POLYMORPHIC HOMEWORK AND LABORATORY SYSTEM: AN INSTRUCTIONAL TOOL FOR COMBATING CHEATING

A Thesis in
Information Sciences and Technology

by
Ryan J. Kohler

© 2018 Ryan J. Kohler

Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science

May 2018
The thesis of Ryan Kohler was reviewed and approved* by the following:

Nicklaus Giacobe  
Assistant Teaching Professor of Information Sciences and Technology  
Thesis Advisor

Jungwoo Ryoo  
Professor of Information Sciences and Technology

Peter Forster  
Associate Teaching Professor of Information Sciences and Technology

Michael Hills  
Associate Teaching Professor of Information Sciences and Technology

Mary Beth Rosson  
Associate Dean of Graduate and Undergraduate Studies

*Signatures are on file in the Graduate School
ABSTRACT

Cybersecurity is a complex and ever changing domain. This requires that cybersecurity professionals be vigilant in their monitoring of complex network environments to prevent and resolve undesired actions. In order for cybersecurity professionals to achieve this they have to learn these techniques in curricula that adapt to the current technologies and techniques available. However, this becomes difficult when students are able to readily find assignment answers online that they can copy as their own work.

This thesis addresses this issue by proposing the design of a system (PolyLab) and implementing a system to combat the ability for students to cheat. This proposed system is capable of automatically generating and grading homework and laboratory assignments that are unique for each student. This reduces the administrative overhead of instructors and does not negatively impact the cognitive workload of students. The system is also capable of use in a variety of domain fields and in a variety of class sizes.

This work evaluates the proposed system through the comparison of two groups of research subjects in a between-groups experiment. One group received network data that the system generated and the other group received the static network data. This study utilizes situational awareness measurement techniques to determine if an impact on cognition exists between the two groups.
# TABLE OF CONTENTS

List of Figures ........................................................................................................ vi
List of Tables ........................................................................................................ viii
Acknowledgements .................................................................................................. ix

Chapter 1 Introduction ................................................................................................. 1
  Cybersecurity Tools .............................................................................................. 1
  Cybersecurity Failures ......................................................................................... 3
  Cybersecurity Curricula ....................................................................................... 6
  Teaching Cybersecurity in a Modern Setting .................................................... 7
  Proposed System .................................................................................................. 8
  Research Questions .............................................................................................. 11
  Contributions of this Thesis ............................................................................... 11
  Summary .............................................................................................................. 13

Chapter 2 Review of Related Literature .................................................................... 14
  Review of Challenge-Based Learning and Virtual Labs in Cybersecurity Education.... 14
  Review of Situational Awareness Literature .................................................. 18

Chapter 3 PolyLab System Development ................................................................ 24
  Concepts Behind PolyLab .................................................................................. 24
  Operation of PolyLab ........................................................................................ 26
    PolyStego ........................................................................................................ 28
    PolyEncrypt ..................................................................................................... 32
    PolyNet ........................................................................................................... 39
  Summary ............................................................................................................ 55

Chapter 4 Human Subjects Experiment .................................................................. 56
  Objective ............................................................................................................ 56
  Lab Assignments ................................................................................................. 56
  Experimental Process ......................................................................................... 57
  Groups ................................................................................................................ 60
  Measures ............................................................................................................ 60
    Situation Awareness Global Assessment Technique (SAGAT) ...................... 60
    NASA-TLX and SART .................................................................................... 61
  Pilot Testing ....................................................................................................... 63
  Results ................................................................................................................ 64
  Participants ......................................................................................................... 64
LIST OF FIGURES

Figure 1. Situational Awareness Model (Endsley, 1988a; Endsley, 1988b) ........................................ 20

Figure 2. Prototype assignment and generation example (Kohler, Santoro, & Giacobe, 2017) ........................................ 25

Figure 3. Hash Generation (Giacobe & Kohler, 2016) .......................................................... 27

Figure 4. Hash generation with date included ........................................................................ 28

Figure 5. Steganography Exercise “hidden in plain sight” (Giacobe & Kohler, 2016) .......... 30

Figure 6. Steganography Exercise Solved (Giacobe & Kohler, 2016) .................................. 30

Figure 7. Another user’s stego exercise .............................................................................. 31

Figure 8. Solved Exercise ..................................................................................................... 32

Figure 9. PolyEncrypt username & password generation example ..................................... 34

Figure 10. PolyEncrypt Delivery System .................................................................................. 35

Figure 11. Hex as ASCII ......................................................................................................... 37

Figure 12. Base32 Encoding .................................................................................................. 37

Figure 13. Base64 Encoding .................................................................................................. 38

Figure 14. Left Shift of 3 ......................................................................................................... 38

Figure 15. Rot47 Ciphertext .................................................................................................... 39

Figure 16. PCAP open in CloudShark .................................................................................... 40

Figure 17. Packet Capture Address Generation (Giacobe & Kohler, 2016) ....................... 41

Figure 18. PolyNet Delivery Homepage .................................................................................. 42

Figure 19. PolyNet Sample Challenge Delivery ...................................................................... 43

Figure 20. CloudShark Home Screen .................................................................................. 44

Figure 21. CherryPy Engine Configuration ............................................................................ 44

Figure 22. CherryPy Trunk and Branch Control ..................................................................... 45

Figure 23. PCAP Generation ................................................................................................ 47

Figure 24. Hashcode Generation .......................................................................................... 47
Figure 25. Example of a condition and a python module call .............................................48
Figure 26. Example BitTwiste System Call ...........................................................................49
Figure 27. PolyNet Grading Login ........................................................................................50
Figure 28. Sample Grading Page ............................................................................................51
Figure 29. PolyNet Grading PCAP Data Generation ...............................................................52
Figure 30. Example Questions Grading ...................................................................................53
Figure 31. Example grade file email .......................................................................................54
Figure 32. Example score file .................................................................................................54
Figure 33. Practice Lab PCAP File in CloudShark .................................................................58
Figure 34. Practice Lab First Answer .....................................................................................58
Figure 35. Practice Lab Second Answer ...................................................................................59
Figure 36. Completion time by study group .........................................................................66
Figure 37. SAGAT scores by study group .............................................................................66
Figure 38. IRB Approval Letter .............................................................................................127
Figure 39. Practice Lab Assignment SAGAT .......................................................................130
Figure 40. Simulate Lab Assignment SAGAT .....................................................................132
LIST OF TABLES

Table 1. Examples of Hacking Tools

Table 2. System Design Requirements

Table 3. Summary of Contributions

Table 4. PolyStego Challenges

Table 5. PolyEncrypt Challenges

Table 6. PolyNet Challenges

Table 7. NASA-TLX (Hart & Staveland, 1988; Giacobe, 2013b)

Table 8. SART (Taylor, 1990; Giacobe, 2013b)

Table 9. Improvements from pilot testing

Table 10. Participant Demographics

Table 11. ANOVA for Completion Times

Table 12. ANOVA for SAGAT Scores

Table 13. Descriptive Statistics for Completion Time

Table 14. Descriptive Statistics for SAGAT Scores

Table 15. MANOVA results due to Experiment Group

Table 16. Summary of Contributions

Table 17. System Design Requirements

Table 18. Study Team Qualifications

Table 19. Study Team Member's Training Status
ACKNOWLEDGEMENTS

I would like to start out by thanking my thesis advisor, Dr. Nicklaus Giacobe, for his feedback, support, and assistance throughout the entire research and writing process. Thank you for drastically improving my technical writing. Without you, this would have been much harder.

Thank you to my thesis committee, Dr. Jungwoo Ryoo, Dr. Peter Forster, and Dr. Michael Hills for taking the time to provide helpful feedback in order to improve the quality of my research. Thank you for taking the time to be on my thesis committee.

Thank you to Dr. David Hall, Dr. Gerald Santoro, Dr. Lisa Lenze, and Dr. Dinghao Wu for advising me throughout this process and for providing invaluable assistance throughout this process. I would also like to thank Dr. Chris Gamrat for providing assistance with literature and for your feedback on my research.

Thank you to all of my lab mates throughout the past 3 years, who have provided advice, commiserated over problems, made me laugh and smile, and made this whole experience a fantastic one.

Lastly, I would like to thank my dad, mom, sister, and all of my friends who have listened to my fears and concerns all the while encouraging and supporting me. Without all of you, this would not have been possible.
Chapter 1

Introduction

As we proceed forward in the digital age, more technologies will be developed and put into use. Users and System/Network Administrators will need to secure these new technologies against attack by unauthorized personnel. This need for enhanced protections brought about the field of cybersecurity. Cybersecurity is a rapidly evolving field where multiple system administrators must work together to monitor a network or networks of computers, and defend them from would-be attackers. This is not an easy task however, as networks are constantly evolving and adapting to the needs of a corporation. Not only are the networks constantly changing, the technologies and software implemented in these networks is in a constant state of change. A system administrator must make sure to keep the networked components up to date and secure from attackers.

These attackers are, in many cases, just as knowledgeable about computer systems as the administrators if not more so. The attackers will often use software packages to find holes in a system and exploit them to gain access or elevated privileges in a network.

Cybersecurity Tools

Table 1 below has a selection of hacking-tools that are commonly used by hackers and penetration testers. The table contains: the name of the tool, a brief description of the tool, website where the tool can be downloaded or purchased, how much the tool costs, and whether or not the tool is open-source (source code is available for download and modification). This table was compiled based on two lists of hacking tools; one by Concise Courses (Concise Courses,
2015) and the other by Abhishek Awasthi of TechWorm (Awasthi, 2015). This table is not an exhaustive collection of hacking tools, as it only shows a sample of tools that are the most well-known and commonly used.

<table>
<thead>
<tr>
<th>Tool Name</th>
<th>Description</th>
<th>Location</th>
<th>Cost</th>
<th>Open Source?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Mapper</td>
<td>Network discovery and security auditing tool. Scans a network and returns:</td>
<td><a href="https://nmap.org/">https://nmap.org/</a></td>
<td>Free</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>hosts, what OS they are using, services active, firewalls, etc...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metasploit</td>
<td>Vulnerability exploitation tool. Scans systems for vulnerabilities and then</td>
<td><a href="https://www.metasploit.com/">https://www.metasploit.com/</a></td>
<td>Free</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>launches attacks against them</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>personnel.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THC Hydra</td>
<td>Password cracking tool. Works against databases, email, LDAP, SSH, etc...</td>
<td><a href="https://www.thc.org/thc-hydra/">https://www.thc.org/thc-hydra/</a></td>
<td>Free; Word</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>lists and dictionaries may cost money</td>
<td></td>
<td>lists and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>dictionaries</td>
<td></td>
</tr>
<tr>
<td>John the Ripper</td>
<td>Password cracking tool. Specializes in dictionary attacks</td>
<td><a href="http://www.openwall.com/john/">http://www.openwall.com/john/</a></td>
<td>Free</td>
<td>Yes</td>
</tr>
<tr>
<td>Nessus Vulnerability Scanner</td>
<td>System vulnerability scanner. Scans systems for and displays system</td>
<td><a href="http://www.tenable.com/products/nessus/select-your-operating-system">http://www.tenable.com/products/nessus/select-your-operating-system</a></td>
<td>Free</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>vulnerabilities.</td>
<td></td>
<td>version available; Paid version available</td>
<td></td>
</tr>
<tr>
<td>Kali Linux</td>
<td>Penetration testing and security auditing Debian-based Linux distribution.</td>
<td><a href="https://www.kali.org/">https://www.kali.org/</a></td>
<td>Free</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Includes 600+ penetration testing tools.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Penetration Testers/Ethical Hackers (White-hat hackers), Black-hat hackers, and Gray-hat hackers commonly use these tools. Ethical Hackers, or White-hat hackers, are professional cybersecurity personnel who an organization provides legal authorization to utilize hacking techniques to help secure their network. Black-hat hackers are the criminal hackers that the news commonly discusses during data breaches. Black-hat hackers hack into networks for monetary gain, fame, protesting, and for the thrill. They perform the hacks without legal authorization from the organization. Grey-hat hackers are the middle ground in the hacking world. They will perform legal hacks to help a company or organization. However, they will also perform illegal hacks for the same reasons as Black-hat hackers (Kovacs, 2015).

System administrators must be able to identify suspicious traffic, block known attack methods, detect attacks, and compromised nodes (networked devices). Administrators then need to patch vulnerabilities, update systems, and make sure that nodes are not vulnerable to other exploits. Defender-side tools aid them. These include antivirus software, firewalls, system updates, and other detection systems. One of the most powerful tools they have is penetration testing. This is where the company will contract a white-hat hacker to attempt to break into the network. After they have completed the hack, the White-hat will then advise the system administrators on how to improve and further secure their network and computers (Kovacs, 2015).

Cybersecurity Failures

Network/System Administrators must constantly protect these networks against attackers who have just as much computer skill as the administrators, if not more. The attackers also only need to succeed in hacking the systems once. Administrators need to succeed in protecting the systems against all attacks, every time. A failure to succeed in any of the above tasks, at any
point, could result in the loss of confidentiality of data, the integrity of data and the availability of
data. This could lead to setbacks in projects, legal action, or potentially loss of life.

These kinds of failures on the part of administrators are all over the news in recent years. In 2007, T.J. Maxx and Marshalls announced that hackers had stolen 45.7+ million credit and
debit cards. At the time security specialists considered this to be the largest breach of customer
information. This hack occurred from January 2003 until June, 28 of 2004. Some of the data
stolen by hackers included driver’s license information (Perlroth, 2013). The size of this breach is
unknown due to the deletion of data as part of “the normal course of business between the time of
the breach and the time that TJX detected it (Jewell, 2007)” The experts would later update the
estimate of 45.7 million to be roughly 90 million (Perlroth, 2013).

In 2011, Sony was hacked 11 times from April to June of that year. The series of hacks
all started with a massive breach in Sony's PlayStation Network, which exposed over 100 million
user accounts (Lee, 2011). Hackers took this data when they circumvented Sony database security
and compromised the database. System administrators took PSN offline for several days during
this time to allow for a complete rebuild of the network and systems (Anthony, 2011). "'Other
hackers and hacking groups realized they could jump on the bandwagon and break into other
Sony properties and get in the news,'" said Richard Wang, manager of Sophos Labs, a security
vendor. "'Really anything that has the Sony brand on it has become a target for someone trying to
make a name for themselves or trying to prove they can break into the website' (Lee, 2011)". The
Sony hack is only one of numerous hacks in recent years, exposing personal data and credit
information.

In 2013, Target released information stating that hackers had stolen roughly 40 million
customer's data. This hack occurred between November 27th and December 15th. Cybersecurity
experts believe that hackers were able to steal the data due to a lack of data security and
monitoring. Dan Kaminsky, the chief scientist for the security consulting company known as
White ops, told reporters that “500 of the Fortune 500 are under constant attack. Nobody should be saying ‘I can’t believe Target got attacked’ because the reality is that everybody is getting attacked (Perlroth, 2013).”

A recent example of a major failure in cybersecurity measures is the U.S. Government’s Office of Personnel Management (OPM) breach. In June of 2015, OPM discovered that hackers had stolen the information of 21.5 million individuals. This information belonged to current, former, and prospective government employees and contractors. According to OPM estimates, 1.8 million of those individuals were the spouses or co-habitants of applicants. These 5.6 million included: fingerprints, personal information (Date of Birth, Social Security Numbers, Addresses, Foreign Travel, Health information, etc.), and/or interviews performed during background investigations. OPM, the Department of Homeland Security, and the FBI are currently working on implementing changes to the systems that will prevent further data breaches in the future. The government provided all individuals affected by this attack with three-years of identity theft protection from a private-sector identity protection organization (U.S. Office of Personnel Management [OPM], 2015a). The cost to OPM and the U.S. Department of Defense (DoD) will be roughly $133,263,550 (OPM, 2015b).

Another recent example of a major failure in cybersecurity measures is the Equifax breach. In September of 2017, Equifax reported that hackers had stolen the information of 143+ million American consumers. This information included social security numbers (SSN) and driver’s license numbers. Pamela Dixon, the executive director of the World Privacy Forum, told reporters, “If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent”. This breach occurred from mid-May to July when it Equifax discovered the breach on the 29th of July. Experts estimate that hackers also stole 209,000+ credit cards and 182,000+ dispute documents. Like the OPM breach, Equifax is offering everyone one
year of free credit protection through an Equifax service (Bernard, Hsu, Perlroth, & Lieber, 2017).

**Cybersecurity Curricula**

As shown above, cybersecurity is a complex and ever changing field with high stakes surrounding the success of operations. In order to keep up with these changes, teaching cybersecurity must use a dynamic and rapidly changing curriculum. This section will discuss the current trends within curricula development and IT jobs.

The complex nature of this field places an even greater burden upon the cybersecurity educators who have to create curricula that meet these needs. Since cybersecurity and information science is evolving so quickly, curricula are quickly becoming out of date. “Given the variety of possible IS career paths, the ‘unified’ IS curriculum may be outdated from the start” (Yen, Chen, Lee, & Koh, 2003). Yen et al explains some of the design logic that goes into creating a typical curriculum. They state that the typical curriculum contains a listing of the number of hours that should be devoted to each subject area. As highlighted above, this becomes problematic if universities do not update these courses and hour devotions often. If left unchecked, these classes can rapidly fall into outdatedness and become useless to the students taking them. Students graduating from an IS program should be able to function in an entry-level position and be able to continue their career development (Couger et al., 1995). This becomes less and less possible as courses teach fewer recent technologies and skills to these students. Part of the issue with this “education gap” (Todd, McKeen, & Gallupe, 1995), is that there is a divide between academics and professionals on what should be known. Employers further continue this issue by not always recruiting based on all of the skills required. Instead they choose to recruit based on a few “hard
skills” if in newspapers and interview the “soft skills”. They recruit differently in an online ad format with “soft skills” being emphasized more heavily and “hard skills” being interviewed for.

As time progresses, so do the number and array of skills required of graduates from an IS program. Studies have shown that more knowledge, skills, and abilities are being required of graduates than before (Gallivan, Truex, & Kvasny, 2004; Trauth, Farwell, & Lee, 1993; Leitheiser, 1992). Researchers examined this phenomenon in detail in a study that performed a content analysis of job advertisements in two different newspapers from different periods, 1988, 1995, and 2001. They found that for each job ad, there was an increase of ~1.2 skills per job listing across this period. This confirms prior findings that also state that employers are expecting workers to know greater numbers of skills (Gallivan, Truex, & Kvasny, 2004; Trauth, Farwell, & Lee, 1993; Leitheiser, 1992).

### Teaching Cybersecurity in a Modern Setting

The contemporary college instructor has to overcome the challenge of the always-connected student who has easy access to homework and lab exercises from previous semesters from sites like CourseHero (www.coursehero.com). In fact, this information is so easily accessible, and the millennial generation is so used to having it available that students may not realize that they are cheating by using these resources.

In order to combat this, instructors need to constantly change their assignments. These could either be one-off changes or complete rewrites of assignments. However, if the changes are not significant or frequent enough, students may be able to find the answers online. Another possibility would be to make multiple versions for a class, but this becomes a scalability issue for large class sizes. No matter what, creating these exercises increases the administrative overhead placed upon the instructor or learning design assistant to create these assignments.
Proposed System

The researcher proposes a system to resolve these issues. Table 2 below lays out the requirements required of this proposed system. This table displays requirement groups and any sub-requirements within the group. These sub-requirements truly define the system as envisioned by the design team.

Table 2. System Design Requirements

<table>
<thead>
<tr>
<th>Requirement Groups</th>
<th>Sub-Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Reduce Administrative Overhead</td>
<td>a) Automatically generate assignments&lt;br&gt;b) Automatically grade assignments&lt;br&gt;c) Minimize instructor required elements&lt;br&gt;d) No more difficult to create than a standard assignment</td>
</tr>
<tr>
<td>2. Modular Design</td>
<td>a) Capable of operating in varied cybersecurity environments&lt;br&gt;b) Capable of operating in outside domains&lt;br&gt;c) Integration with Learning Management Systems (LMS)</td>
</tr>
<tr>
<td>3. Tamper/Cheating Resistant</td>
<td>a) Capable of making meaningful modifications&lt;br&gt;b) Generation scheme is not predictable&lt;br&gt;c) Generation scheme can be easily and quickly modified</td>
</tr>
<tr>
<td>4. Customizable</td>
<td>a) Multiple attempts&lt;br&gt;b) Score file emailing&lt;br&gt;c) Challenge types can be changed</td>
</tr>
<tr>
<td>5. Separate Grading and Delivery</td>
<td>a) Two systems do not communicate&lt;br&gt;b) Non-random generation/grading system</td>
</tr>
<tr>
<td>6. Scalable</td>
<td>a) Usable in small class sizes&lt;br&gt;b) Usable in large class sizes</td>
</tr>
<tr>
<td>7. Minimal Cognition Impact</td>
<td>a) Cognitive workload&lt;br&gt;b) Situation Knowledge&lt;br&gt;c) Perceived Situational Awareness</td>
</tr>
</tbody>
</table>

The first requirement grouping states that the proposed system shall reduce administrative overhead. This defines that assignments shall be automatically generated and graded automatically. This shall require as minimal instructor-required elements as possible and shall be no more difficult and time consuming to create than standard assignments.
The second requirement grouping states that the proposed system shall be modular in its design. This means that the system shall be capable of operating in varied cybersecurity environments. These varied environments shall at a minimum be networking, steganography, and encryption/encoding. This system shall also be capable of operating in outside domains. This includes domains such as statistics, mathematics, decision theory, etc. The system shall also be capable of integration with an LMS. This integration shall be in one of three forms: delivery, grading, gradebook integration. Delivery integration means that the LMS shall utilize the created system to create the assignment and deliver it to user. Grading integration means that the LMS shall take the answer input from the user and grade it using the created system. Gradebook integration means that the created system will be capable of sending a grade file to the LMS which will update its gradebook.

The third requirement grouping states that the system shall be tamper and cheating resistant. This defines that the system shall be capable of a generation scheme that is easily modifiable, capable of meaningful assignment modifications, and not predictable. By making the generation scheme easily modifiable, we ensure that even if a set of answers are made available on a site like CourseHero, the assignments can be regenerated making the answers inaccurate. We further this by requiring that the system be capable of making meaningful changes to an assignment. These changes shall be enough to make each assignment identifiably different from other assignments generated. This generation shall also not be predictable even if someone were to determine the generation scheme that the system uses.

The fourth requirement grouping states that the system shall be customizable. This defines that the system shall support multiple attempts for assignments, emailing score files to numerous email addresses, and challenge types shall also be customizable. Emailing a grade file to an instructor and TAs is useful in instances where there are open ended responses that the system cannot grade by itself or when the instructor maintains a gradebook separate from an
LMS. This is set forth so that instructors can customize their version of the system to meet their specific needs, be it for one assignment, a class, or a set of classes. It also means that the instructor does not need multiple systems to accomplish a set of tasks.

