN) server and a gateway to access the network that is composed of multiple virtualized machines and legacy routers and switches. We are currently designing a series of courses in cybersecurity topics on this proposed infrastructure.

Keywords: Legacy Equipment, Cybersecurity Lab, Open Source.

1 INTRODUCTION

The advance in technology makes existing electronic equipment outdated. Although a lot of equipment can still be used, to save the hassle, most of them are thrown away without reusing them. According to the Electronics TakeBack Coalition report in 2013, we not only generate more e-waste, but we also recycle more in recent years [1]. However, recycling legacy equipment is a long-term effort.

Cybersecurity has become an important topic in recent years, either in industry or in the academia. As President Obama put it at the Cybersecurity and Consumer Protection Summit, "... cyber threats are a challenge to our national security. Much of our critical infrastructure -- our financial systems, our power grid, health systems -- run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before.." [2]. There are many ways to enhance cybersecurity and one of them is by education.

In terms of education at the university level, both of security methodologies and experiential learning are crucial. However, limited funds to support teaching in cybersecurity has become a challenge for institutions. With limited funds, we propose to develop a cybersecurity lab, calling it *CyberLab*, by using legacy hardware and open source software, and expect the students to learn cybersecurity principles and hands on the equipment to verify learned knowledge.

We define legacy equipment as the machines that can be repurposed in educational setting.. Our proposed architecture is generic, but the implementation can be customized to fit different institutions. In our case, since our Technology Service department was retiring servers, we took them to repurpose for *CyberLab*. In the design, we decided to use the servers as containers for student's virtual machines. To use legacy equipment in school settings, there are many challenges, such as old configuration settings in the equipment, complex procedure for system recovery, scalability of the architecture, etc.

In this paper, we present our proposed architecture and report lessons learned from this experience. Our architecture uses PFSense, an open source firewall/router, as a Virtual Private Network (VPN) server and a gateway for accessing the network which is consisted of multiple virtual machines, routers and switches. All of them are legacy equipment. In the following, we briefly introduce the related work in this field and summarize our work from design to implementation. At the end, we end up with discussion and future work.

ISBN: 978-84-617-5895-1

2 RELATED WORK

While networking technologies are constantly developed and deployed in different emerging applications, such as ubiquitous wireless communications, embedded systems and machine learning, the level of heterogeneity of networks increases. Since current network technologies have their own unique characteristics and capabilities, both of interconnectivity and security in heterogeneous environments are considered to be crucial [3]. Furthermore, cyber threats and hazards make current Internet connected devices and infrastructure vulnerable to a wide range of risk [2]. Despite the growing demand for cybersecurity professionals in this heterogeneous environments, relatively few schools offer degree programs that incorporate hands-on training in cybersecurity topics.

Hands-on learning has been proved to be a successful approach to increase students' motivation [4] and collaboration [5] and help students achieve high-level learning goals [6]. Because cybersecurity has a much broader scope than many traditional courses, it is very important to provide hands-on opportunities throughout a setup environment for the students to apply and experiment what they have learned in class. Dealing with realistic and complex problems, students can develop skills, including integrating theory and practice, applying knowledge to develop a feasible solution, and conducting research, etc. [7]

3 CYBERLAB

In this section, we want to introduce the proposed system architecture for cybersecurity education and share one example implementation of this architecture. The goal of the design focuses on creating a generic framework with legacy equipment that allows the students to practice security principles and methodologies via security tools (e.g. Kali Linux), as well as hardware configuration options.

3.1 Design Requirements

Legacy equipment have many limitations, including hardware, software and network configurations. Beyond the specific details of the equipment, the architecture should provide following capabilities:

- Remote Accessibility: accessible to all students at all times
- Modularization: able to partition network into isolated networks for individual and team exercises
- Secure Connection: accessible only to authorized users, including remote users
- Isolated Network: isolate all subnetwork traffic to prevent leaks between networks
- Multiple Users: allow multiple users to access the network at the same time

3.2 System Architecture and Configurations

In addition to above design requirement, the system architecture should have a robust firewall and allows students to access the network through a VPN connection remotely. When the students login to the system (via Terminals), they will access their network of virtual machines. Typically, they will only have one or two virtual machines. All virtual machines are stored in Server_1 or Server_2 as illustrated in Fig. 1. A virtual machine is a software simulation of an operating system (OS), such as Ubuntu, CentOS, Kali, Windows, etc. The students are supposed to use their own machine to connect to the system.

3.2.1 Hardware

Based on Fig. 1 System Architecture, we start to apply legacy equipment to fill up the blocks. To demonstrate that the system architecture works in education settings, we use the legacy equipment from different places to build up a cybersecurity lab as shown in Table 1. The legacy equipment come from Technology Service department, faculty donations, external donations, etc.

