2016

Hackerville: A laboratory environment for security literacy

John Gerrit Van Roekel
Iowa State University

Hackerville: A laboratory environment for security literacy

by

John Gerrit Van Roekel

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Doug Jacobson, Major Professor
Thomas Daniels
James Davis

Iowa State University

Ames, Iowa

2016

TABLE OF CONTENTS

LIST OF TABLES

Page

ACKNOWLEDGMENTS

I would like to thank my committee chair, Dr. Doug Jacobson, and my committee members, Dr. Thomas Daniels, and Dr. James Davis, for their guidance and support throughout the course of this research.

In addition, I would like to thank my wife, Stephanie, my daughters, Holland and Heide, my parents Bill and Jan, and the rest of my family for their love and support throughout the entire program. I would also like to thank my mentor, Mark Nelson, for his support and encouragement, as well as my other friends and coworkers who have been with me on this journey.

CHAPTER 1

INTRODUCTION

1.1 Introduction

As middle and high school students become more entrenched in the digital world, the need to learn how to remain safe online has only increased. According to a Pew Research Center study, 92% of teens go online daily, and 24% of teens are online "almost constantly." (Lenhart, 2016) With so many students being so connected in today's world, it's not enough anymore to tell students to not download suspicious email attachments and have long, strong passwords. Much like financial literacy, students need to learn how to think about cyber security, instead of being handed a list of rules to follow to be safe online. Exploits are constantly evolving, and students must be able to adapt. The earlier we instill security literacy and good practices around safe, secure, online usage, the less it will have to be taught later in life, and the more it will be a natural part of how they think about what it means to be online.

Criminals who use the internet as an attack vector do not have to worry about who their targets are, where they are located, or what they do for a living. With pervasive technologies like email and Facebook, an attacker can send out a large scale attack, targeting thousands or millions of people at a time, with no regard for who their victims are. As such, it is vital for everyone who uses these types of technologies to be prepared for attacks, and be leery of anything that may be suspicious. To do that, they need to have an idea of what suspicious activity looks like, as well as an understanding of why it

is suspicious. Without the knowledge of many different attack vectors criminals may take, as well as a good understanding of how to respond, users will become victims to cyber-attacks, and risk compromising their accounts, their safety, and their employers' sensitive data.

1.2 The Problem

When training students in most fields of study, from chemistry to home-economics to financial education, there is usually a practical component, where students can try out the techniques they are learning. When students can see how their theoretical learning plays out in real life experiments, they are much more able to understand the impacts it can have on their life. If a student learns how to balance a checkbook, but then never tries it they will have a much harder time figuring out how to do it later in life. Likewise, a program trains students in computer security literacy, without a laboratory component where they can see for themselves how some of the techniques work, they will have a much more difficult time spotting potential threats when they get into the real world. Current computer security training for middle and high school students ranges widely, from very basic online safety tips, to in-depth training aimed at students looking to get into the security field. While some of these are good starting points, the only ones that have any hands-on training, are aimed at students who are interested in getting into computer security as a potential field of study. None have labs aimed at all students, to get a good handle on security concepts, as it will relate to them in their everyday lives.

1.3 Proposed Solution

Security-literacy.org has designed a course for middle school and high school students to start seeing the need for security in their everyday interactions online. This course describes security concepts in a way that all students will be able to relate to, not just students who have an interest in computers and computer security. It also teaches about some common security issues, teaches the students how to spot suspicious activity, and begins training students to adapt to the ever emerging threats, by teaching them how to think about security, not just the behaviors they should have.

The proposed project, Hackerville, is a lab that is intended to complement the Security Literacy course. By adding a lab component, students can begin to see the type of activity the course talks about. Hackerville will begin with a framework designed with expansion in mind. In this framework, modules will be housed, which will correspond to each section in the course. These modules would give real world scenarios to help students explore security concepts, such as visiting a malicious site, downloading malware, and receiving phishing emails, while being in a safe environment, and being sure that nothing they do will harm their computer or compromise their data. Students can also learn about creating good, strong passwords, the dangers of reusing passwords, how to watch for malicious transactions in their bank account, and being mindful about posting appropriate content on their social media sites. Each module would tackle a different scenario: Banking, Social Media, Malware, websites with security holes like expired certificates, etc., and the framework will have a central hub where the instructor will have access to each scenario, as well as the students' login information, so that they

can monitor student interactions and determine which modules they will use and when they will use them.

1.4 Importance of this Solution

Just like financial literacy, we need to be training students about digital security earlier, so that when they get older they will have a better understanding of what they need to do to keep safe online. If we wait until these students enter the workforce, they will already be behind and have trouble catching up. Programs in the workplace designed to train workers about security could be greatly enhanced by beginning the training at a much earlier age. When students have a good foundation of understanding security, they will have an easier time spotting security concerns in the future.

The Security Literacy course is a needed enhancement to computer security training for middle and high school students. It teaches students about security concerns, what to be aware of, and how to spot new and emerging threats. The companion lab, Hackerville, can enhance the Security Literacy course with hands-on demonstrations of the security concepts it teaches, and this will only increase students' awareness and understanding of these important security concepts.

1.5 Why Literacy Instead of Awareness

The department of Homeland Security sponsors National Cyber Security Awareness Month (NCSAM) every October. They explain that the purpose of NCSAM is, "to engage and educate public and private sector partners through events and initiatives to raise awareness about cybersecurity, provide them with tools and resources

needed to stay safe online, and increase the resiliency of the Nation in the event of a cyber incident." (U.S. Department of Homeland Security, 2016) Awareness is a good start, but it is not enough to merely have knowledge of the issue of computer security, nor is it enough to have a good top 10 list of security tips to follow. To be truly effective, there must be an ability to apply what is learned, and to adapt what has been learned to new situations. In the ever changing world of cyber-attacks, a user must have the ability to adapt what they have learned, and always be on the lookout for new and emerging potential threats.