The fifth requirement grouping states that the system shall separate the grading and delivery systems. This defines that the system shall not require the delivery and grading systems will not need to communicate. In order to do this, the system should not operate on a random number generator. The issue with random number generators is that we would need to keep track of what random number the system gave to the student. Therefore, if the generation of an exercise takes place on a system that cannot communicate with the grading system, there is no way for the two systems to synchronize the numbers. Even if the systems could communicate, we would have to record what number was given for each student so we can regenerate that assignment later if need be. This requirement is necessary for environments where internet connectivity is not possible such as a cybersecurity environment. Instructors have to deploy numerous cybersecurity assignments in a closed-world system such as a virtual machine (VM). This is due to courses teaching students hacking techniques, malware analysis, code reverse engineering, and other concepts that students cannot perform on an open-world system.

The sixth requirement grouping states that the system shall be scalable. This defines that an instructor can deploy the system in classes of various sizes both small and large. This requirement feeds into the modularity requirement stated above, in that the design must be flexible.

The seventh requirement grouping states that the system shall have minimal cognition impact on users. This defines that a given exercise deployed within this tool shall be no harder or cognitively demanding than a traditionally delivered assignment. We measure this using cognitive workload and situational awareness techniques.
Research Questions

There are two research questions addressed in this thesis. The first research question seeks to determine the feasibility of creating a system that meets the requirements, discusses above in Table 2, placed upon such homework and laboratory assignment generation system. The second research question seeks to understand what effects such a system would have on a subject’s cognitive workload and situational awareness (SA) within the cybersecurity domain.

RQ1: Is it possible to design a system that meets the set design requirements in an extendable and sustainable manner?

RQ2: What impact would such a system have on the cognitive workload and SA of subjects during a cybersecurity homework/laboratory assignment?

The research activity in this thesis explores this research question in an attempt to provide an understanding of how instructors can apply this new tool to cybersecurity education. It also will explore what potential design changes we need to make in order to improve the system. We explored these issues through the use of a human subjects experiment.

Contributions of this Thesis

The contributions in this thesis are in three categories: 1) Literature Reviews; 2) System Development; and 3) Human Subjects Experiment. Table 3 below summarizes each of the contributions of this thesis.
The literature review in Chapter 2 reviews challenge based learning and virtual lab usage as used in cybersecurity education. We will take a look at issues inherent in the usage of these tools as they relate to the proposed system design. This chapter also discusses the situation awareness literature to determine what situation awareness is and how researchers can measure SA. This section goes on to discuss these measurement techniques in order to determine which techniques work best for examining the impact that the proposed system has on human subjects.

Chapter 3 describes the system built to fulfill the aforementioned design requirements. This system, known as the Polymorphic Homework and Laboratory System, also known as PolyLab, already has several use-cases built, but we will focus on the networking use-case for the system. Chapter 4 presents the design of the human subjects experiment designed to test the impact of PolyLab on human cognition. Chapter 4 concludes with the presentation of the results and conclusions from this experiment.

Chapter 5 provides a discussion on the important findings in this research study. This chapter presents an assessment of the contributions and limitations of this study. This thesis and chapter end with a look at future work involving PolyLab and CBL.
Summary

Cybersecurity is a complex and ever-changing field that presents unique problems for system and network administrators. Failure at any point in the efforts of system and network administrators can lead to disastrous consequences for their company and customers. This places a heavy burden upon curricula writers and educators to make sure that future system and network administrators are prepared to face these operating conditions upon graduation.

This thesis presents a tool developed in an attempt to ease the burden of the educator and curricula writer. We discussed several design requirements for this tool. This thesis sought to determine whether or not we can design a system that meets these design requirements. We also ran an experiment to determine the effect that the designed system would have on the cognition of human subjects.
Chapter 2

Review of Related Literature

This chapter outlines two technology domains that have significant promise and potential for solving the issues of teaching cybersecurity. The first domain is challenge based learning and virtual labs. These provide students with hands on experience with cybersecurity concepts that they will utilize in their future careers. The second domain is situational awareness. This domain will allow us to test proposed systems to determine their value in a classroom environment.

Review of Challenge-Based Learning and Virtual Labs in Cybersecurity Education

In cybersecurity education, a common method for teaching students is the Challenge-Based Learning (CBL) methodology (Cheung, Cohen, Lo, & Elia, 2011). CBL methodology requires participants, in this case students, to draw on prior knowledge, creativity, and their fellow team members. This methodology is most commonly implemented through the use of modules or lab assignments. These modules or lab assignments are incredibly useful to students as they apply the book and lecture knowledge to a simulated representation of the real-world. These labs commonly walk students through a very detailed step-by-step set of instructions on completing some technical task. These instructions and data-sets/machines require a high amount of administrative overhead to create and maintain. In order to resolve this, instructors and colleges have recently started implementing these through the use of Virtual Machines (VMs).

Many researchers have developed or studied the use of VMs in cybersecurity education (Micco & Rossman, 2002; Wang, Hembroff, & Yedica, 2010; Willems & Meinel, 2012). One of the main benefits of VMs is that server administrators can reset the systems at the end of the
exercises. This rollback of a VM instance means that each user gets a fresh and unaltered copy of the machine(s). VM labs contain real operating systems, software, tools, and realistic configurations. These VM setups require a substantial amount of processor, memory, and network capabilities. Scalability and administrative overhead are huge issues with VM setups as setting up a new VM requires time and more resources. These labs operate using the principles of CBL labs. Participants load up the VM through a web-based or host-based client thus creating a VM instance that they will utilize until the VM is powered-off. Once the participant logs in, they can perform whatever tasks that the lab requires of them. Schools, universities, and companies commonly utilize this setup to teach concepts and techniques in a controlled environment. These labs are typically very straightforward and provide step-by-step instructions. Upon completion of these labs, participants will shut down the VM and all changes are wiped away so that the VM can be utilized again as if the lab had never been performed. An example of these are the A+ and Linux + labs provided by Computer Technology Industry Association (CompTIA) (https://www.comptia.org/). The A+ labs teach users about troubleshooting and a wide range of networking and operating systems based issues. The Linux+ labs focus in on the Linux environment and provide a similar purpose as the A+ labs. These labs, while somewhat basic, are able to take anyone and teach them how to do troubleshooting and learn about the operating systems covered in the labs. The biggest issue with labs of this type is that there are few of them and repeatability is lacking given the provided VMs. While participants get the hands-on knowledge provided by these labs, they are not able to do it multiple times with different parameters easily.

One of the major problems with VM CBL, as discussed in the paper entitled: Online assessment for hands-on cyber security training in a virtual lab, is that each student gets the same system and same machine (Willems & Meinel, 2012). Therefore the risk of cheating is increased, as each answer is the same across the entire class or training group. This is a common problem
with traditional VM CBL labs as well as many web-based cybersecurity labs such as: Bandit by OverTheWire (http://overthewire.org/wargames/bandit/), National Cyber League (https://www.nationalcyberleague.org/), National Cyber Analyst Challenge (https://cyberanalystchallenge.org/), CyberPatriot (http://www.uscyberpatriot.org/), and Capture the Flag competitions to name a few. These competitions and labs often have only one answer per question. Therefore, when a participant becomes unsure of what a question is asking or is unsure of an answer, they can easily search online for the question. This search will commonly bring up a copy of the entire lab or competition with all of the answers to the questions provided. They are then able to copy the answers and input them as their own. Not only is this cheating it means that the participant did not learn anything from the lab, since they will often not understand the answer they copied.

Bandit by OverTheWire is a good example of this process. Bandit by OverTheWire teaches participants about the Linux command line and commonly utilized commands. Bandit is currently organized into a series of 28 levels (Level 0 – Level 27). Each level relies on the participant having completed the prior level since the password for each subsequent level is found in the level prior to it. However, once one participant has completed the 28 levels, they can publish their answers on the web for anyone to find. A quick search for “bandit overthewire solutions” brings up several results that contain anywhere from basic answers to detailed walkthroughs for the levels. In order to combat this, OverTheWire has changed the solutions several times, but is unable to prevent someone from posting the answers to the new challenges.

cover encoding schemes such as: BASE32, Binary encoded ASCII, Morse Code, and different alphabets. They also include some very basic MD5 encryption challenges. The steganography challenges cover a wide array of steganography techniques. The Enumeration & Exploitation category contains challenges based around code hacking. These challenges involve looking at source code and determining the vulnerabilities within it in order to break the code. The Log Analysis category involves looking at log files for various services, some standard and some less so, to determine what is happening with those services. The Network Traffic Analysis category involves determining what data is being transmitted across a network (passwords, SSNs, etc). The data transmitted across the network utilizes standard protocols, some obscure protocols, and some custom built protocols. The Open Source Intelligence category contains challenges that are based on cybersecurity knowledge and basic HTML knowledge. These are somewhat standard trivia type questions. The Scanning and Reconnaissance category deals with scanning a live system. This involves determining vulnerabilities and exploiting them to garner information from the system. The Password Cracking category involves breaking a series of passwords that range in complexity from simple to very complex. These require participants to utilize brute force and dictionary attack methods to break the passwords. Often, one of the challenges will require participants to build their own dictionary with which to break a set of passwords. The Wireless Access Exploitation category involves analyzing pcaps from wireless networks to determine SSIDs, Passwords, and other data being sent across a wireless network.

Willems and Meinel propose a solution to this issue; this involves dynamically choosing several values from a pre-set list and using them as evaluation answers. These evaluation answers are also used to dynamically generate content in the lab. The system also chooses a number of other values from the list to fill the incorrect options (Willems & Meinel, 2012). This solution works quite well for a small scale assignment or lab. However, it does not eliminate the possibility of cheating as there are a limited number of possible solutions. If this system were to
be used in a larger environment or eliminate the chance of cheating, it would require a large amount of effort from the evaluator to create additional solutions. It would also add a substantial amount of administrative overhead in the form of grading. Anything more than a few variations would become complicated to keep track of for grading. It would also potentially cause issues for assisting participants with issues since an instructor would need to keep track of who got what variation.

The gap in the literature here is based on the need for a system that can deliver CBL labs that are cheating resistant if not impervious. Given infinite resources, instructors could manually create labs for each participant. The problem with this becomes the amount of administrative overhead with the manual generation of these labs. A system could be created that implements the system proposed by Willems and Meinel. This system would generate all of the labs for the instructor and all the instructor would need to do is create the pre-set list of evaluation answers. The issue here again becomes administrative overhead. This time the administrative overhead comes in the form of grading all of these labs and creating enough evaluation answers to make the labs unique. Based on this, a system is needed that can generate CBL labs automatically and grade them automatically while being cheating resistant/impervious, scalable, and not increasing administrative overhead.

**Review of Situational Awareness Literature**

“Situation awareness (SA) is a human cognitive capability that becomes more important in complex work environments, especially where low frequency/high risk events take place” (Giacobe, 2013b). Traditionally this was most important in the military, aircraft piloting, and bank security. However, recently situational awareness has been shown to be important in cybersecurity situations. This is due to the high risk environment that administrators work in.
While it is unlikely that a network will be attacked, if the network is breached there is great potential for severe repercussions.

We are utilizing situational awareness in this thesis as a means to measure the cognitive workload, situational awareness, and impact of proposed systems on users. Since we can modify these metrics to meet our needs we can then use them to test out systems. These metrics will help us to determine what impact the system has and to use these metrics to determine modifications for our systems.

Endsley describes situation awareness in three levels: Perception, Comprehension, and Projection (Endsley, 1988a). Perception is where a subject takes in information from their surroundings. Comprehension is the understanding and processing of this perceived information. Finally, projection is where the subject predicts what will occur in a given time frame based on the perceived and comprehended information (Zhang, Huang, Guo, & Zhu, 2011). Our classes largely focus on L1 and L2 situation awareness for the introductory classes. This allows students to focus on learning the basic concepts. Later classes will start to focus on L3 as L3 is important in the job environment, but this is less commonly discussed in classes.

The three step process described in the previous paragraph is a simplified version of this process. Figure 1 below further breaks the process down further. This model was initially described in terms of a military pilot (Endsley, 1988a; Endsley, 1988b). Here we will be explaining it in cybersecurity terms. An administrator sees some element in the environment (e.g. alert data, warning light, report from analyst, etc.). They then process this information about the environment to find understanding about the situation. This understanding is then used to predict what will occur next. This entire three step process is affected by what their knowledge, training, workload, objectives, and tasking is. Out of this, the administrator makes a decision, again affected by their workload, training, tasking, etc. They then perform what is required by that
decision. These actions then prompt feedback by the environment, which is perceived, understood, and used to predict future events to make decisions.

As one can surmise, and as noted by Wickens (1984) and Fracker (1987), this process puts a huge strain on system administrators. This is further compounded by the amount of data that must be reviewed by system administrators, as each piece of information must be compared against prior knowledge. As more information comes in the workload increases, adding strain to the subject thus decreasing ability, resulting in poor decisions and an inability to perform the actions required by those decisions.

Giacobe brings up a point that many are creating tools to improve situational awareness. However, few of these developers are measuring the change in situational awareness to determine the effectiveness of their tool (Giacobe, 2013a). Therefore, if a tool that is created to improve situational awareness and was tested to see if it succeeded, the tool would be even more valuable.

Giacobe describes a methodology that can be used to test the effectiveness of a tool in its attempt to improve situational awareness of subjects. This methodology involves utilizing

---

**Figure 1. Situational Awareness Model (Endsley, 1988a; Endsley, 1988b)**

As one can surmise, and as noted by Wickens (1984) and Fracker (1987), this process puts a huge strain on system administrators. This is further compounded by the amount of data that must be reviewed by system administrators, as each piece of information must be compared against prior knowledge. As more information comes in the workload increases, adding strain to the subject thus decreasing ability, resulting in poor decisions and an inability to perform the actions required by those decisions.

Giacobe brings up a point that many are creating tools to improve situational awareness. However, few of these developers are measuring the change in situational awareness to determine the effectiveness of their tool (Giacobe, 2013a). Therefore, if a tool that is created to improve situational awareness and was tested to see if it succeeded, the tool would be even more valuable.

Giacobe describes a methodology that can be used to test the effectiveness of a tool in its attempt to improve situational awareness of subjects. This methodology involves utilizing
multiple methods for cognitive assessment. In order to effectively measure a complex phenomenon as situational awareness, a researcher must compromise between time needed to complete and realism to the original subject matter. This need is exaggerated if non-experts are utilized as subjects in the study. This methodology takes two groups of people a control and an experimental group and subjecting them to a simulation of a network environment. Both groups are given the same data; just the display method is changed. The participants are then asked to answer several questions at different times during the simulation. These questions measured the perceived situational awareness of participants, perceived workload, and task efficiency. These were measured using the freeze-probe and post-trial techniques (Giacobe, 2013a).

The freeze-probe technique, an example being Endsley’s Situational Awareness Global Assessment Technique (SAGAT), requires that the simulation be frozen so that the subject can answer a series of questions about his/her SA. While this method does stop the simulation in the middle, it allows for "snapshots" of the current situational awareness of a participant. The biggest criticism of SAGAT and freeze-probe techniques is that they rely on memory and may not be an accurate reflection of a subject’s SA. However, the questions are provided immediately after the scenario begins which lasts only a few minutes (Endsley, Selcon, Hardmian, & Croft, 1998). This prevents the issues that go hand in hand with memory degradation (Endsley, 1988b). Questions can be developed to assess the three levels of SA Perception, Comprehension, and Projection (Endsley, 1988a). An example of a Perception (L1) question would be something like “What port is X service using in the network”. An example of a Comprehension (L2) question would be something like “Why did the host communicate with the server the way it did”. An example of Projection (L3) would be something like “If this firewall rule were applied, how would that effect the network traffic”.

The post-trial technique, like what is used in SART (Taylor, 1990), measures a subjects SA and workload after the trial has been completed. This allows for a continuous trial without the
issue of stopping a trial for evaluation. You also do not have the issue of potentially giving hints about what is being looked for by the researcher. Giacobe (2013b) noted that aside from SART, these tools are not particularly useful outside of their specific field. SART is used in a variety of domains, likely due to its simplicity of setup and use. However, as noted by Endsley et al (1998), the post-trial technique may actually be measuring performance of a task and not actual workloads and SA. Another issue with this technique is that you have to deal with potential memory degradation.

Giacobe (2013b) proposes a combination of SAGAT (Endsley, 1988b) and SART (Taylor, 1990). These tools will be utilized in tandem with NASA-TLX (Hart & Staveland, 1988) to measure cognitive load, and HPSM (Human Performance Scoring Model) (Wellens & Ergener, 1988) to evaluate speed and accuracy of participant responses. HPSM is useful for measuring how quickly and accurately each question was answered in a scenario. This requires a system in place to time each question from delivery to submission. All of these methods, modified for the cyber-domain, combined will assess more aspects of a subject's SA than any one individually could. They will also negate potential measurement errors introduced by any one method.

Based on the discussed SA literature, we believe that SAGAT, SART, and NASA-TLX will yield the best assessment. SAGAT will be useful in determining a participant's understanding of the scenarios presented to them in the study. SART will be useful in measuring how participants feel about what they know about a situation. This includes things like familiarity, complexity, attention division and so on. NASA-TLX will enable us to measure the cognitive workload of participants. This will allow us to determine if participants think that one of the mechanisms is considered to be harder than the other. The issue with both SART and NASA-TLX is that they are self-reported metrics. This may lead to issues of reliability. We will be utilizing part of HPSM for this study. We do not have a system in place to time each question from delivery to submission as our system delivers all questions in one form. We will instead be
timing each subject’s time from scenario delivery to scenario submission and using that to help ascertain performance. Our goal is to find that SA and cognitive workload are not negatively impacted by which group the participants are in.
Chapter 3

PolyLab System Development

This chapter discusses the development of the PolyLab system. We will discuss the concepts behind how PolyLab works and will show a few simple proofs of concept that illustrate the operation of these theoretical concepts. We will then discuss how we have applied these theoretical concepts to the general idea of PolyLab. Next, we will discuss a few use cases that we have developed and deployed. The use cases that we will discuss are: PolyStego, PolyEncrypt, and PolyNet. PolyStego is a system that creates steganography exercises to aid in teaching basic data forensics. PolyEncrypt is a system that creates encoding and encryption exercises to teach students to recognize these and how to break them. PolyNet is a system that teaches students about basic network communications. We will give more attention to PolyNet as it is the basis for the study discussed later in Chapter 4.

Concepts Behind PolyLab

PolyLab utilizes hash algorithms such as MD5 (Rivest, 1992) or SHA-1 (Eastlake 3rd & Jones, 2001) to generate pseudo-randomness in the questions presented to students and to be used to select parameters. These algorithms take any amount of input data and generate a unique fixed-length output. PolyLab uses this value to generate the input parameters for the assignment. The instructor selects parts of this value to use as parameters and places them in the assignment’s template. For a simple example, the first digits of the hash could be the first value for problem #1. The second digits would be the value for problem #2, and so on. The instructor chooses the ordering and selection of the parameters when they create this prototype assignment. The
individual assignment generator uses these selections to fabricate the individual assignment when the student requests it. Figure 2 below illustrates this process.

![Diagram of assignment generation process](image)

**Figure 2. Prototype assignment and generation example (Kohler, Santoro, & Giacobe, 2017)**

PolyLab utilizes the random-looking bits of the hash to generate the assignment for the student, who completes the work offline. Depending on the academic domain, the work could be calculations such as in math, the IP address, or other values in a network security lab, or the parameters of a statistics question in a problem set. Additionally, we can also use the hash value as an index in an array to select an appropriate value from a list of values (names, words, concepts, etc.). The answers to the questions are based on a template, designed by the instructor. Since the hash value is deterministic, we can reproduce it to assess the student’s answer without needing to record and keep track of the pseudo-random value presented to the participant.

In the field of cybersecurity, we often create exercises for the students to complete in an online virtual computer lab. To date, most assessment is limited to either evaluation of screen captures (as proof of completion) or to report a secret code embedded in the task. However, these values or screen captures tempt students to cheat by sharing their answers with others. PolyLab addresses this by creating versions of the assignment with parameters individualized for each student. Since the hash value is unique per student, another student cannot use the same answers.
When the student turns in the assignment, the assessment side of PolyLab re-creates the same hash value utilizes those bits in the order designated by the instructor and creates the answer key. Due to PolyLab using hashes, an instructor does not need to couple the creation of the lab exercise and the evaluation of the answers. In PolyLab, we can disconnect the exercise creation from the evaluation.

This is a critical difference between PolyLab and other randomly chosen parameters. In a truly random question set, some system would have to keep track of which random question the system gave to the individual student, which answer they gave, and then record whether that answer was right or wrong. However, in virtual lab and other complex environments, we often cannot connect the creation and validation components because they are on different systems, sometimes intentionally separated (as in air-gapped networks for cybersecurity education).

PolyLab connects assignment creation and evaluation using hashes using the same hash function and input values (for example username and assignment password). Therefore, PolyLab overcomes the problem of linkages to assessment when the lab exercise must be completed in a space that cannot be connected to the public Internet, LMS, or the Grading System. Instead we can easily re-create the hash value in both systems to link them together without requiring the systems to be able to communicate with each other. In short, PolyLab’s assessment engine will know what questions “abc1234@psu.edu” SHOULD HAVE RECEIVED, and therefore would know what the correct answers SHOULD BE for a given student.

**Operation of PolyLab**

Our initial implementation of PolyLab is coded in python to take hash values to create a problem or question. This system uses partial and full hash segments for this problem generation.
These hash segments can then be used as embedded items, list selection devices, or to generate pseudo-random values.

The system generates these hashes by taking a student’s email address/username and a predetermined password to form a hash. Now that we have this hash, we can create lots of values and items with it as discussed below. Figure 3 below shows this process.

![Figure 3. Hash Generation (Giacobe & Kohler, 2016)](image)

We can convert each of these values from hex to decimal to generate a set of numbers from 0 to 16. We can then use these numbers to make math problems, IP addresses, MAC addresses, etc.

These hashes can be changed/re-generated very easily by changing the password (for example by changing the password for each section or semester). This allows for remaking the assignment very easily. The hash can also change daily by adding the date to the hash generation scheme. This would allow for the assignment to change every day (See Figure 4). The assignments can also be set to change on attempt count. All of these mechanisms allow for an increased attempts and for ease of assignment generation by the instructor.
Day 1: $\text{MD5('nxg13' + 'password1' + '2018-03-25')} = \text{adc2ec2dad7ded71334381b5e54c7f5c}$

Day 2: $\text{MD5('nxg13' + 'password1' + '2018-03-26')} = \text{a58e7d1beabaa14a6636403d8424151}$

Day 3: $\text{MD5('nxg13' + 'password1' + '2018-03-27')} = \text{c347c146f93d7591c1316af362da1a4f}$

Figure 4. Hash generation with date included

PolyLab deploys and hosts all of this information using a python package known as CherryPy. This package is capable of deploying python as a web application through a python webserver. This allows for minimal extra coding and less hassle for web programmers.

