




2015-04-01

An Extensible Technology Framework for Cyber Security Education

Frank Jordan Sheen

Brigham Young University - Provo

Follow this and additional works at: <http://scholarsarchive.byu.edu/etd>

 Part of the [Computer Sciences Commons](#), [Educational Methods Commons](#), and the [Engineering Education Commons](#)

Recommended Citation

Sheen, Frank Jordan, "An Extensible Technology Framework for Cyber Security Education" (2015). *All Theses and Dissertations*. Paper 4375.

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in All Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu.

An Extensible Technology Framework for
Cyber Security Education

Frank Jordan Sheen

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
C. Richard G. Helps
Barry M. Lunt

School of Technology
Brigham Young University
January 2015

Copyright © 2015 Frank Jordan Sheen

All Rights Reserved

ABSTRACT

An Extensible Technology Framework for Cyber Security Education

Frank Jordan Sheen
School of Technology, BYU
Master of Science

Cyber security education has evolved over the last decade to include new methods of teaching and technology to prepare students. Instructors in this field of study often deal with a subject matter that has rigid principles, but changing ways of applying those principles. This makes maintaining courses difficult. This case study explores the kind of teaching methods, technology, and means used to explain these concepts. This study shows that generally, cyber security courses require more time to keep up to date. It also evaluates one effort, the NxSecLab, on how it attempted to relieve the administrative issues in teaching these concepts. The proposed framework in this model looks at ways to ease the administrative burden in cyber security education by using a central engine to coordinate learning management with infrastructure-as-a-service resources.

Keywords: cyber security, education, pedagogy, teaching methods, virtualization, learning management systems

ACKNOWLEDGEMENTS

This research came to fruition because of the continual support of so many individuals. Dale Rowe, my committee chair, was supportive all the way to the final result. Barry Lunt and Richard Helps each helped in narrowing the scope. My peers in the graduate program, Scott Pack, Francis Mensah, Bill Miller, Lane Broadbent, Ryan Amy, Robert LeBlanc, and others, were good friends throughout. My supervisors at work, Todd Berrett and John Sutherland, helped make it possible for me to complete this study while working professionally. Many heartfelt thanks go to my parents, in-laws, siblings, and aunts and uncles for their kind words along the way.

The real heroes throughout this study were my wife and children. Amelia was extremely supportive throughout, and always knew I could do it. Having your husband or father in graduate school, while working full time, is difficult. In the last few years, almost every prayer in our home included “please help Daddy with his thesis.” That unwavering support from family and the Heavens is invaluable. Thank you.

TABLE OF CONTENTS

LIST OF TABLES	vi
LIST OF FIGURES	vii
1 INTRODUCTION	1
1.1 Background and Problem.....	1
1.2 Research Questions and Objectives.....	2
1.3 Methodology.....	3
1.4 Delimitations.....	4
1.5 Summary.....	4
2 REVIEW OF LITERATURE	5
2.1 Cyber Security in Education.....	5
2.2 Course Development and Maintenance	7
2.3 Changes in Hands-On Learning Activities	10
2.4 Learning Management Systems and Cyber Security	14
2.5 Summary.....	17
3 METHODOLOGY	18
3.1 Research Questions and Approaches.....	18
3.2 Strategy of Inquiry	19
3.3 Role of the Researcher.....	21
3.4 Data Sampling and Collection	22
3.5 Analysis and Inference.....	25
3.6 Summary.....	30
4 PROCEDURES.....	31
4.1 Interview	31
4.2 Survey.....	35

4.3	NxSecLab Evaluation Criteria	38
4.4	Summary	39
5	RESULTS AND FINDINGS	40
5.1	Interview and Survey	40
5.2	NxSecLab.....	52
5.3	Answers to Research Questions.....	58
5.4	Summary.....	60
6	PROPOSED LEARNING MANAGEMENT FRAMEWORK FOR CYBER SECURITY EDUCATION	61
6.1	Themes from the Data.....	61
6.2	Proposed Extensible Learning Platform	62
6.3	Framework Evaluation.....	68
6.4	Summary.....	70
7	CONCLUSIONS.....	71
7.1	Overview.....	71
7.2	Future Research	72
7.3	Summary.....	73
	REFERENCES	74
	APPENDIX.....	77
	Survey Questions	77
	Survey Responses	82
	Interview Transcripts	87

LIST OF TABLES

Table 4-1 Points of Discovery and Questions.....	32
Table 4-2 Interview Protocol	33
Table 4-3 Interview Analysis Procedures	35
Table 4-4 Survey Protocol	36
Table 4-5 Survey Questions.....	37
Table 5-1 Responses to Role.....	41
Table 5-2 Learning Levels Responses from Jim and Lou	44
Table 5-3 Learning Level Responses from Wolfgang and Robert	45

LIST OF FIGURES

Figure 3-1 Method Overview.....	19
Figure 5-1 Student Role Survey Question	42
Figure 5-2 Student Role Responses	42
Figure 5-3 Respondent Role Survey Results	43
Figure 5-4 Undergraduate Learning Level Responses.....	46
Figure 5-5 Graduate Learning Level Responses.....	46
Figure 5-6 Course Change Responses from Survey	48
Figure 5-7 Common Teaching Methods Responses from Survey	48
Figure 5-8 Technology Used in Teaching Survey Responses	49
Figure 5-9 IT Capstone NxSecLab Architecture Model.....	54
Figure 5-10 NxSecLab Management Framework (Capstone Report, 2013)	55
Figure 6-1 Proposed Model	63

1 INTRODUCTION

1.1 *Background and Problem*

Cyber security education exposes students to the concept of managing risk in a highly evolving field. New problems, approaches to those problems, and topics change so often in cyber security that instructors are often continually trying to update coursework, in addition to performing other responsibilities in an academic setting. There are a few issues that contribute to the change problem in course content.

First, in order to keep courses relevant, instructors are frequently analyzing whether to re-design security courses. In the author's own observation, some security courses in the last several years have changed from focusing solely on theoretical concepts like cryptography to incorporating a greater focus on network, system, or web application security. An additional challenge has been the integration of physical security and social engineering concepts. These are topics that are very different from designing secure networks, but have become more important in industry. These examples teach important concepts to students, but have taken time and multiple iterations to try to implement.

Second, managing assignments for students can consume a lot of time, not just for the professor or instructor, but teaching assistants (TAs) as well. In the Information and Assurance (IT 466) course at Brigham Young University, the penetration testing assignment had to be carefully monitored as students were required run disruptive attacks against systems, making them unavailable for other students. This would result in some down time in performing the lab work.

During this time, students would have to wait for the system to be manually reset in order to try to complete the objectives. This kind of hands-on lab has been generally well received by students, but it comes at a high administrative cost to professors and TAs, and incurs frustration for students.

Third, the kind of technology used is static. Most networking equipment available to technology programs is configured by hand. This makes the reconfiguration somewhat tedious compared to newer technologies like OpenFlow, OpenContrails, or VMware's NSX. However, even with the capabilities of new infrastructure technologies, the framework that cyber security programs operate in needs to be revisited. The combination of dynamic content, the task of monitoring course activities, and the inflexibility of older IT infrastructure make teaching cyber security difficult.

1.2 *Research Questions and Objectives*

With cyber security programs struggling to develop content, monitor course assignments, and manage IT infrastructure, this research looks to address the following:

Research Question 1 (Q1): What technical teaching methods are used in cyber security courses?

Research Question 2 (Q2): What challenges are faced by programs with cyber security courses?

Hypothesis 1 (H1): The time investment in keeping cyber-security courses up to date is greater than that required by other computing courses.

Research Question 3 (Q3): What sources influence H1? Why?

Objective 1 (O1): Propose a suitable procedural and technical framework that could reduce time overhead by providing standardized methods for repetitive tasks and classroom management.

1.3 *Methodology*

The methodology for this research evaluates the methods used to collect data and evaluate it while considering the research questions. The first objective, to understand what technology and teaching methods cyber security programs use, consists of the following methods:

1. Interview professors or researchers in cyber security to understand their views on the challenges in their programs and curricula.
2. Using the interview data, prepare a survey to collect similar data from a wider audience of cyber security instructors or professors.
3. Using the survey data and interviews, produce criteria designed to reduce the overhead of maintaining security courses, and evaluate the BYU IT Capstone NxSecLab project against these criteria. Develop the criteria into a framework based on the evaluation outcomes.

The first part of the research comprises methods one and two. The problems noted in the background section are mostly drawn from the author's own experience, and through reviewing literature on the subject. Methods one and two are intended to collect a more defined data set and to further confirm or reject the author's assumptions about the field. These methods are based on a case study approach. Creswell noted, "One of the chief reasons for conducting a qualitative study is that the study is exploratory. This means that not much has been written about the topic or the population being studied, and the researcher seeks to listen to participants and build an understanding based on their ideas" (Creswell 2003).

The third method is an evaluation of an attempt to simplify lab administration for a cyber security course. BYU's NxSecLab is a senior capstone project that implements features for cyber security courses into a learning management system. The evaluation of this project showed some

of the concerns and challenges that cyber security programs have. It had some semi-working prototypes, but the implementation was not significant enough for the course to use it. The NxSecLab project will be used as data for the evaluation of method 3.

1.4 *Delimitations*

This study was not designed as an extensive review of cyber security education. The principle objective in the development of this framework is to understand how instructors deal with change in cyber security, and provide a framework that could potentially be used to minimize the input of that change.

An additional note is the lack of a prototype used in this study. This research sets the foundation for a model that could resolve the problems seen in cyber security education, but it does not try to prove this by implementing the model into a prototype.

1.5 *Summary*

This chapter introduced this research by explaining the issues in cyber security that deal with course updating and monitoring. These issues are not uncommon in engineering disciplines, but have an interesting component in that the content can change significantly in short periods of time. As a result, some professors in higher education struggle with this.

The research questions for this research were introduced, as well as the approach and objectives this research takes in order to answer those questions. It concludes by noting some of the delimitations—namely, the limit of scope.

2 REVIEW OF LITERATURE

This chapter provides a review of the literature on cyber security education. It starts by providing an overview of the evolution of cyber security since the 1980s. This is followed by section 2.2 which addresses how IT, computer science, and engineering curricula have matured and integrated with cyber security material. Part of that change includes how learning activities have evolved. It then concludes by reviewing how learning management systems and challenge platforms have been used in cyber security education.

2.1 *Cyber Security in Education*

The term “cyber security” is used to denote the security of electronic systems in which information resides. The idea of teaching security concepts is not new, but started to become more relevant in the 1980s. In 1986, Karen Forcht noted some observations about education and industry where security concepts were concerned. She wrote:

Educators have long struggled with the issue of whether to ignore the data security issue in order to avoid opening a “Pandora’s Box” or whether to face the issue “head-on” in the hope that the students preparing for business or industry will be cognizant of the problem and will be acquainted through college coursework with the basis of approaching and analyzing the situation. (Forcht 1986)

As technology and computing disciplines developed, more time and energy was given towards researching security concepts. In the late 1990s, Mayo and Kearn’s work explored the idea of providing a lab where students could learn computer science concepts in a quasi-hostile

environment (Mayo and Kearns 1999). The lab was designed in such a way that as students tested algorithms, or operating systems, they did so knowing that TCP/IP snooping could be in use. Even though this environment wasn't developed solely for cyber security education, it stands out as an early example of how cyber security concepts started to become more noticeable in education.

Prior to September 11, 2001, it was recognized by educators that there was still a significant lack of security concepts in computing. In May 2001, this was recognized in a journal article by Andrew Yang. He referred to the idea that at the time, the public was just becoming aware of how fragile systems were, and that a need existed to make students in undergraduate computer science programs more aware of these problems (Yang 2001). But the events of September 11, 2001 triggered a new surge in cyber security development in computing education beyond what Yang and others had envisioned. In the United States, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) committee was established under National Security Directive 42 by President George H. W. Bush, and re-designated as the Committee on National Security Systems (CNSS) in 2001 by then President George W. Bush. This committee developed a set of standards that accredited national security systems as well as security programs. Additionally, the International Organization for Standardization (ISO) has published the ISO-27002 standard on secure systems controls. These standards have contributed to a changing direction in international and national policy on cyber security. The result is that educators now see a set of expectations that public industries expect for cyber security professionals (Papanikolaou et al. 2011).

Another contribution to the surge in cyber security education development was the result of funding from the National Science Foundation (NSF) for educating professionals in information assurance (Yasinsac, Frazier, and Bogdanov 2002). Other incentives to entice students to pursue

studies in this domain include the Cybercorps: Scholarship for Service (SFS) program and the Information Assurance Scholarship Program (IASP) from the Department of Defense. Even with this effort, researchers are indicating that government officials and industry leaders are not seeing cyber security graduates who have problem-solving skills or out-of-the-box thinking abilities (Endicott-Popovsky and Popovsky 2014). This has led to concern that the technical programs still have challenges in effectively preparing students for industry positions in cyber security.

2.2 *Course Development and Maintenance*

Over the last decade and a half, a lot of research has been published on how security concepts should be brought into information technology curricula, and how they can be made more effective. Some models have been proposed, and contributing research has been published that focuses on aspects of developing effective cyber security curricula.

Crowley's research into developing information assurance curricula is fundamental. His researched identified the nature of the information assurance, potential roles of students in careers, stakeholders in cyber security education, and an effort to develop a common body of knowledge. His perspective was such that security issues were dependent largely on the context in which they happen, and that from a technical perspective it was dynamic and evolving because of the discovery of vulnerabilities, publishing of exploits, and the types of countermeasures that are required. He also added that information assurance was dependent on so many disciplines. It involved aspects of "psychology, sociology, law, computer science, computer engineering, and management" (Crowley 2003). This means that security is a multi-disciplinary field involving expertise from a wide variety of areas. The active component suggested that "unlike some fields, knowing what to do and why to do it may not increase an organization's Information Assurance", with the end result being that knowing how to apply security concepts was a crucial part of a

security curriculum. These ideas have been referred to repeatedly over the last decade since they were published.

There were, and continue to be, varying degrees of debate on how these ideas should be applied. For example, in the mid 2000s researchers started looking at how best to incorporate security concepts. In Border and Holden's research, they interviewed IT faculty to find out how best to incorporate security education in an IT curriculum (Border and Holden 2003). They noted that everyone felt differently about how best to incorporate security. Some felt it was best to add additional courses, others thought that security specific modules for each topic of study were the best fit. Rowe et al discussed this issue by stating, "Many academics have stated the need for security-across-the-curricula in IT programs. The proposal of a cyber-security emphasis should not be seen as countering this research and we caution strongly against removing security content from IT topics in order to move it to defined cyber-security courses" (Rowe, Lunt, and Ekstrom 2011). After reviewing a few examples of instruction, the approach to incorporate security across curricula advocated by Rowe and others appears to be a common model. It is also the kind of model accredited by NSA/DHS as National Centers of Academic Excellence (CAE).

During this time, research was published showing the experience of educators as they tried to incorporate security concepts into their courses. O'Leary's paper identified an outline of a security program at Towson University. The capstone security course emphasized "defensive tools and techniques at the expense of attacks" (O'Leary 2006). Students were divided into teams, and then focused on defensive topics like firewalls. Then, a later lab would focus on reconnaissance. O'Leary noted that students had to carefully plan out how to secure their systems. When they didn't, they were quickly punished by other teams. That led O'Leary to consider whether the students' education was sufficient to help them detect and respond to sophisticated attacks.

There are examples where research showed how a curriculum could be better designed. Papanikolaou et al. connects with the premise of O’Leary’s and others. The intent of the course was to give students opportunities to think like a hacker and better understand the point of view, tools, and ethical ramifications of such actions. The hands-on labs were developed based on the listing of the OWASP Top 10 Web Application and Security Risks (Papanikolaou et al. 2011). The labs were done using a pre-programmed tool that ran a web server and pages with different vulnerabilities. Papanikolaou noted that having the OWASP Top 10 as a primary part of the course was to have learning be as dynamic as the OWASP initiative. This is one example of how researchers are trying to mature a curriculum to meet the change in industry.

Another example, not directly related to cyber security, shows the effects of constantly evolving information technology on instruction. Richard Help’s dissertation, titled “Evolving Information Technology: A Case Study of the Effects of Constant Change on Information Technology Instructional Design Architecture,” showed a couple of important conclusions. First, that educators identified “change in technology as a primary motivator in changing their courses frequently” (Helps 2010). Second, it showed that there are two models adopted in how instructors approach course design: the heroic conquest model, and the formal garden model. The names speak for themselves. The model that Helps proposed for instructional design in a course where the trends change frequently was to separate out different design layers of the course, to essentially abstract the principle from the application. The idea he presented was essentially that course management and design could be broken into different domains. If the technology used in a certain course was constantly changing, the lecture component of that course could stay the same, and just the applications change. Help’s work showed that educators, from multiple domains, are well aware of the challenges of an evolving coursework.

As time has passed, more experience has been gained as educational programs have been evaluated. In 2014, Endicott-Popovsky and Popovsky developed conceptual and pedagogical models for holistic development of cyber security students. Their model, the Kuzmina-Bespalko-Popovsky model or KBP, included an approach for how to handle all of the dynamic attributes of a cyber-security curriculum including students, industry, trends, content, goals, job market, didactic process, and teachers. Popovsky applied the KBP model to a Secure Software Development Curriculum in which they built the course to meet the objectives of the Asset Protection Model (APM). The goal of the program was to change the way in which students thought about and practiced secure software design. To do this, they used established theoretical models of security practice, in this case the Asset Protection Model or APM. As they considered which topics to teach, and the level of learning, they incorporated Bloom's Taxonomy to consider the kind of learning level expected. The didactic processes considered covered a broad range of ideas from lecturing to inviting guests to discussion groups to watching demonstration videos. These procedures were considered because they "determine how quickly students learn, how engaged they are and their level of excitement for the subject." They reported that since implementing the KBP model into the program in 2005, one of the sub-programs has gone from graduating 11 students to 62.

The debate on the best way to include security topics in a curriculum may continue to be discussed by educators and researchers. This may be done as new data comes out in the experiences in designing and integrating cyber security into courses.

2.3 *Changes in Hands-On Learning Activities*

One of the large areas of research concerned in cyber security education is the development of practical hands-on exercises. Cyber-security courses are "a particularly appropriate topic for

lab-based instruction as many labs are unscripted and ‘open-ended’ allowing multiple correct solutions” (Rowe, Lunt, and Ekstrom 2011). Others have shown in research that hands-on experience is necessary in order to synthesize the topics (Abler et al. 2006). The undercurrent for this demand appears to be for students to learn at the highest levels of learning (Anderson and Krathwohl 2001). This is important because Anderson notes that students learn at the highest levels of analyzing, evaluating, and creating solutions. Experience in these areas make students better prepared to use the skills they have in the real world.

The environments in which technology is used in cyber security courses has changed so much in the last decade that it is important to recognize the impact this has had on learning. As early as 2002, researchers were describing ways in which physical labs with workstations were being used to teach security concepts. Yasinsac noted several characteristics in the development of a security laboratory. They had

- a wholly contained environment that included servers, printers, workstations, and switches;
- a way to control the configuration of the environment by using configuration locking, blocking and cloning; and
- a number of accessible security tools.

Contained environments are even more important for students to learn in today than they were twelve years ago. Because networks are much more advanced today than they used to be, students could easily make mistakes and cause disruptions outside of a contained network. (This is an additional challenge where wireless networks are used). The second concept of using configuration locking is also important. In a security lab that focuses on offensive tactics, the administrator of the lab needs to verify that vulnerabilities remain available. This technique has

evolved over time. The last concept is the accessibility to security tools. Filtering appliances often block internet access for some of these tools. Making them available to students is important because they may be the same tools used by “bad guys.”

In 2003, Shumba outlined her experience in developing a more hands-on cyber-security course that was meant as a way for students to learn security concepts, because “computer science graduates will not go out and invent new encryption algorithms or fire filtering processes.” As a result, the lab was focused on defensive principles. The important concepts from their experience were that students would understand incident response techniques, defense mechanisms, and vulnerability and logging assessments. This example has principles that can be seen throughout the development of hands-on exercises, namely

- the incorporation of practical exercises like configuring a firewall, or maintaining security of user accounts; and
- gaining familiarity with new tools and how they work.

Practical exercises like firewalls, or how to secure accounts, are often not taught in other courses. Security specific courses tend to be a place where this type of material shows up, because it relies on other foundational topics. For example, configuring a firewall with intrusion detection may not be covered in a networking class, but is an application that relies on the topics discussed in a more foundational course.