CHAPTER 2

PRIOR RESEARCH AND CURRENT TOOLS

2.1 Prior Research

Training for computer security has long existed in a professional setting, teaching employees to keep company information secure. While this is necessary, if the training started earlier in life, much like computer use in general, it would be second nature, and people would be much more mindful of the need for security in all digital interactions. But only having knowledge of security is not enough. In "Bloom's Taxonomy for Information Security Education," van Niekerk and von Solms make this distinction using Bloom's Taxonomy. "In Bloom's taxonomy, which is a well know and widely accepted pedagogical taxonomy, knowledge only comprises the very first, and lowest, level of education. One could argue that this level of comprehension is in fact not adequate for most humans who play a role in the information security process." (Van Niekerk & von Solms, 2008)

Security training geared toward middle school and high school students often comes in the form of top 10 lists for safety online (CyberSmart, 2016), or awareness campaigns (Stop. Think. Connect., 2016). Other training is aimed at students who want to get into cyber security as a future career (Hacker High School, 2016), (US Air Force, 2016). Since these are aimed at students wanting to get into security, they will not work as training for all students, since most students are not interested in studying security in depth.

In Idziorek, Rursch, and Jacobson's work on creating a security literacy course, they state: "The goal of literacy-based learning is to elevate a student's knowledge beyond that of simply being aware of the problem so that students and future professionals are able to successfully consider their actions and new events in the context of security and subsequently make informed decisions as to what they should or should not do to protect their personal and private information as well as safeguard their reputations." (Idziorek, Rursch, & Jacobson, 2012) Since knowledge is not enough, security literacy needs to have a place in the education of everyone who uses the internet. Since middle and high school students are using the internet more and more, it becomes more vital that they be introduced to security concepts earlier in their education, and teaching security literacy is a vital step to ensuring that they understand how to handle themselves online. Literacy aims to teach students how to think about security, not just how to defend against current attacks. The Security Literacy course, created by Dr. Jacobson and his colleagues at Iowa State University (Security-Literacy.org, 2016) is the first step in introducing security literacy as a normative educational tool in middle schools and high schools.

Idziorek, Rursch, and Jacobson go on to say, "Throughout the development and delivery of the Introduction to Computer Security Literacy, it has become apparent that the effectiveness of this literacy-based course would be greatly enhanced by an accompanying lab." This lab would need to be a hands-on environment where the students can learn about the security techniques and vulnerabilities first hand, in a secure environment. It would also need to be accessible to all students, not just students who are

interested in computer security, or who are into technology. The following sections will explore possibilities for this lab environment, as well as other training alternatives.

2.2 Current Tools for Security Awareness

Currently, there are many websites and campaigns to spread awareness about online safety and security for teens. These campaigns range from tips on how to be a good "digital citizen" (National Center for Missing & Exploited Children, 2016) to top 10 lists of cyber security tips (CyberSmart, 2016). In this section, we will review several of these campaigns and programs.

2.2.1 Net Smartz Kids

Net Smartz Kids is, "an interactive, educational program of the National Center for Missing & Exploited Children® (NCMEC) that provides age-appropriate resources to help teach children how to be safer on- and offline." (National Center for Missing & Exploited Children, 2016) This site is geared toward school aged children, and promotes online safety and good netiquette through cartoon videos, games, and comics. Many of these videos and games do not go into why you should do the things they promote, other than to say that there are bad people who want to get your information, so don't share it with them. This would be a good site for younger school aged students, who haven't had much experience with going online, and need to be told what they should and shouldn't do online. The cartoons seem to be aimed at a younger audience, and focus on the dos and don'ts of being online.

2.2.2 STOP. THINK. CONNECT.

"STOP. THINK. CONNECT." is, "the global online safety awareness campaign to help all digital citizens stay safer and more secure online." (Stop. Think. Connect., 2016) The campaign has lots of tips and safety checklists on the site, as well as other resources, like posters, to use in awareness campaigns aimed at students. These campaigns can be a great way to get students thinking about security and online safety. However, awareness campaigns, and top 10 lists will not be enough to keep students engaged and thinking about online safety and security throughout their lifetime. With no interactive components, students may not really understand what it means to create good passwords and spot malicious websites and links. The site itself does not seem to be aimed at students, but rather, it is aimed at educators who can use the materials in their classrooms and training when they teach online safety and security. The stated goal of the site is to, "help people understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior." This is a good goal to have when introducing students to the ideas of cybersecurity. But, to truly be effective, it needs to be taken further, from awareness to understanding, and then on to true literacy.

2.2.3 CyberSmart! & Common Sense Media

Common Sense Media is the parent company of CyberSmart, and both of these sites work to "empower students to harness technology for learning and life." (Common Sense Media, 2016) CyberSmart is "a digital learning company and international leader in fostering digital literacy skills." (CyberSmart, 2016) It is aimed at teaching students how to use computers responsibly, and has a top ten list for cyber security tips for teens.

This is a good place to start when you want to begin learning about what to do to keep yourself safe online, but it is far from comprehensive, and since it is a static list, it does not provide any interaction for students, and may go out of date when new attacks come out. Common Sense Media's main focus is on "Digital Citizenship". It takes a holistic approach to teaching students about proper use of the internet, and teaches about things like cyber-bullying, copyright, and how digital media can affect our lives, in addition to some pieces about security and safety online. They do this through videos, lesson plans, student assessments, and activity sheets. This is also a good place to start when teaching kids about the internet in general, and how to be a good citizen. While the site does go into some things to be aware of to stay safe online, and has some tips for creating strong passwords, it is not very comprehensive with regards to security for teens. In addition, without any hands-on training, it will be more difficult for the students to fully grasp the security concepts, and see them in action.