**PolyStego**

PolyStego was one of the first implementations of the assignment generation system that became the PolyLab system. PolyStego takes full hash segments and places them as Easter eggs within an image. For the purposes of this thesis we use Easter egg to mean a hidden chunk of data within some other chunk of data. These exercises are to aid students in understanding steganography and some basic cipher/encryption systems. This activity contained five exercises. Some activities required students to find Easter eggs in the metadata of the files and others required use of ciphers. Table 4 below shows the challenge number and a brief description about each challenge.
<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stego Challenge 1</td>
<td>There is a hidden message somewhere in the metadata for this file. I wonder where this picture was taken??</td>
</tr>
<tr>
<td>Stego Challenge 2</td>
<td>My friend Julius sent me this encrypted image file. He says it's a JPG, but I don't know what he did to encrypt it.</td>
</tr>
<tr>
<td>Stego Challenge 3</td>
<td>This challenge requires you to find the hidden secret message in this image. Hint: Nothing is as it appears. The secret message is hidden in plain sight.</td>
</tr>
<tr>
<td>Stego Challenge 4</td>
<td>You have been contracted by local law enforcement to help. They recovered this image file from a suspect's computer. The secret message is embedded in this file somehow. It also appears that there is some kind of data corruption in the file itself. See if you can figure out how to fix the image file and recover the secret message.</td>
</tr>
<tr>
<td>Stego Challenge 5</td>
<td>You have been asked to help law enforcement with a different case. In this case, the accused is known to use the Linux Operating System and the program steghide has been found on the system. I wonder if he bothered using a password on his files...</td>
</tr>
</tbody>
</table>

One of the challenges required students to find the code “hidden in plain sight”. Students would open the file and see a solid colored image as shown in Figure 5. Upon opening it in an image editor, they should realize that the image is not monochromatic – that is, that the image is not just one color. When the participant floods the background with another color, they see the “secret message” was in a similar, but not exact color. This allows the participant to discover the code, as shown in Figure 6.
Figure 5. Steganography Exercise "hidden in plain sight" (Giacobe & Kohler, 2016)

Congratulations.
You found the secret message
Your Secret Code is
ce86f0c0208c45f6f29c35bf7ecf7a14

Figure 6. Steganography Exercise Solved (Giacobe & Kohler, 2016)
The administrative overhead with creating these kinds of challenges is that we need to fabricate an image with a secret code in it. Once participants know the secret code, they tend to brag about their findings, making that exact secret code no longer usable in future iterations. PolyStego addresses this problem by creating a unique image for every participant. Each person gets their own secret code, an example of a full hash segment. Additionally, we utilized the first several bytes of the hash value to decide which color to make the image, an example of a partial hash segment. In this case, the red value is CE, Green is 86 and Blue is F0, making the purple color seen above in Figure 5 for the background color. We select one of these values and add/subtract 5 to it and use this value for the foreground (text) color, so that it is different, but close enough to the human eye to not appear to be different. Figure 7 and Figure 8 below illustrate that changing the inputs create a vastly different steganography image for students to analyze. These inputs could be userid, email address, or instructor specified components (ie: password, date, etc.).

Figure 7. Another user’s stego exercise
PolyEncrypt

PolyEncrypt was another of the initial assignment generation systems within the PolyLab system. PolyEncrypt helps to teach students about basic encoding schemes and encryption mechanisms. As with PolyStego, PolyEncrypt creates a repeatable unique problem set for each individual student. This allows them to learn what the different encoding and encryption types look like. By knowing the appearance of these data types, students will be more equipped to perform data forensics tasks.

The system utilizes partial hash segments to select items from a list. PolyEncrypt uses a list of 64 first names, 64 last names, and 64 fruits utilized as part of the password. In order to
select the first name, we take six bits from the hash and convert that to decimal, which gives us an index from 0 to 63. We then pick that item from the list of names to use. We repeat this process two more times for the last name and fruit. We then take the next 3 bytes from the hash to create a number between 0 and 4095. The system then uses these items to form first name, last name, and a password. The system then generates a number using hash segments and tacked onto the end of the password. Figure 9 shows an example of this. This password is then encoded/encrypted using a variety of mechanisms. This system would give a student who logs in a series of usernames and passwords for them to determine the plaintext password for that user. Figure 10 below shows an example of this delivery page.
<table>
<thead>
<tr>
<th>Hex</th>
<th>Decimal</th>
<th>First Name</th>
<th>Last Name</th>
<th>Fruit</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
<td>Adam</td>
<td>Anderson</td>
<td>Apple</td>
</tr>
<tr>
<td>01</td>
<td>1</td>
<td>Andrew</td>
<td>Arnold</td>
<td>Apricot</td>
</tr>
<tr>
<td>02</td>
<td>2</td>
<td>Anne</td>
<td>Avery</td>
<td>Avocado</td>
</tr>
<tr>
<td>03</td>
<td>3</td>
<td>Bella</td>
<td>Ball</td>
<td>Banano</td>
</tr>
<tr>
<td>04</td>
<td>4</td>
<td>Blake</td>
<td>Bell</td>
<td>Bilberry</td>
</tr>
<tr>
<td>05</td>
<td>5</td>
<td>Brian</td>
<td>Berry</td>
<td>Blackberry</td>
</tr>
<tr>
<td>06</td>
<td>6</td>
<td>Cameron</td>
<td>Black</td>
<td>Blackcurrant</td>
</tr>
<tr>
<td>07</td>
<td>7</td>
<td>Charles</td>
<td>Butler</td>
<td>Blueberry</td>
</tr>
<tr>
<td>08</td>
<td>8</td>
<td>Connor</td>
<td>Campbell</td>
<td>Boysenberry</td>
</tr>
<tr>
<td>09</td>
<td>9</td>
<td>Dan</td>
<td>Chapman</td>
<td>Currant</td>
</tr>
<tr>
<td>0A</td>
<td>10</td>
<td>David</td>
<td>Clarkson</td>
<td>Cherry</td>
</tr>
<tr>
<td>0B</td>
<td>11</td>
<td>Elizabeth</td>
<td>Davidson</td>
<td>Cloudberry</td>
</tr>
<tr>
<td>0C</td>
<td>12</td>
<td>Emma</td>
<td>Davies</td>
<td>Coconut</td>
</tr>
</tbody>
</table>

03 = Bella

0C = Davies

09 = Currant

520 = 1312

Username: Bella Davies

Password: Currant1312

Figure 9. PolyEncrypt username & password generation example
Figure 10. PolyEncrypt Delivery System

PolyEncrypt utilizes encryption and encoding techniques to “hide” the password. This system utilizes: Binary, Hexadecimal encoded ASCII, BASE32, and BASE64 as its encoding schemes. The system utilizes Rot13 and Rot47 as its encryption schemes. We will start out discussion below with the encoding schemes and move to the encryption schemes. We will also

<table>
<thead>
<tr>
<th>Encrypt Challenge 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Peter Vaughan</td>
<td>Password: Wwhor1142</td>
</tr>
<tr>
<td>Username: Lily Ince</td>
<td>Password: Wnohgvpon2662</td>
</tr>
<tr>
<td>Username: Karen Ince</td>
<td>Password: Xvjselv2453</td>
</tr>
<tr>
<td>Username: Natalie Harris</td>
<td>Password: Znaqnevar3244</td>
</tr>
<tr>
<td>Username: Peter Sanderson</td>
<td>Password: Pnyaehcr1474</td>
</tr>
<tr>
<td>Username: Sally Campbell</td>
<td>Password: Penaoreel1420</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encrypt Challenge 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Jack Simpson</td>
<td>Password: vC2A6hgc</td>
</tr>
<tr>
<td>Username: Steven Lyman</td>
<td>Password: rC2i36CCJ`edd</td>
</tr>
<tr>
<td>Username: Lily Kelly</td>
<td>Password: r96CC3aecc</td>
</tr>
<tr>
<td>Username: Jake Butler</td>
<td>Password: l62C`fe</td>
</tr>
<tr>
<td>Username: Phil Arnold</td>
<td>Password: u:8aaac</td>
</tr>
<tr>
<td>Username: Phil Bali</td>
<td>Password: l6CD:&gt;&gt;@`ggg</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encrypt Challenge 3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Lisa MacDonald</td>
<td>Password: SHVja2xIYmVycnmxMTE5</td>
</tr>
<tr>
<td>Username: Jessica Vaughan</td>
<td>Password: SmFidXRPV2FiyTI4Mjg=</td>
</tr>
<tr>
<td>Username: Bella Sanderson</td>
<td>Password: TGltZTE4NzU=</td>
</tr>
<tr>
<td>Username: Jake Ellison</td>
<td>Password: TWFuZ28zNTgw</td>
</tr>
</tbody>
</table>
go over brief examples for the lesser known ones. Table 5 below contains a list and description for each of the challenges contained within PolyEncrypt.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt Challenge 1</td>
<td>This challenge utilizes Rot13 to encrypt the user’s passwords.</td>
</tr>
<tr>
<td>Encrypt Challenge 2</td>
<td>This challenge utilizes Rot47 to encrypt the user’s passwords.</td>
</tr>
<tr>
<td>Encrypt Challenge 3</td>
<td>This challenge utilizes BASE64 to encode the user’s passwords.</td>
</tr>
<tr>
<td>Encrypt Challenge 4</td>
<td>This challenge utilizes BASE32 to encode the user’s passwords.</td>
</tr>
<tr>
<td>Encrypt Challenge 5</td>
<td>This challenge utilizes Hexadecimal encoded ASCII to encode the user’s passwords.</td>
</tr>
<tr>
<td>Encrypt Challenge 6</td>
<td>This challenge utilizes Binary encoded ASCII to encode the user’s passwords.</td>
</tr>
<tr>
<td>Encrypt Challenge 7</td>
<td>This challenge mimics the format of a Linux Shadow File.</td>
</tr>
</tbody>
</table>

Our first encoding scheme is Binary. Binary contains two states. These states are a 1 and a 0. By stringing them together we are able to represent numbers, symbols, letters, and certain other codes. Information systems utilize Binary as the most basic encoding scheme for data. This encoding scheme is one of the easiest to recognize as it only contains 1s and 0s. This encoding scheme takes the ASCII password and encodes the password into ASCII encoded binary.

Our second encoding scheme is Hexadecimal encoded American Standard Code for Information Interchange (ASCII). ASCII contains 128 characters, 10 are numbers, 26 are lower case letters, 26 are upper case letters, 33 are symbols, and 33 control characters (Mackenzie, 1980). The problem with ASCII is that it has a limited set of characters that it can display. This makes ASCII unusable for complex math, foreign language, programming, etc. In order to solve this problem, researchers and industry created Extended ASCII and Unicode. These encoding schemes allowed for a greater character set which could accommodate these additional requirements. However, for the purposes of our exercise ASCII works well enough, since we do
not need to display any of these additional characters. Once we have our ASCII text, we convert to hexadecimal and display if for the students. This coding scheme can be difficult to recognize at first as it looks similar to Base64 and possibly Base32 if displayed with capital letters. However, if you look closely enough at Hex encoded ASCII you will see that the letters only go to F. Once you notice this, hexadecimal is fairly easily recognized. Figure 11 is an example of Hexadecimal encoded ASCII, using the string “Institute for Electrical and Electronics Engineers” as the base text.

```
49 6e 73 74 69 74 75 74 65 20 66 6f 72 20 45 6c 65 63 74 72 69 63 61 6c 20 61 6e 64 20 45 6c 65 63 74 72 6f 6e 69 63 73 20 45 6e 67 69 6e 65 65 72 73
```

**Figure 11. Hex as ASCII**

Our third encoding scheme is Base32. This encoding scheme uses a 32-character set for its encoding. This character set is the numbers 2-7, and all upper-case letters. Base32 also includes the equals sign (=) as a means of padding data to the length of 8 encoded characters. One of the best ways to recognize Base32 is to look for equals signs at the end. This narrows the encoding scheme down to either Base32 or Base64. From here you can look at your letters. If the letters are all in upper case, then you are looking at Base32. If they are in mixed case, then you are looking at Base64. Figure 12 is an example of Base32, using the string “Institute for Electrical and Electronics Engineers” as the base text.

```
JFXHG5DJOR2XIZJAMZXXEICFNRSWG5DSNFRWC3BAMFXGIICFNRSWG5DSN5XGYSY3TEBCW4Z3JNZSWK4TT
```

**Figure 12. Base32 Encoding**
The fourth and final encoding scheme that we are going to talk about for PolyEncrypt is Base64. Base64 derives from Base32 but, allows for an expanded character-set. This expanded character-set adds lowercase letters, the numbers: 0, 1, 8 and 9, and two symbols (+ and /). Figure 13 is an example of Base64, using the string “Institute for Electrical and Electronics Engineers” as the base text.

\[ SW5zdGl0dXRlIGZvciBFbGVjdHJpY2FsIGFuZCBnYmVzc2VlcmQ=
\]

Figure 13. Base64 Encoding

In addition to the encoding schemes mentioned above, this system also uses two encryption mechanisms. These encryption mechanisms are Rot13 and Rot47. While these encryption mechanisms may be relatively simple, they are important to be able to identify as shift ciphers, also known as substitution ciphers, partially laid the groundwork for modern encryption. Shift Ciphers take the standard alphabet and shift it some number of positions in either direction. Figure 14 shows a shift of three to the left would result in the following Cyphertext Alphabet.

DEFGHIJKLMNOPQRSTUVWXYZABCdefghijklmnopqrstuvwxyzabc

Figure 14. Left Shift of 3

Rot47 is a variant of Rot13 that includes numbers and some common symbols. This rotation further hides the original message. However, unlike Rot13 which uses only letters, since symbols and numbers are included, it makes the fact that someone enciphered the text is more apparent. Like Rot13 it is the inverse of itself and a user can therefore use Rot13 to decipher the cyphertext. This makes Rot47 and Rot13 a fairly simple mechanism for hiding data since people can encipher it and decipher it using the same algorithm. In 1989 at the International Obfuscated
C Code Contest, Westley discovered that compilers can handle Rot13 encoded data and the compiler can still compile correctly (Westley, 1989). Based on this, malware writers could potentially utilize Rot13 and Rot47 to hide their code from signature-based detections and still operate correctly. Figure 15 is an example of Rot47, using the string “Institute for Electrical and Electronics Engineers” as the base text.

```
x?DE:6FE6 7@C t=64EC:42= 2?5 t=64EC@?:4D t?8:@66CD
```

Figure 15. Rot47 Ciphertext

All of these data and encoding mechanisms are important for new cybersecurity professionals to learn. By being able to recognize these, they will have a better understanding of the traffic going across their networks. PolyEncrypt delivers these on a 24-hour cycle. This means that every 24-hours PolyEncrypt generates a new set of challenges for users to go through. By doing this, we allow for increased repetition and experience with the data types to improve recognition by users.

**PolyNet**

PolyNet was our third and final proof of concept system that we will discuss in this paper. This system has continued on to further development and deployment. These activities have students work through network captures. These activities allow students to look at real network traffic and learn about networking and network data, while limiting answer sharing.

PolyNet uses python and a program called BitTwiste to modify packet capture files (PCAP) to make them individualized. BitTwiste is a program from the Bit-Twist\(^1\) package

\(^1\) http://bittwist.sourceforge.net/
developed by Yeow (2006). The version utilized within PolyNet is the current stable release, at time of writing, version 2.0 released on April 21, 2012. This program generates libpcap-based Ethernet packets and is also capable of editing pcap files (Yeow, 2006).

PolyNet generates the hash value and then modifies the packet capture to change the IP addresses, and MAC addresses for each of the computers in the conversation. We also manually modify some of the data to inject a full-hash Easter egg for the participant to find. These changes allow for unique captures for each and every participant. We use BitTwiste to re-write all of the checksums so that the file appears to be valid. This allowed students to get used to looking inside of a packet capture at the actual information and not just IP and MAC addresses. Students can open these pcap files in either CloudShark or Wireshark. CloudShark and Wireshark are both capable of opening pcap files, the former is a web-application and the latter is a desktop application. Figure 16 below show a pcap opened in CloudShark.
Figure 17 below shows the process for generating these values. We first take our hash value and break it up into two value hash segments. Additionally, we only modify the last parts of the IP address (last 3 octets for a private IP and the full 3 octets for a public IP) and MAC addresses (last half). That way, we maintain normal believability of the data. For IP addresses we also make sure that IP addresses that were part of the same subnet initially remain that way in the modified data, as well as making sure that the default gateway for the original dataset remains the default gateway in the modified data. For the MAC addresses, we maintain manufacturers of hardware by using the original 1st half of the MAC address so that we still have something like a Cisco router talking to a Dell workstation. The hash segments are then placed into a string, IPs are converted to hex before placement in the pcap. MAC addresses remain in hex format for usage in the pcap generation.

![Packet Capture Address Generation](image)

- **IP Source**
- **IP Destination**
- **MAC source**
- **MAC Destination**

We ran a pilot test of the PolyNet system to deliver a set of lab assignments in several sections of an introductory networking course and PolyEncrypt in a computer literacy course at a major university in United States. These pilot tests were in 3 sections of the introductory networking course with roughly 48 students in each section and 3 sections of the computer
literacy course with roughly 30 students in each section. The lab delivery worked well and allowed us to modify and improve the PolyNet and PolyLab systems.

**PolyNet Delivery**

This section will explain how PolyNet generates the lab assignments from start to finish. This section will also be including sections of code to illustrate the process. We will be relating this entire process to our design requirements from Chapter 1 in Table 2.

Users of PolyNet, upon logging onto the delivery system see a screen similar to Figure 18 below. This login screen takes the user’s university provided email address, the challenge/lab assignment number, here forward denoted as challenge number, they wish to complete and the attempt number. PolyNet then passes this information to the generation system.

![PolyNet Delivery Homepage](image)

**Figure 18. PolyNet Delivery Homepage**

Upon entering in the appropriate information, users will see a page similar to Figure 19. This will change based on what challenge was selected as different challenges have different
provided information. As can be seen in Figure 19, the user receives the lab packet information, pcap file(s), and a hyperlink that takes them to the separate grading system. Users can then upload these pcaps into a pcap viewer such as Wireshark CloudShark (Figure 20 below; Figure 16 shows a pcap file opened in CloudShark).

![Network Challenge 1](image)

**Network Challenge 1**

**Lab Packet**

[Click here to get the lab packet for Challenge 1](#)

**PCAP File**

[Click here to get Network Exercise PCAP 1](#)

**Grading for Challenge 1**

[Challenge 1 Grading](#)

*Figure 19. PolyNet Sample Challenge Delivery*
As mentioned above, PolyLab operates on the python package CherryPy. CherryPy works off of a tree structure with the main program being the trunk and modules or separate pages being the branches from the tree. The program begins with a host and port specification similar to line 16 and line 17 of Appendix A: A1. CherryPy Trunk Configurations, also shown in Figure 21 below. Line 16 specifies that any connection coming into the server should deliver this page. Line 17 narrows this down to any inbound traffic coming in on port 8081 should receive this page.

```python
cherrypy.server.socket_host = '0.0.0.0'
cherrypy.server.socket_port = 8081
```

Figure 21. CherryPy Engine Configuration

The code then specifies its main instructions via the use of the class formatting and then exposed to the web application, as seen on lines 19 and 20 of Appendix A: A1. CherryPy Trunk
Configurations. The following lines specify what this main part of the program does. Upon specifying this, the program contains a set of instructions that run if the program is the main application. These instructions specify configuration settings for the program. They also specify where to mount each branch onto the trunk program. The program then starts the CherryPy engine. Appendix A: A1. CherryPy Trunk Configurations shows this process in lines 41-49, also shown in Figure 22 below. All of this code together launches and controls the web application. The branches are then referring to separate files that CherryPy hosts at the specified web location. As can be seen below, this same code also launches and controls the grading sections of PolyNet. Therefore, we will not be discussing these code sets in the subsequent section on PolyNet Grading.

```python
if __name__ == '__main__':
    conf = {'/polylab': {'tools.staticdir.on': True,
                        'tools.staticdir.dir': workingdir}}
    cherrypy.tree.mount(Root(), '/', config=conf)
    cherrypy.tree.mount((polynetwork.polynet.Polynet(),
                        '/polynetwork', config=conf))
    cherrypy.tree.mount((polynetwork.polynetgrade.PolynetGrade(),
                        '/pnetgrade', config=conf))

    cherrypy.engine.start()
    cherrypy.engine.block()
```

Figure 22. CherryPy Trunk and Branch Control

Now that we have created the trunk of our web application, we will look at the delivery branch of our application. This branch starts by setting various global variables that the branch will utilize throughout the remainder of the branch. As shown above in Figure 18, PolyNet takes
in the university provided email, challenge number, and attempt number. After the user submits this information, the system runs several checks on the email that the user submitted. The system checks to make sure that the last characters are equal to the appropriate university domain and that the remaining characters are in the format that we expect based on the university’s email assignment scheme. We then strip off the username portion to utilize for our generation scheme.

PolyNet then performs a brief check to make sure that a user is not inputting an attempt number greater than the number of retries that they can have. Appendix A: A2. PolyNet Attempt Checks shows these checks.

Now that the system has performed the initial checks, PolyNet will process the pcap information and create the new pcap file for the user. All of the pcap information is broken into various lists for BitTwiste and PolyNet to process. The system then copies the template pcap file to our destination folder location and then PolyNet calls its generation subroutines to create the new pcap file. Figure 23 below shows this process.
The generation subroutine takes the data that it received and generates the hash that all
operations are based on. As can be seen in Figure 24 below, we hash the student’s userid, the
instructor provided password, and the student specified attempt number. However, this can be
modified to include the use of dates, times, or any other piece of information that the instructor
wishes to utilize. Once the system has calculated this hashcode we call a several python modules
based on the specified pcap data. Figure 25 below shows an example of one of these conditions
and module calls.
As seen in Figure 25 above, PolyNet calls the python subroutine known as bittwiste, which calls the BitTwiste command, and passes it a series of lists. The polypublic module generates this list which takes the publiciplist and useridhash as its arguments. It then proceeds to generate the new public IP addresses. The system makes sure that IP addresses that were part of the same subnet initially remain that way in the modified data, as well as making sure that the default gateway for the original dataset remains the default gateway in the modified data. It performs several checks to make sure that each IP address that it generates is unique and then after performing these checks, the system returns the list of new IP addresses. Appendix A: A3. polypublic Module illustrates this process.