After this time, research started pointing toward virtualization as a way to simplify some of the administration problems in hands-on exercises. Ragsdale’s research built on Yasinsac’s research but broadened the ability and focus of the lab to include not just virtual machines but virtual networking. Ragsdale noted that this provided “an environment where students are free to explore without creating administratively challenging headaches when systems break because of

the use of uncertain tools” (Ragsdale, Lathrop, and Dodge Jr 2003). One of the advantages noted by Ragsdale in the use of virtualization was that “simulations allow the proposed network to be tested by a larger variety of conditions and attacks than would be feasible with a real network.” Virtualization added to the concept that security work needed to be exercised in a wholly contained environment. With virtualization, the need for physical resources like multiple computers or switching equipment was diminished. (However, scaling it would require more equipment in the future). Ragsdale indicated that the following purposes were served by their virtual lab:

- scanning and vulnerability testing
- hardening multiple operating systems
- installing, configuring, and testing security tools
- seeing exploits in an isolated (and non-persistent if desired) network
- building exploits
- planning general defensive measures

Since 2003, virtualization has been a necessary part of allowing students to have meaningful and effective learning exercises with hands-on labs.

In more recent years, virtualization has provided a challenge as well as a benefit in lab assignments. As systems have become more resource intensive, the physical hardware requirements have increased. Additionally, because some labs like penetration testing labs often are subject to outages because of attacks, there is now an increased administrative need to not expose a vulnerable system to an entire class, but to perhaps run several instances of the same system. This results in an increased overhead to maintain a larger set of servers.

There are other types of hands-on exercises that seem to be becoming more prevalent in cyber security, and that is the use of “gaming” exercises, or capture the flag contests. Gaming

exercises are a way for students to use their acquired skills in an organized way to achieve specified objectives (Rowe, Lunt, and Ekstrom 2011). A number of events are built for students with this purpose. (See National Collegiate Cyber Defense Competition for a listing of country wide defense competitions.) These competition-based exercises serve several purposes: they test students' abilities to problem solve, they expose students to employers in the job market, and they expose students to intense collaboration. Many view these types of exercises as an important part of cyber security education (Bai and Taylor 2011) (Rursch and Jacobson 2013).

2.4 *Learning Management Systems and Cyber Security*

In education, learning management systems are used as a way to “share materials, submit and return assignments, and communicate online” (Lonn and Teasley 2009). This tends to be the general reach of learning management systems (LMS) in education. But it was identified as a possibility for LMS to move from “the transmission of information towards the management and facilitation of student learning” (Coaldrake and Stedman 1999). In cyber security emphases and broader programs, learning management systems are now mostly seen as a way to administer certain aspects of a curriculum—like grading, administering quizzes, and collecting assignments or reports. This is about the extent of their operation and practical use.

There are some existing examples of how learning management systems have been developed outside of the traditional mold of what we think an LMS is. The Open Cyber Challenge Platform (OCCP) can be viewed as an LMS for cyber security in that it does one of the main functions of grading. The OCCP is a challenge platform that educators can use to “provide controlled scenarios that teach, demonstrate, and evaluate skills in cyber security areas” (OCCP 2014). The platform is also designed to be extensible and allow for changes to the environment. This could be considered a learning management system in that it provides assignments, monitors

the tools used for teaching, and provides interaction. The National Collegiate Cyber Defense Competition (CCDC) uses a similar platform, but also uses an agent to monitor blue team's systems for availability. Challenge platforms seem to be a successful way of teaching and testing students' knowledge of topics, while easing some of the administration required to evaluate a student's progress.

In the context of higher education, something with the capabilities that could tie in to existing campus solutions may ease the administrative workload while increasing the complexity of such a system. At BYU, the NxSecLab was a capstone project designed to incorporate security labs with grading procedures and infrastructure-as-a-service. This effort was in response to a problem being faced by the IT Security courses. In the capstone team's December 2013 report, the problem statement said:

When doing lab work in security classes, it is not uncommon that students will be working on virtual machines to diagnose and fix vulnerabilities, or to run exploits that cause the systems to be unstable. When working in a classroom environment, often students complain that they are unable to work due to these issues. Instructors and Teaching Assistants are constantly needed to make changes to allow students to work. Students would be much better served by working in their own environments, but the time required for each student to download and start individual virtual machines makes this solution not viable in most circumstances.

It seems that a commercial or open source system could resolve the issue. However, the requirements for the project specified some grading functionality. The following procedures outline how the process was supposed to work:

1. A student logs into the LMS
2. A student starts a lab
3. The LMS communicates with a virtualization layer, in this case VMware's vSphere, and deploys a set of VMs.

4. The virtualization layer provisions space, IP addresses, and networking for the virtual machine.
5. The student completes the lab in a virtual environment, and submits flags for grading.
6. The lab is graded by the LMS based on the outcomes of the student.

The basis for this design was the need for students to have separate environments. As mentioned earlier, the ability to configure and control environments is important. In the classes noted above, there was an additional need to isolate students further so as to not impede on another's work.

NxSecLab was developed over two years of student capstone projects, but never used in production for a course load. It may have worked to demo the functionality, but it was never completely finished. Instead of looking to incorporate available commercial or open source offerings, the project was started from scratch. The user interface was developed in PHP, and connected to another system which runs PowerShell scripts that send operations to VMware's vSphere. The database design is sufficient, but not very robust. All in all, more thought could be put in to make the project successful.

It was noted earlier that having something that could tie into a campus-wide solution could prove to be effective. The NxSecLab did provide a way for students to submit flags, but this system kept the grade on the NxSecLab controller. One advantage that was overlooked was the service oriented architecture (SOA) that is used by BYU's office of IT (OIT). OIT has developed an offering over the last few years to transform offerings and develop web service APIs. The SOA Registry contains operations or functions that authorized parties can use and integrate with their own solutions. This kind of functionality could prove very useful for the NxSecLab, but as of yet has not been considered.

2.5 *Summary*

Cyber security education has undergone a lot of change. The models continue to change and develop for the best ways in which to teach concepts to students. The KBP model stands out as a recent achievement in developing cyber security professionals. Crowley's work on defining the characteristics of cyber security education was foundational in identifying a baseline model for developing curricula.

Additionally, the experience in education with hands-on-learning continues to change. The underlying technology used to teach these concepts has moved from limited physical environments to virtualized ones that scale to allow more students exposure. More exposure to web-application security is gaining traction against the older network security practices, and cyber defense competitions continue to be a prevalent extra-curricular source of learning and evaluation.

3 METHODOLOGY

This chapter outlines the qualitative approach and methods used for this study. It provides an analysis on the validity of those methods. It gives an overview of the case study method, and why it was used to understand the frameworks and context of cyber security education. The role of the researcher is explained, as well as data sampling and collection methods for the interviews and survey. It concludes with a section on the analysis of data from the survey, and the approach taken to evaluate the NxSecLab.

3.1 *Research Questions and Approaches*

This research is focused on two objectives. The first is to understand how cyber security courses are taught and operated. The second is to devise an extensible framework for cyber security courses that could simplify any challenges based on the results of the first question. This means that this thesis is divided into two parts, each requiring different methods.

Overall, the approach taken for this research is qualitative. For the first objective, a qualitative approach made sense based on the fact that the research question is focused on a “search for understanding, a description of things happening more or less at the same time without expectation or causal explanation” (Stake 1995, p 38). However, evaluating the NxSecLab requires a different method altogether. In order to design a software architecture, a method for evaluating software architecture is needed. The idea in evaluating the NxSecLab was to look at the outcomes of the project and determine the merits of it based on standard design principles.

These are the general methods used for this research. See Figure 3-1 for an overview of the methods described.

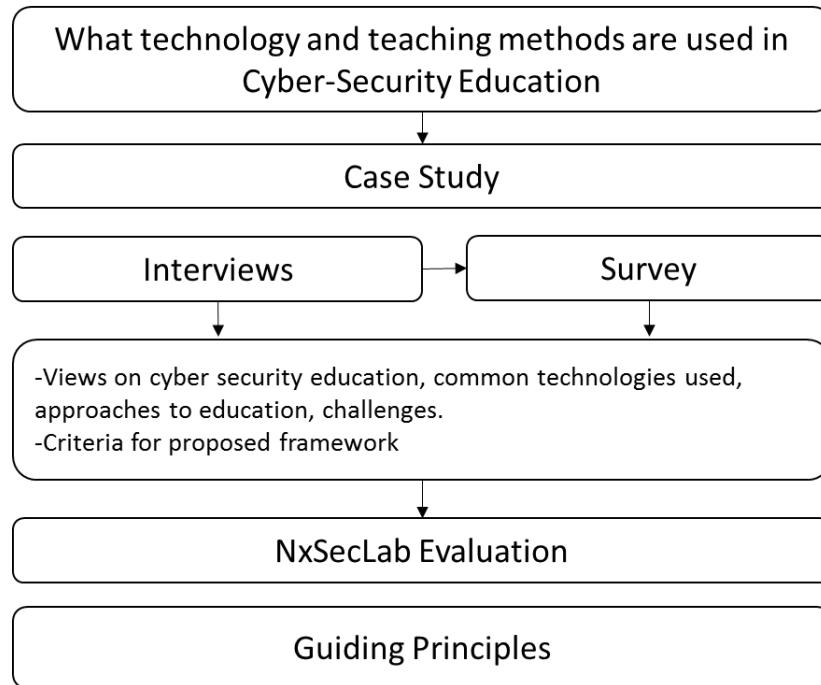


Figure 3-1 Method Overview

3.2 Strategy of Inquiry

In defining the characteristics of this research, a qualitative approach was selected based upon the goal of the research. Within qualitative research Creswell noted five categories, of which case study is the easiest to associate with this work:

“**Case studies**, in which the researcher explores in depth a program, an event, an activity, a process, or one or more individuals. The case(s) are bounded by time and activity, and researchers collect detailed information using a variety of data collection procedures over a sustained period of time. (Stake 1995)”

The strategy employed in this research was to use a case study approach because it appeared to be the best strategy for answering the research questions. The research of Endicott-Popovsky serves as an example of how case study research was used analyze the effectiveness of their model when applied to cyber security education (Endicott-Popovsky and Popovsky 2014).

The methods employed in this research for this strategy included the following:

1. Collect data through semi-structured interviews with professors in cyber security education, across a variety of fields.
2. Review the data to understand themes.
3. Code the data into key words and concepts, and identify differences among the use of the code in the interviews.
4. Design a survey based on the codes and outcomes to get a further sense of how the research questions apply to a broader sample.
5. Analyze the responses of the survey to show a higher level of understanding and abstraction.

Analyzing the software architecture for the NxSecLab does not fall squarely in line with the methods indicative of qualitative research, nor does it fall squarely in line with any public procedures. The methods used to analyze the NxSecLab included:

1. Collect reports, user requirements and code base of the project.
2. Identify architecture based on user requirements and the implementation.
3. Rank, order, or determine the value of the outcomes based on the requirements specified in the project.

These steps outline the strategy used to conduct this research, and are consistent with qualitative methods.

3.3 *Role of the Researcher*

In case study research, it is important to identify and understand the role of the researcher in the study. The author of this research graduated from the Information Technology program at Brigham Young University. This program focused on systems engineering, or the integration of different systems. The ideal role for students was that of administrators capable of engineering disparate systems to work together. My view of this role is that it abides in a certain space that connects computer science, computer engineering, and more business oriented information programs.

My experience as a student and grad student has involved participating in cyber security education from the perspective of a student and a graduate assistant. As a graduate assistant I worked on the NITEP Center of Academic Excellence accreditation. This allowed me to view the reach of cyber security in the IT program, and how it reached into other disciplines as well.

There are connections between this researcher and some of the participants. However, effort was made to increase the scope of participants so that the research would not be considered “backyard” research (Glesne and Peshkin 1992). This was done by using the initial participants to get an idea of the themes, and then extend the questions out to a broader audience by use of a survey. This methodology was presented to the Institutional Review Board (IRB) and approved. The IRB recognized that this research was focused on seeing a perspective of a process, and not directly focusing on individual cases. In order to satisfy the IRB regulations, masking of individuals and institutions was used in order to provide anonymity for their responses.

3.4 *Data Sampling and Collection*

This section reviews the methods used in selecting individuals for participation in the study, and how data from them was collected. It also discusses the methods used for collecting data on the NxSecLab.

Selection of Participants

Qualitative research is different from quantitative in the area of data collection. Where quantitative looks for completely random selection, qualitative “does not necessarily suggest random sampling or selection of a large number of participants and sites” (Creswell 2003). Although cyber security topics are taught in a range of programs and courses, a small group of professors were selected for interview.

Consideration was given to the field in which the professor studied cyber security. Cyber security topics have been found in computer and software engineering, business information, information technology, and computer science programs. Selecting participants with regard for their field of discipline was important in getting an idea of the general consensus among programs that incorporate cyber security concepts.

Interview Participants

For the interview process, four interviewees were selected based on their current coursework or research areas. Effort was made to contact 10–15 professors among 5 other programs in the country, but there were only 4 responses to participate in the interviews—3 from BYU in different colleges, and 1 from UNLV. However, because this procedure was used as a foundational point to validate the questions being asked, a large sample set was not a requirement.

Individuals were considered based on their work in any of the following areas: Cyber-Physical Systems, Penetration Testing, Security and Ethics, Digital Forensics, Authentication and or Trust, Privacy, Security Compliance, and Cyber Security Education.

A small set of individuals who had some experience in the previously mentioned areas were selected for the semi-structured interviews. The participants were selected based on recommendations of individuals who had experience in these areas.

Survey Participants

The sample for the survey had to come from similar fields as the individuals who were interviewed, namely computer science, information technology, or information systems programs. There were three pools used to select individuals from for the survey, because these appeared to be the most open way to reach possible respondents. This meant a limitation in the possible size of the set. Respondents were sought from

1. SIGITE
2. Cyber Security Forum Initiative (CSFI)
3. NAS CAE Accredited Programs

These three groups seemed like areas where an abundance of cyber security educators could be found and who might be willing to participate in the survey.

Interview and Survey Process

The interview and survey process used to meet the first objective of this research was as follows:

1. Select 3–5 interviewees who are in cyber security education. Interview them with a short set of questions, lasting 30–60 minutes.

2. Analyze the responses from the interview and revise the questions as necessary to validate the data being received.
3. Conduct 3–5 more interviews lasting 30–60 minutes.
4. Codify the responses, looking for topics of consensus that can be used in the survey.
5. Design the survey based on the responses, and limit it to 5–10 minutes to take.
6. Test run the survey with my committee.
7. Distribute the survey.
8. Let the survey run.
9. Export the results from the survey for analysis.

Types of Data Collected

The type of data collected from the previous steps varied between paper notes or memos, online notes, and audio files of interviews. The survey resulted in numerical data that could be downloaded in a variety of formats.

The interviews were used because they allowed the researcher to get historical and contextual information about the participant's experience in cyber security research while controlling the line of questioning (Creswell 2003). The interviews were recorded so that an accurate record of the participant's views and comments could be used in the analysis. As noted earlier, some documents were collected that consisted of articles or conference papers published by the interview participants. Interviewees were provided ahead of time a copy of the interview protocol. This protocol included heading information about the interview (time, place, participant), as well as the questions to be asked. This was done so that interviewees had time to consider what their responses might be beforehand.

The following tools were used to record the interviews:

- Audacity
- Microphone
- Google Voice for telephone conversations
- Transcribe, a Google web app for transcribing interviews

The survey data collected responses based on questions from anonymous survey takers.

The data was made available by Qualtrics in a variety of formats for statistical analysis.

3.5 *Analysis and Inference*

The analysis portion of this research was planned with several components in mind. The idea for analyzing this data was based on this idea:

Analysis is a process of generating, developing, and verifying concepts—a process that builds over time and with the acquisition of data. One derives concepts from the first pieces of data. These same concepts are compared for similarities and differences against the next set of data—either expanding concepts by adding new properties and dimensions, or, if there are new ideas in the data, adding new concepts to the list of concepts. Or, if there is still a third option of revising previous concepts if after looking at the new data it appears that another term would be more suitable. *It is important to keep in mind, that if a researcher knew all the relevant variables and relationships in data ahead of time, there would be no need to do a qualitative study* (Corbin and Strauss 2008).

The idea presented by Corbin and Strauss is that the method of analysis in a qualitative study is that one that evolves based on small increments of investigation throughout collection. This is the premise on which the analysis of data was performed for this research.

Because the data would be collected over a period of time, the analysis plan was designed to take place in the following stages:

1. After interviews had been transcribed, they would be analyzed for keywords, themes, or recurring topics among the interviews. This has been referred to as thematic analysis.
2. The transcriptions would then be coded using HyperResearch. The coding process was to use keywords that were referenced in the interview questions, and then the transcriptions were analyzed for variables based on those keywords, or phrases showing those concepts.
3. Following this, the interview questions were looked at again to see if the responses were clear. If the responses being generated were not, the question was modified or a question would be added.
4. Once the interviews were collected, the survey originally designed for the research proposal was modified to match the questions and common codes found in the interviews.
5. Once the time was completed for the survey, the responses were saved and stored using the online account for BYU on Qualtrics.com. The data was also downloaded as XLS files and used in Excel to evaluate the data for other possible metrics like the Chi-Squaredd test.
6. For the analysis, the survey was analyzed using average, median, and standard deviation. In some cases, the use of a Chi-Squaredd test was used to see if the probability that a relationship existed between two different questions was high enough that it needed to be considered.

Thematic Analysis of Interviews

The processed used to analyze the raw interview data was thematic analysis. This is simply a process of looking for themes in the words, phrases, and ideas presented in transcript material.

In his book, *Transforming Qualitative Information*, Richard E. Boyatzis wrote the following:

Thematic analysis is a process for encoding qualitative information. The encoding requires an explicit “code”. This may be a list of themes; a complex model with themes, indicators, and qualifications that are causally related; or something in between these two forms. *A theme is a pattern found in the information that at the minimum describes and organizes possible observation* or at the maximum interprets aspects of the phenomenon (Boyatzis 1998).

The method for analyzing the transcript material for this research follows a thematic process. The transcripts are read over, marked, and themes notated. In the case of this research, using semi-structured interviews provides the starting point. Each question of the semi-structured interviews focuses on an aspect of cyber security education that can be narrowed down to that question. Some of the questions are similar, but each has aspects that make it an easier task to look into the answer and see how it relates to the theme. This method evolves in the next section to simplify the process for analyzing the data.

In qualitative research, one of the difficult tasks is making sure that the coding or analysis process is reliable within a larger set of data. This is called intercoder reliability. This aspect becomes really important on a large scale research project where there are tens, even hundreds of transcripts to review. In those cases, the primary researcher may not be the only one doing the analysis. As a consequence, other researchers would need to use the codebook the same way across different data. In the case of this research, where only four interviews are collected, this is not a significant issue, as other qualitative research has argued that the standard for coding

reliability on exploratory research can be somewhat relaxed (Bernard 2000). What is an issue is making sure that the thematic analysis was validating the data.

Prior to the interviews, the questions were reviewed by Dr. Rowe to verify they would generate responses that were adequate. They were also reviewed by Larry Seawright in BYU's Center for Teaching and Learning. After the first two interviews, these questions and responses were reviewed to see if they were getting responses that dealt with the subject instead of wandering off into other topics. The analysis of these questions and the responses show that the questions were generating responses that were consistent. This simplified the thematic analysis by allowing the primary researcher to see patterns in the responses.

The results of the thematic analysis are provided in chapter 5.

Statistical Analysis of the Survey

In order to enhance the validity of this study, it became necessary to use a secondary source of data on this topic. Four interviews simply did not provide enough data. The interviews did provide a good grounding on which to build a survey, and verify that the questions being asked would give evidence to answer the research questions. The survey was then used to collect data from more sources. This type of effort to validate the data can be recognized as data triangulation (Guion, Diehl, and McDonald 2011). Data triangulation is a way of using "different sources of information in order to increase the validity of a study" (Guion, Diehl, and McDonald 2011). This survey provided a way to validate the study.

After the survey was completed, the data was downloaded in a CSV format. Simple statistics such as mean, median, and standard deviation were then used to evaluate the data. More complex functions, such as Chi-Squaredd were used on some of the data to see how likely two or more answers were due to chance. The procedures for this will be covered in chapter 4.

Evaluation of NxSecLab

One of objectives of this study was to propose a simple procedural and technical framework to resolve the issues found in the interviews and surveys. In order to accomplish this, the data from the interviews and survey were used to develop criteria that would be central to this framework. Then, using the criteria, assess an existing solution. This method was done using the BYU IT NxSecLab capstone project as the existing solution.

The evaluation process of the NxSecLab consisted of a few procedures: outline the criteria for evaluating the NxSecLab, and evaluate the NxSecLab. There exist several different evaluation methods for looking at software architecture, or usability of a system, but all of those procedures require a rigorous process for collecting numerical data to quantify the results. The evaluation simply looks to assess the efforts of the NxSecLab against the set of criteria found from the data. That is the overarching theme of the evaluation.

The criteria needed to be able to be measure against something relevant in the field. This is where the interview and survey data, as well as the principal researcher's own experience, came into play. This background served as the measuring stick for which the criteria could be set, and the NxSecLab evaluated. The procedures used for this evaluation are outlined in Section 4.3. The criteria are a set of questions that look to compare the framework the NxSecLab was built on against how cyber security education currently functions.