2.3 Current Tools for Security Training

In addition to the awareness training that several sites offer, there are also websites that target students with an interest in computer security. Some have self-directed training with hands-on components for students to better understand the concepts they are being taught. Others have competitions and camps for students to participate in, where they learn about cyber security. In this section, we will review two programs aimed primarily at middle school and high school students.

2.3.1 Hacker High School

Hacker High School is a self-directed program that teaches students, "what they need to know to be better hackers, better students, and better people." (Hacker High School, 2016) It has, at the heart of the training, self-contained lessons that students go through on their own to learn about different security aspects. It takes on the more positive definition of "hacking", describing it as, "a method of problem solving that combines resourcefulness, logic, creativity, and study." (Hacker High School, 2016) But, by having "hacker" in the name of the site, it is setting itself up as a certain type of training, targeting a very specific demographic, mainly, students who are into technology, who want to learn about "hacking" in whatever form that takes. While it does have good lessons, and hands on techniques, it is very much geared toward a more technically minded audience, teaching things like the command line and network security essentials, which students probably won't use on a regular basis, unless they go into IT as a career field. While this site does have some good information and training for students interested in technology and learning about security, students not interested in learning about the ins and outs of technology will get bored by this, and will not be interested in learning to this depth.

2.3.2 Cyber Patriot

Cyber Patriot is a program designed by the Air Force Association, and is designed to, "inspire students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future." They do this through three programs. The first program is the National Youth Cyber Defense

Competition. This competition has students secure and defend a network as if they were the IT department for a small company. This is a good place for students to show off skills they have learned in cyber defense, and good motivation to learn those skills, but not every student will want to participate in a competition like this, nor is it a training program that will, in itself, help students learn security. The second program is AFA Cybercamps. This is a summer camp program to help students learn how to keep themselves, and their data, safe online. These summer camps are sponsored and held at local high schools, and other organizations, and are only available during the summer. The AFA Cybercamps are targeted at students who are interested in cyber security, and would like to pursue it as a hobby, or as a future potential career. Again, these are not for all students, especially students who are not interested in learning about securing and breaking into computers. The third program is the Elementary School Cyber Education Initiative. The program is designed to introduce security concepts to students, begin teaching students about careers in cybersecurity, and to understand the importance of security. This program is aimed at elementary students, so would not be the best fit for middle school and high school students, and it is again aimed at students who may have an interest in going into the security field as a career someday. These programs are good options for students interested in going into the computer security field, but for the majority of students, they will be at a much higher level than what they want to learn about.

Table 1. Current Tool Overview

Tool	Main Purpose	Advantages	Drawbacks
Net Smartz Kids	Promotes online safety and good netiquette through cartoon videos, games, and comics.	• Teaches students about being good cyber-citizens • Helps when beginning to learn about staying secure • gives them tips for staying safe and secure online	• Not as appropriate for middle and high school students • Doesn't go into the reasoning for the tips • No hands-on training
Stop. Think. Connect	Safety awareness campaign that helps people stay safe and secure online	• Good tips about how to stay safe online • Good way to get students to start thinking about security	• No hands-on training • Only touches on the awareness and knowledge aspects of security, does not try to teach literacy
CyberSmart & Common Sense Media	Teaches students about how to properly use the internet, with training about cyber-bullying, copyright, and other aspects of online usage	• Holistic approach to teaching appropriate internet usage • Talks about security and safety while teaching about appropriate use	• No real hands-on learning • Not very comprehensive when it comes to security training, only teaching a few basics
Hacker High School	Self-paced training for cyber security	• Hands-on training, going at your own pace • Good explanation of security concepts	• Geared toward students who are interested in security and technology • Not aimed at all students
Cyber Patriot	Competition and summer camps for cyber security	• Thorough training in many aspects of security • Great for students interested in cyber security as a field of study	• Mainly just for students who want to do security as a career • Not as accessible to all students

2.4 Research Summary

There are a lot of tools on both ends of the spectrum to teach computer security to middle and high school students. With all of the training in awareness, being a good digital citizen, and top ten lists for staying safe online, there should be a place for security literacy, something that would truly help students learn to be safe, without just giving them a list of dos and don'ts, while being at a level that will be understandable for all students. There seems to be a large gap in the middle of this spectrum that fulfills that duty.

On the one end of the spectrum, teaching security awareness is just not enough to train middle and high school students to become proficient enough in staying safe online, and learning how to continue staying safe through the evolution of the attacker's methods. While it may give them a list of rules to follow, it does not give them a lifelong path to follow to remain safe online when new threats come on the scene.

On the other end of the spectrum, there are several good options for learning computer security in depth. While these are a great tool for students who are technologically minded, and students who want to go into computer security as a career, it is far more training than would benefit the average middle or high school student. Since the average student just wants to go online and use the internet as a tool, they will not be engaged and have the required technical knowledge to fully make use of the in depth security training these programs provide. On top of that, since they are not interested in it, they will be much less engaged, and much more likely to not get any useful information out of the training.

This leaves us with a hole needing to be filled. The Security Literacy course is the first major piece to solving this issue. A complementary lab component, teaching hands-on skills is the next phase of that project.

CHAPTER 3

METHODOLOGY FOR PROPOSED FRAMEWORK

3.1 Framework Methodology

The main purpose of this framework is to create an interactive lab environment to complement the Security-Literacy.org course for middle and high school students. This will be a central hub for all of the lab modules used in the course. Here, modules can be added as new training is added to the course. The framework will include a central location for the instructor to access to all of the student information, such as last login, password, and security questions, as well as each module's data and settings. An instructor will be able to decide which modules they want to use, when to introduce them to the students, and the order they want to present them.