The system then passes this list to the bittwiste module. The module performs some data sanitation and checks to the passed lists to make sure that they are as expected. The system then makes a series of subprocess calls to BitTwiste via the python subroutine known as bittwiste which changes the appropriate portion of the pcap file. Figure 26 below shows an example of some of these subprocess calls. Appendix A: A4. bittwiste Module shows this whole module process.
After all of these modules and subroutines have finished their processes, the user is then able to download the pcap files that the system generated for them. This process takes a matter of fractions of a second to a full second to complete. Some labs contain lab packets or multiple pcap files. If that is the case, the system will run additional modules to create these additional files for the user. Users will then be able to submit their answers to the grading within the PolyNet Grading system which is a completely separate system from the delivery. Users are capable of working on their assignments offline using Wireshark or CloudShark and then submit their answers at a later time.
**PolyNet Grading**

The goal of this section is to automatically grade the generated assignments. This section will discuss the grading process and post-processing of the data for PolyNet. This section will also be including sections of code to illustrate the process. We will be relating this entire process to our design requirements from Chapter 1 in Table 2.

Users of PolyNet, upon logging onto the grading system, see a screen similar to Figure 27 below. This login screen takes the user’s university-provided email address, the challenge number they wish to complete, and the attempt number. PolyNet then passes this information to the grading system.

![PolyNet Grading Login](image)

**Figure 27. PolyNet Grading Login**

Upon entering in the appropriate information, users will see a page similar to Figure 19. This will change based on what challenge was selected as different challenges have different
questions being asked. This particular challenge (Challenge 1) asks users about a web-server transaction and a set of DNS queries. Additional labs ask about ARP transactions, DHCP requests, throughput calculations, and many other types of networking questions.

![Grading Challenge 1](image)

**Figure 28. Sample Grading Page**

Now that we have discussed the user facing side, we will discuss the supporting code. As shown above in Figure 27, PolyNet takes in the university provided email, challenge number, and attempt number. After the user submits this information, the system runs several checks on the email that the user submitted. These checks are the same checks as run in the delivery system.
The system checks to make sure that the last characters are equal to the appropriate university domain and that the remaining characters are in the format that we expect based on the university’s email assignment scheme. We then strip off the username portion to utilize for our generation scheme. PolyNet then performs a brief check to make sure that a user is not inputting an attempt number greater than the number of retries that the instructor has allowed. PolyNet also checks to make sure that the user is not attempting to grade an attempt that they have already completed or that they are attempting to grade an attempt that skips any that the system has not yet graded. Appendix A: A2. PolyNet Attempt Checks shows these checks.

Once PolyNet has performed these checks, it will produce the appropriate web form asking for the user’s answers to that challenge’s questions. When the user submits, the system will generate all of the IP addresses, MAC addresses, and Ports that the user should receive from the delivery system and compares the user’s answers against what the answers should be. Figure 29 below shows the pcap data generation. The generation follows a similar process as the one laid out in Figure 25 above and Appendix A: A3. polypublic Module.

```python
publiciplist = ['64.186.152.93'];
newpubliciplist = pnetgrader.operations.operations((userid,
password0, attempt, publiciplist, 0));
privateiplist = ['192.168.108', '192.168.108.2'];
newprivateiplist = pnetgrader.operations.operations((userid,
password0, attempt, privateiplist, 1));
maclist = ['00:50:56:ee:98:59', '00:0c:29:61:82:89'];
newmaclist = pnetgrader.operations.operations((userid,
password0, attempt, maclist, 2));
```

Figure 29. PolyNet Grading PCAP Data Generation
Once the system has generated all of the pcap data, PolyNet will compare the user’s answers with the answers that the user should have given. Upon determining if the user’s answer was correct or not, the system will add the user provided answer as well as other parameters to a set of lists. If the given answer was incorrect, the system will add the question number and a brief description of the question to a different list. Figure 30 below shows a sample set of question grading mechanisms.

```python
# Compare user inputted answers with expected answers.

# Public IP
if( params.get('publicip') == newpubliciplist[0] ):
    correct += 1
else:
    incorrect.append('1. Public Ip')

expectedans.append(newpubliciplist[0])
studentans.append(params.get('publicip'))
questionnum.append('1')

# Secret Code
if( params.get('secretcode') == useridhash ):
    correct += 1
else:
    incorrect.append('2. Secret Code')

expectedans.append(useridhash)
studentans.append(params.get('secretcode'))
questionnum.append('2')
```

Figure 30. Example Questions Grading
Once the system has graded all of the questions and it has created all of the lists, the system compiles all of the lists to create an output grade file. PolyNet then passes this grade file to an email module that can email the file to the instructor and the TA(s). Appendix A: A5. Grade File Compilation shows how the system compiles the grading file. Figure 31 and Figure 32 below show an example of the email that the system sends to the instructor and an example of the grade file.

Attached is the assessment score for network challenge 0, attempt number 0. If there are any issues or questions, please consult with your instructor.

Figure 31. Example grade file email

<table>
<thead>
<tr>
<th>Challenge Number: 0</th>
<th>Attempt Number: 0</th>
<th>Score: 1/2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLEASE CHECK FOR INSTRUCTOR GRADED ITEMS BEFORE INSERTING FINAL GRADES!</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question Number</td>
<td>Expected Answer</td>
<td>Student Answer</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>1</td>
<td>25.127.242.33</td>
<td>21.127.242.33</td>
</tr>
<tr>
<td>2</td>
<td>47f312bed81962d5b3eabedbe157c3f</td>
<td>b71cf9efbd922f900c1558cd2abe58be</td>
</tr>
<tr>
<td>Incorrect Items:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Secret Code</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 32. Example score file

PolyNet currently has five challenges that it deploys. Table 6 below lists the challenges and provides a description for each.
Table 6. PolyNet Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Challenge 0</td>
<td>This challenge is a practice challenge to familiarize students with CloudShark/Wireshark and the PolyNet interface.</td>
</tr>
<tr>
<td>Network Challenge 1</td>
<td>This challenge furthers a student’s understanding of how CloudShark/Wireshark operates and the data contained within a pcap file.</td>
</tr>
<tr>
<td>Network Challenge 2</td>
<td>This challenge teaches students about TCP protocols and TCP communications.</td>
</tr>
<tr>
<td>Network Challenge 3</td>
<td>This challenge teaches students about the ARP protocol and Ethernet frame analysis.</td>
</tr>
<tr>
<td>Network Challenge 4</td>
<td>This challenge is currently under development.</td>
</tr>
<tr>
<td>Network Challenge 5</td>
<td>This challenge teaches students about the dynamic host configuration protocol (DHCP) and how the whole DHCP cycle operates.</td>
</tr>
</tbody>
</table>

Summary

This chapter discussed the design and development of the PolyLab system. We started by discussing the underlying concepts of PolyLab and then began discussing the various use-cases that have been developed and deployed. The first system we discussed was PolyStego. This system currently has five challenges that users can go through. Each of these deals with various mechanisms within steganography. The second system we discussed was PolyEncrypt. This system currently has seven challenges that users can go through. These challenges cover several different encoding and encryption mechanisms that cybersecurity professionals will need to be able to recognize. The third and final system that we discussed in this chapter was PolyNet. This system currently has five different challenges that users can go through. This system has been deployed in introductory to networking and telecommunications classes to handle lab assignment delivery and grading for instructors. These labs cover various aspects of network traffic and data transmissions.
Chapter 4

Human Subjects Experiment

The objective of this chapter is to show the impact that the proposed system, laid out in Chapter 1 and expanded in Chapter 3, had on subjects during a simulated laboratory assignment. Therefore, this chapter attempts to answer the following research question:

**RQ2: What impact would such a system have on the cognitive workload and SA of subjects during a cybersecurity homework/laboratory assignment?**

This chapter shows the design and implementation of the human subjects studied performed as part of this thesis. We discuss the process utilized in completion of this experiment and the results of this experiment.

**Objective**

The objective of this experiment is to determine the impact of the PolyLab system on the cognitive workload of subjects during a simulated laboratory assignment. This study utilizes two assignment types (“standard” and “polymorphic”). This study compares these groups based on four mechanisms: time for completion, SAGAT, NASA-TLX, and SART. We hope to find that the system creates **no negative impact on human cognition**.

**Lab Assignments**

This study was broken into two sections: the practice lab and the simulated lab assignments. Each of these assignments contains a packet capture that simulates real world
network traffic in a local area network (LAN). Based upon subject group, participants see the “standard” or the “polymorphic” version of the lab assignments. The “polymorphic” version of the lab is a modified version of the “standard” lab assignment utilized within an introductory telecommunications class. The PolyLab system created these modifications as discussed in Chapter 3.

**Experimental Process**

Upon arrival for the study, subjects received an informed consent document (see Appendix B, for IRB#00008660). Subjects received time to read over the document and ask any questions before the researcher asked them to sign the document. The researcher then gave each subject a unique subject number that they were to utilize during the study to identify themselves in each portion of the lab assignments and survey instruments in order to join the different study sections together. The researcher then assigned each subject to either the “standard” or the “polymorphic” lab at random initially and then manually to make even groups.

Following this, the researcher presented the subjects with the demographics questionnaire, which asked the subject’s age, gender, ethnicity, educational standing, and professional background. Appendix C contains the full demographics questionnaire.

Upon completion of the questionnaire, the researcher directed the subjects to CloudShark and the PolyLab interface shown in the previous section. Subjects proceeded to go through a practice lab that allowed them to become familiar with the CloudShark and PolyLab Scoring interface. This practice lab asked subjects a basic networking question about the packet capture and a question that requires the subjects to delve deeper into the CloudShark interface to find an answer buried in the packet data. These questions acted as a modified version of a SAGAT questionnaire. Upon opening the practice lab pcap file, subjects saw an interface that displayed
the collected network data (Figure 33). The first question of the assignment asks subjects to locate the IP address of the public server (highlighted in Figure 34). Subjects would then enter this IP address onto the submission form.

Figure 33. Practice Lab PCAP File in CloudShark

Figure 34. Practice Lab First Answer

The lab then asks subjects to find the secret code within the network data. This code is found in packet 26 in the http request data (highlighted in Figure 35). Upon completion of the
practice lab, subjects were given time to ask questions upon completion of this practice lab to clarify any issues with the interfaces.

<table>
<thead>
<tr>
<th>Frame 26</th>
<th>Frame 27</th>
<th>Frame 28</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 0 8.995793 22.73.155.101 192.168.126.73 TCP 1514 HTTP/0.91-rhonda[1687] [PSH, ACK] Sep4795 dcrev1973 3432434455 3645434545 [TCP segment of a reassembled]</td>
<td>27 0 8.995857 22.73.155.101 192.168.126.73 HTTP 1177 HTTP/1.1 100 OK (image/no-trm)</td>
<td>28 0 8.996017 192.168.126.73 33.73.155.101 TCP 64 wendy[1687] = http/0.91 [ACK] larp0.7738 dcrev1973 3432434455 3645434545</td>
</tr>
</tbody>
</table>

Figure 35. Practice Lab Second Answer

After this practice lab, subjects were asked to complete a simulated lab assignment based on what group they were in, either the “standard” or the “polymorphic” lab group. This simulated lab assignment was a modified assignment from a standard computer networking and telecommunications course. The assignment focused on evaluating ARP traffic on a network to determine computer roles and the structure of web communications between a computer on a LAN and a webserver that resides outside of that LAN. Subjects answered several questions about the communications in the packet capture, computer roles, and several other factors about the data provided to them. These questions acted as a modified version of a SAGAT questionnaire.

After the completion of the practice and simulated lab assignments, the researcher provided the subjects with the post-trial NASA-TLX and SART assessments. Once subjects had completed these post-trial assessments, they received the scores for their practice and simulated lab assignments. Subjects did not receive these scores until after the post-trial assessments to prevent interference between the scores and how well the subjects thought they did. Upon
completion, the researcher debriefed the subjects, answered any questions that they had, and thanked them for their participation.

Groups

We divided the subjects into two groups for this study. The standard group received the unmodified version of the networking labs. These labs have the default IP addresses and MAC addresses contained within the lab assignments. The polymorphic group received a version of the networking labs that we have polymorphed. This means that the labs have modified IP addresses and MAC addresses contained within the lab assignments. These modified addresses are all unique to the participants.

Measures

Situation Awareness Global Assessment Technique (SAGAT)

The subject received an in-trial questionnaire (See Appendix D) that took the form of a lab assignment questionnaire for each lab exercise. Each received a similar questionnaire with some changes made based on which of the two experimental groups they were in. We recorded the amount of time taken to complete each exercise in order to determine if a time difference between the groups existed.

The Situation Awareness Global Assessment Technique (SAGAT) focuses on assessing a subject’s situation knowledge. A majority of these questions focused on the subject’s knowledge of the various elements within the scenarios. These questions asked the subjects about their basic understanding of the network they were looking at. These questions included: IP addresses, MAC
addresses, communications specifics, etc. These questions, within SA, were examining the subject’s Level 1 SA. A few additional questions asked about the subject’s understanding of the scenario, such as why certain information is absent from the data, why certain communications were performed in a certain way. These questions sought to determine the subject’s Level 2 SA. We did not attempt to assess Level 3 SA (prediction of the future) in this experiment. We did not attempt to assess Level 3 SA as these lab exercises are not currently designed to work with prediction of network traffic. The SAGAT was scored on a scale of 0-2 (practice lab) and 0-100 (simulated lab assignment).

**NASA-TLX and SART**

Following the completion of the 2nd scenario, we asked the subjects to complete two post-trial questionnaires. After subjects reported their unique participant number, the first questionnaire asked subjects to rate their experience using the NASA-TLX format developed by Hart and Straveland (1988) and the questions utilized by Giacobe (2013b) (See Appendix E and Table 7 below). Hart and Straveland (1988) designed NASA-TLX to measure the cognitive workload of a subject. We organized the survey in a 7 point Likert scale format to allow for a greater degree of user choice. The anchors for this were 1 being Least/Bad and 7 being Most/Good.
Table 7. NASA-TLX (Hart & Straveland, 1988; Giacobe, 2013b)

<table>
<thead>
<tr>
<th>NASA-TLX Item</th>
<th>Description</th>
<th>Question Asked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mental Effort</td>
<td>The amount of mental activity that was required.</td>
<td>How mentally demanding was the task?</td>
</tr>
<tr>
<td>Physical Effort</td>
<td>The amount of physical activity that was required.</td>
<td>How physically demanding was the task?</td>
</tr>
<tr>
<td>Time Pressure</td>
<td>The amount of pressure felt due to the rate at which task elements occurred.</td>
<td>How hurried or rushed was the task?</td>
</tr>
<tr>
<td>Performance</td>
<td>How successful you think you were in doing what we asked you to do.</td>
<td>How successful were you in accomplishing what you were asked to do?</td>
</tr>
<tr>
<td>Overall Workload</td>
<td>The total workload associated with a given task.</td>
<td>How hard did you have to work to accomplish your level of performance?</td>
</tr>
<tr>
<td>Frustration Level</td>
<td>Level of irritation, discouragement, and stress felt.</td>
<td>How insecure, discouraged, irritated, stressed and annoyed were you?</td>
</tr>
</tbody>
</table>

The second questionnaire was a SART questionnaire developed by Taylor (1990) and questions utilized by Giacobe (2013b) (See Appendix F and Table 8 below). Taylor (1990) designed SART to measure a subject’s perceived situation awareness. This also measures how a subject feels about what they know about a situation. As with the NASA-TLX questionnaire, we organized the survey answers in a 7 point Likert scale format. The anchors for this were 1 being Least/Bad and 7 being Most/Good. Subjects received no time limit to complete these surveys.

Table 8. SART (Taylor, 1990; Giacobe, 2013b)

<table>
<thead>
<tr>
<th>SART Item</th>
<th>Question Asked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stability</td>
<td>How UNSTABLE was the situation that was presented in the scenario?</td>
</tr>
<tr>
<td>Complexity</td>
<td>How COMPLEX was the situation that was presented in the scenario?</td>
</tr>
<tr>
<td>Variability</td>
<td>How VARIABLE was the situation that was presented the scenario?</td>
</tr>
<tr>
<td>Stimulating</td>
<td>How STIMULATING was the situation that was presented in the scenario?</td>
</tr>
<tr>
<td>Concentration</td>
<td>To what degree did the situation in the scenario require you to CONCENTRATE YOUR ATTENTION?</td>
</tr>
<tr>
<td>Attention Division</td>
<td>To what degree did the situation in the scenario require you to DIVIDE YOUR ATTENTION?</td>
</tr>
<tr>
<td>Spare Mental Capacity</td>
<td>While addressing the situation in the scenario, how much SPARE MENTAL CAPACITY would you say you had?</td>
</tr>
<tr>
<td>Information Quantity</td>
<td>Please rate the QUANTITY OF INFORMATION that was presented in the scenario.</td>
</tr>
<tr>
<td>Information Quality</td>
<td>Please rate the QUALITY OF INFORMATION that was presented in the scenario.</td>
</tr>
<tr>
<td>Level of Familiarity</td>
<td>How FAMILIAR does the situation in the scenario feel to you?</td>
</tr>
</tbody>
</table>
Pilot Testing

We tested the PolyLab system in three sections of an introductory networking and telecommunications course as well as two sections of a computer literacy class. Throughout the testing of the system, participants and researchers took notes and pilot participants gave feedback on the system’s operation. The feedback they provided and the notes that we took allowed for improvements in the system and system functionality. Table 9 below shows some of the improvements made to the system based on feedback.

Table 9. Improvements from pilot testing

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Too many steps</td>
<td>There was a lot of clicking involved in navigating the interface between delivery and grading.</td>
<td>Modified the delivery system to provide a hyperlink that would redirect to the grading system (this did not connect them aside from the hyperlink).</td>
</tr>
<tr>
<td>Coding issues</td>
<td>Pilot testing found numerous bugs and errors in the code.</td>
<td>Modified the system to resolve errors and package issues.</td>
</tr>
<tr>
<td>Directions not always clear</td>
<td>The lab information was not as nuanced as it should have been to denote different sections of the lab assignment.</td>
<td>Added headings and integration of the lab packet into the delivery/grading system.</td>
</tr>
</tbody>
</table>

The first improvement was in the delivery system. Initially participants had to download the pcap files and lab information then go to a separate webpage and reinput all of their information again to do the grading of the assignment. This made the assignments overly complicated and involved. We resolved this by adding a hyperlink on the delivery page that would redirect the browser to the appropriate grading page and enter in all of the user information automatically.

The second improvement was in the whole system. Participants and the research team discovered numerous coding issues that created unintended behaviors within the system. Some of these ranged from creating unreal IP addresses to typical list iteration errors and syntax errors.
We resolved these errors by identifying the location of the code bug and changing it to what it should have been.

The third and final improvement was largely to the grading system. Participants struggled understanding the lab instructions as they were not clearly defined and broken into logical chunks. This was resolved by generating a lab packet and delivery this to the students to use. We also added headings and section breaks to denote changes of focus area within the grading system.

Results

Participants

We recruited fourteen subjects for this study. Subjects came from cybersecurity and telecommunications courses at a large university in the northeastern part of the United States. Recruited subjects came to the lab for a 90-120 minute networking laboratory experiment. We informed them that they would be analyzing computer network data and be answering some short surveys about their experiences. We did not offer any form of financial compensation to the study subjects that we recruited.

We separated the subjects into one of two groups the standard or the polymorphic lab at random initially and then manually to make even groups. All participants were male, except for two in the polymorphic group and one in the standard group. The average age of the standard subjects was 19.43 years, while the polymorphic subjects averaged 20.75 years of age (Table 10). Three individuals did have prior experience with PolyNet. However, their completion times and scores, aside from the main lab assignment completion time, were not statistically significant
from their group’s times and scores. Even though their main lab assignment completion time was statistically significant, we do not believe it would have impacted the analysis.

Table 10. Participant Demographics

<table>
<thead>
<tr>
<th></th>
<th>Polymorphic (N=8)</th>
<th>Standard (N=7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant Age (years)</td>
<td>M = 20.75</td>
<td>M = 19.43</td>
</tr>
</tbody>
</table>

Main Effect

We can see the main effect of group (Standard or Polymorphic) on the two primary dependent variables (Completion Time and SAGAT) below in boxplots of these values (Figure 36 and Figure 37). C0 denotes the practice lab that we asked participants to complete to familiarize themselves with CloudShark and the PolyNet interface. C1 denotes the lab assignment that we asked subjects to complete upon completion of the practice lab assignment. We timed and scored both lab assignments. The box plots below display the reported values in minutes (time) and score percentage (SAGAT scores). The numbers on the right-hand side of the boxplots correspond to the horizontal line on the plots and denote the median values for time and score. The numbers on the left-hand side of the boxplots correspond to the crossed circle on the plots and denote the mean values for time and score.
We subjected participant completion times to a one-way analysis of variance based on study group (Polymorphic, Standard) (See Table 11). We also subjected the SAGAT scores to the same one-way analysis of variance (See Table 12). We subjected these factors to a one-way
analysis of variance in order to determine if there was a significant difference in the scores or times as a whole and not just in terms of mean score or time. Upon completion of the ANOVA, we determined that these factors were not significantly different between the groups.

Table 11. ANOVA for Completion Times

<table>
<thead>
<tr>
<th>Source</th>
<th>DF</th>
<th>Adj SS</th>
<th>Adj MS</th>
<th>F-Value</th>
<th>P-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group (C0)</td>
<td>1</td>
<td>10.30</td>
<td>10.30</td>
<td>0.50</td>
<td>0.492</td>
</tr>
<tr>
<td>Error (C0)</td>
<td>13</td>
<td>267.30</td>
<td>20.56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total (C0)</td>
<td>14</td>
<td>277.60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group (C1)</td>
<td>1</td>
<td>16.30</td>
<td>16.30</td>
<td>0.57</td>
<td>0.464</td>
</tr>
<tr>
<td>Error (C1)</td>
<td>13</td>
<td>371.30</td>
<td>28.56</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total (C1)</td>
<td>14</td>
<td>387.60</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 12. ANOVA for SAGAT Scores

<table>
<thead>
<tr>
<th>Source</th>
<th>DF</th>
<th>Adj SS</th>
<th>Adj MS</th>
<th>F-Value</th>
<th>P-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group (C0)</td>
<td>1</td>
<td>1860</td>
<td>1860</td>
<td>0.91</td>
<td>0.357</td>
</tr>
<tr>
<td>Error (C0)</td>
<td>13</td>
<td>26473</td>
<td>2036</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total (C0)</td>
<td>14</td>
<td>28333</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group (C1)</td>
<td>1</td>
<td>1143</td>
<td>1143.3</td>
<td>1.88</td>
<td>0.193</td>
</tr>
<tr>
<td>Error (C1)</td>
<td>13</td>
<td>7900</td>
<td>607.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total (C1)</td>
<td>14</td>
<td>9043</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The above tables, the change in group did not yield any statistically significant difference between the two groups. The effect of group on completion time yielded an F ratio of $F(1, 14) = 0.50, p > .05$ and $F(1, 14) = 0.57, p > .05$, indicating that the mean change in time between the
two groups was non-significant in either lab assignment. The effect of group on SAGAT scores yielded an F ratio of F(1, 14) = 0.91, p > .05 and F(1, 14) = 1.88, p > .05, indicating that the mean change in SAGAT scores between the two groups was non-significant in either lab assignment. See Table 13 and Table 14 below for further details.