3.6 *Summary*

This chapter presented a study on the methods used in this research. It explained that the case study approach was used to answer the research questions, because it provided a way of exploring the subject of cyber security education. The role of the researcher was explained. Additionally, an overview the sampling and collection procedures was examined, as well as the process of analysis.

4 PROCEDURES

This chapter outlines the procedures followed to create the interviews used in gathering preliminary data. It includes a brief overview of the interview protocol and explains how the interview data was analyzed. It then details how the analysis of the interview data was fed into the survey design, and what protocols were used to administer and analyze the survey. It explains the procedures used to analyze the survey data. It also explains the procedures used to evaluate the NxSecLab project.

4.1 *Interview*

One of the important aspects of this research is the questioning used in the interviews and in the surveys. The questions needed to be written to avoid bias, assuming an expected answer, confusion or wordiness, and, most importantly, questions that get results that don't help answer the research questions (Driscoll and Brizee 2010). The primary researcher met with the Center for Teaching and Learning to discuss this, and left with some clear ideas on how to do this. Further examples helped to clarify how to design questions (see Driscoll and Brizee 2010).

Interview Goals

The interview method was used in order to answer a few important questions. These questions were:

1. What domain does the subject function in? (e.g., Computer Science, Information Technology, Business Systems.)
2. How did professors perceive the effort in maintaining security coursework?
3. What did they rely on to update coursework?
4. How did they perceive the levels of learning?

The idea of using these questions was to get the researcher exposure to a broader set of challenges. The framework in this research would be less meaningful if it could be used by only one domain. If an understanding of how different domains teach security concepts could be reached, the framework may have broader appeal.

Interview Protocol

The following table outlines the points noted above and the questions used to collect data on them:

Table 4-1 Points of Discovery and Questions

1. Role for Students	What roles does your program envision students have after graduation as a result of their taking your security course/courses?
2. Pedagogy Models	Where does your course stand in relation to cyber security theory and the practice of it? Does it lean more heavily towards one or the other?
2a. Pedagogy Models	How does this affect how you maintain your courses and lab assignments?
3. Level of Effort	What do you rely on to make your course/program flexible to the changes in cyber security in the field?
4. Levels of Learning	Bloom's Taxonomy provides a good reference on the kinds of learning that students do in courses, which can be many kinds. What kind do you perceive as being the most important in your course?
4a. Levels of Learning	How do you incorporate this into your courses?
5. Learning Management Systems*	Learning management systems have become a common tool in education. Could you envision how security lab assignments might be integrated with a learning management system? What would be good or bad about this?

*Used in interview draft version 1.1. All other questions used in 1.0, and 1.1.

Table 4-1 lists the questions used for the first three interviews. The fourth interview outline had one additional question added. Question 5, noted above, was aimed at exploring the possibilities of using an LMS along cyber security courses not just to extend quizzes, tests, or reading assignments, but as a way of delivering hands-on assignments through a cloud-like portal.

The actual procedure for interviewing was a multi-step process. The table below lists the steps and procedures of the interview protocol:

Table 4-2 Interview Protocol

<i>Step</i>	<i>Explanation</i>
1. Invite respondent	Each respondent was sent an email with an explanation of the research as well as a copy of the consent form and the interview questions.
2. Schedule time	Each interview was scheduled for a 30–60 minute block of time.
3. Collect standard consent	At the beginning of the interview, consent would be received verbally or by accepting a consent form.
4. Start recording interview	
5. Start interview questions	Ask questions from the interview form, while sometimes asking follow up questions not on the sheet.
6. Stop recording interview, and save file	

After the interview, protocol was completed. The transcription process started shortly thereafter. The interviews were exported as .wav files, and imported into the Transcribe Chrome app. The Transcribe app allowed for the pausing and starting of the audio without a foot pedal, using keyboard shortcuts. This made the transcription process less cumbersome than using something like Audacity and notepad. In all, the transcripts resulted in 83.6 minutes of audio, and 13,105 words. Once the interviews were transcribed, they were ready to be analyzed.

Interview Analysis

The interviews were each printed and read over. Notes were taken by hand, and general ideas marked through. It seemed fairly obvious that the themes were based on the questions, and that the respondents were generally able to stay on the topic. This was validating, and showed that for the most part, the questions did get answers that were relevant.

After this step, the interviews were coded in HyperResearch. The code list use consisted of the following: Bloom's, Curriculum Development Difficulty, Learning Management Systems, Pedagogy, Role, and Staying Current. The codes were applied by using the auto encode feature. The feature allowed the researcher to specify a term or multiple terms, and then let the author specify which code should be applied. This could sometimes produce some results that were unwanted, for instance, when the interviewer mentioned the terms, but it also highlighted some interesting aspects. For example, in discussing the roles for students, one researcher said:

Like for instance I tell some of the students that even if they just go out and they products [*sic*]so ya know product descriptions come to them or they read things in the in the computing news about attacks and things, I like them to be able to read and understand what they're reading. A lot of time recognize errors. Because there is just a lot of misinformation or inaccuracies or and so I just hope they have a solid kind of ground in terminology and meaning.

This quote was informational not for just the Role code, but also the Bloom's code where it showed up later. The instructor was explaining their role, but when considered in the context of the instructor's goals for learning noted the importance of understanding.

A process was needed to analyze the interviews in a consistent method. The table below shows the process used in analyzing the interviews.

Table 4-3 Interview Analysis Procedures

<i>Step</i>	<i>Explanation</i>
1. Transcribe notes	Each interview is transcribed using “Transcribe,” a Google Chrome web app. Each interview was then saved to a .txt file.
2. Review and mark transcript	After the transcripts are printed, a reading of the transcript takes place to look at the transcript for main ideas and specific points of detail.
3. Find key phrases and terms	The .txt file of the transcript is imported into HyperResearch. The document was coded based on key words from the questions and where they appeared. In the case of the question regarding Bloom’s taxonomy, each part of Bloom’s received an individual code.
4. Identify themes using textual examples	Themes were identified by grouping the source text together for certain codes. For example, in the case of student roles, the role code would show all of the context items of student role.
5. Summarize findings	Write a summary of the findings.

4.2 *Survey*

After the interviews were transcribed, reviewed, and coded using HyperResearch, the results were analyzed using the procedures noted above. The information from the interviews was used to feed the survey. Where appropriate, the questions from the interview were re-adjusted to not be open ended. Using the interviews and the responses to the interviews, a series of answers were used as options for the survey. This process was done under the assumption that the interviews could yield data that represented a broader audience.

The survey process consisted of designing the questions, testing them with beta respondents, and verifying the process for analyzing the responses. When the first questions were written in July, the author iterated through the questions three to four times before asking the beta respondents to review them. Once the respondents looked at the question and gave feedback, the author revised the questions again. After this process, the survey was ready for distribution. In order to distribute the survey, the survey target groups’ contact information was collected. Then,

using emails, online forums, and mailing lists, the survey was distributed. The following sections outline the survey protocol that was used and the analysis procedures used in analyzing the survey data collected.

Survey Protocol

The survey protocol is outlined in Table 4-4 by showing the explanation for each step. Table 4-5 shows the questions used in the survey. Each question is shown along with the options available to the respondents for answers.

Table 4-4 Survey Protocol

<i>Step</i>	<i>Explanation</i>
1. Write Survey Questions	The survey questions were drawn from the questions of the interview and responses, but were modified to be simple multiple choice questions.
2. Review Survey Questions	After the initial writing of the survey questions, the questions were reviewed with the committee. The questions were analyzed to see if they would evoke appropriate responses that related to the material.
3. Test Run	For the test run, the survey was made available online and sent to the author's thesis committee. The members reviewed the survey and sent responses back with clarifying remarks.
4. Distribution	The survey was distributed through the CSFI forum, a manually compiled list of subjects from NSA CAE institutions, and the SIGITE group. The survey respondent numbers increased heavily after the SIGITE email was sent out. Survey opened September 19 th , 2014.
5. Collection	The survey was automatically collected on Qualtrics. Survey was closed on November 6 th , 2014.

Table 4-5 Survey Questions

<i>Question</i>	<i>Possible Answers</i>
1. What is your role in teaching?	Teaching Assistant — Undergraduate, Teaching Assistant — Graduate, Instructor, Teacher K–12, Professor, Trainer
2. Please indicate below the degree to which students are less likely, likely, or more likely to take roles in the following fields upon graduation from your program.	Options included: Developer or Programmer, System Administration, Systems Audit, IT Management, Security Analyst or Engineer.
3. For students who take your cyber security courses, please indicate below the levels of learning described in your cyber security undergraduate course learning outcomes	Respondents were asked to check individual items from: Remember, Understanding, Applying, Analyzing, Evaluating, Creating
4. For students who take your cyber security courses, please indicate below the levels of learning described in your cyber security graduate course learning outcomes.	Respondents were asked to check individual items from: Remember, Understanding, Applying, Analyzing, Evaluating, Creating
5. Respondents were asked to rank feedback from students on course material, instructor clarity, skill development, course outcomes.	Mostly negative, somewhat negative, neutral, somewhat positive, mostly positive
6. Select a response from below.	Three possible responses: I run a more traditional class, I run a flipped class, and other.
7. Indicate how often you use the following items in teaching.	Respondents asked to give a value to the use of items from the list of quizzes, seminars or discussions, research assignments, projects, lectures, and learning activities.
8. Have you ever use any of the following technology in teaching?	List included several different technologies with yes or no answers.
9. Rank the items from the security domain on how much time is devoted to it.	Respondents given a list of 10 items from the CISSP domains.
10. How much of each item do you change over the course of a year?	Respondents given a table including lab exercises, lectures, projects, reading assignments, exams, and asked to give a percentage value of change for each
11. My security course is . . .	Less difficult to maintain than other courses, neutral, more difficult to maintain than other courses.

Survey Analysis

The survey collected a lot of different data. Over the 12 items in the survey, if each were broken out into individual multiple choice questions there would be a total of 54 questions. This lends itself to a lot of different methods of analysis. Qualtrics automatically calculates average and standard deviation on the data. More complex analysis using a Chi-Squaredd test would have to be done by hand. After some discussion with a professor in BYU’s statistics department, it was

determined that the Chi-Squared could be useful if the sample was closer to 50, which it wasn't. At best, for most of the questions designed, the population mean of a response could be estimated with a calculated standard error. Standard error of the mean is calculated as $SE_{\bar{x}} = s / \sqrt{n}$. Where s is the standard deviation of the sample, and n is the sample size. The results of these procedures for the questions from the survey are included in Chapter 5.

4.3 *NxSecLab Evaluation Criteria*

The interview and survey data from this study set up the premise for what the real challenges in cyber security were. The NxSecLab had to be compared against some baseline, and the criteria for that baseline came from the interview and survey data. That criteria set is central to the proposed framework of this research. The areas of consideration were the design, deliver, activity, and return of assignments and projects. Those areas appeared to be the most common criteria for which the NxSecLab could be evaluated against current cyber security education, and the most appropriate to answer the research questions.

The criteria areas were then given a set of questions that needed to be considered. The following outlines the criteria focus areas:

1. Design
 - a. How does the project affect how assignments are designed?
 - b. What does it change about aspects of the course?
 - c. How does it affect how assignments are delivered?
 - d. How does delivery affect student collaboration?
 - e. How are resources delivered in the NxSecLab?

2. Operation

- a. What does this achieve for the execution process of an assignment for both instructor and student?
- b. What challenges or benefits are there for student collaboration?
- c. How does the execution affect remote learning?
- d. How are assignments monitored for availability?
- e. How are student groups managed?
- f. How is the submission process affected?
- g. How is feedback given to students?
- h. How do students receive grades or assessments?

These procedures outline the general procedures and criteria used in evaluating the NxSecLab.

4.4 *Summary*

This chapter outlined the procedures used to conduct this research. The interview procedures, including the protocol and analysis were outlined. The survey design, protocol and analysis were included. The criteria and procedures used for evaluating the NxSecLab were defined.

5 RESULTS AND FINDINGS

This chapter is separated to show the results of the interview and survey, and later shows the evaluation of the NxSecLab. The interview and survey results show that cyber security education can cover a fairly broad range of programs. They also show what kind of teaching methods dominate instruction, what kind of technology is most used, and what kind of expectations professors have for student learning.

The evaluation of the NxSecLab shows a number of well thought considerations, as well as issues presented in the original design. The NxSecLab had some requirements that were extremely unique, and could really change how cyber security (as well as other technical disciplines) manages coursework. The project also had some architectural components that could tip administrating a course to be easier or harder.

The results section first covers the interview and survey together. Then it explains the results from the NxSecLab evaluation.

5.1 *Interview and Survey*

It was noted in section 3.1 how the interview and survey would be used to gather information about how cyber security education functioned in the current framework. These procedures collected a significant amount of data, so much that it has been difficult to navigate all the possible questions. This section will review the results based on the questions and responses from the interviews, and then show the data collected from the survey.

Student Roles

The interview and survey each had a question that looked to determine the area of focus which the professor worked in. For the interview, the question simply asked what kinds of roles the professor expected the students to have upon graduation. The survey question was modified to include the answers given from the interview, and provide the respondents with options. The answers showed just how varied the roles can be. The following table shows some overview of the responses:

Table 5-1 Responses to Role

Alias	Response
Jim	There's probably a small set of students I want them to get enough background that they can go to a <u>graduate program</u> . Either come here or go elsewhere and focus on security. I also think many of the students are not going to work in a security specific job. You know, and I'd say probably the <u>vast majority will just become programmers in all sorts of areas</u> , and I just want to alert them to security issues.
Lou	For those students . . . our goal is to develop <u>managers who are capable of IT</u> . They definitely start off as <u>practitioners</u> , but I think the ultimate goal is that they become <u>managers</u> .
Wolfgang	I guess there's a variety of roles. Those that go into security careers go as <u>pen-testers, incident responders, security analysts</u> . Sometimes <u>coders, systems administrators</u> , etc.
Robert	The ideal job it's training them for is along the <u>management consulting or compliance</u> side. Or, a third party consulting company will go and do <u>audit engagements</u> .

The answers to this question in the interview resulted in a number of different roles being apparent:

- Developer or Programmer
- IT Management

- IT Audit
- Security Engineer or Analyst
- System Administration

These answers were then fed into the survey. Figure 5-1 shows the question, and Figure 5-2 shows the responses:

Please indicate below the degree to which students are less likely, likely, or more likely to take roles in the following fields upon graduation from your program:			
	less likely	likely	more likely
Developer or Programmer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
System Administration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Systems Audit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
IT management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Analyst or Engineer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 5-1 Student Role Survey Question

#	Question	less likely	likely	more likely	Total Responses	Mean
1	Developer or Programmer	<u>15</u>	<u>10</u>	<u>2</u>	27	1.52
2	System Administration	<u>7</u>	<u>10</u>	<u>10</u>	27	2.11
3	Systems Audit	<u>10</u>	<u>15</u>	<u>2</u>	27	1.70
4	IT management	<u>4</u>	<u>14</u>	<u>9</u>	27	2.19
5	Security Analyst or Engineer	<u>7</u>	<u>10</u>	<u>10</u>	27	2.11

Figure 5-2 Student Role Responses

Figure 5-2 indicates that the role the respondent expected a student to take was more likely a security analyst or engineer, system administrator, then systems audit or IT management. The least likely role was a developer or programmer.

Instructor Type

One added piece of information for the survey was to question what kind of role the educator had in teaching. The respondents were given a list of possible choices which included: Teaching Assistant — Undergraduate, Teaching Assistant — Graduate, Instructor, Teacher K–12, Professor, and Trainer. The results from the survey showed that the respondents were largely in the professor category. See Figure 5-3.

#	Answer	Response	%
1	<u>Teaching assistant - under graduate</u>	0	0%
2	<u>Teaching assistant - graduate</u>	0	0%
3	<u>Instructor</u>	2	7%
4	<u>Teacher K-12</u>	0	0%
5	<u>Professor</u>	24	89%
6	<u>Trainer (e.g. professional certifications)</u>	1	4%
	Total	27	100%

Figure 5-3 Respondent Role Survey Results

Levels of Learning

One question considered throughout the study was the kind of learning expected by a professor for their security courses. In order to gauge instructors' perceptions about what they wanted their students to achieve, a question was used in the interview to ask respondents about where, on Bloom's Taxonomy, they thought most of their students' learning occurred. They were shown a diagram of Bloom's and asked to talk about those responses. Table 5-2 shows the raw data for Jim and Lou. Table 5-3 shows the raw data for Wolfgang and Robert. After the interviews, the author determined that depending on the level of education (graduate or under-graduate)

professors may have different goals for each. As such, the survey included an option for respondents to answer the question based on levels of learning for both graduate and undergraduate coursework. During the interview process, the author found some confusion among respondents based on this question.

Table 5-2 Learning Levels Responses from Jim and Lou

Alias	Response
Jim	It clearly has <u>remembering, understanding components</u> . I think because we do the <u>hands on labs, there's definitely some applying</u> . In terms of analyzing, ya know, we give them problems where... for instance they essentially do a collision attack and a pre-image attack on sort of a hash function. We make it small enough that they can actually do the attacks and we sort of have them do an experiment to say, "You know the mathematician says the cost of this attack should be such and such, let's do this attack in practice and they can see 'Oh, if I take my averages and see it, I can plot that exact kind of a curve'". So there's a bit of analyzing in that, and a number of other labs. <u>I don't know what the difference necessarily is between analyzing and evaluating</u> . But I would say we're definitely there. I mean, in terms of creating, I think from our graduate school I'd sort of say well...
Lou	Well in general it's great to be at the top, <u>creating and evaluating</u> things. So, um, I'd like stuff to be up there. So for my tests, I don't really like the remembering and understanding pieces... So, for the final exam, um I actually do it on [learning management system], and I make it open internet, and have them work from the lab computers with all their tools, and then I ask them questions from past hands-on labs. And I have them do stuff, because I think it's . . . I think it's more meaningful that way. <u>So in that sense they are evaluating, they're analyzing, they're applying</u> , um, I guess I don't really have them create things per se, other than reports.

Table 5-3 Learning Level Responses from Wolfgang and Robert

Alias	Response
Wolfgang	I think for the level of courses, which are the 400–500 courses, we’re looking at mostly <u>analyzing and above</u> . At least that’s where I’m trying to get. I want them to be thinking. It is fine remembering a knowledge and getting to a test because you remember the terminology, but it’s not going to help you in practice. You got to be able to apply it. To be able to use it to um, <u>I guess analyze or assess problems</u> , to be able to come up with solutions, to see how effective those solutions are, so evaluation, to be able to uh create solutions, and that’s, I think that’s why students are kind of getting such good placement, and being paid so much now is because they’re doing that really well.
Robert	So, on my test, my application ones are always trying to <u>create</u> something that’s based upon the security approach. I try to get to the creating level, but I kind of [inaudible] for that. So usually it’s more of the <u>analyzing and evaluating</u> than it is the creation. I give them plenty of things where I say look at this, tell me what’s wrong with this. Or, we have speakers come in and they do it all, so. And that’s what a lot of these labs are like. If we say here’s a password file, you guys break it, and tell me what’s there. <u>It’s sort of more in the middle to high tier</u> .

Two of the respondents expressed that they thought about this question differently among their courses. It is apparent from Jim and Wolfgang’s responses that they considered learning levels different between graduate and undergraduate students. When it came time to run the survey, the distinction was added. Questions 3 and 4 on the survey essentially ask the same thing, but focus the attention towards undergraduate and graduate students. Figures 5-4 and 5-5 indicate the responses from the survey regarding this subject. The figures indicate that for undergraduates, respondents looked to have these students more in an applying area of study. For graduates, professors seem to expect that students are doing more evaluative work. The questions didn’t elaborate on what the learning levels may mean, the intent being that it should be left to the respondent to determine what the outcome meant.

#	Answer	Response	%
1	Remembering	11	52%
2	Understanding	17	81%
3	Applying	18	86%
4	Analyzing	16	76%
5	Evaluating	12	57%
6	Creating	6	29%

Figure 5-4 Undergraduate Learning Level Responses

#	Answer	Response	%
1	Remembering	4	33%
2	Understanding	7	58%
3	Applying	8	67%
4	Analyzing	9	75%
5	Evaluating	10	83%
6	Creating	7	58%

Figure 5-5 Graduate Learning Level Responses

The number of responses was lower when considering the learning levels, but clearly shows a distinct difference in the expectations professors had on what the goals were for security courses at different levels of education.

Pedagogy and Teaching Methods

The sections in the interview and the survey on teaching methods and technology provided the most insight in preparing a framework to improve cyber security education. How security courses are taught and the way technology is used varied widely between interview respondents. However, the survey also showed that there are some technologies that are heavily used and others

that are not. The list respondents were asked to choose from was not exhaustive, but simple enough to see that there was a definite lack of usage from some tools that are touted as making infrastructure more flexible.