The framework proposed is created using PHP and MySQL. These were chosen for several reasons. First, both PHP and MySQL are Free and Open Source Software, which means that they are open to everyone, and will not require special or expensive software to use in development, or to be installed on the server. Second, PHP and MySQL are also very widely used, so there are lots of tutorials available for anyone who will be developing or maintaining this project in the future. Additionally, PHP is used in several popular websites, such as Facebook (Zhao, 2016) and Wikipedia (Wikimedia, 2016) And lastly, since the framework has a MySQL back end, other languages can easily interface with it, allowing others to develop modules in the language of their choice.

3.2 Rationale for the Framework Design

The reason the framework is designed this way is three-fold. For the framework to be compatible with the Security Literacy course, it must be located in a place that is fully controlled by the same people who control the Security Literacy course. That means that to be effective in being a lab for the course, the maintainers of the course must have full control of how the modules are created and maintained, or they would not be able to confidently include lab sections in their coursework. Second, the modular design of the framework is critical to being able to have multiple developers work on the lab. Without the modular design, developers of the modules would either have to worry about making changes that would corrupt other modules, and they would have to recreate portions that should work the same way in each of the modules, and may cause inconsistencies in the programming. Third, with a centralized instructor section, the instructor will be able to go to just one place to find all of the information they need to run the lab. Without that, they would have to search all over for each module, and might miss out on some aspects of the course because of it.

3.3 Framework

3.3.1 Framework Overview

The framework for Hackerville will be a place for the instructor to administer the lab work and demonstrate the security concepts taught in the course, as well as a place for the students to get hands-on training with the same concepts. The students will be able to see first-hand, in a safe and secure environment, what to watch for when interacting with

the digital world. They will learn about the security concepts from the course by trying each of the concepts without having to worry about compromising their accounts or their computer.

This framework was created using PHP, but it was created in a way that new modules don't have to be developed in PHP. As long as the chosen language can utilize a MySQL back end, each new module can be created in a different language, run on a separate node on the network, and have its own style, look, and feel.

There are three main design components to the framework of Hackerville. First, the framework is built around a centralized student login. Each module will be routed through a single student login page, so that a new login will not need to be created for each module. There will be a separate database for student data common to all modules, such as the student login and password, last login time, and security questions. Second, there will be the ability for any new modules to connect directly to the framework, by separating out each modules' data into separate databases. With the separation of data, the developers and maintainers of the modules will not have to worry about interfering with other modules. They can be sure that they are only affecting the module they are working on. Third, there will be a central home page for the instructors to keep track of the student login details and each module's data. It is important that the instructors have a central place to make administering the lab work much easier. They will be able to login and see all of the classes they are currently running, and will be able to get to any module's data quickly and easily. These components have been carefully designed to

make the lab as robust, accessible, and adaptable as possible, for both instructors of the course and maintainers of the code.

3.3.2 Instructor Page

The instructor's home page will be a central hub for all class activities. After logging in, a landing page will be displayed with an overview of all of the instructor's classes, showing how many students are in that class, the class number, and any notes the teacher has input about the class. Each class section will have links to each module available. Below the class overview section will be a section to add a new class. At the bottom of the page will be a section for any deactivated classes for that instructor.

The login and registration pages for the instructor are modified versions of the open source "Simple Registration/Login Code in PHP" from user 'simfatic' on GitHub (https://github.com/simfatic/RegistrationForm). They have been modified to use the instructor's registered email address as the user name, so the instructor doesn't have to keep track of a separate user name. When an instructor initially visits the site, they will be prompted to register with their full name, email address, and a password. An email will be sent to them to have them verify their registration, then they will sign in and begin using the site. On the login page, there will also be a link to reset the password. Once the instructor is logged in, there will be a logout button on each page.

The class overview section will display a list of active classes for the instructor, with details displayed for each class: the class number, number of students, and notes about the class. There will be options to view, edit, and disable each class, as well as a section for each of the modules under each class section. The view class option will

allow an instructor to view the details of the students, including the student number, password, last login, and password expiration date. The edit option will allow a teacher to edit the notes they have entered for the class, edit the class number (as long as it is not the same as any other classes the instructor has), and add students to the class. This will not allow an instructor to decrease the students, so that data will not be accidentally lost, and students will not have their access accidentally revoked. If an instructor needs fewer students in the class, they can simply use only the number of students they need, and ignore the rest. Instructors will be able to disable classes by utilizing the Deactivate option. Once the instructor deactivates the class, the students in the class will no longer be able to log into the system. All of the data will remain in the database, so if the instructor disabled the class by accident, they can easily reactivate the class, and the instructor will have access to view historical data as well. All of the instructor's deactivated classes will populate at the bottom of the main instructor screen.

Between the section of active classes, and the deactivated classes below, there will be a section to add a class. This section will allow an instructor to enter a class number, the number of students, and notes on the class. The class number will be a string field, where any characters can be entered so that the instructor is not restricted to only alpha-numeric characters. This will be a unique field for each teacher. This way, it will be easy to distinguish between the classes at a glance, while allowing different teachers to name their classes the same as each other. It is recommended that the instructor include the year, semester, and class period or class time, as the "class number", but any combination of data that will help the instructor remember the classes is permitted. The

notes will only be used as an informational reference field for the instructor. When an instructor saves the class, the student data will be created in the database, based on the number of students the instructor has input. The students will be created with a student number, unique in that class under that instructor, an initial password of 5 random letters, and the internal instructor and class ids. The instructor, class, and student ids will be combined, with hyphens between each, to create a unique id for the student to use for logging into the system. The format for this id will be <instructor_id>-<class_id>-<student_id> (ex: 17-45-3; 22-63-22). This is the number that will be displayed in the class overview section.