<table>
<thead>
<tr>
<th>Table 13. Descriptive Statistics for Completion Time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
</tr>
<tr>
<td>Polymorphic (C0)</td>
</tr>
<tr>
<td>Standard (C0)</td>
</tr>
<tr>
<td>Polymorphic (C1)</td>
</tr>
<tr>
<td>Standard (C1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 14. Descriptive Statistics for SAGAT Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
</tr>
<tr>
<td>Polymorphic (C0)</td>
</tr>
<tr>
<td>Standard (C0)</td>
</tr>
<tr>
<td>Polymorphic (C1)</td>
</tr>
<tr>
<td>Standard (C1)</td>
</tr>
</tbody>
</table>

**Multivariate Analysis of Variance of Dependent Variables (MANOVA)**

We collected a total of twenty (20) different measures during and following the trials. These include the completions times (collected in minutes for each trial), SAGAT (scored from 0 to 100 with 10 points given for each correct answer, divided in equally for multipart questions).
six (6) categories of NASA-TLX (scored from 1 to 7 on a Likert scale), and ten (10) categories in
the SART evaluation (scored from 1 to 7 on a Likert scale). We computed a Multivariate
Analysis of Variance (MANOVA) in order to identify which measures were statistically
significant due to our independent variable of group. All of our MANOVA measures use the
Wilks’ Lambda (λ) to test for statistical significance.

Experimental group resulted in NASA-TLX complete, NASA-TLX & SAGAT Scores,
NASA-TLX & SAGAT Score C1, NASA-TLX & Completion Times, NASA-TLX &
Completion Time C0, and NASA-TLX & Completion Time C1 as being statistically significant.
There was a statistically significant difference in cognitive workload based on experimental
group, \( F(6, 8) = 4.632, p = 0.025 \); Wilks’ \( \lambda = 0.224 \). There was also a statistically significant
difference in cognitive workload & SAGAT Scores based on experimental group, \( F(8, 6) = 5.015, 
p = 0.032 \); Wilks’ \( \lambda = 0.130 \). There was also a statistically significant difference in cognitive
workload & SAGAT score C1 based on experimental group, \( F(7, 7) = 5.995, p = 0.015 \); Wilks’ \( \lambda 
= 0.143 \). There was also a statistically significant difference in cognitive workload & completion
times based on experimental group, \( F(8, 6) = 4.685, p = 0.038 \); Wilks’ \( \lambda = 0.138 \). There was also
a statistically significant difference in cognitive workload & completion time C0 based on
experimental group, \( F(7, 7) = 4.953, p = 0.026 \); Wilks’ \( \lambda = 0.168 \). There was also a statistically
significant difference in cognitive workload & completion time C1 based on experimental group,
\( F(7, 7) = 3.867, p = 0.048 \); Wilks’ \( \lambda = 0.206 \).

However, upon further investigation it was determined this was due to three individuals
in the polymorphic group who had prior experience with the PolyNet interface. Upon removing
these individuals from the MANOVA analysis, the NASA-TLX complete, NASA-TLX &
SAGAT Scores, NASA-TLX & SAGAT Score C1, NASA-TLX & Completion Times, NASA-
TLX & Completion Time C0, and NASA-TLX & Completion Time C1 were no longer
statistically significant at the .05 level. Differences were non-significant for every other measure collected in this experiment as shown in Table 15.

<table>
<thead>
<tr>
<th>Responses Tested</th>
<th>Test Statistic</th>
<th>F</th>
<th>DF Numerator</th>
<th>DF Denominator</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completion Times &amp; SAGAT Scores</td>
<td>0.84370</td>
<td>0.463</td>
<td>4</td>
<td>10</td>
<td>0.762</td>
</tr>
<tr>
<td>SART Complete</td>
<td>0.25364</td>
<td>2.207</td>
<td>8</td>
<td>6</td>
<td>0.175</td>
</tr>
<tr>
<td>NASA-TLX Complete</td>
<td>0.22352</td>
<td>4.632</td>
<td>6</td>
<td>8</td>
<td>0.025</td>
</tr>
<tr>
<td>NASA-TLX Complete &amp; Completion Times &amp; SAGAT Scores</td>
<td>0.08938</td>
<td>4.075</td>
<td>10</td>
<td>4</td>
<td>0.094</td>
</tr>
<tr>
<td>SART Complete &amp; Completion Times &amp; SAGAT Scores</td>
<td>0.17185</td>
<td>0.803</td>
<td>12</td>
<td>2</td>
<td>0.677</td>
</tr>
<tr>
<td>SART &amp; NASA-TLX a.</td>
<td>0.03240</td>
<td>4.978</td>
<td>12</td>
<td>2</td>
<td>0.179</td>
</tr>
<tr>
<td>NASA-TLX &amp; SAGAT Scores</td>
<td>0.13009</td>
<td>5.015</td>
<td>8</td>
<td>6</td>
<td>0.032</td>
</tr>
<tr>
<td>NASA-TLX &amp; SAGAT Score C0</td>
<td>0.21945</td>
<td>3.557</td>
<td>7</td>
<td>7</td>
<td>0.058</td>
</tr>
<tr>
<td>NASA-TLX &amp; SAGAT Score C1</td>
<td>0.14295</td>
<td>5.995</td>
<td>7</td>
<td>7</td>
<td>0.015</td>
</tr>
<tr>
<td>NASA-TLX &amp; Completion Times</td>
<td>0.13799</td>
<td>4.685</td>
<td>8</td>
<td>6</td>
<td>0.038</td>
</tr>
<tr>
<td>NASA-TLX &amp; Completion Time C0</td>
<td>0.16798</td>
<td>4.953</td>
<td>7</td>
<td>7</td>
<td>0.026</td>
</tr>
<tr>
<td>NASA-TLX &amp; Completion Time C1</td>
<td>0.20545</td>
<td>3.867</td>
<td>7</td>
<td>7</td>
<td>0.048</td>
</tr>
<tr>
<td>NASA-TLX Complete (not including subjects with prior PolyNet experience)</td>
<td>0.23347</td>
<td>2.188</td>
<td>6</td>
<td>4</td>
<td>0.235</td>
</tr>
<tr>
<td>NASA-TLX &amp; SAGAT Scores (not including subjects with prior PolyNet experience)</td>
<td>0.05861</td>
<td>6.023</td>
<td>8</td>
<td>3</td>
<td>0.084</td>
</tr>
<tr>
<td>NASA-TLX &amp; SAGAT Score C1 (not including subjects with prior PolyNet experience)</td>
<td>0.05733</td>
<td>7.046</td>
<td>7</td>
<td>3</td>
<td>0.068</td>
</tr>
<tr>
<td>NASA-TLX &amp; Completion Times (not including subjects with prior PolyNet experience)</td>
<td>0.10593</td>
<td>3.165</td>
<td>8</td>
<td>3</td>
<td>0.186</td>
</tr>
<tr>
<td>NASA-TLX &amp; Completion Time C0 (not including subjects with prior PolyNet experience)</td>
<td>0.09278</td>
<td>4.191</td>
<td>7</td>
<td>3</td>
<td>0.133</td>
</tr>
<tr>
<td>NASA-TLX &amp; Completion Time C1 (not including subjects with prior PolyNet experience)</td>
<td>0.18837</td>
<td>2.462</td>
<td>7</td>
<td>4</td>
<td>0.201</td>
</tr>
</tbody>
</table>
Summary

In summary, this experiment attempted a series of situational awareness measures in a simulated networking lab exercise. We utilized two experimental groups (standard and polymorphic) to test the PolyNet system. We analyzed the situational awareness measures through the use of box plots, ANOVA, and MANOVA statistical techniques. We found that there was no statistical significance between the two groups in terms of scores or completion times. Upon utilizing MANOVA, we initially found statistical significance for five interaction factors, but determined that this was due to three subjects who had utilized PolyNet before. This chapter then presented these analyses in the form of charts and tables along with some descriptive analysis of the data.
Chapter 5

Discussion and Conclusion

This chapter outlines the findings presented in this thesis. These findings come from the system development discussed in Chapter 3 and the human subjects experiment discussed in Chapter 4. This chapter reviews the research questions presented in Chapter 1 and highlights conclusions about them. These findings have implications on cybersecurity education and therefore the whole domain of cybersecurity. This thesis concludes with a discussion about future work that others could conduct to further explore the effectiveness of this system and its continued development.

Contributions

Table 16 below outlines the major contributions of this thesis. The literature review explore the domains of challenge based learning, cyber-competitions, and SA. This literature review sought to determine what work others had performed in attempt to resolve the issues facing cybersecurity education and the cybersecurity domain in general. The findings of the literature review informed the development of the PolyLab system. We then tested this system in a human-subjects experiment to determine the impact it had on cognitive workload. We review the important findings in each of these contributions in the following sections.
Table 16. Summary of Contributions

| Literature Reviews | 1. A literature review of challenge-based learning (CBL) and virtual labs usage in cybersecurity education.  
2. A literature review of SA that discusses different perspectives and measurement techniques. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Development</td>
<td>3. The development of a prototype system that attempts to solve issues inherent in challenge based learning and virtual lab based techniques.</td>
</tr>
<tr>
<td>Human Subjects Experiment</td>
<td>4. The design, conduct and analysis of human subjects to measure the impact that the designed system had on performance using multiple SA assessment instruments and assignment scoring</td>
</tr>
</tbody>
</table>

**Literature Review**

Reviews of literature of two bodies of domain knowledge provide the research team with background information on challenge based learning and SA. This provided a foundational understanding of how cybersecurity education currently utilizes virtual lab environments and competitions to provide students with real world experience in a topic area. We reviewed the SA literature in order to understand how we can measure situational awareness. The SA measures that we identified as being particularly useful for our study were: SAGAT, NASA-TLX, Time to complete, and SART. We utilized this understanding of SA measurement techniques in order to test our proposed system.

**System Development**

Table 17 below outlines the design requirements that we presented that a proposed system would need to meet. In Chapter 3 we discussed the theory behind the development of the PolyLab system and several example use cases for PolyLab. This section will discuss how we implemented each requirement from Table 17 into PolyLab. We will finish this section by discussing what it took to develop PolyLab and how instructors are utilizing PolyLab now.
Table 17. System Design Requirements

<table>
<thead>
<tr>
<th>Requirement Groups</th>
<th>Sub-Requirements</th>
</tr>
</thead>
</table>
| 1. Reduce Administrative Overhead     | e) Automatically generate assignments  
                                          f) Automatically grade assignments 
                                          g) Minimize instructor required elements  
                                          h) No more difficult to create than a standard assignment |
| 2. Modular Design                      | d) Capable of operating in varied cybersecurity environments  
                                          e) Capable of operating in outside domains  
                                          f) Integration with Learning Management Systems (LMS) |
| 3. Tamper/Cheating Resistant           | d) Capable of making meaningful modifications  
                                          e) Generation scheme is not predictable  
                                          f) Generation scheme can be easily and quickly modified |
| 4. Customizable                        | d) Multiple attempts  
                                          e) Score file emailing  
                                          f) Challenge types can be changed |
| 5. Separate Grading and Delivery       | c) Two systems do not communicate  
                                          d) Non-random generation/grading system |
| 6. Scalable                            | c) Usable in small class sizes  
                                          d) Usable in large class sizes |
| 7. Minimal Cognition Impact            | d) Cognitive workload  
                                          e) Situation Knowledge  
                                          f) Perceived Situational Awareness |

The first requirement grouping states that the proposed system shall reduce administrative overhead. We have implemented this by taking template assignments and modifying instructor specified elements. Once an instructor has specified these elements, PolyLab will automatically generate the polymorphic version of the file/assignment. PolyLab is then able to automatically grade the student submissions leaving as few items for instructor grading as possible. While the initial effort required to make a polymorphic assignment is greater than creating one standard version of the lab assignment, this is an acceptable cost. This initial cost is the only cost required of instructors as the system can create a near infinite number of unique
assignments automatically and the instructor does not need to do anything beyond changing one
or two values if they choose to do so.

The second requirement grouping states that the proposed system shall be modular in
design. As discussed in Chapter 3, we have already developed three use cases within the
cybersecurity field: PolyStego, PolyEncrypt, and PolyNet. We are currently developing a module
called PolyBandit which will be capable of teaching command line mechanisms for Windows and
Linux. Also, currently in development is a module called PolyMultiply which will be able to
deliver and grade multiplication problems to students. At the time of writing, we have not been
able to integrate PolyLab with the LMS known as Canvas. However, we are in the process of
figuring out the APIs and integrations required to do so.

The third requirement grouping states that the system shall be tamper/cheating resistant.
As discussed in Chapter 3, the system utilizes a hashing algorithm to generate the assignments
based on the instructor provided templates. This hashing algorithm creates a unique fixed length
output based on the inputs and cannot be predicted. Also as discussed in Chapter 3, instructors
can add different factors to the generation and grading system to easily and quickly change the
systems operations.

The fourth requirement grouping states that the system shall be customizable. We have
implemented an attempt mechanism within PolyNet to allow students to retry the assignments.
The instructor can easily modify the system to customize the number of attempts that students
have. We have also added in a grade file email mechanism. This allows the system to send a copy
of the grade file to the instructor and anyone else that he/she wishes to receive it such as TAs. As
discussed above, instructors can easily and quickly modify challenge types with minimal
administrative overhead to meet the instructor’s needs.

The fifth requirement grouping states that the system shall have a separate grading and
delivery mechanism. We implemented this by creating two branches within CherryPy, one for the
delivery and one for the grading. Since the system operates using a hashing algorithm, both systems can create the same hash by utilizing the same inputs to create the same values for grading and delivery. This also makes the system non-random in nature which reduces student ability to predict outputs.

The sixth requirement grouping states that the system shall be scalable. We have run pilot tests in class sizes ranging from 24 students to class sizes of 40+ students and did not run into issues. However, we have not tested the system in class sizes of anything substantially larger than 40 students. Additional testing will be required to determine if the system is scalable to classes of Massive Open Online Course (MOOC) size.

The seventh requirement grouping states that the system shall have minimal cognitive impact on users. In order to test this we ran a human-subjects experiment. We shall discuss this requirement and the experiment in a later section of this chapter.

We will finish this section by discussing what it took to develop PolyLab and how instructors are utilizing PolyLab now. PolyLab took roughly 2.5 years at ¼ FTE to develop. Ryan Kohler performed this development from nothing to current deployment state, with Dr. Nicklaus Giacobe, Dr. Jungwoo Ryoo, and Dr. Chris Gamrat providing technical guidance and advice. PolyNet in whole amounts to roughly 3,468 lines of code, of which, roughly 61.9% of which is Python and 38.1% of which is HTML. One individual assignment within PolyNet, not counting the subroutines just the delivery and grading, takes roughly 400 lines of code and roughly 1-2 weeks at ¼ FTE. The resources needed to create this system are a webserver with CherryPy and python code. Depending on assignment requirements, these resource needs can change substantially. Based on this, we believe that it is sustainable to create and maintain this process. While initial development took 2.5 years at ¼ FTE, now that the base code has been developed, future development will take less time. We also believe that the system is extendable as we
created additional challenges in various domains with minimal additional administrative overhead.

Instructors are currently utilizing PolyEncrypt to teach students encoding and encryption mechanisms in a Computer Literacy class at a major university in the northeastern United States. They are also utilizing PolyNet to teach students networking concepts in an Introduction to Telecommunications class at a major university in the northeastern United States. College recruiters will be utilizing PolyCTF, completion of development, to create interest among High School students in cybersecurity and data sciences.

**Human Subjects Experiment**

To test the impact of the PolyLab system on human cognition, we ran a human-subjects experiment. This experiment split subjects into one of two groups (standard and polymorphic) and had them complete a practice networking lab assignment and a simulated networking lab assignment. The standard group received the default unmodified version of the practice and simulated networking lab assignments. The polymorphic group received a polymorphic version of the practice and simulated networking lab assignments. This experiment did not yield any statistically significant results, once we removed three subjects with prior experience with PolyNet from the MANOVA analysis. These subjects, having seen similar labs before completed the assignments slightly faster than the rest of their group. However, this was not statistically significant on its own and so we did not remove these three subjects from the larger analysis.

These results yield an interpretation that there is no negative cognitive impact due to the PolyNet system, and thus the PolyLab system as a whole, upon subjects. This means that subjects did not perceive the PolyLab assignment as being harder or more cognitively difficult. We know this because, there was no statistically significant difference between the two groups (standard
and polymorphic). Therefore, we can say that we met our seventh design requirement group. We can say this as there was no statistically significant cognitive impact upon subjects when run through the experiment.

The results also yield an interpretation that the system may in fact improve a subject’s knowledge retention and increase their perceived performance. This interpretation comes from the fact that the three participants who had prior experience with PolyNet seemed to perform slightly better than their counterparts. This caused the statistical significance among the various SA measures and interactions therein. However, this will require further study to determine the long-term effects of the PolyLab system.

**Future Work**

Potential future work in the direction of this thesis includes: testing the system with an increased number of participants. This will provide a greater confidence that the system is placing no statistically significant cognitive impact on the polymorphic group. We also recommend utilizing a greater diversity within the sample pool to collect as many reference points as possible.

A second line of research is to perform a longitudinal study or study subjects with varying levels of experience with PolyLab. This will allow us to determine what effects, if any, PolyLab has in the long-term on users.

The third line of research is further development of the PolyLab system. As stated in the system design section, use cases in fields other than cybersecurity need to be developed and tested. We are currently discussing with the Geography and Statistics department as well as a university testing center on how we can implement PolyLab in their domains. We also discuss the need to implement LMS integration to further reduce the administrative overhead place upon instructors by traditional assignments.
Other use cases in cybersecurity are currently in progress as mentioned before. PolyCTF is a system that will be able to deploy and run CTF events for a variety of skill levels. This system will be able to resolve several issues inherent within traditional CTF scenarios. Another system is a Learning Linux & Windows command line exercise. This system will help teach students how to utilize the command line to perform tasks traditionally performed within the graphical user interface. The final concept scenario in development currently is a system that will help to teach SQL to students. This system will provide students with data that they then enter into certain tables and databases to run queries on.


Appendix A

PolyLab Code

A1. CherryPy Trunk Configurations

# -*- coding: utf-8 -*-
import cherrypy
import polynetwork.polynet
import polynetwork.polynetgrade

# Global Variables

workingdir = '/data/websites/polylab'

# Make the CherryPy server answer on any IP address that is received by this
# server.
# This makes the CherryPy server run from inside of a NAT boundary where the
# inside
# and outside IP addresses may be different.
cherrypy.server.socket_host = '0.0.0.0'
cherrypy.server.socket_port = 8081

class Root(object):
    @cherrypy.expose
    def index(self):
        return '''
<html>
<head>
<title>PolyLab</title>
<link rel="stylesheet" href="polylab/style.css" type="text/css" />
</head>
<body>
<div id="content">
<h1>PolyLab</h1>
<br>
This is the base webpage for PolyLab. Please click on the links below to take
you to the correct activity.
<br>
<h3>PolyNet</h3>
<a href="polynetwork">PolyNet Delivery</a>
<br>
<a href="pnetgrade">PolyNet Grading System</a>
</div>
</body>
</html>"""
if __name__ == '__main__':
    conf = {'/polylab': {'tools.staticdir.on': True, 'tools.staticdir.dir': workingdir}}
    cherrypy.tree.mount(Root(), '/', config=conf)
    cherrypy.tree.mount((polynetwork.polynet.Polynet(), '/polynetwork', config=conf))
    cherrypy.tree.mount((polynetwork.polynetgrade.PolynetGrade(), '/pnetgrade', config=conf))
    cherrypy.engine.start()
    cherrypy.engine.block()

A2. PolyNet Attempt Checks

found = False
for sublist in challenge0attemptlist:
    if sublist[0] == userid:
        found = True
        break
    count = count + 1
if found:
    if( int(attempt) > int(challenge0attemptlist[count][2]) ) :
        return """<html>
<head>
<link rel="stylesheet" href="polylab/style.css" type="text/css" />
<title>PolyNet</title>
</head>
<body>
<div id="content">
<p>You have input an attempt number that is higher than the number of attempts you have made. You inputed """"+attempt+"""" as your attempt number. However, you are not allowed to take more than """"+str(challenge0attemptlist[count][2])+"""" attempt(s). Please input a number less than """"+str(challenge0attemptlist[count][2])+"""" as your attempt number.</p>