The interviewer asked a few questions in the interview that seemed to vary the responses. Respondents were asked the following questions:

- Where does your course stand in relation to cyber security theory and the practice of it? Does it learn more heavily towards one or the other? How does this affect how you maintain your courses and lab assignments?
- What do you rely on to make your course/program flexible to the changes in cyber security in the field?

The responses showed quite a bit of variation. In one exchange, the interviewer asked what the effect was of the professor changing the tools used in the course. The respondent said, “Oh oh it’s pretty easy. Every year I’ve been changing the tools. That’s not a big deal. If it’s a technical tool it’s taken out of the tests, the lectures, the questions. So it’s a very modular approach.” Another respondent expressed the same idea. That idea is that in teaching cyber security concepts, professors try to abstract the tie that some applications have towards theory.

The respondents from the survey were not asked the exact same question, but they were asked about how much their courses change from year to year. Specifically, question 10 asked the survey respondents to specify a percentage amount of change each year for lab exercises, lectures, projects, reading assignments, and exams. The following table shows the data retrieved from that question:

#	Answer	Min Value	Max Value	Average Value	Standard Deviation	Responses
1	<u>Lectures</u>	0.00	100.00	37.72	25.72	18
2	<u>Reading Assignments</u>	0.00	100.00	51.60	30.84	15
3	<u>Lab Exercises</u>	10.00	98.00	51.13	20.85	15
4	<u>Exams</u>	0.00	100.00	61.56	34.60	16
5	<u>Projects</u>	10.00	100.00	51.38	29.87	16

Figure 5-6 Course Change Responses from Survey

The number of responses for this question was much lower than others. Even though the Lab Exercises item had the fourth smallest average value, it does have the smallest standard deviation showing that the responses were closer to mean.

An additional question that was used in the survey was to determine how much of a certain method was used in teaching. The respondents were given a list and asked to give percentages based on the use of each item in their course. The following graph shows which items were used most in teaching:

#	Answer	Min Value	Max Value	Average Value	Standard Deviation
1	<u>Learning Activities</u>	0.00	100.00	21.96	23.97
2	<u>Quizzes</u>	0.00	30.00	8.21	9.25
3	<u>Research Assignments</u>	0.00	80.00	11.50	16.67
4	<u>Projects</u>	0.00	100.00	17.61	20.48
5	<u>Lectures</u>	0.00	60.00	20.71	20.40
6	<u>Seminars or other discussions</u>	0.00	50.00	9.29	11.28

Figure 5-7 Common Teaching Methods Responses from Survey

One issue for the researcher on this question was allowing the respondent to determine the difference between projects and learning activities. It is difficult knowing how to balance the

options given to respondents. Can learning activities and projects be grouped together? If so, does that show that learning activities are the dominant method for teaching cyber security courses? The response doesn't lend itself well to answering that question.

Technology Usage

Cyber security programs depend heavily on running systems for students to test functionality and teach principles. The interviews did not ask specific questions about how technology was used in teaching security courses, but there were some relevant pieces of information that came out about how technology is used. One respondent talked about how one of the assignments is for students to take the AES encryption standard and implement it in software. Another respondent mentioned that their students did the majority of their lab work outside of a structured class time, the reason being that when you function in that environment, you go as fast as the slowest individual. Technology usage seemed to have some variance in use based on the respondents' answers.

The survey asked respondents to answer yes or no to whether they had used certain types of technology. The table for this question produced the following data:

#	Question	Yes	No	Total Responses	Mean
2	Workstation Virtualization (e.g. VMware Workstation, Oracle VirtualBox)	20	3	23	1.13
1	Server Virtualization (e.g. vSphere, System Center Operations Manager with VMM, KVM, XenServer)	15	8	23	1.35
7	Integrating Project/Problem based activities that automatically report to a Learning Management Systems (e.g. Blackboard, Gradebook)	14	9	23	1.39
4	Cloud platforms for deploying virtual machines (e.g. OpenStack, Eucalyptus, vCloud Automation Center)	11	12	23	1.52
3	VM templates with customization scripts	11	12	23	1.52
5	Configuration Management Platforms (e.g. Puppet, Chef, JuJu)	4	19	23	1.83
6	Software Defined Networking (e.g. OpenFlow, NSX)	2	21	23	1.91

Figure 5-8 Technology Used in Teaching Survey Responses

This table indicates that workstation virtualization is the most highly used technology of these choices. Server virtualization comes next, followed by learning management system assignments. Integrating project/problem based activities that automatically report to an LMS could easily be thought of as a quiz or an exam, and as a result can be seen as an ambiguous question. The researcher was trying to find out if a framework similar to what is being proposed in this research had been used. It is clear that item could be taken a number of different ways.

The rest of the table is interesting in that it shows almost even responses between cloud platforms and VM templates. This seems to indicate that some attempt is being made to automate the deployment of VMs for assignments or research. The last objects are newer technologies. Software such as Puppet is relatively new in the industry, but has been used to scale application deployment at a fast pace. The Puppet and Chef tools are used for configuration management. Some sort of agent is installed into an OS, and that agent accepts configuration parameters from a central source. For example, if a developer is looking to build a platform to deploy an application, they can use a Puppet manifest that saves that configuration. In Chef, the manifest is referred to as a recipe.

Course Maintenance

The last item worth noting regarding the survey and interviews was the data that collected the perception that instructors have on maintaining their courses. Two of the interviews show the respondents expressly indicating that their security courses require more work to keep up to date than their non-security courses. Here's one exchange:

FJS: How does maintaining this course kind of compare to something else that you teach?

Robert: Oh this course requires the most work to keep it up to date.

FJS: Ok.

Robert: All the other ones are a lot easier.

The survey included a question that asked respondents to select between less, neutral, or more for how difficult maintaining their security course was compared to others. Of the 20 responses to that question, 5 said neutral, and 15 said it was more difficult than other courses they taught.

The interview and survey portion has several insights. Cyber-security education appears to commonly use active learning assignments for nearly 50% of time. The types of learning that professors expect undergraduate students to do hovers mostly on applying, and for graduate students it is on evaluating. The common teaching methods are to use engaged learning activities, and course maintenance is more burdensome than other courses. In no instance did a respondent to course maintenance say it was less difficult than other courses.

Statistical Results

The survey questions collected offered the chance to look at them for further analysis. It was mentioned previously in Chapter 4 that the standard error of the mean was calculated for all of the results. This data is available in the Appendix. For some of the questions, the standard error of the mean estimates that the responses from the general population are not far off from what was retrieved in the survey results. For example, in the survey results, Q9_1 asked if respondents had ever used server virtualization in teaching. The standard deviation for the responses was 0.476. The standard error of the mean was 0.099, estimating that the population response to be within roughly 10% of what the respondents in the survey said.

Another statistic looked at was the Chi-Squared test. The Chi-Squared test is used to test whether there is a difference between the expected and observed responses for categorical data. This test could be used to compare the responses of respondents for multiple categories, but it requires an equal number of responses in each category. This research had one issue in that respondents weren't required to answer all questions, which meant that some questions had more

answers than others. Removing the differences made the sample sizes much smaller in some cases (e.g. going from 20 respondents to 12 or 15).

The best statistics to look at in the responses are the obvious ones included in the Qualtrics report. The Qualtrics report included sufficient analysis of the data to develop the model proposed in this study.

5.2 *NxSecLab*

An explanation of the current framework may help to see what the NxSecLab was trying to do. Currently, BYU uses a home-grown learning management system called Learning Suite. Learning Suite has a lot of functionality that students could expect to see in other learning management systems. It has assignment delivery, return, course announcements, calendars, contact information, and online testing tools. On the flip side of this, the lab environment that the BYU Cyber Security Research Lab currently uses is based on VMware's vSphere. This acts as a platform for delivering the systems used for testing and supporting the class. The NxSecLab was designed as a way to marry some of the features of each, at least from the end-user's perspective. A student logs in, they can see labs for a course, start the lab to provision the resources needed, get the information to get started, and do the lab. When the student finishes, the lab completes. To the end-user, there's some added functionality here not now available. For example, in the current framework, when a lab starts, everything is manual. The templates are deployed, configured, and verified to be running properly. In some cases, maybe the TA works through the lab to verify that it will run for students. After that's completed, an announcement is sent out to the course with the IP address range for systems that are running. Part of the NxSecLab design is to relieve this administrative challenge. And it is a challenge. When filtering the survey results down to the respondents who said they used server virtualization, 12 of the 14 said the courses

were more difficult to manage. It is unclear why, but one could speculate that the kind of scenario the NxSecLab was trying to resolve is the kind of issue most programs deal with.

This section proceeds by discussing the architectural design of the NxSecLab and follows with assessments based on the criteria.

Overview of NxSecLab Purpose and Architecture

NxSecLab was a project developed in the Cyber Security Research Lab at Brigham Young University that looked to function as a cyber-challenge platform, or a suite for running penetration-testing types of activities. However, over the course of two senior capstone projects, it started to incorporate a larger set of user requirements that focused on usability for students, professors, and teaching assistants. Through these iterations, it became more than just a cyber-challenge platform, but a tool that started to have some functionality of a learning management system. It had scoring, group collaboration, feedback from instructors, and was able to retrieve and start assignments.

The model that was developed by the capstone team can be seen in Figure 5-9. This figure outlines the model developed by the NxSecLab. This model shows how the central engine tied together several functions from the user requirements. Group collaboration, student VM management, real time feedback, and the scoring engine were all features that fed into the engine. The engine then processes that information and makes it available to the end-user through a web interface.

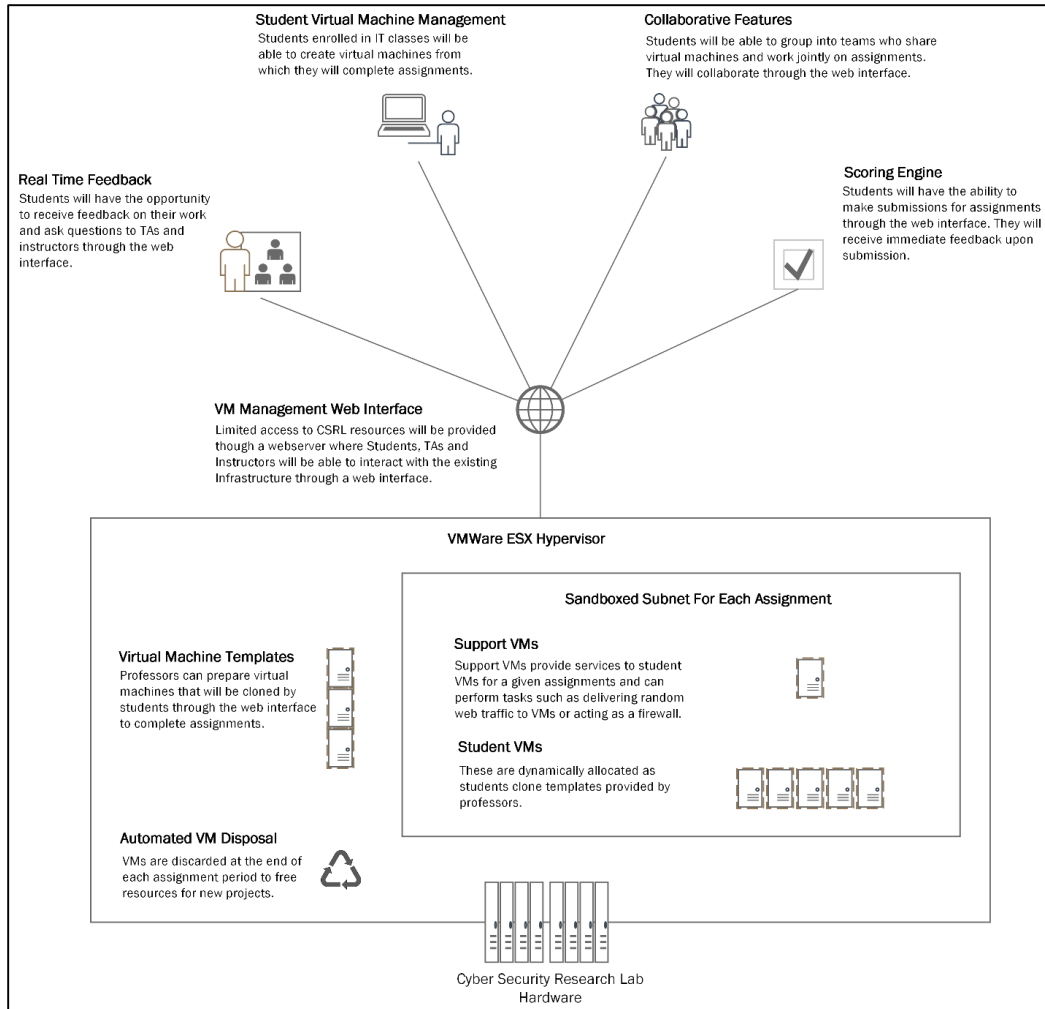


Figure 5-9 IT Capstone NxSecLab Architecture Model

The students' model sought to be a central web application that incorporated several features and interacted with virtualization components as needed. The implementation used consisted of a scoring engine and grading system that checked submissions against tuples from a database table, the collaboration system developed with node.js, scheduled lab provisioning, lab lifecycle functions, the student and teacher interface, and the VM management engine. The implementation model can be seen in Figure 5-10.

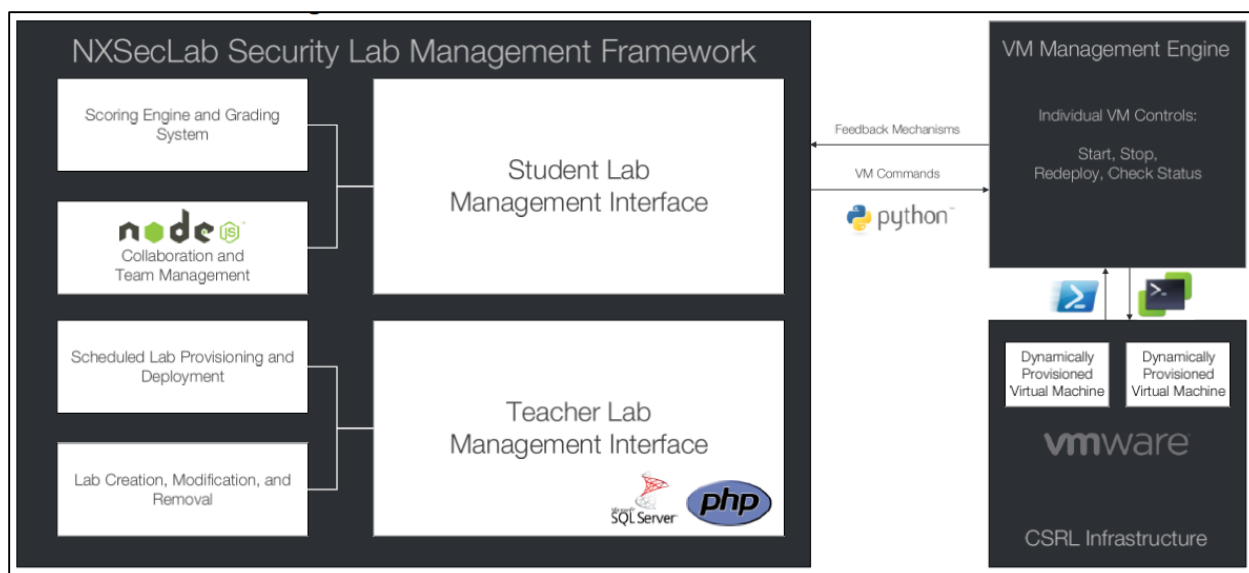


Figure 5-10 NxSecLab Management Framework (Capstone Report, 2013)

The model use focused on several custom built solutions to incorporate the required functionality. The technical design of the system was sufficient in some cases, but the evaluation of the NxSecLab found that the model could be improved by putting some of the burden back on the systems that already had the required functionality.

Impact on Cyber Security Course Design

The impact on course design is one that's hard to estimate for a few reasons. First, this evaluation doesn't use readily quantifiable data. Second, the time it takes to actually start using a new tool versus continuing to do things the old way is hard to estimate. But those are some of the things the researcher considered with this project.

When considering the effect the NxSecLab has on lab design, professors still have to have images pre-built with the necessary software. When looking at the actual deployment of the lab, instructors just need to configure a new lab and then it's ready for students to deploy. The de-

coupling of lab deployment from lab administration makes the system seem like it can scale to larger class sizes.

The other feature that is important is the scoring engine. From examining the source code for the scoring engine, the instructor submits what the correct flag is, and the students then submit their flags. The PHP function simply compares the two. The NxSecLab then saves the scores, and holds them until the instructor can manually submit them to some other learning management system to record the grade. There are a couple of items worth noting. One has to consider if a scoring engine that only scores correct answers is sufficient. Should it be broader? The other question is determining whether the additional work of having to take the students' scores from the scoring engine and input them on another learning management tool is unreasonably cumbersome.

The last question considered with the design was how this changes resources for students. Allowing students to use systems in a sandbox environment removes some of the barriers they may face when having to use their own equipment. If the NxSecLab also had a function where students were given their own VMs for the length of the course, this could facilitate more learning. However, it shifts an added burden to the instructor to have an infrastructure that has more depending on it.

Impact on Cyber Security Course Operation

Another goal of the NxSecLab is to ease the operation of cyber security assignments on instructors. It does this by addressing VM lifecycle, VM configuration, scoring, group management, and collaboration.

VM lifecycle, the creation and deletion of VMs, is one task that could seem very tedious and time consuming. Depending on the hardware, VM deployment could take several minutes to

hours depending on the amount of services that need to be deployed. The NxSecLab uses cloning to deploy VMs. This does take a significant amount of time to do.

One of the requirements of the project was for the NxSecLab to assign and report the IP address of a VM. The process for this operation was to ask a DHCP server if it had a lease for a MAC address that was created with a VM. If it did, it returned the address. If not, it returned saying it couldn't find it. This model is essentially built just on using a DHCP server and querying it for responses.

Long term integration with some sort of IP management tool and DNS should probably be considered. There are some issues with the implementation. Simply querying a DHCP server doesn't address problems where perhaps a static address gets assigned in a lab image. Another issue is the way the tool is designed to get the IP address information. The function of determining the IP address for a VM is extremely static. The NxSecLab engine runs a PHP script, which calls a PowerShell script that interacts with Netsh on a Windows server running DHCP. This process might not be that different if Windows IPAM were used. Essentially, the concern over IP management with NxSecLab is how easy it is to retrieve the information. Using a static function does not seem very easy.

Group management in the NxSecLab is a unique feature that allows the groups to be created and tie them to specific resources. It also has the specification to allow scores to be submitted as a whole for the team or individually. Another feature requested was for the chat system to work with groups. This kind of functionality really seems to improve the management of collaborative efforts for instructors and TAs. The burden of recording the groups and organizing the information is removed almost entirely from the instructor. This is one feature that stands out as truly unique in this project.

General Assessment

After the last iteration, it was determined that much of the project wasn't usable for the course. UI issues regarding users needed to be resolved. However, the architectural design of the system really lends itself to only be usable with Hyper-V or VMware because of how the calls are made to custom PowerShell scripts. The project could be more robust if it was designed to use web services. So many cloud based platforms that service IaaS types of models support web services calls that managing VM operations could be made simpler with that kind of model. One requirement that wasn't dealt with for the NxSecLab project was returning feedback based on the PowerShell task. VMware's Web Service API includes a task info data-object that can return the status of the task. Using the web service APIs of VMware could have brought more functionality to the project and made it more usable.

Another issue is the lack of monitoring and debugging in the source code. For a course using the NxSecLab, one consideration might be how to handle outages. This may be as simple as telling the student to re-deploy a lab if they lose some information. Some consideration needs to be given to how the assignments are monitored and how issues are dealt with. The lack of error reporting in the source code makes troubleshooting more difficult.

5.3 Answers to Research Questions

The results and findings of this research looked to address the research questions by using qualitative methods to collect data and to use an evaluation procedure against the NxSecLab.

This study found that in answer to Q1, the technical teaching methods for cyber security programs lean heavily towards using labs and projects that use virtualization. Automation tools are not heavily used.

In answer to Q2, the results show that lectures, readings, labs, exams, and projects all change, at least 30% a year, and are as high as 60% for some methods. This means that the problems these instructors face is fairly high turnover on the material and content used for a course. Q11 showed that $\frac{3}{4}$ of the respondents all consider these courses harder to maintain than others they teach. The perception is prevalent in this field that it requires significant effort to maintain, which leads to the answer of H1. The respondents generally seemed to indicate that more time was needed to keep these courses up to date.

The factors that contribute to this appear to be many. The survey results do not directly address H3, but there are several items that could be interpreted as answers. Namely:

- Technology use in these programs seems to indicate that a lack of automation is used.
- Courses use several interactive or engaged teaching methods. These kinds of methods require the instructor to facilitate learning for students by preparing environments where the principles can be seen in action.
- The respondents all seemed to indicate levels of learning that require students to apply or evaluate.