Each module summary page will open with information about the module and an overview of the student data for that module. The module overviews and detail sections will be different, based on what kind of data will be available for the students to interact with, and the instructor will have varying levels of control over what data can be added, removed, or changed. Some modules will allow the teacher to manipulate the data, adding, updating, or removing it, to simulate normal or abnormal activity. Others will only allow the instructor to remove data, if, for example, a site needs to be monitored and policed.

3.3.3 Student Pages

The student section will begin with a central login. The student will initially log in with their student id, in the format: <instructor_id>-<class_id>-<student_id> (ex: 17-45-3; 22-63-22), and the randomly generated password that was created when the instructor set up the class. Upon logging in for the first time, they will be prompted to

change their password. On this screen, there will be a message telling them to choose a good password, and also informing them that the instructor will have access to this password, so they should not reuse a password they are using for another site

After the initial login, a student will be able to request their password on the main login screen, if they have forgotten it, or change their password, if it has been compromised. After they have logged in, they will be able to log out with a link on each page. This will need to be added to each page, but can be a link to the central logout script.

The login page will be a central page that each of the modules can redirect to, both to do the initial login, as well as to check to ensure the student is still logged in, preventing the student from getting to a page without logging in. There will be centralized scripts for logging in, changing the password, setting up the initial password and security questions, resetting the password, and logging out. These will be used within each of the modules to avoid having to reprogram all of the login information each time a new module is created.

3.4 Modules

3.4.1 Module Overview

Each module in Hackerville will have several common elements, in addition to having some freedom in the way they are designed. The common elements throughout each module will include: a connection to the single, common student login; a separate database for each module, containing data unique to its module; and a section in the instructor home page for administration of that module.

Having these common elements will accomplish three main things. First, it will allow the developers of the modules to focus on creating the modules themselves, and not spend time on components that have already been created. Second, it will allow the instructors to easily view student activity in each module, in a centralized location. And third, it will allow each developer to work in a compartmentalized unit, knowing exactly which data goes with which module, without worry of overwriting another section's data, or having data change based on what other modules are doing.

With the separation of the modules, there will be more freedom to have the individual modules look and feel appropriate for the type of site the module is trying to emulate. Each module will be able to be programmed in any language, as long as it can implement a MySQL database. The modules can reside on different nodes on the network, so that each can have its own, unique, URL. And the modules can each have their own style, look, and feel, appropriate to the site they are emulating. Since each module will be completely separated, they can each be created by different developers, and new modules can be added at any time without disturbing any of the currently running modules. Each module will have a database created to house its own data, but they will all be able to use the student ids from the student database to identify which data goes with which student, without forcing each module to keep its own table for students. This will also allow the instructor to have a single page to look at all of their students, and be able to see all of the modules and data for each student, all in one place.

Each module will tackle a specific topic. They will each be created with a topic in mind, and will be able to show the students a different aspect of security, which may

be specific to the site the module will emulate. There will be some modules that will be able to tackle more broad topics, such as password use, reuse, and complexity. These topics may be able to be integrated into pre-existing modules, using them as examples of why the specific topics should be important to the students. For example, using a social media site to demonstrate why password reuse is an insecure practice. While this isn't a problem unique to social media, it will demonstrate to students why the principal should be important to them.

3.4.2 Instructor Module Sections

Each class overview in the instructor page will have a section with all of the available modules. When an instructor clicks on a module, they will be taken to an overview page for that module. Each module's summary page will be different, depending on the data needed to administer the module, and what they instructor needs to know about the student activity. Depending on the module, there may be sections where the instructor can add, delete, or modify data that the students see. There may also be logging of student activity and the ability to check on student progress throughout the module.

The instructors will be able to see all of the modules at once, and will be able to decide when to introduce each one, and how many they ultimately want to use in the coursework. In the Security Literacy course, there will be suggestions for the instructor as to which module to use when, and how to introduce it to the students, as well as what they should do to simulate any actions that the students should be watching out for.

3.4.3 Student Module Sections

Most of the student modules will begin at the login page. This page may look different for each module, based on how a typical page of that type would look. The login will be shared between modules, but a different façade can be created for each site to use, so that the login looks like it should for that type of site. Each module will use the same login credentials, utilizing the shared student login database.

After the student logs in, the modules will simulate real-world webpage that the students would use. These sited will have some of the functionality of the real-world sites, but only to the extent that they can show the security concepts being taught in the Security Literacy course. The module's main purpose is to show potential security issues that the students may run into, so the modules will mainly focus on the security concept, and build around that security concept, rather than being a fully functional site that completely emulates the real-world counterpart.

3.4.4 Sample Module: Hackerville Credit Union

The Hackerville Credit Union module is intended to show the students potential security issued with their banking webpage. The students will need to watch out for malicious transactions in their bank account, and be careful about how they choose their login credentials, including a secure password, and good security questions, that others would not know the answers to. There will eventually be other security issues integrated into the module, such as email alerts telling the student that their account has been compromised (some of which will be legitimate, and some which will contain links to malicious sites), and emails with malicious attachments that look like they are from the

bank. The module will be able to show several security vulnerabilities, and the instructor can use it for several sections of the Security Literacy course.

The instructor module will begin with an overview of the students and their account information. An instructor will be able to drill down on an individual student to see their individual transactions, and add new transactions at the individual student level. In the overview page, there will also be the option to add new transactions to all of the student accounts at once. Each of these transactions, both individual student transactions, and class level additions, will be able to be added as normal transactions, or marked as malicious by the instructor when they add the transaction to the account or accounts. This marking of malicious transactions will only be seen by the instructor, and to the student, it will just look like another normal transaction on their account. This way, it can be used to have the students watch for potential malicious transactions on their accounts, without tipping them off to the nature of the transaction.