<meta http-equiv="refresh" content="5; url=/polynetwork" />
</div>
</body>
"""
else:
    if( int(attempt) > int(challenge0attempt) ) :
        return """""""<html>
<head>
<link rel="stylesheet" href="polylab/style.css" type="text/css" />
<title>PolyNet</title>
</head>
<body>
<div id="content">
<p>You have input an attempt number that is higher than the number of attempts you have made. You inputed """"+attempt+"""" as your attempt number. However, you are not allowed to take more than """"+str(challenge0attempt)+"""" attempt(s). Please input a number less than """"+str(challenge0attempt)+"""" as your attempt number.</p>
""""
""""
A3. polypublic Module

def publicgen(publiciplist, useridhash):
    newpubliciplist = []
    publiciplist = publiciplist
    useridhash = useridhash
    x = 0
    a = 1
    b = 3
    useridhashinc = ''
    while( x < len(useridhash) ):
        inthash = int(useridhash[x],16)
        inthash = inthash + 1
        if( inthash == 17 ):
            inthash = 0
        useridhashinc = useridhashinc + str(hex(inthash)[2:])
        x += 1
    useridhashrev = useridhash[::-1]
    useridhash = useridhash + useridhashinc
    useridhash = useridhash + useridhashrev
    useridhash = useridhash + useridhashinc[::-1]
    x = 0
    sameoctet = False
    while( x < len(publiciplist) ):
        #Extract parts of the hash to use for polymorphic public ip addresses and construct them
        sameoctet = False
        octetcount = 0
        c = 0
        d = 0
        if( x > 0 ):
            while( c < len(str(publiciplist[x])) and octetcount < 3 ):
                c += 1
                if( str(publiciplist[x])[c] == '.' ):
                    octetcount += 1
            while( d < x and sameoctet == False):
                if(( str(publiciplist[x])[0:c] == str(publiciplist[d])[0:c] )):
                    octetcount = 0
                    c = 0
                    while(( c < len(str(newpubliciplist[d])) and octetcount < 3 )):
                        c += 1
                        if(( str(newpubliciplist[d])[c] == '.' )):
                            octetcount += 1
                    threeoctet = str(newpubliciplist[d])[0:c]
                    sameoctet = True
d += 1
if( sameoctet == False):
    lastdigithash = useridhash[-1:]
    publicipoctet1 = str(int('1'+lastdigithash,16))
    publicipoctet2 = str(int(useridhash[a:b],16))
    a += 1
    b += 1
    publicipoctet3 = str(int(useridhash[a:b],16))
    a += 1
    b += 1
    publicipoctet4 = int(useridhash[a:b],16)
    a += 1
    b += 1
if( str(publiciplist[x])[-2:] == '.1' ):
    publicipoctet4 = str(1)
else:
    if( publicipoctet4 == 0 or publicipoctet4 == 1 ):
        publicipoctet4 = '2'
    elif( publicipoctet4 == 255 ):
        publicipoctet4 = '254'
    else:
        publicipoctet4 = str(publicipoctet4)
if( sameoctet == True ):
    newpublicip = threeoctet+'.'+publicipoctet4
else:
    newpublicip = publicipoctet1+'.'+publicipoctet2+'.'+publicipoctet3+'.'+publicipoctet4
unique = True
if( x > 0 ):
    # make sure that there are no collisions with already used public
    i = 0
    while( i < len(newpubliciplist) and unique ):
        if( newpublicip in newpubliciplist ):
            unique = False
        else:
            i += 1
        if( unique ) :
            newpubliciplist.append(newpublicip)
            x += 1
        else:
            newpublicip = 0
else:
    x += 1
    newpubliciplist.append(newpublicip)
return newpubliciplist
import os
import subprocess

def bittwiste(filepath, filename, origportion, newportion, portionchange):
    # this function takes in a filepath filename and the various parts of a
    # pcap that are to be changed
    # the function will then perform the appropriate bittwiste commands
    filepath = filepath
    filename = filepath+filename
    origportion = origportion
    newportion = newportion
    portionchange = portionchange

    # determines what portion of a pcap is to be changed
    # 0 for ip addresses; 1 for mac addresses; 2 for tcp port numbers; 3
    # for udp port numbers
    if( portionchange == 0 ): # ip addresses
        x = 0
        filecount = 0
        newfilecount = 2
        if( len(origportion) != len(newportion) ) :
            return "<html><body>Error!!!!!!!</body></html>"
        while( x < len(origportion) ) :
            orig = str(origportion[x])
            new = str(newportion[x])
            if( filecount == 0 ) :
                filecount = 1
                subprocess.call( { 'bittwiste -I '+filename+'] O ' +filepath+'tmp_m'+str(filecount)+'.pcap -T ip -s '+orig+','+new+'] -d '+orig+','+new, shell=True} )
                subprocess.call( { 'bittwiste -I ' +filepath+'tmp_m'+str(filecount)+'.pcap O ' +filepath+'tmp_m'+str(newfilecount)+'.pcap -T arp -p '+orig+','+new+'] -q '+orig+','+new, shell=True} )
                filecount = newfilecount
                newfilecount += 1
            else :
                subprocess.call( { 'bittwiste -I ' +filepath+'tmp_m'+str(filecount)+'].pcap O ' +filepath+'tmp_m'+str(newfilecount)+'].pcap -T ip -s '+orig+','+new+'] -d '+orig+','+new, shell=True} )
                filecount = newfilecount
                newfilecount += 1
            x += 1
    else :
        subprocess.call( { 'bittwiste -I ' +filepath+'tmp_m'+str(filecount)+'].pcap O ' +filepath+'tmp_m'+str(newfilecount)+'].pcap -T ip -s '+orig+','+new+'] -d '+orig+','+new, shell=True} )
        filecount = newfilecount
        newfilecount += 1

A4. bittwiste Module
elif( portionchange == 1 ): # mac addresses
    x = 0
    filecount = 0
    newfilecount = 2
    while( x < len(origportion) ):
        orig = origportion[x]
        new = newportion[x]

        if( filecount == 0 ):
            subprocess.call(['bittwiste -I '+filename+ ' -O '+filepath+'tmp_m'^str(filecount)+'.pcap -T eth -s ' +orig+','+new+ ' -d ' +orig+','+new, '
                               shell=True])
            subprocess.call(['bittwiste -I '+filepath+'tmp_m'+str(filecount)+'.pcap -O '+filepath+'tmp_m'+str(newfilecount)+'.pcap -T arp -s ' +orig+','+new+ ' -t ' +orig+','+new, '
                               shell=True])
            filecount += 1
            newfilecount += 1
        else:
            subprocess.call(['bittwiste -I '+filepath+'tmp_m' +str(filecount)+'.pcap -O '+filepath+'tmp_m' +str(newfilecount)+'.pcap -T eth -s ' +orig+','+new+ ' -d ' +orig+','+new, '
                               shell=True])
            subprocess.call(['bittwiste -I '+filepath+'tmp_m' +str(filecount)+'.pcap -O '+filepath+'tmp_m' +str(newfilecount)+'.pcap -T arp -s ' +orig+','+new+ ' -t ' +orig+','+new, '
                               shell=True])
            filecount += 1
            newfilecount += 1

    subprocess.call(['mv '+filepath+'tmp_m'+str(filecount)+'.pcap '+filename+'; rm '+filepath+'tmp_m*.pcap', shell=True])

elif( portionchange == 2 ): # tcp port numbers
    x = 0
    filecount = 0
    newfilecount = 2
    while( x < len(origportion) ):
        orig = origportion[x]
        new = newportion[x]

        if( filecount == 0 ):
            subprocess.call(['bittwiste -I '+filename+ ' -O '+filepath+'tmp_m'^str(filecount)+'.pcap -T tcp -s ' +orig+','+new+ ' -d ' +orig+','+new, '
                               shell=True])
            subprocess.call(['bittwiste -I '+filepath+'tmp_m'^str(filecount)+'.pcap -O '+filepath+'tmp_m'^str(newfilecount)+'.pcap -T tcp -s ' +orig+','+new+ ' -d ' +orig+','+new, '
                               shell=True])
            filecount += 1
            newfilecount += 1

    subprocess.call(['mv '+filepath+'tmp_m'+str(filecount)+'.pcap '+filename+'; rm '+filepath+'tmp_m*.pcap', shell=True])
```python
elif( portionchange == 3 ): # udp port numbers
    x = 0
    filecount = 0
    newfilecount = 2
    while( x < len(origportion) ):  
        orig = origportion[x]
        new = newportion[x]
        if( filecount == 0):
            subprocess.call(('

    subprocess.call(('

    subprocess.call(('

    subprocess.call(('

    subprocess.call(('

        subprocess.call(('

        subprocess.call(('

        subprocess.call(('

        subprocess.call(('

        subprocess.call(('

```

A5. Grade File Compilation

```python
subprocess.call(('

subprocess.call(('

subprocess.call(('

subprocess.call(('

subprocess.call(('

subprocess.call(('

subprocess.call(('

subprocess.call(('

```
i = 0
for item in questionnum:
    subprocess.call({'echo' '+item' 't 'str(expectedans[i])'+ 't 'str(unidecode(studentans[i]))'+ 'r
n' '+fileprefix'+'+challenge' '+attempt'.txt', shell=True})
    i = i+1
subprocess.call({'echo' '+fileprefix'+'+challenge' '+attempt'.txt', shell=True})
subprocess.call({'echo' '+fileprefix'+'+challenge' '+attempt'.txt', shell=True})
subprocess.call({'echo' 'Incorrect items: ' 'r
n' '+fileprefix'+'+challenge' '+attempt'.txt', shell=True})
for item in incorrect:
    subprocess.call({'echo' '+item' 'r
n' '+fileprefix'+'+challenge' '+attempt'.txt', shell=True})

pnetgrader.emailgrade.emailgrade({userid, challenge, attempt, userid'+'+score' '+challenge' '+attempt'.txt, fileprefix'+'+challenge' '+attempt'.txt})
Appendix B

Institutional Review Board Documents

This appendix contains the information about the Institutional Review Board (IRB) protocol utilized in this thesis work. This Appendix includes the informed consent document and the IRB approval letter.

IRB Application

Table 18. Study Team Qualifications

<table>
<thead>
<tr>
<th>Role</th>
<th>Full Name</th>
<th>Individual’s Responsibilities</th>
<th>Individual’s Qualifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal Investigator</td>
<td>Ryan Kohler</td>
<td>This person will recruit the subjects, consent the subjects, administer the study, analyze the data, and write-up the conclusions of the study.</td>
<td>Ryan is a 3rd year graduate student. He has experience in study design, experiment design through classes. He also has experience with the underlying data that is used in this study.</td>
</tr>
<tr>
<td>Study Team Member #1</td>
<td>Nicklaus Giacobe</td>
<td>Dr. Giacobe will advise and oversee this project as the committee chair of the PI’s MS Committee. He will advise in the recruiting, consenting of subjects, administration of the study, and evaluation and presentation of results.</td>
<td>Dr. Giacobe is an Assistant Teaching Professor in the College of IST. He has performed similar studies in the past and has worked with this kind of study and data previously.</td>
</tr>
</tbody>
</table>
Table 19. Study Team Member’s Training Status

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Organization</th>
<th>Roles</th>
<th>Training Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nicklaus Giacobe</td>
<td>Information Sciences and Technology (UNIVERSITY PARK)</td>
<td>Advisor</td>
<td>IRB Training Completed (expires 4/2/2020)</td>
</tr>
<tr>
<td>Ryan Kohler</td>
<td>Information Sciences and Technology (UNIVERSITY PARK)</td>
<td>Principal Investigator</td>
<td>IRB Training Completed (expires 1/16/2019)</td>
</tr>
</tbody>
</table>

Protocol Title:
Provide the full title of the study as listed in item 1 on the “Basic Information” page in CATS IRB (http://irb.psu.edu).
Exploring the effectiveness and usability of the Polymorphic Homework and Laboratory System in a simulated lab environment

Principal Investigator:
Name: Ryan J. Kohler
Department: College of Information Sciences and Technology
Telephone: 814-470-7334
E-mail Address: rvk5191@ist.psu.edu

Version Date:
Provide the date of this submission. This date must be updated each time the submission is provided to the IRB office with revisions.
11/17/2017

Clinicaltrials.gov Registration #:
Provide the registration number for this study, if applicable.
Not Applicable

Important Instructions for Using This Protocol Template:
1. Add this completed protocol template to your study in CATS IRB (http://irb.psu.edu) on the “Basic Information” page, item 7.
2. This template is provided to help investigators prepare a protocol that includes the necessary information needed by the IRB to determine whether a study meets all applicable criteria for approval.
3. Type your protocol responses below the gray instructional boxes of guidance language. If the section or item is not applicable, indicate not applicable.
4. For research being conducted at Penn State Hershey or by Penn State Hershey researchers only, delete the instructional boxes from the final version of the protocol prior to upload to CATS IRB (http://irb.psu.edu). For all other research, do not delete the instructional boxes from the final version of the protocol.
5. When making revisions to this protocol as requested by the IRB, please follow the instructions outlined in the Study Submission Guide available in the Help Center in CATS IRB (http://irb.psu.edu) for using track changes.

If you need help...

University Park and other campuses:
Office for Research Protections Human Research Protection Program
The 330 Building, Suite 205
University Park, PA 16802-7014
Phone: 814-865-1775
Fax: 814-863-8699
Email: irb-orp@psu.edu

College of Medicine and Hershey Medical Center:
Human Subjects Protection Office
90 Hope Drive, Mail Code A115, P.O. Box 855
Hershey, PA 17033
(Physical Office Location: Academic Support Building Room 1140)
Phone: 717-531-5687
Fax number: 717-531-3937
Email: irb-hspo@psu.edu

Table of Contents

1.0 Objectives
2.0 Background
3.0 Inclusion and Exclusion Criteria
4.0 Recruitment Methods
5.0 Consent Process and Documentation
6.0 HIPAA Research Authorization and/or Waiver or Alteration of Authorization
7.0 Study Design and Procedures
8.0 Subject Numbers and Statistical Plan
9.0 Confidentiality, Privacy and Data Management
10.0 Data and Safety Monitoring Plan
11.0 Risks

12.0 Potential Benefits to Subjects and Others

13.0 Sharing Results with Subjects

14.0 Subject Stipend (Compensation) and/or Travel Reimbursements

15.0 Economic Burden to Subjects

16.0 Resources Available

17.0 Other Approvals

18.0 Multi-Site Research

19.0 Adverse Event Reporting

20.0 Study Monitoring, Auditing and Inspecting

21.0 Future Undetermined Research: Data and Specimen Banking

22.0 References
1.0 Objectives

1.1 Study Objectives

Describe the purpose, specific aims or objectives. State the hypotheses to be tested.

The aim of this study is to understand what effects the Polymorphic Homework and Laboratory System (PolyLab) has on subject cognitive workload and how they go about completing homework and laboratory assignments within the cyber-security domain.

In terms of testable hypotheses, we will investigate the following:

- PolyLab has minimal effect on cognitive workload
- PolyLab has reductive effect on cheating

1.2 Primary Study Endpoints

State the primary endpoints to be measured in the study. Clinical trials typically have a primary objective or endpoint. Additional objectives and endpoints are secondary. The endpoints (or outcomes), determined for each study subject, are the quantitative measurements required by the objectives. Measuring the selected endpoints is the goal of a trial (examples: response rate and survival).

The endpoint goal of the study is to determine what effects PolyLab has on the cognitive workload of subjects during a cyber-security homework/laboratory assignment and what effect it has on method of assignment completion.

1.3 Secondary Study Endpoints

State the secondary endpoints to be measured in the study.

Not Applicable

2.0 Background

2.1 Scientific Background and Gaps

Describe the scientific background and gaps in current knowledge.

In cyber-security education, a common method for teaching students is the Challenge Based Learning (CBL) methodology (R. Cheung, J. Cohen, H. Lo, & F. Elia, 2011). CBL methodology requires participants, in this case students, to draw on prior knowledge, creativity, and their fellow team members. This methodology is most commonly implemented through the use of modules or lab assignments. These modules or lab assignments are incredibly useful to
students as they apply the book and lecture knowledge to a simulated representation of the real-world. Recently these labs have become commonly implemented through the use of Virtual Machines (VMs).

Many researchers have developed or studied the use of VMs in cybersecurity education (M. Micco & H. Rossman, 2002; X. Wang, G. Hembroff, & R. Yedica, 2010; C. Willems & C. Meinel, 2012). One of the main benefits of VMs is that the system can be reset at the end. This rollback of a VM instance means that each user gets a fresh and unaltered copy of the machine(s). However, as discussed in the paper entitled: Online assessment for hands-on cyber security training in a virtual lab, this means that each student gets the same system and same machine (C. Willems & C. Meinel, 2012). Therefore the risk of cheating is increased, as each answer is the same. This is a common problem with many web-based cyber-security labs such as: Bandit by OverTheWire, National Cyber League. These labs have only one answer, making the answers quite easy to find on the internet or by asking a fellow student. Willems & Meinel propose a solution to this issue; this involves dynamically choosing several values from a pre-set list and using them as evaluation answers. These evaluation answers are also used to dynamically generate content in the lab. The system also chooses a number of other values from the list to fill the incorrect options (C. Willems & C. Meinel, 2012). This solution works quite well for a small scale assignment or lab. However, it does not eliminate the possibility of cheating as there are a limited number of possible solutions. If this system were to be used in a larger environment or eliminate the chance of cheating, it would require a large amount of effort from the evaluator to create additional solutions.

2.2 Previous Data

Describe any relevant preliminary data.

Not Applicable

2.3 Study Rationale

Provide the scientific rationale for the research.

This study compares two groups, a control group and an experimental group. These two groups will be recruited from a subset of classes and clubs within the Pennsylvania State University. This study will provide information with which to compare the two groups in order to determine if the intervention (the PolyLab tool) had any statistically significant effect on the subject’s understanding and completion of the simulated lab assignment given.

3.0 Inclusion and Exclusion Criteria

Create a numbered list below in sections 3.1 and 3.2 of criteria subjects must meet to be eligible for study enrollment (e.g., age, gender, diagnosis, etc.). Indicate specifically whether you will include any of the following vulnerable populations: (You may not
include members of these populations as subjects in your research unless you indicate this in your inclusion criteria.) Review the corresponding checklists to ensure that you have provided the necessary information.

- **Adults unable to consent**
  - Review “CHECKLIST: Cognitively Impaired Adults (HRP-417)” to ensure that you have provided sufficient information. HRP-417 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

- **Individuals who are not yet adults (infants, children, teenagers)**
  - If the research involves persons who have not attained the legal age for consent to treatments or procedures involved in the research (“children”), review the “CHECKLIST: Children (HRP-416)” to ensure that you have provided sufficient information. HRP-416 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

- **Pregnant women**
  - Review “CHECKLIST: Pregnant Women (HRP-412)” to ensure that you have provided sufficient information. HRP-412 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

- **Prisoners**
  - Review “CHECKLIST: Prisoners (HRP-415)” to ensure that you have provided sufficient information. HRP-415 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

- **Neonates of uncertain viability or non-viable neonates**
  - Review “CHECKLIST: Neonates (HRP-413)” or “CHECKLIST: Neonates of Uncertain Viability (HRP-414)” to ensure that you have provided sufficient information. HRP-413 and HRP-414 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

### 3.1 Inclusion Criteria

List the criteria that define who will be included in your study.

Subjects will be recruited from within the College of Information Sciences and Technology. Participants will either be subjects that are currently enrolled in IST 220 (Networking and Telecommunications) or have completed IST 220.

### 3.2 Exclusion Criteria

List the criteria that define who will be excluded in your study.

Those who are under the age of 18 will be excluded since consent will be difficult to acquire from a parent or legal guardian. Subjects will also be excluded if they are not currently enrolled in IST 220 or have not completed IST 220. Subjects will also be excluded from the study if they have taken or are taking IST 220 with Dr. Giacobbe or someone who is or has used his lab-set or PolyLab.
3.3 Early Withdrawal of Subjects

3.3.1 Criteria for removal from study

Insert subject withdrawal criteria (e.g., safety reasons, failure of subject to adhere to protocol requirements, subject consent withdrawal, disease progression, etc.).

If the subject chooses to withdraw from the study, their responses will be excluded from the analysis. No other early withdrawal condition is anticipated.

3.3.2 Follow-up for withdrawn subjects

Describe when and how to withdraw subjects from the study; the type and timing of the data to be collected for withdrawal of subjects; whether and how subjects are to be replaced; the follow-up for subjects withdrawn from investigational treatment.

No follow-up with withdrawn subjects will be attempted.

4.0 Recruitment Methods

4.1 Identification of subjects

Describe the methods that will be used to identify potential subjects or the source of the subjects. If not recruiting subjects directly (e.g., database query for eligible records or samples) state what will be queried, how and by whom. StudyFinder: If you intend to use StudyFinder (http://studyfinder.psu.edu) for recruitment purposes, please indicate this in section 4.1 along with any other methods for identifying subjects. Note that information provided in this protocol should be consistent with information provided on the StudyFinder page in your CATS IRB study.

For Penn State Hershey submissions using Enterprise Information Management (EIM) for recruitment, attach your EIM Design Specification form on the Basic Information page in CATS IRB (http://irb.psu.edu). See HRP-103 Investigator Manual, “What is appropriate for study recruitment?” for additional information.

Subjects will be identified by advertising in classes and club meetings relating to the nature of this study. These classes and clubs include: IST 220, IST 451, SRA 221, and the CCSO club.
### 4.2 Recruitment process

Describe how, where and when potential subjects will be recruited (e.g., approaching or providing information to potential subjects for participation in this research study).

The research team will discuss the study with professors and club advisors to inform them of our goals and to allow for any questions. The research team will then attend a club or class meeting and present a short (~5 slide summary of the study). While this is occurring, a sign-up sheet will be passed around that includes a list of available time slots. Questions will be answered at the end of the short presentation.

### 4.3 Recruitment materials

List the materials that will be used to recruit subjects. Add recruitment documents to your study in CATS IRB ([http://irb.psu.edu](http://irb.psu.edu)) on the “Consent Forms and Recruitment Materials” page. For advertisements, upload the final copy of printed advertisements. When advertisements are taped for broadcast, attach the final audio/video tape. You may submit the wording of the advertisement prior to taping to preclude re-taping because of inappropriate wording, provided the IRB reviews the final audio/video tape.

**StudyFinder:** If you intend to use StudyFinder ([http://studyfinder.psu.edu](http://studyfinder.psu.edu)) for recruitment purposes, you do not need to upload a separate recruitment document for information placed on the StudyFinder site to your study in CATS IRB. Necessary information will be captured on the StudyFinder page in your CATS IRB study.

A short presentation that provides a summary of the study will be utilized to recruit subjects.

### 4.4 Eligibility/screening of subjects

If potential subjects will be asked eligibility questions before obtaining informed consent, describe the process. Add the script documents and a list of the eligibility questions that will be used to your study in CATS IRB ([http://irb.psu.edu](http://irb.psu.edu)) on the “Consent Forms and Recruitment Materials” page.

**StudyFinder:** If you intend to use StudyFinder ([http://studyfinder.psu.edu](http://studyfinder.psu.edu)) for recruitment purposes, any scripts (phone, email, or other) used when contacting StudyFinder participants as well as any eligibility screening questions must be added to your study in CATS IRB ([http://irb.psu.edu](http://irb.psu.edu)) on the “Consent Forms and Recruitment Materials” page.

Subjects will be screened based on age, IST 220 completion status and the professor with whom they are taking or took IST 220 with. If the participant is under the age of 18, is not currently enrolled in/has completed IST 220, or is
taking or took IST 220 with Dr. Nicklaus Giacobe, Dr. David Norloff, or Dr. Marc Rigas, the survey and simulation will end.

The screening process will occur as part of the initial demographic question set which will be provided to subjects after informed consent is obtained. This will be provided in the same location in which the study will take place.

5.0 Consent Process and Documentation

Refer to “SOP: Informed Consent Process for Research (HRP-090)”, for information about the process of obtaining informed consent from subjects. HRP-090 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

5.1 Consent Process

5.1.1 Obtaining Informed Consent

5.1.1.1 Timing and Location of Consent

Describe where and when the consent process will take place.