Each of these items contributes to the reason why cyber security courses appear to be more difficult to maintain than other courses.

Objective 1 (O1) looks to incorporate the findings from the survey, interviews, and NxSecLab analysis into a model that could bring some relief to instructors regarding cyber security course work. The outcome of this effort follows in Chapter 6.

5.4 *Summary*

This chapter detailed the results from the interviews, survey, and NxSecLab evaluation. The interviews showed that cyber security instructors face challenges keeping courses current, and detailed the methods in use in a few different programs. The surveys showed what kind of expectations, methods, and technology are used heavily in training based on a wider sample. It also showed that nearly every respondent considers cyber security courses more challenging to keep up to date than others they teach.

The chapter concludes with an evaluation of the NxSecLab, and shows the strengths and weakness of the model it was designed with. The NxSecLab depends heavily on resources to develop a custom tool. It does present concepts that could make managing challenge courses useful, but lacks some points of integration that could make the system more robust.

6 PROPOSED LEARNING MANAGEMENT FRAMEWORK FOR CYBER SECURITY EDUCATION

This chapter provides an overview of the themes from this research. It details the proposed technical model for how cyber security programs could better manage coursework and research. This model consists of a technology architecture designed to ease the assignment lifecycle, monitoring of technical labs, and simplify the development costs associated with building custom platforms to do the same functions. By using a service-oriented architecture, along with available IaaS platforms, cyber security instructors can build robust solutions that offer flexibility and extensibility as they adapt new content to explain security principles.

6.1 *Themes from the Data*

In doing a study that involved interviewing and surveying instructors from a variety of disciplines, some common themes matured from the data. The kind of roles students are being trained for, the kind of teaching methods that are common, and the frustrations with security training all became apparent. These themes represent common issues that educators see in cyber security education.

One of those themes is the engaged learning aspect of cyber security courses. Some programs may not rely heavily on learning challenges, but active learning assignments seem to be a large part of this kind of course. This often means that professors are using virtualization technologies to run labs. This is easier than using physical hardware, but unless there is some sort

of configuration management system or automation system involved in the configuration, educators will undoubtedly see a scaling issue. This was one of the issues that the NxSecLab tried to address, and is one of the issues seen generally.

Another theme in the data is the rate at which course content changes. It's understandable that content for cyber security education would be updated. One of the interviewees said, "Well, every year I tweak all my labs. Maybe that's not totally accurate. I definitely re-assess them all every year, but there's usually changes every year to the labs. Sometimes I hope that there are major changes, but sometimes they're not." As much as instructors hope to update or tweak labs, the time and resources required to do such changes aren't available. Another one of the interviewees mentioned how they're really only able to make significant changes to labs when they have a really good teaching assistant who spends time on it during the summer. The lack of resources which these kinds of updates need in order to be made often aren't available.

The NxSecLab tried to address these issues by developing a system that abstracted the deployment of assignments from the administration of them. Although it could function sufficiently as it is currently designed, it does not allow flexibility or extensibility without significant development time to write custom scripts or functions. Even though it provides a scoring engine, the scoring engine doesn't alleviate the work that's required by the TA or instructor to make sure the grades are submitted. If this kind of model were used in an online learning system, a TA or instructor would have to regularly check for submissions on the NxSecLab and export them over to the main learning management system.

6.2 *Proposed Extensible Learning Platform*

All of these issues are addressed by the framework proposed in this research. The framework outlined in this section seeks to simplify the administration of the tasks often seen as cumbersome

by abstracting operational roles away from the sources they are used for. It also supports extensibility by using web services functions. See Figure 6-1 for an overview of the proposed framework.

This model consists of three layers: the NxSecLab layer that ties a service oriented architecture (SOA) and IaaS platform. The SOA and IaaS objects then are responsible for abstracting service functions from the NxSecLab engine. This feature makes it possible for the NxSecLab to not have manual code changes when an API function changes in either a learning management system, authentication service, server virtualization, or network virtualization. The way the NxSecLab is currently designed, any time some functionality changes in the hypervisors it has to be reflected back in the code design. Each of these components will be addressed individually.

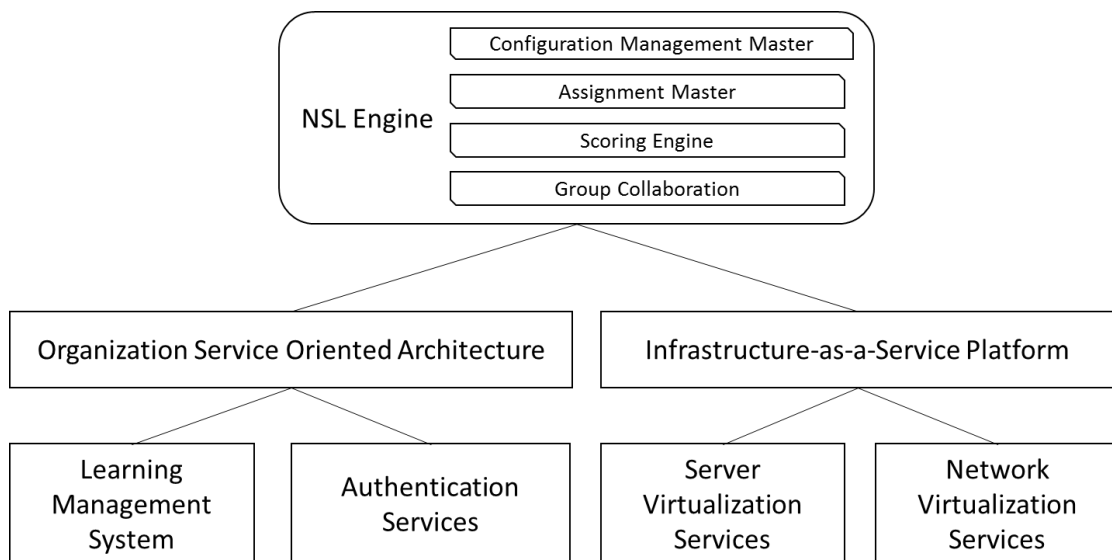


Figure 6-1 Proposed Model

Framework Recommendations

The NxSecLab Engine functions as a way to bridge two very different technologies. Learning management systems as we now know them have never been tied directly to infrastructure-as-a-service platforms. The NxSecLab Engine needs to be responsible for the following:

- Assignment Creation — this consists of creating new assignments and mapping them to infrastructure resources.
- Resource Deployment — this consists of the operations of taking requests from students or administrators to deploy VMs or networks, and report back to the student what resources are to be used in the assignment. The configuration management engine (of which there are several available) is responsible for taking configuration actions and deploying them out to VMs that are created by the IaaS service. Configuration management systems need to be used to simplify lab creation. It is easier to specify in a config file what version needs to be on a system instead of deploying the image, installing a specified version of software, and saving it back.
- Resource Deletion — Once a lab has been completed, the NxSecLab is responsible for sending the calls to remove the resources.
- Scoring — The scoring engine needs to be able to hold scores for assignments and notify the student what the result is. The scoring engine should function through the service oriented architecture to submit scores for assignments to the organization's dominant learning management platform.
- Group Collaboration — the NxSecLab should provide a way for students to communicate with team members and/or TAs and instructors. This is one feature from the NxSecLab

capstone project that could facilitate more functionality for students, and should be kept with the model.

The NxSecLab Engine essentially acts as the point that combines resources from an educational institution with the resources of IaaS.

Service Oriented Architecture

There was a recent paper that was self-published by Kin Lane called “The University of API” that discussed how some service oriented architecture and web services have been developed at universities. Brigham Young University stands out among UC Berkley, University of Michigan, University of Washington, the University of Warsaw, and the University of Waterloo in that it has implemented a strategy in the central office of IT to make the services available through web API’s. This strategy simplifies how the university provides access to the information it controls. In the case of BYU, the SOA registry offers APIs for organizations or individuals to access certain functionality. As more functions get added, this resource will continue to offer more interesting functionality.

Where the NxSecLab is concerned, using the SOA web services provided by the central IT office allows the NxSecLab to interact with two important functions: the campus learning management tool and central authentication services. These components allows several possibilities:

- Score submission — The SOA registry for BYU allows organizations to make calls back to the campus wide learning management system. This requires that the SOA registry have an API for the score submission, and that the learning management system has an API for that system. Some learning management systems do include APIs for making web service

calls. This functionality would remove the operational task of copying scores from the NxSecLab into the learning management tool.

- **Assignment Creation** — the SOA registry does include functionality for a web service call to be accepted that creates an assignment on the learning management system.
- **Course Enrollment** — the SOA registry could offer a function for the NxSecLab to retrieve a list of enrollees in a course.
- **Central Authentication** — The web services that allow authentication resources could allow students to use single-sign on with the NxSecLab. This feature could remove the burden of having to manage an entire user system. One benefit to this is that issues with accounts could be deferred back to the OIT support desk for response, whereas now they have to be dealt with directly by an instructor or TA.

The benefits of using the SOA not only simplify the management of the course, but they also add functionality for students. By using a single account, or tying back to a university-wide learning management system, there is less for students to worry about when taking a course.

IaaS Platform

The need to abstract operational tasks with server virtualization is a necessary component in easing the issues of course administration. One of the requirements of the original NxSecLab was to be flexible enough to support different hypervisors. There are several solutions that do this already, and there will continue to be development for it as organizations start to require the flexibility to move services back and forth between clouds. What cyber security programs really need in this case is simply the ability to swap out hypervisors without causing a disruption to the dependent services. This could be due to cost, efficiency, or relevance of a virtualization tool.

Web service functions are becoming more prevalent in cloud platforms. For example, OpenStack has been designed with this in mind. When a web service call to the OpenStack API to deploy an instance is called, a number of parameters are available including availability zone. In OpenStack, when a compute resource is configured one of the parameters is what availability zone it's in. This parameter points to compute drivers that could be Linux KVM, VMware ESXi/vCenter, Hyper-V, QEMU, or XenServer. This functionality allows resources for labs to be deployed among a number of different resources.

The other feature that IaaS platforms are starting to integrate with is software-defined networking solutions. OpenStack can connect to a number of different SDN controllers. VMware's vCloud supports using NSX. SDN Support can significantly change how students use networks to run lab assignments. Having an abstraction layer that simplifies this makes the NxSecLab easier to design and deploy. This layer includes:

- Multi-Hypervisor support — As long as the IaaS platform supports multi-hypervisors, the option here to run labs on other hypervisors is available.
- Logical L2 Networking — SDN solutions provide logical L2 networking, usually over the VXLAN standard which runs at L3. This functionality could provide the ability to logically isolate VMs without having to constantly re-configure physical switching components.
- Web Service Calls — The web services functionality in this kind of system allows simpler modification to IaaS calls. Instead of using a custom script, as the API updates with new technology, the NxSecLab engine just needs to be modified to support the call. Some APIs, like the ones available with OpenStack, support a wide variety of functions. This gives the flexibility to make the decisions to the NxSecLab wide, without requiring significant development to do them on their own.

The proposed platform introduced in this research focuses on making functionality available through a web service. This functionality could simplify how courses are designed, managed, and how students learn cyber security principles. The SOA framework at BYU is one example of how web services used by a university can be used to simplify how instructors administer classes and resources for students.

6.3 *Framework Evaluation*

The framework proposed in this study was developed through an evaluation of the NxSecLab. This evaluation focused on the technical aspects of course management, what repetitive procedural steps could be simplified, and how well the NxSecLab addressed the concerns found in the interviews and survey material. There are a number of items to consider in how this model, built on the one proposed by the NxSecLab project, can resolve the inefficiencies seen in cyber security education.

First, this model looks to integrate functionality without adding more management. Where the NxSecLab looks to have separate authentication and separate scoring repositories, this model looks to use what already exists where it's available.

Second, this model proposes an architecture that's fundamentally different from how the NxSecLab was originally implemented. The capstone team tried to deliver a project as best as they knew how; however, not using a robust web API limited the flexibility of the prototype. In order to run VM commands, they wrote their own scripts in PowerShell. If they had used a web API, that work could have been avoided. In the future if this model is implemented it would allow functional abstraction of the management plane from the virtualization layer.

Third, it looks to incorporate automation in a way that relieves a lot of the administrative work in creating and deploying lab assignments. In the current environment, the following tasks have to be taken:

- VM created and OS installed (or cloned)
- Configuration changes (hostname, interfaces)
- Packages installed
- Converted to template
- Individual template manually deployed and manually configured as needed for labs

This means that when labs or assignments are created and deployed, there is a significant amount of manual intervention. This could be resolved by using a configuration management framework for the following procedures:

- VM created and OS installed with configuration management agent
- Converted to template
- Configuration file created specifying packages, files, hostnames, etc.
- VMs deployed and receive configuration from master server.

These steps provide some relief to this process by allowing the administration of lab assignments to scale better than it does now.

Although the analysis was sufficient to propose a framework, more could be done to further evaluate it. As was shown in the statistical analysis, the amount of data collected for Chi-Squared tests was not enough. More responses to the survey could have shown whether the probabilities of the Chi-Squared were due to chance. The framework could be provided to other institutions and evaluated. The limitation with this method is that the model expects a web services layer to

interact with. Something else could be used, but this could negate the model and specifically the recommendation to use a central SOA registry for an institution.

The framework can change. The types of architectures, technology, and models at present will adjust which may affect how this framework is implemented. If, for example, an institution's web services began to incorporate an API that allowed departments on a campus access to their own infrastructure resources, this model could change so that the functionality of the NxSecLab engine is completely abstracted from the services it uses by an API. At such a point, the proposed framework would need to be re-visited and investigated.

6.4 *Summary*

This chapter showed the themes observed in this study, and explained the proposed model. It showed how certain technologies could be used to marry learning management functionality with an IaaS platform. Central to this framework is the use of web services or a service oriented architecture that allows flexibility in how services are used. By using web services, as underlying applications change, those who maintain the SOA registry can make changes without impacting the applications that interact with the SOA APIs. This section showed how the data from this study and the evaluation of the NxSecLab were used to develop a possible model for making cyber security education more time efficient.

7 CONCLUSIONS

7.1 *Overview*

This research explored the problems and inefficiencies seen by cyber security educators in administering courses. It details an extensible technology framework that looks to resolve these inefficiencies by using a technology engine to integrate learning management systems with infrastructure-as-a-service. The benefits of the proposed model include

- less dependency on the system to run critical functions like authentication, or virtual machine management;
- more tie-ins with existing university-wide systems—eliminating the interim grading steps for certain kinds of assignments; and
- more flexibility in what IT infrastructure platforms are used.

This study used the data collected from the survey, interviews, and NxSecLab evaluation to propose a model that could be more flexible for instructors.

Additionally, the study looked to determine what educators see as problems, and what kind of technology is in use that could be contributing to this problem. The researcher interviewed educators from different fields to explore the vernacular and problems seen across different but similar fields. As an extension of this effort, the researcher prepared a survey that was distributed to hundreds of individuals. The survey had 38 attempts, with 26 respondents completing the survey. These procedures were used to develop criteria that were used to assess the BYU IT Capstone NxSecLab project, and see how it attempted to improve cyber security education. The

result of this study is a proposed framework that prescribed an integration tool that simplifies how learning management systems are used along with infrastructure-as-a-service platforms in cyber security education.

7.2 *Future Research*

Future research could take place by considering the following:

API Extensions: The framework noted here used a web services layer that allowed integration with a wide variety of institutional systems. Consideration could be given to what kind of cyber security functions in the classroom could use more extensibility from that layer.

Auto-Configured Research Environment: Often researchers looked to assess the impact of zero-day exploits. A service could be created to interact with the NxSecLab engine, to monitor CVEs and automatically create configuration management instructions (e.g. Puppet manifest) to deploy a test environment using the specified build or package numbers in the CVE. This process could then be used by the assignment master to create evaluation-based labs that allow students to look at new bugs.

Security Assessment: The framework mentioned in this model could be evaluated for its security design. The risk in integrating learning management systems that control grades and lab environments for students to learn security principles is obviously a concern with this framework. A careful analysis of an implementation would be necessary.

Usability Evaluation: This framework was based off of cyber security educators' feedback about issues in course management. An implementation could be evaluated for usability, keeping in mind the data collected during this study.

7.3 *Summary*

In this research, the current paradigm in which cyber security education operates was explored. A technical and procedural framework was designed using that information and compared against the NxSecLab. The proposed model incorporates learning management functionality, along with IaaS to simplify repetitive tasks and make cyber security education more functional and flexible to the demands of an ever changing field.

REFERENCES

- Abler, R., D. Contis, J. Grizzard, and H. Owen. 2006. "Georgia Tech Information Security Center Hands-on Network Security Laboratory." *Education, IEEE Transactions on* 49 (1): 82–87. doi:10.1109/TE.2005.858403.
- Anderson, L. W., and D. R. Krathwohl. 2001. *A Taxonomy for Learning, Teaching, and Assessing : A Revision of Bloom's Taxonomy of Educational Objectives*. New York: Longman.
- Bai, Y., and C. Taylor. 2011. "Cyber Defense Competition: Enhancing Student Competency in Information Security." In *Proceedings of the 2011 Conference on Information Technology Education*, 305–6. SIGITE '11. New York, NY, USA: ACM. doi:10.1145/2047594.2047675.
- Bernard, R. 2000. *Social Research Methods: Qualitative and Quantitative Approaches*. Thousand Oaks, CA: Sage.
- Border, C., and E. Holden. 2003. "Security Education Within the IT Curriculum." In *Proceedings of the 4th Conference on Information Technology Curriculum*, 256–64. CITC4 '03. New York, NY, USA: ACM. doi:10.1145/947121.947179.
- Boyatzis, R. E. 1998. *Transforming Qualitative Information: Thematic Analysis and Code Development*. *Transforming Qualitative Information Thematic Analysis and Code Development*. http://books.google.com/books?hl=en&lr=&id=_rfCIWRhIKAC&pgis=1.
- Coaldrake, P., and L. Stedman. 1999. "Academic Work in the Twenty-First Century." *Occasional Paper Series, Higher Education Division, DETYA 99H*.
- Corbin, J., and A. Strauss. 2008. *Basics of Qualitative Research*. Third.
- Creswell, J. W. 2003. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. *Journal of Investigative Surgery: The Official Journal of the Academy of Surgical Research*. Vol. 25. doi:10.3109/08941939.2012.723954.
- Crowley, E. 2003. "Information System Security Curricula Development." *Proceeding of the 4th Conference on Information Technology Education - CITC '03*, 249. doi:10.1145/947121.947178.
- Driscoll, D. L., and A. Brizee. 2010. "Creating Good Interview and Survey Questions." *OWL*. <https://owl.english.purdue.edu/owl/resource/559/06/>.

- Endicott-Popovsky, B. E., and V. M. Popovsky. 2014. "Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals." *ACM Inroads* 5 (1). New York, NY, USA: ACM: 57–68. doi:10.1145/2568195.2568214.
- Forcht, K. A. 1986. "The Need for Including Data Security Topics in the College Business Curriculum." *SIGSAC Rev.* 4 (3). New York, NY, USA: ACM: 9–11. doi:10.1145/1058414.1058416.
- Glesne, C., and A. Peshkin. 1992. *Becoming Qualitative Researchers: An Introduction*. White Plains, NY: Longmans.
- Guion, L., D. Diehl, and D. McDonald. 2011. "Triangulation: Establishing the Validity of Qualitative Studies." *University of Florida, IFAS Extension*. <http://edis.ifas.ufl.edu/pdf/files/FY/FY39400.pdf>.
- Helps, R. G. 2010. "Evolving Information Technology: A Case Study of the Effects of Constant Change on Information Technology Instructional Design Architecture."
- Lonn, S., and S. Teasley. 2009. "Saving Time or Innovating Practice: Investigating Perceptions and Uses of Learning Management Systems." *Computers & Education* 53 (3): 686–94. doi:10.1016/j.compedu.2009.04.008.
- Mayo, J., and P. Kearns. 1999. "A Secure Unrestricted Advanced Systems Laboratory." In *The Proceedings of the Thirtieth SIGCSE Technical Symposium on Computer Science Education*, 165–69. SIGCSE '99. New York, NY, USA: ACM. doi:10.1145/299649.299742.
- O'Leary, M. 2006. "A Laboratory Based Capstone Course in Computer Security for Undergraduates." *SIGCSE Bull.* 38 (1). New York, NY, USA: ACM: 2–6. doi:10.1145/1124706.1121346.
- OCCP. 2014. "About the OCCP Project." <https://opencyberchallenge.net/wiki/About>.
- Papanikolaou, A., V. Karakoidas, V. Vlachos, A. Venieris, C. Ilioudis, and G. Zouganelis. 2011. "A Hacker's Perspective on Educating Future Security Experts." In *Informatics (PCI), 2011 15th Panhellenic Conference on*, 68–72. doi:10.1109/PCI.2011.47.
- Ragsdale, D. J., S. D. Lathrop, and R. C. Dodge Jr. 2003. "A Virtual Environment for IA Education." In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, 17–23. doi:10.1109/SMCSIA.2003.1232395.
- Rowe, D. C., B. M. Lunt, and J. J. Ekstrom. 2011. "The Role of Cyber-Security in Information Technology Education." In *Proceedings of the 2011 Conference on Information Technology Education*, 113–22. SIGITE '11. New York, NY, USA: ACM. doi:10.1145/2047594.2047628.