The student module will begin with the login. In the future, two-factor authentication may be added for extra security. Once the student logs in, they will be taken to a page with an overview of their accounts. They will have a debit and credit account in the Hackerville Credit Union, and will need to manage both of them and monitor them for malicious transactions. They will be able to drill down on each account to see all of the transactions that have occurred on their account, with the transaction number, transaction description, amount, and whether it is a debit or credit to their account. On each page, they will have a logout button, which will lead to the centralized logout function. In the future, there will be an email address associated with the bank

account as well, and students will regularly receive emails from the bank, telling them that their monthly statement is ready, that they need to log in to change their password, and giving them some security warnings about their accounts. Some of these emails will be legitimate, and some will be malicious. It will be the student's responsibility to investigate these emails, and see if they can find the "markers" of the different types of malicious emails.

CHAPTER 4

LESSONS LEARNED AND FUTURE WORK

4.1 Lessons Learned

Initially, this project began as a single, large site, with the module being programmed as a part of the framework. There was one large database for all student data and module data. This worked well when thinking of the site as a complete lab, without considering the implementation of other modules. The student login was programmed as a part of the module, and this module was the only thing the login would be used for. When programming the instructor interface, the initial setup was a holistic view, where the instructor could see the login information and the module data for the students, all in one place. Again, this was a good way for the instructor to see all of the information at once, when only considering the single module that was being created. If the intent of this project was only to have the single module, this would have been a good implementation strategy, but since the intent was to build a framework, where other modules would be incorporated, the framework needed to be rethought, and rebuilt from the ground up.

The project was restarted with the central login and the instructor hub at the center of the framework. Once the central hub for the instructors was established, the path forward was much more clear. The central hub began with a list of classes, and the ability to drill down to the login information for the students. Since this login information would be used for many of the modules, it made sense to separate it out in the instructor view, so that the instructor had direct access to it. Now, the login

information was available outside of any one particular module, since it served a broader purpose, and could be used for any of the modules. With that class list and login information moved to a separate place, it was a simple next step to include a section under each class for its modules, and the data necessary to administer those modules.

From there, the central student login was the next logical step. Generic pages for use with login, logout, and password resets were the central resource that would make it much easier for new modules to be created. Making it so other developers wouldn't have to reprogram the elements common to many modules was vital in producing a framework that was easy to add to. This also made it much easier for the developers to be able to focus on the modules themselves, rather than everything necessary to make the modules work.

The next step was to create a test module, and ensure that implementing the module would be straightforward, and minimal effort would be required to get it to work within the framework. This will create a model for how new modules can be created and integrated into the framework, and how the framework handles logins and the instructor hub for new modules.

After figuring out how to create the framework, the pieces began falling into place, and it became much more clear how to turn the project into more than just a website. As the framework took shape, it became easier to see how the modules would fit in, which duties the framework needed to handle, versus which duties the modules could take on, and how each piece could fit into place, to make the framework be the most efficient, both for developers of the modules, and the instructors who would be

teaching the course. This was critical in getting the framework stable, and viable to have a modular setup. Once a protocol was established, it became easier to fill in the gaps that the framework had, and determine which pieces the framework should handle, and which the modules should take care of.

The other piece that became much clearer as the framework took shape, and the work of the modules and framework began to separate, was how the data structures would be handled in the database. Initially, the student data was all combined in one database, including the module data, the student login, and the class structures. This worked just fine with one developer and one module. But as the number of modules increases, and more developers join the project, it becomes very important that the developers keep the data for their module separate from other modules, so that they won't overlap, and data from one module will not affect other modules. As a result, the databases needed to be separated. There is now one database for all of the generic student data. This includes the student data, class structure, and login information. Each module would now have its own database, where the data specific to that module will now reside. With the data separated in this fashion, each module can call the student database for the login, student data, and class data, and can call its own database for the data specific to that module. With the data segregated this way, the creator of the module can be certain that they are only affecting data for their module. They can also modify the structure of the data table, add remove, or modify tables as needed, and have their module interact with the data in whatever way is appropriate for the purpose of the module, while being certain that they are not affecting any other module in the process.

Separating the data, the instructor page, and the duties of the framework and modules created a clear purpose and direction for the framework. The segregated features of the design makes the modules easier to develop and integrate into the framework, and the central hub feature of the design forms a unified way to bring all of the modules together. In this way, the framework can act as a true framework, and not just another webpage that is difficult to add to and modify.

4.2 Future Work

4.2.1 Future Framework Enhancements

The biggest enhancement to the framework will come in the form of an internal email system for the students. There are many additional pieces that can fall into place for each of the modules once the email system is implemented, including two-factor authentication, malicious emails to test the students, and legitimate alert emails that the students must filter out to get important information for their accounts. This email system will be highly restricted, only allowing a webmail style login, and only allowing students to send and receive emails within this internal system. No emails will be able to go out from a student email to a real email outside of the system, and the only emails they will receive will come from inside the system, usually triggered by the instructor. This will ensure that the system will remain a safe environment for students to learn about security vulnerabilities and malicious attacks.

Another major improvement to the framework will be the look and feel of the site and the modules. Currently, the framework is relatively bare bones. It does not have the look or feel that you see with modern websites, because no CSS or JavaScript is currently

implemented in the design or implementation of the framework or the sample module. A major improvement to the instructor page, as well as the student login, will come in the form of cosmetic enhancements. These will make the user experience much better, and make the entire application feel like other modern websites the users are familiar with. The intent of this project was not to create a modern web application, but to merely set up the framework for a lab environment that would evolve and grow as the Security Literacy course grows. With those changes will come cosmetic updates to keep the application looking and feeling modern, so that it will not become an out of date application that people won't use anymore. As modern web techniques and standards improve and advance, the framework will be able to advance and improve with them. Since the framework was created to be an application to build on, the façade can be created and updated separately, and will be improved upon over time. This will ensure that the framework will continue to be relevant, no matter when the framework is used.