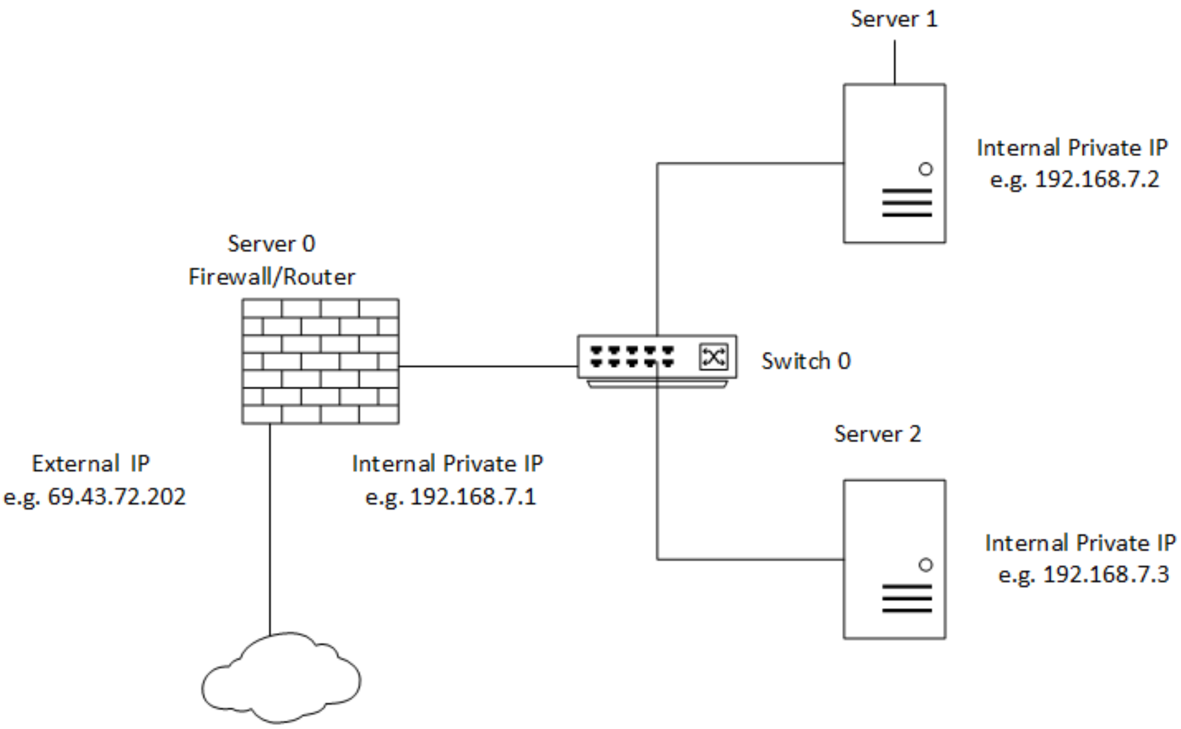

Figure 1: System Architecture.

3.2.2 Network Configurations

Budget constraint is the main issue in the design. Therefore, we decided to use open source or free proprietary software for our network implementation.

First, we installed PFSense on Server_0. PFSense is an open source firewall/router software based on FreeBSD. In the testing, we found that it can be installed on many legacy hardware. A Pentium grade processor is more than enough to have a robust system. PFSense is well known for its reliability and offers many features that are often only found in very expensive commercial firewalls. PFSense is commonly deployed as a perimeter firewall, router, and as a VPN server.

All management operations can be performed from PFSense web-interface. We opted to use it as our Firewall, Router and VPN concentrator. We use OpenVPN and every student is given a VPN account to access the network.

Second, to provide network separation, we use Cisco Catalyst 3550 Layer 3 switch to represent Switch in Figure 1. The switch provides 24 ports to expand the network and we use it to create multiple Virtual Local Area Networks (VLANs) to isolate the students' virtual networks and machines. Currently, we also have other equipment for future expansion, including (1) Cisco 3550 24 port switch; (2) 10 Cisco 2950 layer 2 switches; and (3) 6 Cisco 2600 routers.

As mentioned in the hardware section, the CyberLab currently uses two Dell PowerEdge R620 servers (Server_1 and Server_2). To better use these hardware, we installed VMware ESXi (version 6 servers) software on both servers. ESXi is a free server virtualization software from VMware. With 2TB of hard drive, each server gives us an opportunity create multiple virtual machines and subnets. Since it is installed on the server hardware, all students can easily copy an image (of a server) on a local machine as a backup or deploy a new machine as needed. Multiple Linux and Windows images are also deployed for the students. To facilitate two-way communication via the Internet, each virtual machine is assigned a unique IP address from 24 Internal subnets. If there is a need for class projects, the students can also request to be assigned a block of IP addresses.

Table 1: The list of hardware that are used to implement *CyberLab*.