Rursch, J. A., and D. Jacobson. 2013. "This IS Child's Play: Creating a 'Playground' (computer Network Testbed) for High School Students to Learn, Practice, and Compete in Cyber Defense Competitions." In *Frontiers in Education Conference, 2013 IEEE*, 1776–78. doi:10.1109/FIE.2013.6685143.

Stake, R. E. 1995. *The Art of Case Study Research*. Sage.

Yang, T. A. 2001. "Computer Security and Impact on Computer Science Education." *J. Comput. Sci. Coll.* 16 (4). USA: Consortium for Computing Sciences in Colleges: 233–46. <http://dl.acm.org/citation.cfm?id=378613.378722>.

Yasinsac, A., J. Frazier, and M. Bogdanov. 2002. "Developing an Academic Security Laboratory." In *6th National Colloquium for Information System Security Education, Redmond, WA*.

APPENDIX

Survey Questions

This section describes the survey format and shows the questions used for the survey.

Q1. Implied Consent

Q2. What is your role in teaching?

1. Teaching assistant — undergraduate
2. Teaching assistant — graduate
3. Instructor
4. Teacher K–12
5. Professor

Q3. Please indicate below the degree to which students are less likely, likely, or more likely to take roles in the following fields upon graduation from your program:

1. Developer or Programmer
2. System Administration
3. Systems Audit
4. IT management
5. Security Analyst or Engineer

For Q3, respondents selected less likely, likely, or more likely for each of the options above.

Q4. For students who take your cyber security courses, please indicate below the levels of learning described in your cyber security undergraduate course learning outcomes:

- Remembering
- Understanding
- Applying
- Analyzing
- Evaluating
- Creating
- NA

For Q4, respondents selected check boxes for each option that applied.

Q5. For students who take your cyber security courses, please indicate below the levels of learning described in your cyber security graduate course learning outcomes:

- Remembering
- Understanding
- Applying
- Analyzing
- Evaluating
- Creating
- NA

For Q5, respondents selected check boxes for each option that applied.

Q6. Select an option from the dropboxes that best describes your answer

1. Feedback from students on course materials is
2. Feedback from students on instructor clarity is
3. Feedback from students on intellectual skill development is
4. Feedback from students on outcomes of the course is

For Q6, respondents selected from mostly negative, somewhat negative, neutral, somewhat positive, and mostly positive.

Q7. Please select an answer from the statements below:

- I run a more traditional classroom with lectures, and the students do their work outside of the lecture.
- I run a flipped classroom where students prepare for the class and come prepared to discuss the reading or work on projects together.
- Other

For Q7, respondents were able to select only one option.

Q8. Please indicate how often the items below are used in teaching your course by giving them a percentage in the field to the right.

1. Learning Activities
2. Quizzes
3. Research Assignments
4. Projects
5. Lectures
6. Seminars or other discussions

For Q8, respondents were given percent fields on the right. The totals were auto calculated.

Q9. Have you ever used any of the following in building exercises for cyber security courses?

- Server Virtualization (e.g, vSphere, System Center Operations Manager with VMM, KVM, XenServer)
- Workstation Virtualization (e.g, VMware Workstation, Oracle VirtualBox)
- VM templates with customization scripts
- Cloud platforms for deploying virtual machines (e.g, OpenStack, Eucalyptus, vCloud Automation Center)
- Configuration Management Platforms (e.g, Puppet, Chef, JuJu)
- Software Defined Networking (e.g, OpenFlow, NSX)
- Integrating Project/Problem based activities that automatically report to a Learning Management System (e.g, Blackboard, Gradebook)

For Q9, respondents were asked to select yes or no for each of the bullet point items.

Q10. Please drag and drop the items below to rank based on how much time is devoted to each of the CISSP domains:

- Access Control (Concepts, Attacks, Effectiveness)
- Network Security (Design, Components, Attacks)
- Information Security Governance and Risk Management (Policy, Personnel, Information Classification)
- Software Development Security (SDLC, Application Environment and Security Controls)
- Cryptography (Concepts, Digital Signatures, Cryptanalytic Attacks, PKI)

- Security Architecture and Design (Security Models, Countermeasure Principles, Vulnerability and Threat Analysis)
- Operations Security (Incident Response, Attack Prevention, Penetration Testing)
- Legal, Regulations, Investigations, and Compliance
- Business Continuity and Disaster Recovery Planning
- Physical (Environmental) Security

For Q10, respondents were asked to sort each bullet point according to its priority.

Q11. How much of each item below do you change over the course of year? Please think about this only with regards to cyber security courses:

1. Lectures
2. Reading Assignments
3. Lab Exercises
4. Exams
5. Projects

For Q11, respondents were allowed to drag a line bar between 0 and 100 to indicate how much of each item changed with regards to the course.

Q12. Please indicate how keeping your security course current compares with other courses you may teach.

- My security course is
 - Less difficult to maintain than other courses
 - Neutral

- More difficult to maintain than other courses
- NA

For Q12, respondents were allowed to select only one of the options.

Survey Responses

In the following section, figures are included showing the survey response data. For each question in the previous section, Qualtrics automatically assigned a numeric value for each response.

V1	Q1	Q2	Q3_1	Q3_2	Q3_3	Q3_4	Q3_5	Q4_1	Q4_2	Q4_3	Q4_4	Q4_5	Q4_6	Q4_7
R_agCcgTEtb7Hexlb	1													
R_2aHodufInMgESe9	1	6	1	1	2	2	3							1
R_ewKk9u5xqN7LZD7	1													
R_dp5CYSrOlzfuP6B	1	5	1	3	2	2	3	1	1	1	1	1		
R_9sOsJDIVa3HXfPT	1													
R_7aOkCU1qAXpge1v	1	5	1	3	2	2	3	1	1	1	1	1		
R_esOKixzvFXhyi2x	1	5	2	2	2	3	1		1	1				
R_6heNPFVW7pzIRZ3	1	5	2	1	2	3	3							1
R_6rLn0SF6BouZ0oZ	1	3	1	3	2	2	2	1	1	1	1	1		
R_9SlcqYYX3qBwZgx	1	5	1	2	2	2	3	1	1	1	1	1		
R_25oZRzdHyPiT7O5	1													
R_9QS0Fbienw0wfGt	1	5	1	3	2	3	2		1	1	1	1	1	1
R_a4ccDgaAxy5mstL	1	5	2	2	2	3	3	1	1	1	1	1	1	1
R_d6Je6Sf68pzQESx	1	5	1	2	2	2	2				1			
R_5jyw36D7Ywnienr	1	5	1	2	2	2	2			1				
R_bDVi3AFWRTTiECN	1	5	2	1	1	2	1							1
R_4lxe9nP0ZRoJOSj	1	5	1	1	2	2	3							1
R_0krYSyLO67S47pX	1	5	2	3	3	2	3	1	1	1	1	1	1	1
R_9snnP0ctyLMO8n3	1													
R_1FvfX9oZczF9U45	1	5	1	3	3	3	3		1	1	1	1		
R_3UVRE1C23DshA6F	1	5	3	3	2	3	2	1	1	1	1	1	1	1
R_9zE7Ltn8WTGqNkV	1	5	2	1	1	1	1		1	1				
R_4YsfZxzQh1Jbqy9	1	5	2	3	2	3	3				1			
R_3NLjdeun3JLQEnz	1	5	3	2	1	1	2		1	1	1	1		
R_4UBdaPhAK3Q5u2p	1	5	1	3	1	3	2	1	1	1				
R_5oKK0sMgkk8RDkJ	1	5	2	2	2	1	2	1	1	1	1	1	1	1
R_eetjH4dNis9bn4V	1													
R_eS6se2e46F2TbOR	1	3	1	3	1	2	1	1	1	1	1			

Survey Responses Q1–Q4

V1	Q5_1	Q5_2	Q5_3	Q5_4	Q5_5	Q5_6	Q5_7	Q6_1	Q6_2	Q6_3	Q6_4	Q7
R_agCcgTEtb7HexIb												
R_2aHodufInMgESe9					1			5	5	5	5	1
R_ewKk9u5xqN7LZD7												
R_dp5CYSrOlzfuP6B								4	4	5	4	3
R_9sOsJDIVa3HXfPT												
R_7aOkCU1qAXpge1v							1	5	5	5	4	3
R_es0KixzvFXhyi2x		1	1	1	1			4	5	4	4	2
R_6heNPFVW7pZlRZ3	1	1	1	1				3	4	4	4	1
R_6rLn0SF6BouZ0oZ	1	1	1	1	1	1		4	4	4	4	1
R_9SlcqYYX3qBwZgx							1	5	5	4	4	1
R_25oZRzdHyPiT7O5												
R_9QS0Fbienw0wfGt			1	1	1	1		5	5	5	5	3
R_a4ccDgaAxy5mstL	1	1	1	1	1	1		5	5	5	5	2
R_d6Je6Sf68pzQESx					1	1		5	5	5	5	2
R_5jyw36D7Ywnienr							1	3	3	3	3	3
R_bDVi3AFWRRTTIECN	1	1	1	1	1	1		5	5	5	5	3
R_4Ixe9nPOZRoJOSJ		1	1	1	1			4	5	4	4	1
R_OkrYSyLO67S47pX							1	4	5	5	5	1
R_9snnPOctyLMO8n3												
R_1FvfX9oZczF9U45				1	1	1		5	5	5	5	3
R_3UVRE1C23DshA6F							1	5	5	5	5	2
R_9zE7Ltn8WTGqNkV							1	3	3	3	3	1
R_4YsfZxzQh1Jbqy9						1		5	5	5	5	3
R_3NLjdeun3JLQEnz		1	1	1	1			5	5	4	4	1
R_4UBdaPhAK3Q5u2p							1	5	5	3	5	3
R_5oKK0sMgk8RDKJ							1	4	5	3	4	2
R_eetjH4dNis9bn4V												
R_eS6se2e46F2TbOR							1	4	4	4	4	3

Survey Responses Q5–Q7

V1	Q8_1	Q8_2	Q8_3	Q8_4	Q8_5	Q8_6	Q9_1	Q9_2	Q9_3	Q9_4	Q9_5	Q9_6	Q9_7
R_agCcgTEtb7HexIb	0	0	0	0	0	0							
R_2aHodufInMgESe9	50	5	25	10	5	5	1	1	1	1	2	2	1
R_ewKk9u5xqN7LZD7													
R_dp5CYSrOlzfuP6B	5	25	0	40	20	0	1	1	2	2	2	2	2
R_9sOsJDIva3HXfPT													
R_7aOkCU1qAXpge1v	100	20	80	100	60	50	2	1	2	2	2	2	2
R_es0KixzvFXhyi2x	35	0	5	40	20	0	2	1	2	2	2	2	1
R_6heNPFVW7pzlRZ3	10	10	0	20	45	15	2	2	2	2	2	2	2
R_6rLn0SF6BouZ0oZ	0	0	0	0	0	0	1	1	1	1	1	2	1
R_9SlcqYYX3qBwZgx	30	10	10	0	40	10	1	1	2	1	2	2	2
R_25oZRzdHyPiT7O5	0	0	0	0	0	0							
R_9QS0Fbienw0wfGt	50	0	10	20	0	20	1	1	1	1	2	2	1
R_a4ccDgaAxy5mstL	10	10	40	20	10	10	1	1	1	1	1	2	1
R_d6Je6Sf68pzQESx	20	0	0	10	50	20	1	2	1	1	2	1	1
R_5jyw36D7Ywnienr	10	30	10	10	30	10	1	1	2	2	2	2	1
R_bDVi3AFWRTTiECN	30	5	2	3	60	0	2	1	1	2	2	2	2
R_4Ixe9nP0ZRoJ0sJ	5	10	25	25	25	10	2	1	2	2	2	2	1
R_0krYSyLO67547pX	10	0	10	10	40	30	1	1	2	2	2	2	2
R_9snnP0ctyLMO8n3	0	0	0	0	0	0							
R_1FvfX9oZczF9U45	15	10	20	25	15	15	1	1	1	1	2	2	1
R_3UVRE1C23DshA6F	20	5	10	30	20	15	2	1	1	1	2	2	1
R_9zE7Ltn8WTGqNkV	20	10	10	10	50	0	1	1	1	1	1	1	1
R_4YsfZxzQh1Jbqy9	10	10	15	25	30	10	1	1	1	1	1	2	1
R_3NLjdeun3JLQEnz	10	0	10	30	40	10	1	1	1	1	2	2	2
R_4UBdaPhAK3Q5u2p	40	20	10	20	0	10	1	1	2	2	2	2	1
R_5oKK0sMgk8RDKJ	45	10	10	25	5	5	1	1	2	2	2	2	1
R_eetjH4dNis9bn4V	0	0	0	0	0	0							
R_eS6se2e46F2TbOR	70	30	0	0	0	0	2	1	2	2	2	2	2

Survey Responses Q8–Q9

V1	Q10_1	Q10_2	Q10_3	Q10_4	Q10_5	Q10_6	Q10_7	Q10_8	Q10_9	Q10_10	Q11_1	Q11_2	Q11_3	Q11_4	Q11_5	Q12_1
R_agCcgTEtb7HexIb																
R_2aHoduflnMgESe9	3	2	1	9	10	4	5	6	7	8						4
R_ewKk9u5xqN7LZD7																
R_dp5CYsrOlzfuP6B	1	2	7	10	8	4	3	6	9	5	40	47	39	40	41	3
R_9sOsjDIva3HXfPT																
R_7aOkCU1qAXpge1v	2	1	4	9	5	6	3	7	8	10	100	100	60		100	4
R_es0KixzvFXhyi2x	2	4	3	5	6	1	8	7	9	10	41	81	43	100	61	2
R_6heNPFwV7pzlRZ3	6	7	3	4	1	5	8	9	2	10	32	32		81	27	3
R_6rLn0SF6BouZ0oZ	1	3	5	7	8	6	4	2	9	10	40	40	50		40	3
R_9SlcqYYX3qBwZgx	3	1	2	6	8	7	4	9	5	10	25	30	40	30	20	3
R_25oZRzdHyPiT7O5																
R_9QS0Fbienw0wfGt	3	1	5	8	6	2	4	9	10	7	0	75	50	0	50	2
R_a4ccDgaAxy5mstL	1	9	3	4	5	7	6	8	2	10	52		52	40	45	3
R_d6le6Sf68pzQESx	1	4	2	6	7	8	3	5	9	10	35			81		3
R_5jyw36D7Ywnienr	1	2	3	10	4	5	6	7	8	9	99	98	98	98	98	3
R_bDVI3AFWRtTiECN	2	9	4	1	5	3	6	10	7	8	30	15	40	100	15	3
R_4lxe9nP0ZRoJ0sJ	3	1	8	6	4	2	5	9	7	10	25	80	80	95	50	2
R_0krYSyLO67S47pX	5	6	1	10	8	2	3	4	9	7	33	65	40	50	80	3
R_9snnP0ctylLMO8n3																
R_1FvfX9oZczF9U45	1	2	6	4	5	3	8	7	9	10						3
R_3UVRE1C23DshA6F	1	4	6	7	10	2	3	5	8	9	40	55	75	55	75	2
R_9zE7Ltn8WTGqNkV	2	3	1	5	6	7	8	9	10	4						3
R_4YsfZxzQh1Jbqy9	3	2	4	8	1	9	5	7	6	10	40	40	50	40	90	3
R_3NLjdeun3JLQEnz	5	1	3	6	2	4	7	8	9	10				75		3
R_4UBdaPhAK3Q5u2p	1	2	8	10	6	3	4	7	9	5						3
R_5oKK0sMgkk8RDkJ	2	1	8	7	3	4	5	9	6	10	10	0	10	100	10	2
R_eetjH4dNis9bn4V											17	16				
R_eS6se2e46F2TbOR	1	2	4	10	3	5	6	7	8	9	20		40	0	20	3

Survey Responses Q10–Q12

Interview Transcripts

Jim

[00:01:09]

FJS So let me just give you a brief overview of what the research is and kind of set how this the intention of this. At least in the IT department, the changes that happen out in industry and the world of security result in a lot of change in curriculum and in how courses are managed. And since we're not the only program that does that, we know there are lots of different departments that do that, the idea is to see how difficult is managing that change in other programs. And to see what people are doing right and doing differently, and see what kind of headaches that higher education programs have in managing this. Does that make sense?

[00:02:00]

JIM Yeah, and then just to make sure. So you're, so you're, you wanna know, I mean, because we're in a fast changing field how is the curriculum kind of keeping up with change so.

FJS Exactly.

JIM K.

FJS So the first question that I have to kind of help me is to understand um what roles does your program envision students have after graduating as a result of their taking your courses?

JIM Ok. And you want me to talk about my courses not our I'm not speaking for the department.

FJS Just just for your courses.

JIM Ok. So, um, so I'll focus on my Sec sec security class.

FJS What's the course number just.

JIM Course number is ----- . That's the undergraduate course and that's where a large number of students . . . Now I teach a graduate course and I teach some lower division programming courses, but since you're interested in cyber security.

FJS yeah

JIM now let's talk about that so. So I look at my course as I'm the only faculty member doing security. So we don't have a broad security program with many courses. So, and, um, really the role my course plays is it covers a broad range of topics to sort of introduce people to this security field and I look at it as mumble see probably three groups. But, there's probably a very very for a small set of students I want them to get enough background that they can go to a graduate program. Either come here or go elsewhere and focus on security.

FJS ok.

JIM So it really just gives them really an intro to that. I also think many of the students are not going to work in a security specific job. You know, and I'd say probably the vast majority will just become programmers in all sorts of areas, and I just want to you know alert them to security issues. To many of them this is the first time they've really heard about software security issues. So I wanna I um um I basically give them an introduction to some some uh really concrete topics in the field. Kind of introduce them to the issue, and maybe prepare them so they can go on and continue to learn.

FJS ok.

JIM So I hope that anything that I that they that this is so new and interesting and urgent and important and that they'll be both interested to keep learning and that they'll have some accurate foundation.

FJS Yeah.

JIM Like for instance I tell some of the students that even if they just go out and they products s-ya know product descriptions come to them or they read things in the in the computing news about attacks and things, I like them to be able to read and understand what they're reading. A lot of time recognize errors. Because there is just a lot of misinformation or inaccuracies or and so I just hope they have a solid kind of ground in terminology and and meaning.

FJS Yeah.

JIM Uh, and then maybe and maybe uh I hope you know some students could actually go into a security focused position. But ya know I think unless people come and work in my lab, I wouldn't say my course is enough to have them actually go out and get a security position. Because I think so much in our industry the people who the people in the crucial uh positions ya know aren't really there from their school training, it's they get so much experience so so um, so I think some of our students could be hired into an area where security is uh is a.... ya know... an important aspect. But I think they're going to need more training and more experience before they could

FJS really do it.

JIM Yeah, assume ya know a ya know a security role. To be responsible for security in a product development.

FJS So just as a followup. Why do you think that experience is necessary compared to just learning about it?

JIM Ummm . . . probably because I I, let's see. That's a good question. I think part could be because, you know, I introduce them to some fundamental topics. Like, I'll do some examples. Like here are two, a 1/3 of my course is cryptography. We learn about asymmetric encryption, HMAC, one-way hash, just some fundamental primitives that are part of many actually security systems. So they can learn about those those those primitives, but uh you know that's just a starting

point to actually and you know they learn that they probably never in their lifetime to actually build a ha ha security system that makes use of these. Um, But they could at least understand when they read other specifications how how it's working and why things are there. They can recognize flaws . . .

FJS Yeah

JIM And and and you know, snake oil. Ha, When ha, it gets brought to them. And and they would need ooo you know what do I want to stay that yeah, I I think those are fundamentals but once they, you know, or go work in the mobile world I I , it's back to this change. I think things are changing so rapidly that the protocols we have today are gone. And you know I was talking about WEP ya know 5 to 10 years ago and it's kind of irrelevant these days.

FJS Yeah

JIM Or um you know TLS is pop– very common right now, but things will replaced in 5–10 years. So.

FJS Ok, So it's.

JIM So.

FJS. So it's really kind of you look at something that's current so when it changes you have a background to understand the change.

JIM Yeah yeah, so I'd probably say that. so..

FJS So, one other thing you'd mentioned was that you mentioned concrete topics. Is that kind of what you mean by that?