4.2.2 Future Hackerville Credit Union Module Enhancements

One of the major enhancements that will add a lot to the Hackerville Credit Union module is the implementation an email system to the entire framework. With it, the instructor will be able to send out several different emails regarding the bank to their students. Several different emails will be available for the module, and will accomplish different goals. The simplest email the instructor would send out would be a legitimate email from the Credit Union. This email would have the bank's true URL, and would be informational in nature, either instructing the student to change their password, or to inform the student about new services the credit union is offering. The next type of email

would be one where it informs the student that their account may have been accessed by an unauthorized user. Some of these emails would contain malicious attachments, with instructions to look at the attachments for more information, and some would contain links to a malicious site asking them to login and verify their credentials. This site will save the credentials so that the instructor can login and see which users have fallen for the phishing email, and instruct the students on what to look out for to be aware of phishing emails in the future. A third type of email would advertise "helpful services" to customers at the bank. There are several malicious attacks that could be performed at this point, which will be outlined in the "bad.hackerville.org" section below. Having an email service will open up many opportunities in the future for adapting the emails and the attack vectors to the newest, real-world attacks, making this an ongoing project for years to come.

Other enhancements to the Hackerville Credit Union module could include two-factor authentication, and demonstrating how that protects the user from attackers who might somehow get a hold of their login information. Having an HTTPS version of the site, as well as an HTTP version of the site could demonstrate how easy it is to sniff login credentials without encryption, and the module could be adapted for other security demonstrations as well.

4.2.3 Future Additional Modules

The following are potential future modules that can be added into the Hackerville lab framework. These modules will each provide unique experiences for the students, and will allow them to see different security vulnerabilities for various types of websites

and web applications. Each of these additional modules will be great enhancements to the lab, and will be important additions to the security literacy training program. The framework has been built to allow modules to be added in any order, and to allow more modules to be added, whether they are in the list below or not. This way, as more types of websites and web applications come out, the lab will be able to handle additions to fit necessary training.

4.2.3.1 tmi.hackerville.org – A Social Network Clone

Social Networking plays a large role in the social lives of many teens. As such, bringing demonstrations of insecurity to a social networking platform clone could show students how insecure they are and some ramifications of insecurity, they might take more to heart because it is something they care about.

4.2.3.2 mail.hackerville.org – A Local Email Client

Email will play a vital role in showing how malicious attacks can come from seemingly secure sources. By having an internal email system, the emails that come in can be carefully crafted, and can come from seemingly trusted sources. The internal email also has the advantage of restricting the access and activity available to students. This can be limited to only receiving emails, and only from the internal email system. This system would be set up as a web-based email service, connecting to the existing student login. This email system could be reused for many of the modules, not just the existing one.

4.2.3.3 shopping.hackerville.org – An Online Shopping Site

Online shopping is very prevalent in today's society, and as such, it is important that students see the security risks that come along with it. This module could connect to the students' bank accounts in the Hackerville Credit Union module, and could then show the dangers of other people accessing their bank account information, or their shopping account information.

4.2.3.4 games.hackerville.org – An Online Gaming Site

Many students may already be playing online games, either in web browsers or on their computers over the internet, and may not know what to watch out for in online gaming sites. This module could include malicious downloads to "update" your computer to play the newest web-based games. It could also include links or ads, either in the module, or through emails, that would lead to malicious sites, which could in turn do other bad things, as described in the bad.hackerville.org section below.

4.2.3.5 videos.hackerville.org – A Video Hosting Web Application

Videos can go viral very quickly, and without the training to understand the differences, and differentiate safe sites from unsafe ones, students can easily be led to a malicious site that seems to hold the next viral video. Like the gaming module, this site could be a malicious site, asking you to download some updated software to play the videos, which would really just be malicious software. This could be used to help students see what warnings your browser and machine give, when downloading potentially malicious content, and live out an attack, where they can be sure that their machine is safe from real attacks.

4.2.3.6 bad.hackerville.org – A Malicious Node

This node will be where all of the malicious content originates and resides. It can include sites that clone the Hackerville Credit Union or the TMI social networking site, grabbing the login information of unsuspecting students who are not careful to look for the correct URL before entering their credentials. It can be the origination point for the malicious phishing emails. And it can be a place for the instructor to give demonstrations on poor security implementations and the types of warnings a browser should give when a user visits one of those insecure or malicious sites. It can host the pages for drive-by downloads, "viruses", and other malware created specifically for this training, and these modules. Other pages could produce pop-ups that ask if the student really wants to navigate away from this page, with yes and no options. These could contain malicious content behind both buttons, teaching them that if they get a message like that from an untrusted source, it's best to just close the browser entirely and start over.

Since this module will host many different forms of malicious content, it will be the module that will evolve the most. As new attack vectors pop up in the wild, this module will be constantly added to, giving students a better idea of what is out there and how to recognize and stop it from infecting their machine and stealing their data. This natural evolution of the node will be vital to showing the students the ever evolving nature of attacks, and help them to create a better awareness of how to be vigilant against attacks, wherever they come from, and whatever form they may take at the time.

4.3 Future Work after Hackerville Lab

While the modules in the Hackerville Lab will continue to grow over time, there are other projects that could branch out from this lab, to begin to train others in security literacy. The Hackerville Lab and the Security Literacy course are aimed at both middle school and high school students, but the site could be broken into two separate entities, with different modules being maintained for middle and high schooler students, which are focused on issues more specific to their age group. Having the high school track build on the middle school track would be a good way for students to keep up with new attacks, and continue to have security be at the forefront of their mind when living their digital lives. Additionally, if a student took the course in middle school, and then took the course again a few years later, it would be a different and more advanced course when they take it again in high school.