Devices	Specification	Functions
Server 0	● Model: Dell ● CPU: Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz 2 CPUs ● RAM: 4 Gigabytes ● Hard Drive: WD 1 TB	Firewall Router VPN PFSense
Server 1	● Model: Dell PowerEdge R620 ● CPU: Intel(R) Xeon(R) CPU E5-26400 @ 2.50GHz 12 CPUs Processors 24 ● RAM: ECC 64 GB ● Hard Drive: 128 GB ● Others: 1 Rack Unit (RU)	Virtual Machine container: ESXi version 6. Holds a set of Windows 8, 8.1, 10, Windows server 2012, Kali Linux, Ubuntu, CentOS
Server 2	● Model: Dell PowerEdge R620 ● CPU: Intel(R) Xeon(R) CPU E5530 @ 2.40GHz 8 CPUs Processors 16 ● RAM: ECC 48 GB ● Hard Drive: 885 GB ● Others: 1 Rack Unit (RU)	Virtual Machine container: ESXi version 6. Holds student virtual machines images Windows 8, 8.1, 10, Windows server 2012, Kali Linux, Ubuntu, CentOS
Switch	● Model: Cisco Catalyst 3550 Layer 3 Switch ● 24 10/100 ports ● 2 Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports; ● Others: 1 Rack Unit (RU)	Multi- Layer Network switch

4 DISCUSSION AND FUTURE WORK

In this paper, we propose a generic system architecture for Cybersecurity education and realize it with legacy equipment from different donors. Although *CyberLab* is promising for Cybersecurity education, it has a few limitations. For example, although all legacy equipment were contributed by different donors, including Technology Service department, faculty and external organizations, the hardware capabilities (2 GHz * 2 CPUs or 2.5 GHz * 12 CPUs) might still be more powerful than regular old machines. In addition, configuration process needs a lot of manual setup and there is an overhead for software preparation. However, all of these can also be considered as a good opportunity for students because it is a real Cybersecurity setup in practice.

Based on the built *CyberLab*, we plan to offer a few cybersecurity courses, including Network Security, Computer Security, Wireless Security, Mobile App Development, Security Principle, etc. The syllabi are under development, but it is promising to use it based on the initial testing.

In the future, there are a few directions to move on. First, since Wi-Fi is pervasive, more and more security issues happen between user computers and Wi-Fi Access Points (AP). In the *CyberLab*, we will add a few Wi-Fi APs for students to practice on deciphering packet transmission to increase their awareness of the vulnerabilities in networking. In addition, Bluetooth (Classic Bluetooth and Bluetooth Low Energy) devices will also be included into the system.

According to comScore, there are 197.4 million people in the U.S. owned smartphone (79.3% market penetration) by the end of 2015 [8] and the replacement cycle is about 21.6 months [9]. Although the software might be outdated, most of replaced smartphones still work well with Internet connection and web browsing. For the *CyberLab*, these outdated smartphones are good to be a user client for verifying sending and receiving network packets such as Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP) and Internet Protocol (IP). Furthermore, students can use them to simulate VPN connections that are common in some countries.

REFERENCES

[1] Facts and Figures on E-Waste and Recycling http://www.electronicstakeback.com/wp-content/uploads/Facts_and_Figures_on_EWaste_and_Recycling.pdf

[2] Remarks by the President at the Cybersecurity and Consumer Protection Summit https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

[3] A. Ray, J. Åkerberg, M. Björkman and M. Gidlund, "Towards security assurance for heterogeneous industrial networks," Industrial Electronics Society, IECON 2015 - 41st Annual Conference of the IEEE, Yokohama, 2015, pp. 004488-004493

[4] Eunja Hyun; Hyunmin Yoon; Sooryun Son, "Relationships between user experiences and children's perceptions of the education robot," Human-Robot Interaction (HRI), 2010 5th ACM/IEEE International Conference on , vol., no., pp.199,200, 2-5 March 2010.

[5] D. Ausubel, J. Novak, and H. Hanesian, Educational Psychology: A Cognitive View, 2nd Ed, New York: Holt, Renehart, and Winston, 1978.

[6] Macías, J.A., "Enhancing Project-Based Learning in Software Engineering Lab Teaching Through an E-Portfolio Approach," Education, IEEE Transactions on , vol.55, no.4, pp.502,507, Nov. 2012.

[7] J. R. Savery, “Overview of Problem-based Learning: Definitions and Distinctions”, Interdisciplinary Journal of Problem-based Learning, vol. 1, no. 1, pp.9-20, 2006.

[8] comScore Reports December 2015 U.S. Smartphone Subscriber Market Share http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-December-2015-US-Smartphone-Subscriber-Market-Share?

[9] Kantar Worldparnel ComTech. “Smartphones: The time of double-digit growth is over. Deal with it!”, 2016. http://us.kantar.com/media/1214139/2016-18-feb-kantar_smartphones-wp-1735__2_.pdf