[00:07:07]

JIM Yeah, I guess when I say concrete topics, I'd say maybe uh maybe in many respects when I say maybe concrete topics maybe maybe I say I kind of hmm . . . bes . . . some foundational th th

some things you talk about the changing fields yeah I'd say once the field is changing so fast if anything I I might focus on things don't change so rapidly. Sort of you know fundamental principles or sort of the core core topics that are going to keep persisting for a long time. But they're, they're going to be changing in a few years, and then so so uh uh let me see what I can come up with some examples. Umm, yeah I think in the cryptography case I introduce some primitives to them and talk about a couple of standard id-ideas protocols now that . . . so so that they can go out and ual you know a vast array of protocols and technologies they encounter they can recognize where these things are used.

[00:07:58]

FJS Yeah

JIM Um, but I don't I don't uh, you know, we're not sort of changing the protocol or moving kind of moving every semester with the thing, No I'm I'm I'm sticking with things that I prob-probably keep in my curriculum for probably 5 years or so um. Um. You know with the web attacks I mean walo we teach them the basic here's what SQL injection is, and here's what a buffer overflow attack is.

FJS Yeah

[00:08:19]

JIM Umm That just teaches them kind of the the intro to it. And we don't go, ya know, I don't go off and maybe say uh what's the latest variant of you know of w web browser and cross-site scripting has been very much of a moving target. Well, I probably trying to teach them the general idea and then go out and now study it. Ok so what's happening now, and what's this latest thing that just happened in Chrome that they fixed.

FJS Ok

[00:08:43]

JIM I don't really focus on that.

FJS Ok. That's good to know. Ummm, the next question I have is and this is kind of built off the previous question. Where does your course stand in relation to cyber security theory and the practice of it. Does it learn more heavily towards one or the other? And you had mentioned you have a lab to where people can get more experience, but in the curriculum where's the where's the bounds there.

[00:09:07]

JIM Yeah so I'd say uh I don't know I'd like to think I probably have an equal focus, and what I mean by that is let's take the cryptography section. So I definitely have theory in the sense that we we you know we sort of learn from the book or on paper, here's here's what symmetric encryption is, here's you know here's AES, here's public key crypto is. So we learn about these things, you know, kind of kind of text book chalkboard definitions, but then the students have programming labs where they actually implement AES.

FJS Yeah.

JIM And they build a toy implementation of RSA. And they do, ohh there's an HMAC attack, a message extension attack that's been known for a number of years, and they do it. So so, they go in the lab and actually build things or execute attacks.

F. Ok

[00:09:50]

JIM Umm. And so and I like and so I call it my sort of hands on practical learning. And I really like that because that makes it really concrete. If you just do the book learning ahh, you know,

sometimes people just don't you forget it, and it doesn't really mean anything. So so in that sense I f-feel like I kind of got half and half.

FJS. So, and I I think that's it's interesting because you know the IT program might focus on cryptography, here's all kinds of attacks that you do, this I think lends itself more to accomplishing the goals that you have. Some-

JIM Right.

FJS might go into a graduate program umm, somebody who's actually going to be a programmer-

JIM Right.

FJS And then people who go into security because then they have that fundamental basis.

JIM Right.

FJS Umm do you have any other comments on that?

JIM Yeah, no. Ya know I so I do that with cryptography in a sense we really do talk about the theory and then do the hands on programming. And I place a here a I'll speak uh a little bit as I see it. I do this kind of a course. Math has a cryptography course. My stuents have taken it, it's purely textbook. And ya know all their assignments are pencil and paper. So you know that's almost you know entirely theory. Although they although they, you know, conceptually work out real world attacks. And and you know my course is kind of half and half in the sense that I don't go as deep into all the theory properties as they do, and we spend you know, a portion of our time doing that so so about 1/3 of my class is cryptography. I'd in into the software security area, we talk about SQL injection, cross site scripting, buffer overflow attacks, and then again password cracking, there's those are some topics. And we have some programming labs that we do in that area. So again it's it's it's kind of you know the mix I like to talk about the idea, expose them to sort of one practical you know working of it. But it very much is is kind of touching the surface.

I I I'd say we do a few things, I try to learn them very very well, but with the idea that "Oh, it it really is just a ya know you could do a whole course on the ins and outs of SQL injection and all of its variants. So so because I have this course where I do 1/3 cryptography, a 1/3 protocols, a 1/3 web software security. It ends up kind of being a.

FJS So what you've mentioned that you kind of like to keep something stable for about 5 years right? So the follow up question is how does this affect how you maintain your courses and lab assignments. Umm, is it just kind of I'm going to hold this 5 years, or what indicates that you need to make a change?

JIM Ohh, good question. Yeah, that that it you know, that 5 year thing is kind of something I tended part of it is just a practical matter that you know it takes effort to create a really excellent lab and uh ha and so maybe ever year I try to to you know we might modify a lab or introduce something new. So so, I'd say we sort of have it's a gradual change.

FJS Ok

[00:12:43]

JIM Um.

FJS It's not overbearing, is it?

JIM Oh, uhh no. No. I wouldn't say it's overbearing. And that's just because I just kind of limit it to that. Maybe an argument could be made that we could really invest huge energy into uh you know, revamping and redoing everything ever year, but that's umm, it's uh some of this relies on when I get really good TAs who are very talented. That's when we can maybe make some changes.

FJS Ok

JIM Um. Here's let's see if I can come up with a couple of examples. Well so we, I try to have some buffer overflow attack labs. So we've just slowly been migrating them. So so for instance

a few years ago we had people. The first one introduced, people performed a simple buffer overflow attack. Then since EE had a 324 course where they did the bombs, some really low level, very excellent labs from Carnegie Mellon, then I changed my labs that were more about learning the defenses. Like you know, kind of like, uh, turning off stack execution, and what are what are these compiler generated canaries. And we sort of learned about this, and had a had a lab where they read about some things and compile their program and see how their defenses worked. Now that um EE is not going to offer that course anymore, so I've now brought in that buffer overflow lab from EE into my course. Now the students are doing a more, they're they're actually doing an SQL injection attack.

FJS So is that because the EE program now requiring your course or is it that they're just getting rid of it completely?

JIM Well they're um I'm actually kind of getting mixed signals on that. We we we stopped requiring it in our program. So many of our students and and I'd heard that it was going away although I've got a mixed signal just the last couple of months. Someone said, "No, it's going to be renumbered, and it still be taught." So I actually don't know.

FJS Oh, ok.

JIM But, but that but just a few of our students are still taking it. Because it's optional.

FJS Ok.

JIM So so I've kind of tried to bring some of that material here.

FJS Ok.

JIM Umm.

[00:14:41]

FJS So them, it sounds like one of the, it sounds like there's several things that might contribute to how you change a course. One is just your view at a point . . .

JIM Yes.

FJS When you look at it. Umm, the other issss, umm, perhaps what kind of new contributions either within the department or TAs that could facilitate more change.

JIM Yes.

FJS And then the other is just the courses that are available. Yep, how it relates to other courses. Yep. And a lot of it you know is my own knowledge in the sense that there's not a good a text book out there ya know with these labs all ready to go. And so, some of the labs as I introduce them, for instance, I I really ya know taught myself what are buffer overflow attacks and how they work and as my own knowledge increased the labs kind of kept up with my own. Sigh, you know education. I'd say that's happened in a couple of areas.

[00:15:35]

FJS That's uh interesting thing you mentioned. You mention that there's not a really good textbook available. Do you have like a standard uh book listing that you require, or how often does that change?

[00:15:44]

JIM Yeah, uhh it changes frequently. So I'd say in the 10 years roughly I've been teaching the course I had some required textbooks early on, but the last 2–3 years I don't have a textbook. It's partly because I do this uh ya know I cover cryptography and software security kind of a range of issues. And so so lately I just rely on resources on the web, Uh . . .

FJS And then your own curriculum outlines that you've used in the past . . .

JIM Yep, that's right. Slides and outlines and the the labs the labs and homework assignments are a big part that they've just been created over time. Let's see let me think there was something you said just a minute ago I wanted to make another comment on. Umm . . .

Another thing I would say, here's another sort of my own philosophy that I think relates to the whole topic you've been talking about. Which is I'm not so concerned that I've got to you know have you know s-say the most recent exploit example to you know teach the students, um I actually feel like I want to I'm here to teach the students how to learn. You know, give them a problem to solve that's that's uh kind of appropriate to their level and that they can get here here's my best example. That we teach them symmetric encryption, and in the last 5 years I've had them actually AES. Now when I started out there, I wasn't actually going, I never thought of actually doing this because first of all, students you don't want to write your own implementation of AES and use it. Ha. and it's a standard that's there, there's free software all over the place.

FJS yeah

[00:17:21]

JIM But I had one of my graduate students, who he wanted to understand encryption. So he got the spec, and he sat down and he implemented it. He didn't look at, he didn't look at [mumble] he did it for understanding, and by doing that he he really learned it well, and he said it was very, he really enjoyed doing this. And by seeing him do that, so I ended up one time in the lab I what I asked the students to do, I said, "Here's the specification for AES, it's actually kind of hard to understand." Partly I wanted to give them an experience, people write specifications, and they're there, and they're sometimes not so easy to understand. And they didn't actually do a very good job of it.

FJS: Yeah

JIM So try to sit down and implement it. And they kind of learn it's kind of hard sometimes to implement something from a spec, and there's there's questions that aren't answered. So so I like them to to get that experience, and when they implement AES suddenly, before encryption is this magical thing, I don't know, bits go in and bits come out, you know it seems all magical, but when they actually implement it they learn that Oh, we do this thing that the mathematicians actually gave us that that the machine to do this, and when they see how it works, now they know what a block cipher is, you know crystal clear. And how I wondered if this was really appropriate for them, are students cheating, are they going off to look. So I encouraged them, I sort of just challenged them, "Hey, see if you can implement this in 3-5 hours without going and looking at someone else's code." If you do that, then I like them to tell me about it, and most of them are telling me that they figured it out on their own. And I've had several students say, "I got a job because I told someone I had implemented AES." And in the end of the year reports, I've had several people say that the AES lab was their favorite lab. That kind of, you know so, that kind of surprised me. I wouldn't have expected that. So while in the end, none of them are going to go out and get a job to implement AES, but . . .

FJS That experience that's . . .

JIM But but yea, and I like the idea that once it's starting back for me, it's just that students came to something, this looked mysterious and hard. "I didn't understand it, and I was kind of intimidated by it. And then I actually approached it and I did it." And they feel this sense of so it's just that learning process. In some sense I feel like it was it was just that learning process now I say "great, now you can go out and just remember this. You go out in your life, and because we have this changing field, I feel it's not my job to keep up with the changing field, it's to teach them that your secret to success is to be able to take anything and say I can figure this out. He he, and

I've done this before and it was fun. And I looked at something first and it was all seemed like Greek and I was a little intimidated at first, but with a little effort I figured it out, and I made it work."

FJS Awesome.

JIM It's it's in some sense that's almost more important to me than saying you know I taught you about the 15 most current things.

FJS Yesss.

JIM I mean you have to be careful there because I can say well I don't even have to teach you security, so I just so so I want that's why I don't feel so urgent that I've got to that's important to change my course rapidly. It's all sort of that would be really hard to do. What I'm really going to do , is give them a few really current and credible activities that give them good, teach them how to learn and give them confidence.

FJS That's awesome. So I think you kind of answered this next question. What do you rely on to make your course or program flexible to the changes in the cyber security field. And I think that kind of what I understand is that um that's not the main purpose to make it match what's in the field, it's to be able to teach them how to handle what's in the field. Does that make sense?

[00:20:43]

JIM Yeah yeah, I think so too to a degree. The only thing I'd say there, what do I rely on? Well, my own attending conferences and paying att- so one is I have to put significant effort in trying to stay current.

FJS Yeah, and so it's kind of a judgment call on. So for instance say you go to Defcon, and all of sudden they aren't talking about Stuxnet like they were 2 years ago, now it's all social engineering.

JIM Right

FJS Does that make sense?

JIM Yes. Well ya it's it's here's one example, where I'll admit I haven't kept up entirely. We'll take the buffer overflow example. I've been teaching people about stack based overflows and I think that's a good technology and an idea to learn about, but in some sense they realize we're more and more getting where there's built in defenses that that I think it's valuable to know the history of that, but it may not be as relevant as it was say 10 years ago . . . when . . .

FJS When you could run a buffer overflow on anything.

JIM On any machine, that's right. IT, you know, people are using rotten or return oriented programming or or ROP. So I sort of know now that that's kind of becoming an advanced technique for what people are doing and I'm still in the process of gee, should I should I learn enough about that and we ought to be doing a ROP kind of introduce that into a lab, that's sort of a it's it's a I still need to learn more about that, and it may difficult in the sense that well, before people get into ROP it'd probably be better for them to start and understand the the you know stack based buffer overflow first, then understand why the defenses stopped that, and now how people have moved on to here's another uh

FJS So it kind of makes you you, one thing I thought about while you were saying that is that it kind of seems like you're more dependent on trends like longer trends than necessarily something that's immediate. So like buffer overflow.

JIM Yes yes yes

FJS The reason we still talk about buffer overflow is because it was relevant for soooo long, right?

JIM Right.

FJS And uh, so looking at ROP, return orient programming, it's more something that you've recognized over the last few years it's still around, it still continues to be a problem, that's what may necessitate introducing this into the course. Is that right?

JIM And now, and I'd say, "Well if students have learned what I currently teach them about buffer overflows, then then they could go out on their own and understand ROP." With the background I give them. But but that's probably a debatable point. People people could try to decide is well is that true, or should we . . . I think one argument could be made that hey ROP should be front and center now. But there are still, well we also get new even though on a lot of platforms we've got these defenses, new smaller embedded systems, those concepts are still relevant. Ww can't say that the traditional buffer overflow idea is out of date.

[00:23:39]

[00:23:44]

FJS Have you ever taken anything out of a course?

JIM Yeah, I mean I've or, you know, As I've taught I've reduced my cryptography I'm slowly squeezing it and doing less and less, and trying to add more software and web security. So that's kind of the trend in a way, of the course I'm doing.

FJS Ok. Alright so the last question deals with Bloom's Taxonomy? Have you ever seen this before?

JIM I think I did in the document you sent the other day, but I don't think I've ever really seen this before.

FJS So umm, I don't know all of the background behind Bloom's taxonomy, but it's basically a kind of a level of what. How what kind of learning happens in a course right. The lowest would be remembering, then there's understanding, applying, analyzing, evaluating, and creating. With

creating being the most effective. Right? So this is really just kind of a subjective question, but really how do you, where do you think that your course fits along the lines of these things?

[00:24:53]

JIM Yeah, I think, well. I mean, ya know. It it clearly has remembering, understanding components. I mean I think because we do the hands-on labs. [mumble] there's definitely some applying. In terms of analyzing, ya know, students we give them we give them problems where they uh for instance we we have sort of a a ya know in the one way hash section they do a they essentially do a collision attack and a pre-image attack on sort of a toy hash function. We make it small enough that they can actually do the attacks and and we sort of have them do an experiment to say ya know the mathematicians says the cost of this attack should be such and such, let's do this attack in practice and they can see "Oh, if I take my averages and see it I can plot that exact kind of a curve." So there's a bit of analyzing, ya know in that, and a number of other labs. I don't know what the difference necessarily is between analyzing and evaluating. But I would say we're definitely there. I mean, in terms of creating, I think from our graduate school I'd sort of say well . . .

FJS That's more of a graduate level type of thing.

JIM Yeah, so. Yeah, that's right. I'd probably say yeah we're definitely getting in, we're we're a 100% applying. Our I think we definitely do analyzing. The difference between analyzing and evaluating, ya know I'm not sure. We don't there's there's not large projects that require deep kind of evaluations. So . . . I'm probably in the evaluating, analyzing . . .

FJS Do you think this creating component of, do you think that has a place in school?

JIM Um . . . yeah . . .

FJS Like, for instance let's say you do a 600-level course for your master's students, and you say "build, ya know. Find something to break." Is that a good thing to have them do? Or?

JIM Yeah. So I think in our graduate level I think we have aspects of create that's where we expect people to take their knowledge and do something sort of new and novel. That you know.

FJS Yeah.

JIM We may not even know the answer, right? So so that they can propose their own ideas. But in a 400-level class, I mean there's you know, people may say there's mild bits of creativity when they do a problem they kind of do their own ya know . . .

FJS Like a project?

JIM Do their own attack, or they figure things out on their own. Maybe to them that's more a creating because you know they're not just reading it and borrowing ideas from someone else.

FJS Yeah.

[00:27:22]

JIM But, a lot of what we do in the 400 level class are still pretty . . . ya know, pretty basic. They're small, incremental, given a bunch of information that hopefully they can deduce or inductively figure out what to do.

FJS. Yeah.

JIM But it's not creative.

FJS And I think part of that question, the other big component is what are the expectations of the students, right? So if I'm in a 400-level class, I may not expect that I'm going to go in, and I'm going to find some application to break. It could, and that might be, why people like that AES lab so much is that this just brought a whole new level of understanding to me. And that's what I kind of expected.

JIM Yeah Yeah.

FJS Umm. Is this something you ever really . . . so you'd mentioned the AES lab, when you're thinking of and designing labs how often do you perhaps consider the outcome to match something like this? Does that make sense?

JIM I I'm probably, most of the labs I do I'd definitely say are applying, meaning it's applying and analyzing so it's more like, "Ok we've learned this concept here, now let's see how it really works in practice so I would say it's probably applying and then if they have to do any kind of reporting of results and summarizing. So yeah, I think it's probably analyzing and applying.

FJS K.

JIM That's part of these, you know these are large classes and they get us a topic that it's kind of an introduction, ya know we're introducing them even though they're experienced in computing and programming, it's the first time they've really been exposed to this topic.

FJS That's an interesting point. Is exposure may have been limited before.

[00:29:10]

JIM Yeah, so. If we were designing a longer curriculum, I think once people had had my class, I could see the top students who really already come in with some experience and really get energized by it, ya know then they could break into a thing, or breaking systems, or go to capture the flag and go and do some serious problem solving. And can they take this background they have and go deep problem solving, or try to design and create their own system. "Hey, so what would you do to protect your own web application?" You know, something more out of the box.

[00:29:51]

FJS Ok. Do you think there's a vision for that? Like are there other programs that do things like that?

JIM Ummm . . .

FJS Is there anything that stands out in your mind as that programs pretty impressive in how they do things?

JIM Yeah, so I know of universities around who have at least from a research stand point, I'm more familiar with kind of the graduate level, and you know they can go there and there's multiple courses and multiple faculty members. I can't say that I really know at the undergraduate level what those universities are doing. I know from a few labs that we borrowed from Carnegie Mellon, and a few places. So I know that there are people who are kind of doing hands on labs, but I haven't really encountered anything, there's nothing you know really uhh you know revolutionary, or exciting that's getting attention, or at least that's come to my attention.

FJS Ok

JIM I can't point you to anything.

FJS That was just a curiosity question. Well I don't think I have any other questions. Do you have any other questions or comments you want to add in?

JIM Nope, we're good. I hope that this has been helpful.

FJS This has been really helpful. I think this is exactly what I wanted to get out of it.

[00:31:00]

Lou

[00:00:45]

FJS Well, let me just give you an overview of the research and that should kind of help you understand what it is I'm looking for.

LOU k.

FJS Um, so basically, you know, anybody that deals with cyber security recognizes that they have to kind of keep up with the trends, right? And, that has an effect on how curriculum is managed, how courses are taught, um, and so that's what this is trying to explore is to see how deep that that change is.

LOU k.

[00:01:18]

FJS Um, so the first question I have is, "what roles does your program envision students have after graduation as a result of their taking your courses that are security focused?"

LOU Well, first of all we have, let's see how many security proper classes do we have. We have one security class in our master's, one forensics class, then we have in undergrad a business processes and control class. Which is sort of like like this CISSA, it's like internal control but for systems.

FJS Ok.

LOU And then that's it. So we have those three classes. So, we don't really have an information security program per se, but we do have those three.

FJS Ok.

LOU But for those students who do take those classes, we hope that they, our goal is to develop managers who are capable of IT.

FJS Ok.

LOU Um, they definitely start off as practitioners, but I think the ultimate goal is that they become managers. And so I teach the forensics, and I teach the security class now. And I, my goal is to have them be aware of some of the major issues, and so that they can manage information security

as a function. We want them to understand that information is a resource and that it needs to be protected. It needs to be managed like any other business risk.

FJS Ok.

[00:02:52]

Printing questions break

[00:03:47]

LOU And then at Olu, and I've been at other universities, but just doing research.

FJS Ok.

LOU My experience with teaching these topics is from Georgia State, and here.

FJS Ok. And then research, so but as a researcher you're able to see other people kind of maybe dealing with it, right?

LOU With teaching? Uh, Yeah, well though. I don't really look at other people's teaching curriculum really. Like my research doesn't really have to do with teaching, so. I guess I don't really have any insight there.

FJS Ok. Alright so that first question . . .

LOU But I do have colleagues that teach this topic, too. And I sort of keep apprised at what they teach, and stuff like that.