In the middle school version, the course could begin introducing concepts that are important to learn about early on, things like secure passwords, password reuse, and watching for signs that a site is malicious. The middle school version of the course would get them thinking about security concepts, and help them to begin watching for the things they are being taught. When the students have mastered those concepts, they can be introduced to more advanced concepts in the high school course, as well as an expansion of the ideas they learned in the middle school course. The high school course could either begin with a brief overview of what the middle school course covered, both to help students remember what they learned in their earlier course and for the students who weren't in the first course to begin with, or it could cover the topics that were

covered in the middle school version, but cover them more in depth, and add concepts that require a better understanding and deeper knowledge of those concepts, and then continue on to more advanced concepts later in the course.

Another project that could be branched from this lab framework is a university version of the Security Literacy course. This could begin as a 100 level course, recommended or required for all students. The course could follow a similar path as the course for high school students, but could be more advanced and more tailored to the online habits of a university student. The lab would follow a similar format, creating modules for university level students, and tailoring them to a university student's digital lifestyle and concerns. These modules could be less aimed at entertaining school-aged kids, and be more professional and academic in nature, preparing students for life after college. New modules could include things like a very basic workplace database system, where the student would have access to fake bank account information for clients of the company, and a simulation of that data being leaked. Other modules could include things like health records or medications, and show similar security issues, such as password reuse, or poor encryption.

After that initial course, courses more specific to the student's major could also teach security concepts, and have lab components that are tailored to security concerns of the field the student is learning about. For example, if a student is in a finance or accounting major, the lab component could have to do with a finance department, and the information they will be expected to keep secure in future employment after they finish their degree. For a student majoring in engineering, the lab could deal with company

design secrets, things the student would need to keep secure to ensure the company keeps its competitive advantage. For medical majors, labs could focus on HIPAA related data, and ensuring confidentiality to their clients. And for students taking courses that will lead them to work with children, the labs could be focused around keeping the children safe, by not allowing their information to get out to the public, where child predators would have access to it.

Each major, and each field of work, has its own security concerns. Every workplace has a reason to keep information safe and secure, and putting these security concepts in the context of those work environments will help students recognize how vital it is to truly understand security, and why it is important in all areas of their life.

These modules, based on various majors, should be integrated into existing major courses, and taught by instructors within that area of study. By doing so, the instructors can give much more detailed reasoning and real world scenarios to the students, so they can understand that security isn't just an IT concern. Security needs to be taken seriously by everyone, or there will be a complete breakdown, and everything is much more vulnerable. Integrating security into the existing major coursework will have a much higher impact on students because it is coming from the instructors they know and trust, and it will be given in the context of the students' intended careers, leading to a much better understanding of why it will be important in their everyday work situations after they graduate. Ultimately, this should be a better motivation for them to learn why information security is necessary and important, than just having a single course dedicated to security literacy.

CHAPTER 5

CONCLUSION

Through the many iterations of this project, a lab framework has been built that will serve as a great supplement to the Security Literacy course that has already been written. Through the modules, each section of the course can have a hands-on component where students can see security vulnerabilities at work. They can begin to recognize different markers for malicious attacks, and can be introduced to important security concepts that they will be able to put into practice right away in their digital lives. This will be a great starting point for them to begin to understand why security is important, and what they can do to protect their information, identity, and online accounts. Having a hands-on lab that they can test out for themselves will allow them to test security concepts, and see malicious vulnerabilities in the safe confines of a lab environment, where they will never expose their data or accounts to any true threat.

With this framework, modules can continually be built and implemented, and new security concerns can be demonstrated in a safe environment as the security landscape continues to grow. Attackers will never stop evolving their attack vectors, so to teach security concepts we must continue to evolve as well, and this framework is set up to do just that.

References

Common Sense Media. (2016, October 16). *Common Sense Media*. Retrieved from Our Mission: https://www.commonsensemedia.org/about-us/our-mission

CyberSmart. (2016, October 16). *CyberSmart.* Retrieved from CyberSmart!: http://cybersmart.org/

Hacker High School. (2016, October 16). *Hacker High School*. Retrieved from About Hacker High School: http://www.hackerhighschool.org/about.html

Idziorek, J., Rursch, J., & Jacobson, D. (2012). Security Across the Curriculum and Beyond. *2012 Frontiers in Education Conference Proceedings*, (pp. 1-6). Seattle, WA.

Lenhart, A. (2016, October 16). *Teens, Social Media & Technology Overview 2015*. Retrieved from Pew Research Center: http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/

National Center for Missing & Exploited Children. (2016, October 16). *Net Smartz Kids*. Retrieved from About Us: http://www.netsmartzkids.org/AboutUs

Security-Literacy.org. (2016, October 16). *Security Literacy*. Retrieved from Security Literacy: http://security-literacy.org/

Stop. Think. Connect. (2016, October 16). *Stop. Think. Connect.* Retrieved from Campaign: https://stopthinkconnect.org/campaigns/other

U.S. Department of Homeland Security. (2016, September 16). *National Cyber Security Awareness Month*. Retrieved from Homeland Security: https://www.dhs.gov/national-cyber-security-awareness-month

US Air Force. (2016, October 16). *AFA CyberPatriot*. Retrieved from What is CyberPatriot?: https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx

Van Niekerk, J., & von Solms, R. (2008). Bloom's Taxonomy for Information Security Education. *IFIP IEEE Information Security South Africa*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.145.1859

Wikimedia. (2016, October 16). *Wikimedia: Organization Summary*. Retrieved from Open HUB: https://www.openhub.net/orgs/wikimedia

Zhao, H. (2016, October 20). *HipHop for PHP: Move Fast*. Retrieved from Facebook for Developers: https://developers.facebook.com/blog/post/2010/02/02/hiphop-for-php--move-fast/