Consent will take place before the beginning of the study. Upon arriving at the study location, participants will be informed of the credentials of the principal investigator, background information about the study’s rationale and importance, and the study’s procedure. Participants will be told explicitly that their participation is completely voluntary, that their information will remain confidential and anonymous and that they are free to withdraw participation at any time. The participants will then be asked to read and voluntarily sign the informed consent form.

5.1.1.2 Coercion or Undue Influence during Consent

Describe the steps that will be taken to minimize the possibility of coercion or undue influence in the consent process.

During the consent process, participants may reread sections of the consent form. Contact information for the principal investigator will also be listed on the informed consent page. Within the informed consent, participants will be told explicitly that their participation is completely voluntary, that their information will remain confidential and anonymous, and that they are
free to withdraw participation at any time. They will be given contact information if they decide to withdraw.

5.1.2 Waiver or alteration of the informed consent requirement

If you are requesting a waiver or alteration of consent (consent will not be obtained, required information will not be disclosed, or the research involves deception), describe the rationale for the request in this section. If the alteration is because of deception or incomplete disclosure, explain whether and how subjects will be debriefed. Add any debriefing materials or document(s) to your study in CATS IRB (http://irb.psu.edu) on the “Supporting Documents” page. NOTE: Review the “CHECKLIST: Waiver or Alteration of Consent Process (HRP-410)” to ensure you have provided sufficient information for the IRB to make these determinations. HRP-410 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

Not applicable.

5.2 Consent Documentation

5.2.1 Written Documentation of Consent

Refer to “SOP: Written Documentation of Consent (HRP-091)” for information about the process to document the informed consent process in writing. HRP-091 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

If you will document consent in writing, describe how consent of the subject will be documented in writing. Add the consent document(s) to your study in CATS IRB (http://irb.psu.edu) on the “Consent Forms and Recruitment Materials” page. Links to Penn State’s consent templates are available in the same location where they are uploaded and their use is required.

Consent will be obtained through the use of a printed informed consent form. One form will be provided to the participant for them to keep. A second form will be signed by the participant acknowledging that they have read the form and agree to voluntarily participate in the study. The form will also be signed by the PI of the study.

5.2.2 Waiver of Documentation of Consent (Implied consent, Verbal consent, etc.)

If you will obtain consent (verbal or implied), but not document consent in writing, describe how consent will be obtained. Add the consent script(s) and/or information sheet(s) to your study in CATS IRB (http://irb.psu.edu) on the “Consent Forms and Recruitment Materials” page. Links to Penn State’s consent templates are available in the same location.
location where they are uploaded and their use is required. Review “CHECKLIST: Waiver of Written Documentation of Consent (HRP-411)” to ensure that you have provided sufficient information. HRP-411 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

If your research presents no more than minimal risk of harm to subjects and involves no procedures for which written documentation of consent is normally required outside of the research context, the IRB will generally waive the requirement to obtain written documentation of consent.

Not applicable.

5.3 Consent – Other Considerations

5.3.1 Non-English Speaking Subjects

Indicate what language(s) other than English are understood by prospective subjects or representatives.

If subjects who do not speak English will be enrolled, describe the process to ensure that the oral and written information provided to those subjects will be in that language. Indicate the language that will be used by those obtaining consent.

Indicate whether the consent process will be documented in writing with the long form of the consent documentation or with the short form of the consent documentation. Review the “SOP: Written Documentation of Consent (HRP-091)” and the “Investigator Manual (HRP-103)” to ensure that you have provided sufficient information. HRP-091 and HRP-103 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

This research will not involve non-English speaking subjects.

5.3.2 Cognitively Impaired Adults

Refer to “CHECKLIST: Cognitively Impaired Adults (HRP-417)” for information about research involving cognitively impaired adults as subjects. HRP-417 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

5.3.2.1 Capability of Providing Consent

Describe the process to determine whether an individual is capable of consent.
If a subject is able to read and sign the consent form, they will be considered cognitively capable for this study.

5.3.2.2 Adults Unable To Consent

Describe whether and how informed consent will be obtained from the legally authorized representative. Describe who will be allowed to provide informed consent. Describe the process used to determine these individual’s authority to consent to research.

For research conducted in the state, review “SOP: Legally Authorized Representatives, Children and Guardians (HRP-013)” to be aware of which individuals in the state meet the definition of “legally authorized representative”. HRP-013 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

For research conducted outside of the state, provide information that describes which individuals are authorized under applicable law to consent on behalf of a prospective subject to their participation in the procedure(s) involved in this research. One method of obtaining this information is to have a legal counsel or authority review your protocol along with the definition of “children” in “SOP: Legally Authorized Representatives, Children, and Guardians (HRP-013).” HRP-013 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

Informed consent may not be granted from legally authorized representatives.

5.3.2.3 Assent of Adults Unable to Consent

Describe the process for assent of the subjects. Indicate whether assent will be required of all, some or none of the subjects. If some, indicate which subjects will be required to assent and which will not.

If assent will not be obtained from some or all subjects, provide an explanation of why not.

Describe whether assent of the subjects will be documented and the process to document assent. The IRB allows the person obtaining assent to document assent on the consent document and does not routinely require
assent documents and does not routinely require subjects to sign assent documents.

Not Applicable

5.3.3 Subjects who are not yet adults (infants, children, teenagers)

5.3.3.1 Parental Permission

Describe whether and how parental permission will be obtained. If permission will be obtained from individuals other than parents, describe who will be allowed to provide permission. Describe the process used to determine these individual’s authority to consent to each child’s general medical care.

For research conducted in the state, review “SOP: Legally Authorized Representatives, Children and Guardians (HRP-013)” to be aware of which individuals in the state meet the definition of “children”. HRP-013 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

For research conducted outside of the state, provide information that describes which persons have not attained the legal age for consent to treatments or procedures involved in the research, under the applicable law of the jurisdiction in which research will be conducted. One method of obtaining this information is to have a legal counsel or authority review your protocol along with the definition of “children” in “SOP: Legally Authorized Representatives, Children, and Guardians (HRP-013).” HRP-013 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

Not Applicable

5.3.3.2 Assent of subjects who are not yet adults

Indicate whether assent will be obtained from all, some, or none of the children. If assent will be obtained from some children, indicate which children will be required to assent. When assent of children is obtained describe whether and how it will be documented.

Not Applicable
6.0 HIPAA Research Authorization and/or Waiver or Alteration of Authorization

This section is about the access, use or disclosure of Protected Health Information (PHI). PHI is individually identifiable health information (i.e., health information containing one or more 18 identifiers) that is transmitted or maintained in any form or medium by a Covered Entity or its Business Associate. A Covered Entity is a health plan, a health care clearinghouse or health care provider who transmits health information in electronic form. See the “Investigator Manual (HRP-103)” for a list of the 18 identifiers. HRP-103 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

If requesting a waiver/alteration of HIPAA authorization, complete sections 6.2 and 6.3 in addition to section 6.1. The Privacy Rule permits waivers (or alterations) of authorization if the research meets certain conditions. Include only information that will be accessed with the waiver/alteration.

6.1 Authorization and/or Waiver or Alteration of Authorization for the Uses and Disclosures of PHI

Check all that apply:

☑ Not applicable, no identifiable protected health information (PHI) is accessed, used or disclosed in this study. [Mark all parts of sections 6.2 and 6.3 as not applicable]

☐ Authorization will be obtained and documented as part of the consent process. [If this is the only box checked, mark sections 6.2 and 6.3 as not applicable]

☐ Partial waiver is requested for recruitment purposes only (Check this box if patients’ medical records will be accessed to determine eligibility before consent/authorization has been obtained). [Complete all parts of sections 6.2 and 6.3]

☐ Full waiver is requested for entire research study (e.g., medical record review studies). [Complete all parts of sections 6.2 and 6.3]

☐ Alteration is requested to waive requirement for written documentation of authorization (verbal authorization will be obtained). [Complete all parts of sections 6.2 and 6.3]

6.2 Waiver or Alteration of Authorization for the Uses and Disclosures of PHI

6.2.1 Access, use or disclosure of PHI representing no more than a minimal risk to the privacy of the individual
6.2.1.1 Plan to protect PHI from improper use or disclosure
Include the following statement as written – DO NOT ALTER OR DELETE unless this section is not applicable because the research does not involve a waiver of authorization. If the section is not applicable, remove the statement and indicate as not applicable.

Not Applicable

6.2.1.2 Plan to destroy identifiers or a justification for retaining identifiers
Describe the plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research. Include when and how identifiers will be destroyed. If identifiers will be retained, provide the legal, health or research justification for retaining the identifiers.

Not Applicable

6.2.2 Explanation for why the research could not practicably be conducted without access to and use of PHI
Provide an explanation for why the research could not practicably be conducted without access to and use of PHI.

Not Applicable

6.2.3 Explanation for why the research could not practicably be conducted without the waiver or alteration of authorization
Provide an explanation for why the research could not practicably be conducted without the waiver or alteration of authorization.

Not Applicable

6.3 Waiver or alteration of authorization statements of agreement
By submitting this study for review with a waiver of authorization, you agree to the following statement – DO NOT ALTER OR DELETE unless this section is not applicable because the research does not involve a waiver or alteration of authorization. If the section is not applicable, remove the statement and indicate as not applicable.

Not Applicable

7.0 Study Design and Procedures
7.1 **Study Design**

Describe and explain the study design.

The design of this study is to determine if there is a cognitive difference between traditional paper labs and the simulated lab assignment system of PolyLab. Completion times, lab scores and survey data will be compared between the two groups to determine what effect, if any the PolyLab system had on subject’s work.

7.2 **Study Procedures**

Provide a description of all research procedures being performed and when they are being performed (broken out by visit, if applicable), including procedures being performed to monitor subjects for safety or minimize risks. Include any long-term follow-up procedures and data collection, if applicable.

Describe where or how you will be obtaining information about subjects (e.g., medical records, school records, surveys, interview questions, focus group topics, audio or video recordings, data collection forms, and collection of specimens through invasive or non-invasive procedures to include the amount to be collected and how often). Add any data collection instruments that will be seen by subjects to your study in CATS IRB (http://irb.psu.edu) in the “Supporting Documents” page.

7.2.1 **EXAMPLE: Visit 1 or Day 1 or Pre-test, etc. (format accordingly)**

Provide a description as defined above and format accordingly.

This study involves a demographic survey followed by a set of practice labs, and then the simulated lab assignment.

1. After the subject arrives for their chosen time slot, they will be given the consent form by the researcher.

2. The consent form will be explained by the researcher and the participant will be asked to sign the form. If they choose not to sign, they will be thanked for their time and the study will end without any further questions or steps.

3. Subjects will answer demographic questions about their age, gender, ethnicity, prior experience with networking, job experience, IST 220 completion status, and international background. If participants have not completed or not currently enrolled in IST 220, or have taken/taking IST 220 with Dr. Nicklaus Giacobe, Dr. David Norloff, or Dr. Marc Rigas the subjects will be thanks for their time and the study will end without any further questions or steps.

4. The subject will then be given a practice lab to familiarize the participant with the web interface. This lab should only take 10-20 minutes to complete.
5. Subjects will then be given 100-110 minutes to complete a simulated lab assignment. Subjects in the control group will be given the traditional lab assignment. The experimental group will be given a modified assignment generated by the PolyLab tool.

6. Subjects will be given a short situational awareness questionnaire. This questionnaire is designed to assess cognitive workload and awareness of the networking environment.

7. Upon completion of the scenario, subjects will be asked to complete several questions about the interface, networking environment, and their understanding of the simulated assignment.

7.2.2 EXAMPLE: Visit 2 or Day 2 or Post-test, etc. (format accordingly)

Provide a description as defined above and format accordingly.

Not Applicable.

7.3 Duration of Participation

Describe the duration of an individual subject’s participation in the study.

This study will take approximately 90-120 minutes to complete.

8.0 Subject Numbers and Statistical Plan

8.1 Number of Subjects

Indicate the total number of subjects to be accrued.

If applicable, distinguish between the number of subjects who are expected to be enrolled and screened, and the number of subjects needed to complete the research procedures (i.e., numbers of subjects excluding screen failures.)

We are looking to recruit approximately 12 subjects (6 subjects per group).

8.2 Sample size determination

If applicable, provide a justification of the sample size outlined in section 8.1 – to include reflections on, or calculations of, the power of the study.

The sample size we are looking for is a sample of opportunity. As this is a pilot study to determine the effectiveness of a system, we are looking more for ways to improve, than statistical significance.
8.3 Statistical methods

Describe the statistical methods (or non-statistical methods of analysis) that will be employed.

We will utilize an unpaired t-test to determine if the two groups (PolyLab and Paper Lab) are statistically the same or different. We will be comparing the two groups in regards to time for completion, and cognitive workload.

9.0 Confidentiality, Privacy and Data Management

For research being conducted at Penn State Hershey or by Penn State Hershey researchers only, the research data security and integrity plan is submitted using “HRP-598 – Research Data Plan Review Form Application Supplement”, which is available in the Library in CATS IRB (http://irb.psu.edu). Refer to Penn State College of Medicine IRB’s “Standard Operating Procedure Addendum: Security and Integrity of Human Research Data”, which is available on the IRB’s website. In order to avoid redundancy, for this section state “See the Research Data Plan Review Form” in section 9.0 if you are conducting Penn State Hershey research and move on to section 10.

For all other research, in the sections below, describe the steps that will be taken to secure the data during storage, use and transmission.

9.1 Confidentiality

9.1.1 Identifiers associated with data and/or specimens

List the identifiers that will be included or associated with the data and/or specimens in any way (e.g., names, addresses, telephone/fax numbers, email addresses, dates (date of birth, admission/discharge dates, etc.), medical record numbers, social security numbers, health plan beneficiary numbers, etc.).

If no identifiers will be included or associated with the data in any way, whether directly or indirectly, please indicate this instead.

Each participant will be identified by a unique number assigned to the subject by the study team. Participant’s name, age, and basic demographic information will be collected as part of the study.

9.1.1.1 Use of Codes, Master List

If identifiers will be associated with the data and/or specimens (as indicated in section 9.1.1 above), describe whether a master record or list containing a code (i.e., code number, pseudonyms) will be used to separate the data collected from identifiable information, where that
master code list will be stored, who will have access to the master code list, and when it will be destroyed.

If identifiers are included or associated with the data as described in section 9.1.1 above, but no master record or list containing a code will be used, it will be assumed by the IRB that the investigator plans to directly link the identifiers with the data.

A master list will be kept that associates name with the unique number assigned to the subjects by the study team. This master list will be stored on a password protected computer. This list will only be accessible by the investigators listed on this form. The master list will be destroyed by June 1, 2019.

9.1.2 Storage of Data and/or Specimens

Describe where, how and for how long the data (hardcopy (paper) and/or electronic data) and/or specimens will be stored. NOTE: Data can include paper files, data on the internet or websites, computer files, audio/video files, photographs, etc. and should be considered in the responses. Refer to the “Investigator Manual (HRP-103)” for information about how long research records must be stored following the completion of the research prior to completing this section. HRP-103 can be accessed by clicking the Library link in CATS IRB (http://irb.psu.edu).

Please review Penn State’s Data Categorization Project for detailed information regarding the appropriate and allowable storage of research data collected according to Penn State Policy AD71. Although the IRB can impose greater confidentiality/security requirements (particularly for sensitive data), the IRB cannot approve storage of research data in any way or using any service that is not permissible by Penn State Policy AD71.

Data will be stored on the Survey System’s servers for the duration of the data collection portion of the study. Once the data collection effort has ended, the data will be removed from the server and stored on password-protected systems and a shared cloud storage account between the researchers (Penn State Box service). Only those affiliated with this research will have access to the cloud storage location and the data.

The data will be stored by the researchers for a period of three years past the date of completion of the requirements for the master’s thesis.
9.1.3 Access to Data and/or Specimens

Identify who will have access to the data and/or specimens. This information should not conflict with information provided in section 9.1.1.1 regarding who has access to identifiable information, if applicable.

The data will be accessible by the researchers named in this study.

9.1.4 Transferring Data and/or Specimens

If the data and/or specimens will be transferred to and/or from outside collaborators, identify the collaborator to whom the data and/or specimens will be transferred and how the data and/or specimens will be transferred. This information should not conflict with information provided in section 9.1.1.1 regarding who has access to identifiable information, if applicable.

There are no outside collaborators.

9.2 Subject Privacy

This section must address subject privacy and NOT data confidentiality.

Indicate how the research team is permitted to access any sources of information about the subjects.

Describe the steps that will be taken to protect subjects’ privacy interests. “Privacy interest” refers to a person’s desire to place limits on whom they interact with or to whom they provide personal information.

Describe what steps you will take to make the subjects feel at ease with the research situation in terms of the questions being asked and the procedures being performed. “At ease” does not refer to physical discomfort, but the sense of intrusiveness a subject might experience in response to questions, examinations, and procedures.

The research team will not have any additional sources of information about the subjects.

The research subject’s privacy will be maintained by ensuring that all data is secured in a password protected system.

The subject may end their participation at any time during the study. The instructions during the consent process describe this to the subject prior to the initiation of the survey.
The room that the study will take place in is segmented such that there is physical separation from the rest of the room. Therefore, no intrusion is possible as the door will be shut and labeled showing that a study experiment is in progress. All other occupants will be made aware that there is an experiment going on at the given time. They will be asked to vacate the room or make minimal noise during the experiment.

10.0 Data and Safety Monitoring Plan

This section is required when research involves more than Minimal Risk to subjects. As defined in “SOP: Definitions (HRP-001)”, available in the Library in CATS IRB (http://irb.psu.edu), Minimal Risk is defined as the probability and magnitude of harm or discomfort anticipated in the research that are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests. For research involving prisoners, Minimal Risk is the probability and magnitude of physical or psychological harm that is normally encountered in the daily lives, or in the routine medical, dental, or psychological examination of healthy persons. Please complete the sections below if the research involves more than minimal risk to subjects OR indicate as not applicable.

10.1 Periodic evaluation of data
Describe the plan to periodically evaluate the data collected regarding both harms and benefits to determine whether subjects remain safe.

Not Applicable.

10.2 Data that are reviewed
Describe the data that are reviewed, including safety data, untoward events, and efficacy data.

Not Applicable.

10.3 Method of collection of safety information
Describe the method by which the safety information will be collected (e.g., with case report forms, at study visits, by telephone calls and with subjects).

Not Applicable.

10.4 Frequency of data collection
Describe the frequency of data collection, including when safety data collection starts.

Not Applicable.
10.5 **Individuals reviewing the data**

Identify the individuals who will review the data. The plan might include establishing a data and safety monitoring committee and a plan for reporting data monitoring committee findings to the IRB and the sponsor.

Not Applicable.

10.6 **Frequency of review of cumulative data**

Describe the frequency or periodicity of review of cumulative data.

Not Applicable.

10.7 **Statistical tests**

Describe the statistical tests for analyzing the safety data to determine whether harms are occurring.

Not Applicable.

10.8 **Suspension of research**

Describe any conditions that trigger an immediate suspension of research.

Not Applicable.

11.0 **Risks**

List the reasonably foreseeable risks, discomforts, hazards, or inconveniences to the subjects related to the subjects’ participation in the research. For each potential risk, describe the probability, magnitude, duration, and reversibility. Consider all types of risk including physical, psychological, social, legal, and economic risks. If applicable, indicate which procedures may have risks to the subjects that are currently unforeseeable. If applicable, indicate which procedures may have risks to an embryo or fetus should the subject be or become pregnant. If applicable, describe risks to others who are not subjects.

Please keep in mind that loss of confidentiality is a potential risk when conducting human subject research and should be addressed as such.

Possible physical discomfort will be no more than a user might expect from spending two hours at a computer in a standard office setting. We do not expect this discomfort to be significant and offer several break/stretch opportunities during the study.

Loss of confidentiality is a low risk. The demographic information that we are requesting is minimal and if, in the unlikely event of accidental disclosure of a participant’s identity and study performance, the risks to the participant are negligible. We are *not* collecting other PII, such as social security numbers, etc. The cognitive assessments that
we are taking are not well known in industry and are not used by human resource
managers for performance evaluation of employees.

The collected data will be protected by storing it on password protected computers.
Additionally, the files will be stored on network file shares in which only personnel who
are on this application are allowed access. Any data that is captured with the online web
survey tool (Qualtrics) will be stored on their servers for the duration of the study. Only
the PI and the personnel who are listed on this application will have access to this data.
Finally, the paper documents including signed consent forms will be stored in a locked
file cabinet in the PI's locked office.

All participants will be given a sequentially-derived study-specific ID number to be used
on all study submissions. This number is not linked to any external identification.

In terms of physical discomfort, the study will be time-limited (120 minutes). Several
stretch breaks will be offered to the participant during the study.

12.0 Potential Benefits to Subjects and Others

12.1 Potential Benefits to Subjects

Describe the potential benefits that individual subjects may experience from
taking part in the research. If there is no direct benefit to subjects, indicate as
such. Compensation is not considered a benefit. Compensation should be
addressed in section 14.0.

The primary benefit to subjects from participating in this research is that the
subject may be presented with network data or an assessment technique that
they have not previously experienced.

12.2 Potential Benefits to Others

Include benefits to society or others.

The benefits to society are twofold, instructors will be able to create
assignments that are different from semester to semester and across subjects
and a mechanism for delivery and grading assignments to classes of 100+
subjects will be available for use.

13.0 Sharing Results with Subjects

Describe whether results (study results or individual subject results, such as results of
investigational diagnostic tests, genetic tests, or incidental findings) will be shared with
subjects or others (e.g., the subject’s primary care physicians) and if so, describe how it will
be shared.

Results of this study will not be shared with participants.
14.0 Subject Stipend (Compensation) and/or Travel Reimbursements

Describe the amount and timing of any subject stipend/payment or travel reimbursement here. If there is no subject stipend/payment or travel reimbursement, indicate as not applicable.

If course credit or extra credit is offered to subjects, describe the amount of credit and the available alternatives. Alternatives should be equal in time and effort to the amount of course or extra credit offered.

If an existing, approved student subject pool will be used to enroll subjects, please indicate as such and indicate that course credit will be given and alternatives will be offered as per the approved subject pool procedures.

Not Applicable.

15.0 Economic Burden to Subjects

15.1 Costs

Describe any costs that subjects may be responsible for because of participation in the research.

There are no costs related to participation in this study.

15.2 Compensation for research-related injury

If the research involves more than Minimal Risk to subjects, describe the available compensation in the event of research related injury.

If there is no sponsor agreement that addresses compensation for medical care for research subjects with a research-related injury, include the following text as written - DO NOT ALTER OR DELETE:

It is the policy of the institution to provide neither financial compensation nor free medical treatment for research-related injury. In the event of injury resulting from this research, medical treatment is available but will be provided at the usual charge. Costs for the treatment of research-related injuries will be charged to subjects or their insurance carriers.

For sponsored research studies with a research agreement with the sponsor that addresses compensation for medical care for research-related injuries, include the following text as written - DO NOT ALTER OR DELETE:

It is the policy of the institution to provide neither financial compensation nor free medical treatment for research-related injury. In the event of injury resulting from this research, medical treatment is available but will be provided at the usual charge. Such charges may be paid by the study sponsor as outlined in the research agreement and explained in the consent form.
It is the policy of the institution to provide neither financial compensation nor free medical treatment for research-related injury. In the event of injury resulting from this research, medical treatment is available but will be provided at the usual charge. Costs for the treatment of research-related injuries will be charged to subjects or their insurance carriers.

16.0 Resources Available

16.1 Facilities and locations
Identify and describe the facilities, sites and locations where recruitment and study procedures will be performed.

If research will be conducted outside the United States, describe site-specific regulations or customs affecting the research, and describe the process for obtaining local ethical review. Also, describe the principal investigator’s experience conducting research at these locations and familiarity with local culture.

Study procedures will be performed in a lab space within the Westgate building at the Pennsylvania State University Main Campus. Recruitment will take place during meetings of clubs and classes at the Pennsylvania State University Main Campus.

16.2 Feasibility of recruiting the required number of subjects
Indicate the number of potential subjects to which the study team has access. Indicate the percentage of those potential subjects needed for recruitment.

The study team has access to approximately 630 subjects across the classes and clubs eligible to take part in the study. For this study we will need approximately 2-3% of these total subjects to complete this study.

16.3 PI Time devoted to conducting the research
Describe how the PI will ensure that a sufficient amount of time will be devoted to conducting and completing the research. Please consider outside responsibilities as well as other on-going research for which the PI is responsible.

The primary investigator is a full-time graduate student at the Pennsylvania State University. The PI is expecting to dedicate approximately 20 hours a week until the study is completed.

16.4 Availability of medical or psychological resources
Describe the availability of medical or psychological resources that subject might need as a result of their participation in the study, if applicable.
It is not expected that participants will need medical or psychological resources as a result of this study.

16.5 Process for informing Study Team

Describe the training plans to ensure members of the research team are informed about the protocol and their duties, if applicable.

Additional training will not be necessary for the study team members.

17.0 Other Approvals

17.1 Other Approvals from External Entities

Describe any approvals that will be obtained prior to commencing the research (e.g., from cooperating institutions, community leaders, schools, external sites, funding agencies).

Not Applicable.

17.2 Internal PSU Committee Approvals

Check all that apply:

☐ Anatomic Pathology – Hershey only – Research involves the collection of tissues or use of pathologic specimens. Upload a copy of HRP-902 - Human Tissue For Research Form on the “Supporting Documents” page in CATS IRB. This form is available in the CATS IRB Library.

☐ Animal Care and Use – All campuses – Human research involves animals and humans or the use of human tissues in animals

☐ Biosafety – All campuses – Research involves biohazardous materials (human biological specimens in a PSU research lab, biological toxins, carcinogens, infectious agents, recombinant viruses or DNA or gene therapy).

☐ Clinical Laboratories – Hershey only – Collection, processing and/or storage of extra tubes of body fluid specimens for research purposes by the Clinical Laboratories; and/or use of body fluids that had been collected for clinical purposes, but are no longer needed for clinical use. Upload a copy of HRP-901 - Human Body Fluids for Research Form on the “Supporting Documents” page in CATS IRB. This form is available in the CATS IRB Library.

☐ Clinical Research Center (CRC) Advisory Committee – All campuses – Research involves the use of CRC services in any way.
 Conflict of Interest Review – All campuses – Research has one or more of study team members indicated as having a financial interest.

 Radiation Safety – Hershey only – Research involves research-related radiation procedures. All research involving radiation procedures (standard of care and/or research-related) must upload a copy of HRP-903 - Radiation Review Form on the “Supporting Documents” page in CATS IRB. This form is available in the CATS IRB Library.

 IND/IDE Audit – All campuses – Research in which the PSU researcher holds the IND or IDE or intends to hold the IND or IDE.

 Scientific Review – Hershey only – All investigator-written research studies requiring review by the convened IRB must provide documentation of scientific review with the IRB submission. The scientific review requirement may be fulfilled by one of the following: (1) external peer-review process; (2) department/institute scientific review committee; or (3) scientific review by the Clinical Research Center Advisory committee. NOTE: Review by the Penn State Hershey Cancer Institute Scientific Review Committee is required if the study involves cancer prevention studies or cancer patients, records and/or tissues. For more information about this requirement see the IRB website at: http://www.pennstatehershey.org/web/irb/home/resources/investigator

### 18.0 Multi-Site Research

If this is a multi-site study (i.e., the study will be conducted at other institutions each with its own principal investigator) and you are the lead investigator, describe the processes to ensure communication among sites in the sections below.

#### 18.1 Communication Plans

Describe the plan for regular communication between the overall study director and the other sites to ensure that all sites have the most current version of the protocol, consent document, etc. Describe the process to ensure all modifications have been communicated to sites. Describe the process to ensure that all required approvals have been obtained at each site (including approval by the site’s IRB of record). Describe the process for communication of problems with the research, interim results and closure of the study.

Not Applicable.

#### 18.2 Data Submission and Security Plan

Describe the process and schedule for data submission and provide the data security plan for data collected from other sites. Describe the process to ensure
all engaged participating sites will safeguard data as required by local information security policies.

Not Applicable.

18.3 **Subject Enrollment**

Describe the procedures for coordination of subject enrollment and randomization for the overall project.

Not Applicable.

18.4 **Reporting of Adverse Events and New Information**

Describe how adverse events and other information will be reported from the clinical sites to the overall study director. Provide the timeframe for this reporting.

Not Applicable.

18.5 **Audit and Monitoring Plans**

Describe the process to ensure all local site investigators conduct the study appropriately. Describe any on-site auditing and monitoring plans for the study.

Not Applicable.

19.0 **Adverse Event Reporting**

19.1 **Reporting Adverse Reactions and Unanticipated Problems to the Responsible IRB**

By submitting this study for review, you agree to the following statement – DO NOT ALTER OR DELETE:

In accordance with applicable policies of The Pennsylvania State University Institutional Review Board (IRB), the investigator will report, to the IRB, any observed or reported harm (adverse event) experienced by a subject or other individual, which in the opinion of the investigator is determined to be (1) unexpected; and (2) probably related to the research procedures. Harms (adverse events) will be submitted to the IRB in accordance with the IRB policies and procedures.
20.0 Study Monitoring, Auditing and Inspecting

20.1 Auditing and Inspecting

By submitting this study for review, you agree to the following statement – DO NOT ALTER OR DELETE:

The investigator will permit study-related monitoring, audits, and inspections by the Penn State quality assurance program office(s), IRB, the sponsor, and government regulatory bodies, of all study related documents (e.g., source documents, regulatory documents, data collection instruments, study data etc.). The investigator will ensure the capability for inspections of applicable study-related facilities (e.g., pharmacy, diagnostic laboratory, etc.).

21.0 Future Undetermined Research: Data and Specimen Banking

If this study is collecting identifiable data and/or specimens that will be banked for future undetermined research, please describe this process in the sections below. This information should not conflict with information provided in section 9.1.1 regarding whether or not data and/or specimens will be associated with identifiers (directly or indirectly).

21.1 Data and/or specimens being stored

Identify what data and/or specimens will be stored and the data associated with each specimen.

Not Applicable.

21.2 Location of storage

Identify the location where the data and/or specimens will be stored.

Not Applicable.

21.3 Duration of storage

Identify how long the data and/or specimens will be stored.

Not Applicable.

21.4 Access to data and/or specimens

Identify who will have access to the data and/or specimens.

Not Applicable.
21.5 Procedures to release data or specimens

Describe the procedures to release the data and/or specimens, including: the process to request a release, approvals required for release, who can obtain data and/or specimens, and the data to be provided with the specimens.

Not Applicable.

21.6 Process for returning results

Describe the process for returning results about the use of the data and/or specimens.

Not Applicable.

22.0 References

List relevant references in the literature which highlight methods, controversies, and study outcomes.


Informed Consent Document

CONSENT FOR RESEARCH

The Pennsylvania State University

Title of Project: Exploring the effectiveness and usability of the Polymorphic Homework and Laboratory System in a simulated lab environment

Principal Investigator: Ryan Kohler
E 347/348 Westgate Building
University Park, PA 16802-6823
814-470-7334
Advisor: Dr. Nicklaus A. Giacobe

1. Why is this research study being done?
This study is being conducted for research purposes to measure the effectiveness of the Polymorphic Homework and Laboratory System, or PolyLab, tool in a simulated networking class lab assignment. In this study, we ask participants to complete a simulated lab assignment utilizing the PolyLab tool or the standard lab assignment. The PolyLab tool is a system designed to aid in grading for the instructors and to create unique labs for the students so that each student gets a different assignment. We seek to determine if this system performs similarly to a regular written assignment. This knowledge will be utilized to assist in future design choices for the PolyLab system. It will also assist in the determination of how to deploy this in the classroom environment. This study is not being funded by any grants.

2. Procedures to be followed:
You will participate in a simulated networking class lab assignment. We will begin the task with a brief demographic survey that asks questions about you and your prior work experience. You will be provided with training materials in the form of practice labs and assignments. These practice labs and assignments are designed to help you learn the features of the interface that you will be using for the simulated lab assignment. During the scenario, your time and answers to lab questions will be recorded. Also during the scenario, you may be presented with a randomly-timed short SA query. If you receive such a query, you will return to the scenario after the survey has been completed. After the scenario, you will complete several assessment questionnaires that will ask about your understanding of the interface and the networking environment that you were presented with in the scenario.
3. **Benefits:**

The primary benefit to you from participating in this research is that you may be presented with network data or an assessment technique that you have not previously experienced.

The benefits to society are twofold, instructors will be able to create assignments that are different from semester to semester and across students and a mechanism for delivery and grading assignments to classes of 100+ students will be available for use.

4. **Duration/Time:**

The amount of time you spend in the simulated assignment and pre-trial demographic survey is up to you. The entire duration of your visit to the lab is expected to be no more than 120 minutes.

5. **Discomforts/Risks**

Possible physical discomfort will be no more than a user might expect from spending two hours at a computer in a standard office setting. We do not expect this discomfort to be significant and offer several break/stretch opportunities during the study.

Loss of confidentiality is a low risk. The demographic information that we are requesting is minimal and if, in the unlikely event of accidental disclosure of a participant's identity and study performance, the risks to the participant are negligible. We are *not* collecting other PII, such as social security numbers, etc. The cognitive assessments that we are taking are not well known in industry and are not used by human resource managers for performance evaluation of employees.

The collected data will be protected by storing it on password protected computers. Additionally, the files will be stored on network file shares in which only personnel who are on this application are allowed access. Any data that is captured with the online web survey tool (Qualtrics) will be stored on their servers for the duration of the study. Only the PI and the personnel who are listed on this application will have access to this data. Finally, the paper documents including signed consent forms will be stored in a locked file cabinet in the PI's locked office.

All participants will be given a sequentially-derived study-specific ID number to be used on all study submissions. This number is not linked to any external identification.

In terms of physical discomfort, the study will be time-limited (120 minutes). Several stretch breaks will be offered to the participant during the study.

6. **Statement of Confidentiality:**

We use a web-based survey system to collect data. This system relies on SSL/HTTPS. The data is securely encrypted in transit between the web browser and the survey website. It is stored by a
third party professional web survey company on their servers until all responses have been collected. Data is securely encrypted in transit to the researcher and stored on a computer system that is professionally managed, audited and password protected. Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties.

You will be assigned a three-digit study participant number. This number is the only data that links your responses in your pre-trial survey, consent form and the in-trial and post-trial performance data from the simulation.

In the event of a publication or presentation resulting from the research, no personally identifiable information will be shared. Data collected on you and your performance will be anonymized prior to release. We will not be including any personally identifying information in our data analysis or in any of the publishable products that may result from this research.

Data that we collect from your participation will be securely stored for at least 3 years after the completion of the study and will be destroyed no earlier than December 31, 2020.

7. Right to Ask Questions:

Please call the head of the research study (principal investigator), Ryan Kohler at 814-470-7334 if you:

- Have questions, complaints or concerns about the research.
- Believe you may have been harmed by being in the research study.

You may also contact the Office for Research Protections at (814) 865-1775, ORProtections@psu.edu if you:

- Have questions regarding your rights as a person in a research study.
- Have concerns or general questions about the research.
- You may also call this number if you cannot reach the research team or wish to offer input or to talk to someone else about any concerns related to the research.

8. Voluntary Participation:

Your decision to be in this research is voluntary. You can stop at any time. You do not have to answer any questions you do not want to answer. Refusal to take part in or withdrawing from this study will involve no penalty or loss of benefits you would receive otherwise.

You must be 18 years of age or older to consent to take part in this research study. If you agree to take part in this research study and the information outlined above, please sign your name and indicate the date below.

You will be given a copy of this consent form for your records.
<table>
<thead>
<tr>
<th>Signature of Subject</th>
<th>Date</th>
<th>Printed Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Obtaining Consent</td>
<td>Date</td>
<td>Printed Name</td>
</tr>
</tbody>
</table>
IRB Approval Letter

EXEMPTION DETERMINATION

Date: January 4, 2018

From: Philip Frum, IRB Analyst

To: Ryan Kohler

<table>
<thead>
<tr>
<th>Type of Submission:</th>
<th>Initial Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title of Study:</td>
<td>Exploring the effectiveness and usability of the Polymorphic Homework and Laboratory System in a simulated lab environment</td>
</tr>
<tr>
<td>Principal Investigator:</td>
<td>Ryan Kohler</td>
</tr>
<tr>
<td>Study ID:</td>
<td>STUDY000008660</td>
</tr>
<tr>
<td>Submission ID:</td>
<td>STUDY000008660</td>
</tr>
<tr>
<td>Funding:</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
| Documents Approved: | • Demographic Questions.docx (0.01), Category: Data Collection Instrument  
• HRP-591 - Protocol for Human Subject Research v2.pdf (1.01), Category: IRB Protocol  
• NASA-TLX Questions.docx (0.01), Category: Data Collection Instrument  
• Networking Assignment Questions.pdf (0.01), Category: Data Collection Instrument  
• Practice Lab Assignment Questions.pdf (0.01), Category: Data Collection Instrument  
• Subject Stimuli.docx (0.01), Category: Data Collection Instrument |

The Office for Research Protections determined that the proposed activity, as described in the above-referenced submission, does not require formal IRB review because the research met the criteria for exempt research according to the policies of this institution and the provisions of applicable federal regulations.

Continuing Progress Reports are not required for exempt research. Record of this research determined to be exempt will be maintained for five years from the date of this notification. If your research will continue beyond five years, please contact the Office for Research Protections closer to the determination end date.

Changes to exempt research only need to be submitted to the Office for Research Protections in limited circumstances described in the below-referenced Investigator...
Manual. If changes are being considered and there are questions about whether IRB review is needed, please contact the Office for Research Protections.

Penn State researchers are required to follow the requirements listed in the Investigator Manual (HRP-103), which can be found by navigating to the IRB Library within CATS IRB (http://irb.psu.edu).

This correspondence should be maintained with your records.

Figure 38. IRB Approval Letter
Appendix C

Demographic Questionnaire

1. What is the participant number that the researcher gave you?

2. To which gender do you most identify?
   a. Female
   b. Male
   c. Not Listed
   d. Prefer Not to Answer

3. What is your age?

4. Are you of Hispanic, Latino, or of Spanish Origin?
   a. Yes
   b. No
   c. Prefer Not to Answer

5. How would you describe yourself?
   a. American Indian or Alaska Native
   b. Asian
   c. Black or African American
   d. Native Hawaiian or Other Pacific Islander
   e. White or Caucasian
   f. Prefer Not to Answer

6. Student Standing
   a. Freshman
   b. Sophomore
   c. Junior
   d. Senior
   e. Graduate Student (Masters)/IUG
   f. Graduate Student (Ph.D.)

7. What is your IST 220 or equivalents completion status?
   a. Completed
   b. In Progress
   c. Incomplete

8. Did you take or are you taking IST 220 or equivalents with Dr. Nicklaus Giacobe, Dr.
   David Norloff, or Dr. Marc Rigas?

9. Aside from College classes, do you have any prior course experience with networking? If
   so, please explain below.

10. Do you have prior job experience working with networking? If so, please explain below.

11. My native language is?
a. English
b. Bi-Lingual (with English and ______)
c. Not English (Enter language below)
Appendix D

Situation Awareness Global Assessment Technique (SAGAT)

Practice Lab Assignment

Question 0: What is the participant number that the researcher gave you?

Question 1: What is the IP address of the public server in this communication?

Question 2: What is your Secret Code? It will be 32 characters in length. Here is an example of a secret code: b71cf9cfd922f800c1558cd2abe50be

Submit

Figure 39. Practice Lab Assignment SAGAT
Networking Assignment

Question 0: What is the participant number that the researcher gave you?

Question 1: Identify the ARP request from 192.168.143.241 looking for the address of 192.168.143.1. What is the MAC Address of 192.168.143.241? Note: you need to dig into the data to get the full 48-bit (hex) MAC address. Hint - We want you to provide the hex MAC address, so it doesn't start with "Dell".

Question 2: Identify the next ARP response. What is the MAC Address of 192.168.143.17? Note: you need to dig into the data to get the full 48-bit (hex) MAC address. Hint - It doesn't start with "Cisco".

Question 3a: Identify an ARP request from 192.168.143.1 looking for the address of 192.168.143.142. What is the destination MAC address of this request?

Question 3b: Why do you think that 192.168.143.1 sent this request in this fashion?

- A. The message was sent to all Fs (MAC address contained only F values) as that is the easiest way to get the router to respond to a message.
- B. The message was sent to all Fs (MAC address contained only F values) as the ip of the destination host is unknown.
- C. The message was sent to all Fs (MAC address contained only F values) as that is the address of the destination host.
- D. The person who sent the message did not study hand enough in their networking class and got Fs on all of their assignments.

Question 4: Assuming the other host is turned on and responds, explain why you don’t see the response in this packet capture?

- A. The person with the packet capture thought it was not needed and so deleted the response.
- B. The packet was sent with a flag that hides it from view in a packet capture.
- C. The network contains switches and as the response was sent in unicast and thus not viewable.
- D. Packet captures only capture network traffic on one subnet. The other host is therefore not on this subnet.

Question 5: What role do you think that 192.168.143.1 plays in this network? Explain the reasoning behind your conclusion.

This section uses the Macbeth.pcap file.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message.

Question 6: What is the 48-bit Ethernet address of the computer that made the request?

Question 7a: What is the 48-bit destination address in the Ethernet frame?

Question 7b: What node does this MAC address correspond to? (Hint: the answer is not the web server).

- A. This MAC address belongs to a proxy server that is being used to forward all traffic.
- B. This MAC address belongs to the router right before the web server. This is due to the web server being on a different network and so we need to go through its router in order to talk with it.
- C. This MAC address belongs to our router, also known as the default gateway. This is due to the fact that the traffic coming from our network would need to be translated to allow traffic across the WAN.
- D. All of the above are correct.

Next answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message. This will be the packet with the beginning of the text file in it. You should be able to see the text of Shakespeare's Macbeth in the packet in the bottom of the window.

Question 8a: What is the value of the Ethernet source address?
Figure 40. Simulate Lab Assignment SAGAT
Appendix E

NASA-TLX Questionnaire

1. What is the participant number that the researcher gave you?

2. How mentally demanding was the task?
   1 2 3 4 5 6 7

3. How physically demanding was the task?
   1 2 3 4 5 6 7

4. How hurried or rushed was the pace of the task?
   1 2 3 4 5 6 7

5. How successful were you in accomplishing what you were asked to do?
   1 2 3 4 5 6 7

6. How hard did you have to work to accomplish your level of performance?
   1 2 3 4 5 6 7

7. How insecure, discouraged, irritated, stressed, and annoyed were you?
   1 2 3 4 5 6 7
Appendix F

SART Questionnaire

1. What is the participant number that the researcher gave you?

2. How COMPLEX was the situation that was presented in the scenario?
   1  2  3  4  5  6  7

3. How STIMULATING was the situation that was presented in the scenario?
   1  2  3  4  5  6  7

4. To what degree did the situation in the scenario require you to CONCENTRATE YOUR ATTENTION?
   1  2  3  4  5  6  7

5. To what degree did the situation in the scenario require you to DIVIDE YOUR ATTENTION?
   1  2  3  4  5  6  7

6. While addressing the situation in the scenario, how much SPARE MENTAL CAPACITY would you say you had?
   1  2  3  4  5  6  7

7. Please rate the QUANTITY OF INFORMATION that was presented in the scenario?
   1  2  3  4  5  6  7

8. Please rate the QUALITY OF INFORMATION that was presented in the scenario?
   1  2  3  4  5  6  7

9. How FAMILIAR does the situation in the scenario feel to you?
   1  2  3  4  5  6  7
VITA of Ryan J. Kohler

Education
The Pennsylvania State University (May 2018)
- MS in Information Science and Technology
- Thesis Topic: “Polymorphic Homework and Laboratory System: An Instructional Tool for Combating Cheating”
- BS in Security and Risk Analysis (with honors)
- Minor in History and Viola Performance
- NSA/DHS National Centers of Academic Excellence in Cyber Defense: Certificate of Achievement

State College Area High School (2013 with honors)

Experience

**Penn State Applied Research Laboratory**
Advanced Technology Department
*Undergraduate Research Engineer*
October 25, 2013 – Current
- Red/Blue Team Testing
- Big Data Analysis
- Designed and developed hardware & data transmission systems
- Operated a Hadoop Cluster with MapReduce, Yarn and HDFS
- Managed security and cloud servers

**Penn State College of Information Sciences and Technology**
*Graduate Student Researcher and Teaching Assistant*
April, 2016 – Current
- Developed a polymorphic homework and laboratory system to reduce cheating
- Python, BASH, and Cherrypy
- Teaching assistant for senior capstone writing and introduction to cybersecurity classes

Presentations and Publications


Gamrat, C., Giacobe, N., & Kohler, R. (September 2017). Ensuring Integrity of Course Assignments with Polylab. In Teaching Community Luncheon at the College of Information Sciences and Technology.


Honors
- Schreyer Honors College (2014-2018)
- Eagle Scout, March 2013