FJS Yeah. So the next question uh is just where does your course stand in relation to cyber security theory and the practice of it? Does it lean more heavily towards one or the other and how do you balance that?

LOU Hmm . . . Umm. [long pause] Well, I think I try to make a good balance, I try to. I think if it's just the hands-on, then I think that you know, you could pick up the skills at a trade school, and I think the purpose of a university should teach principles and critical thinking. If you don't

do that then, I think, there's not as much reason to be at a university. So I try to make it balanced, but at the same time you can't really learn stuff, or to have useful skill unless you can actually do things. So, I try to make my labs half and half. So it's half um like some principle they're learning, and the second half they actually apply it and do something. That's the goal anyway, not all of my labs are that way, or that balanced. But I'd like them to be like that.

FJS Ok.

[00:05:54]

FJS So . . .

LOU Like for example, the passwords I teach like the psychology of passwords, I teach the formulas of password strength, help them understand like the limitations of password cracking, that kind of thing. So those kind of theoretical principles, and then there's the hands on piece where we actually crack passwords.

FJS Ok. Umm, one thing I've heard, and so, when I had taken it from you there was lot of cryptography. At least in my opinion, it felt like it was more cryptography than whatever I'd ever really done before. And then there was, ok here's how this works, now here's a homework assignment. What's changed in that area?

LOU So, did you have security and forensics with me?

FJS I think it was 560-something.

LOU Yeah, I think you never had forensics with me.

FJS Yeah, I don't think it was forensics. I think it security

LOU Yeah you were in 560, yeah. So, hmm, so it's still, we still talk about the formulas and things um, we probably talk about it a little bit more I think. We talk about block ciphers, um, different modes of operation, that was more the way I had last time, so we definitely go deep into the crypto

although it's not like the math crypto class. We don't really go through all the formulas, but definitely the principles of it and . . .

FJS What do you think necessitated that change?

LOU Well that's not actually a change from what we had before, but it's just that we didn't cover block ciphers, and I think that it's such an important building block that we needed to cover.

FJS Ok.

LOU So it's just all modern crypto. The work horse is a block cipher. So the reason why I came to those conclusions was just reading books about cryptography like um, this one. This is probably one of the best books I ever read, Cryptography Engineering. [unintelligible] Chrono [unintelligible] Security Engineering. It's a good book but it's not as . . .

FJS That's the one we used in the class

LOU Yeah.

FJS Was the Anderson book.

LOU Yeah. So this is mine right here. So I kind of changed the book. It used to be, do I have it up here anymore? It used to be this, and I really didnt like it. I like this because, it just sort of fits my view of security. It's um, it's not just the technical, or not just the cryptological, but it's also sociological, or psychological.

FJS Well there was also more added context to the book.

LOU Yeah, there's tons of like events, and stuff like that. So anyways.

FJS Ok. So, um. so from what you've said, how does that kind of affect how you maintain your course and lab assignments?

LOU Um, [cough]. So how does what affect it, specifically?

FJS Um, maybe the your balance. Like . . .

LOU Oh, like half theoretical, half applied?

FJS Yeah, how does that effect the assignments you create, and the labs that you do? How often do you say, “Okay we probably need to introduce a new topic, or we probably need to change this lab, or update it.” How often does that happen?

[00:09:32]

LOU Um, Well, every year I tweak all my labs. Um [pause] maybe that’s not totally accurate. Um, I definitely re-assess them all every year. Umm, but there’s usually changes every year to the labs. Sometimes I hope that there are major changes, but sometimes they’re not. Like, um, like in forensics this year there’s a module on password cracking, and in the past I’ve always used rainbow tables, but because GPU password cracking is so much faster nowadays um that I think the utility of rainbow tables is pretty limited. And because of that, I moved that out of the security class. Now we just use hashcat, we don’t even use rainbow tables anymore. Forensics, I think it still might be useful if you’re just trying to crack one single password, and um, windows passwords are are not salted so you can use rainbow tables but I’m not actually sure that it’s still better than hashcat. Because hashcat is so fast now, and so now this summer I’m going to compare the performance of rainbow tables compared to hashcat, and if hashcat wins out I’m not even going to teach rainbow tables.

FJS Ok.

LOU So there’s stuff like that I mean, like Kali Linux, um, the new version of BackTrack so I still I change that up, but the applied piece of the lab I definitely try to make current, and reflect practice as much as I can.

FJS Ok.

LOU The principles are more static, and I think that's the way they should be. They should be more independent of the underlying technology.

FJS Yeah. Um, what do you rely on to make your courses flexible to those changes in the field? Like, is there a degree of um how often do you have to see something changing before you say we need to add this in to the course? For instance like that rainbow tables thing.

LOU Well, I don't really have a set mechanism, like this is what I use and when this thing reaches level red I switch things out. But what I do do is I have a pretty extensive blog roll, and Twitter roll. And I guess it sounds sort of stupid but, um, actually I find it really useful. Basically, essentially, my entire Twitter feed is security and forensics people. I don't have like celebrities and crap like that. It's just, and they post stuff all the time about things that they're seeing, and I think it's a really useful way to keep up with what's going on. And actually my security class, I review the last 12 months of security events, and it's pretty interesting to see trends, like over the past year, and so that definitely helps a lot, too.

FJS Was that something you just did for your lecture preparation, or was that assignments for students, saying go out and look at this.

LOU It was actually both. So one is for my first lecture, I recap the last 12 months to show them like this is so relevant. This is really important to your careers, even if you don't want to go into security specifically. So, and I don't review things just for that one lecture but just to keep abreast of what are the major happenings, and then I have another assignment where my students have to review a current event and write about it. Something like that. Or review current technology and write a security assessment for it.

FJS Ok. Um, next question, are you familiar with this?

LOU Yeah.

FJS Bloom's Taxonomy, um, is that something, how do you see that fitting into security courses?

LOU Hmm. Well in general it's great to be at the top, creating and evaluating things. So, um, I'd like stuff to be up there. So for my tests, I don't really like the remembering and understanding pieces. So I don't really do multiple choice. So I have quizzes for readings, but those are strictly to give students a carrot if they do their reading. That's it. Because students used to tell me on their evals that I like the reading but I didn't do it because you didn't require me to. So, for the final exam, um I actually do it on Learning Suite, and I make it open internet, and have them work from the lab computers with all their tools, and then I ask them questions from past hands-on labs. And I have them do stuff, because I think it's . . . I think it's more meaningful that way. So in that sense they are evaluating, they're analyzing, they're applying, um, I guess I don't really have them create things per se. Other than . . . reports

FJS It's hard to do . . . somebody has to know a lot to just go find an application and start testing it for vulnerabilities, right.

LOU Yeah, but that process is sort of creative, so I might say that pen-testing or evaluating a security application that could reach the creative level. I mean, you're not making a tool from scratch, but you are being creative in how you apply it.

FJS Yep

[00:14:58]

FJS Umm.

LOU So, I mean not all of my questions are that way. And there are things that I test for understanding, but even then um because it's open internet it forces me not to have stuff that's readily Google-able, and so it sort of forces me to make, make the questions more applied.

FJS Yeah.

LOU So. Anyway, that's the goal. I'm sure I'm not you know perfect in getting these things high, but the goal is to get them higher.

FJS K. Alright I'm trying to think if I have any other questions that aren't necessarily on this, but are similar. Um, here's the other question that I have is how do you manage labs? Do you have like a TA that manages different labs or . . .

LOU You mean the creating of them?

FJS Or, yeah, or the managing of them, if you say, "here's a lab, go ahead and do it." Do you get notified if there's problems, does a TA handle that? How does that work?

LOU So the way my labs work is I lecture, the goal is for about 30 minutes.

FJS Ok.

LOU And then we, we break immediately to hands-on labs. And then, the reason that I do that is because I think people get tired of lectures, even really good lectures they just get tired of it after a while. So we break, then we go to hands-on labs. Myself, and my TA go around and answer questions, make sure they're good. And then, usually my office hours are immediately after class. If students want to they can stay there and continue working on it, and then work with me. And then my TA stays the same hour, and then my TA comes a separate time too in addition.

FJS So is that lab strictly for that time period or do you have labs that say run for a week. Students can work 24/7 on it

LOU Oh yeah yeah yeah. It's due a week later, but oftentimes students just um they start it in class, because we ask them to, and then they continue after the class. And then, um, some of them finish up I mean in those first two hours, or they come back and work later in the week and do it.

FJS So, do you have an example of a lab that's like that, and what the goal is in it.

LOU They're all like that. So, um, yeah like the last one it's not a, I mean, it doesn't really matter which one I give you because they're all like this. But the last one they did in Forensics, um, it's called e-discovery, and it's just part of the forensics process to support lawsuits, and I give them like this gigantic corpus of e-mails from Enron. So they're actual emails, and I have them de-duplicate the e-mails and then run relevant search queries to get down to a narrow dataset. So I get them from like a couple hundred thousand e-mails, down to like 40 or 50. And then once they do that, they've finished the assignment. So [cough] that's the hands-on piece of the lab, and we get that right after the class.

[00:18:15]

FJS So is it accurate to say that most of the labs are designed to um they don't necessarily depend on you if something breaks?

LOU Um, yeah. I mean, some tool breaks, or if the instructions don't work. If the tool breaks, then it's not really my fault that happens. But if the instructions are wrong, that does, I mean that is my fault. Which one are you getting at though, because they're not the same?

FJS So for like, let's say, you're running a penetration testing lab, and you have a mock up environment of that, if the students break that, how do you manage going back in make sure it's running so that they can come back. I don't know if that's something you do, but an example like that.

LOU Umm, I'm trying to think if I have an example like that, I have um . . .

FJS It just depends on whether or not that kind of work is relevant to your course, right?

LOU Yeah, I try to make things um have each student they're attacking or trying to break, in that way, if the student breaks something, it doesn't affect the whole class. So I think I've designed it that way so that there isn't really an example anymore where people share stuff. But it used to be

like, my forensics project, I have an incident response project and it used to be that they all had to check one server for evidence and they used to trample over each other's evidence. Like the whole project. So this year, I made 8 servers, and each team has their own server to check out.

FJS Ok. That makes sense.

LOU Yeah, there's really not something that if it breaks then I have to fix it. But, my job is to get the labs deployed without any um typos or mistakes in the instructions, and then make sure the tools work. And they're actually pretty hard. I think a good lab is not easy, because I don't know you can make it super hard and then students complain, or make it too easy and they don't really get anything out of it. Um, but the other thing I try to do. I don't know if this is relevant to what you're studying, so tell me if it's not. I try to have two parts to each lab, and they're not all at this ideals, but this is the ideal that the first half they have rote steps that tell them how to use a tool, that way they don't feel lost.

FJS That way they don't have to Google something and their Google-fu isn't great, so they're . . .

LOU He he, yeah exactly, or they're not, they don't get frustrated because they get thrown in and they don't know how to use this particular tool. So I give them a set of steps, this is how you use Metasploit, these are the specific tasks, and then once I do that, I give them a different part 2 of the lab is open-ended, and I say, "ok, using the things that you've learned previously, be creative in how you apply them to do this." I mean the first one, it gets people's feet wet, but it's not that, it doesn't really stretch them, it's not very high on Bloom's Taxonomy, but the second one does because it helps, they have to be more critical in what they do, or creative.

FJS Ok, so just one other question I have, you've been doing this for a couple of years at BYU.

Do you ever hear anything back from students who've taken these classes?

LOU You mean from industry?

FJS Yeah.

LOU Yeah, sometimes. It's nice when I do.

FJS What kind of feedback do they give you?

LOU Good things. From forensics, they're usually surprised by how relevant, or how useful it is, or it, the, um they use it before they thing they would have. So that's sort of cool, like e-discovery things or um just the forensic process um yeah I'm trying to think of specific examples from the security class, but . . .

FJS Do you have a lot of students that actually, I mean, because I remember taking it and then there were a bunch of kids that were like, "I'm talking to so and so about you know being on their security team." I'm wondering if that's still . . .

LOU It helps them get jobs for sure. And we have an emphasis now in our master's program and um so they take our classes, and they take some of Dale's classes, and they can even take others like in CS and stuff like that. And now, it's pretty cool they're going directly into security and before students couldn't really do that. They were sort of in a catch-22, "how do you break into security if you don't really have any experience?" But now they're hiring directly into security practices and that's really cool.

Wolfgang

[00:00:22]

FJS So, the point of this interview is to just kind of understand how the cyber security program adjusts and the approach that it takes to teaching cyber security. So the first question just says,

“what role does your program envision students have as a result of their taking your security course or courses?”

WOLFGANG This far enough? (reference to distance from microphone). I guess there’s a variety of roles. So we we kind of a split, those who go on to security careers and those who don’t. Um, that those that go into security careers go as pen-testers, incident responders, security analysts. Sometimes coders, systems administrators, etc. And those that don’t, tend to still benefit from the security experience. They basically, it strengthens whatever domain they want to go into, whether it’s databases, or human computer interaction. You know a lot of people don’t think of security as covering those, but it does. So . . .

FJS The next question, I don’t have a follow up on the other one, where does your course or courses stand in relation to cyber security theory and the practice of it? Does it lean more heavily towards one or the other?

WOLFGANG I think we sit straight down the middle of the line, which is where I like us to be. We spend um, I mean, I teach only kind of senior and graduate courses in security. So most of the underpinning theory has been done already. But we do go over, kind of conceptually, the security topics. The, they they spend a lot of the time, at least 50% of the time in labs doing practical skill development, really trying to get a better grasp and how to synthesize, and kind of um, develop solution rather than just following scripts. So yeah, I would say we’re heavy, maybe 50/50 but of the lab time we spend it’s not scripted labs, it’s kind of self . . . it’s kind of solution driven. They’re given a problem or scenario, and they’ve got to find a solution. [inaudible] Take a quick here or do this

FJS So, what what do you do that makes it so that they have the capabilities to develop solutions? What do they have to do in order to get to that point?

WOLFGANG Think. Really, I'm trying to get them to understand some of the security issues conceptually, and then be able to develop appropriate solutions for different types of scenarios. So, you know, the scenario of recovering data from a thumb drive is going to be completely different than responding to a malware outbreak in a hospital for example. Umm, you know, you deal with things differently, and so I'm trying to get them to think about uh in the context of scenario, trying to make different technologies available so that if they have to build a firewall as part of lab then they're not forced to use one particular method or technology to do that. Umm, I try and provide them with a range of software products and techniques, and then let them figure out what would be best applied.

FJS Ok. Um, that kind of goes into this next follow up which just says, "How does this affect how you maintain your courses and lab assignments?"

WOLFGANG Umm, Keeping them up to date is always a challenge, like the course content, depending on the course changes between 20–70% a year. Like pen-testing probably changes 70% of the course content, um forensics probably about 20%, and IAS right down the middle of those two around 50%. Um, mainly because the technology's moving so quick, and security threats, I mean like the SSL problem we just had is a great example. You know, we've never really looked much at that because we've assumed that's been fairly safe. And now we're finding out it's not. So there seems kind of add and look too. Umm.

FJS So, kind of what you're saying is that you want kids to develop a solution, and you do that by giving them a range of technology to use to meet the objectives of whatever assignment they're working on. But, when it comes to maintaining the course, you're having to make adjustments.

WOLFGANG Yeah, um, it's so I mean, one of the ideas in giving them more technologies is to reduce the overhead. So so there's two overheads in maintaining the course, one is kind of

personal, making sure I stay up to date with things and am current with technology, and the other is making sure their labs are up to date. The first part, there's not really much I can do other than kind of keep reading, keep practicing, keep honing my own skills, but the second part um, trying to do that labs where they're more scenario methodology driven, and the technology is separated from the kind of learning objective if you like. You know, they've got a system which is being um has a bunch of ports that shouldn't be available publicly. So they need to build a firewall, bring it back to when we used it before. So, if I say here's a script to go and do this on iptables every year that would have to be updated, or ya know every few years. If I give them one that's using a different product or some commercial product, then chances are we have to update that at the start and get the new firmware or whatever it is for it. But if we, if I say we have a pool of software resources they can use, and then just say their objective is to reduce traffic on these ports. Then they can pick a/the technology, then there's still an overhead but the overhead's not mine in terms of maintaining the course, it becomes the student's in terms of choosing the technology, and I think that's actually, I mean I learn a lot from just doing that and maintaining the course, but I think the students learn a lot from the opportunity to choose from a technology, and say, "Ok, I'm choosing this one because I'm more familiar with it, or because I think it's better suited to the problem, or whatever."

FJS That makes sense. Ok so, what do you rely on to make the course or program flexible to changes in the cyber security field? So you just mentioned some of that overhead is on the student's to pick what to choose.

WOLFGANG That really, I think it's about choices. It's about giving them as much freedom to choose or kind of tailor their education at least the practical side of it to themselves. The concepts, ya know, are fairly resilient they don't change that much, but the implementation hmm, things

change or if they have different needs or want to get something outside of it then giving them flexibility on how they do things, or even labs they could choose sometimes we might be talking about public key encryption infrastructure, they could be doing a self-signed cert for a website or they could be building PKI servers and ya know if we can have it so they can, it's it's part of that lab that they can choose whether or not they want to sign a website or sign a VPN if they want to uh ya know whatever they want to use that for. We can try and make that a little bit flexible.

FJS Ok. Umm

WOLFGANG We want to allow them to adapt to new problems or situations so they can kind of move towards . . . like this OpenSSL one we can tackle all that without changing a great deal.

FJS Yeah. So this is Bloom's Taxonomy. How do you kind of, where do you think you fit on that scale? And how do you try, where's the balance on that scale for you?

WOLFGANG I think for the level of courses, which are the 400–500 courses, we're looking at mostly analyzing and above. At least that's where I'm trying to get. I want them to be thinking. It's fine remembering a knowledge and getting to a test because you remember the terminology, but it's not going to help you in practice. You got to be able to apply it. To be able to use it to um, I guess analyze or assess problems, to be able to come up with solutions, to see how effective those solutions are, so evaluation, to be able to uh create solutions, and that's, I think that's why students are kind of getting such good placement, and being paid so much now is because they're doing that really well. They have the opportunity to . . . I'll give you an example, when I was doing my JavaScript class as an undergrad it was a case of I'll be given a script that says, "here's a bit of code, type this in, compile it or run it, what happens. Now, change it so that it does this." Then I'd go, "Ok, I need to change 10 iterations to 20 iterations, and now report back on it." And that's fine for like the lower three things, but for IT, we're trying to get them to say, "Ok, here's

the problem, I'm familiar with the technologies, how do I apply them and produce something that fixes the problem.”

FJS That makes sense.

WOLFGANG Is that alright?

FJS Yeah

WOLFGANG Ok.

FJS Ok, so um.

WOLFGANG Did I pass?

FJS Yeah, you passed. I have one other question that's not on here, that seeing as one that I need to ask. And that you mentioned that's overhead for you, in managing courses. Umm, in your ideal situation, how would that be simplified?

WOLFGANG I don't know that it can be. Umm, so there's always going to be . . . Are you talking about the labs, or the personal?

FJS Everything.

WOLFGANG Yeah, I don't know that there can be. I think it's kind of just the nature of the domain. I mean, like, you know history doesn't really change. Whereas IT is constantly evolving, you know, we've got tablets today we didn't have 5 years ago, we've got phones today that are more powerful than computers 10 years ago. Everything's moving, there's attacks we haven't thought of. So there's always going to be a pretty big overhead to maintaining it. Umm, the idea of minimizing it. You know infrastructure that can support labs like that, are where this is leading. If we want to give them the freedom to do it, then we need to have the ability do that quickly without a huge development cycle each time. And just add and implement and improve labs continuously. Um, and that kind of thing the the infrastructure can support quite well.

FJS One thing I've noticed a little bit, in looking at this is that online programs may not um contain everything that's discussed and taught in a university, like maybe in this type of program, but they already have an infrastructure behind them, they already have systems in place that help them manage those kinds of things. So, I wonder in their situation if they boiled it down to a certain point where the overhead really is just keeping themselves up to date. I mean, yes there's overhead when they have to make new things that have to be done by students, but at the same time, they have a foundation in place where teaching security concepts online to students is already the foundation of how to do it, is already there. So.

WOLFGANG Yeah. Yeah.

Robert

[00:01:14] Consent

FJS So, I don't know anything about what you do at UNLV, or what you do. But I wanted to find out what role does your program envision that students have after graduation, as a result of taking your courses?

ROBERT Um, which course? Are you talking about our program, or like . . .

FJS Do you have like a forensics or a security course that you teach?

ROBERT A security course . . .

FJS Yeah.

ROBERT We have an elective that's a graduate elective course in the MIS program.

FJS Ok, so it's in your graduate level courses?

ROBERT Yep.

FJS Ok. So what you do you kind of roles do you see students having as a result of taking that course?

ROBERT The course provides kind of a high level overview of what security and/in management is. It exposes them to tools in various areas, and um, what that course tends to do is spark interest in the area. And so then it inspires them to go out and get jobs. The ideal job it's training them for is along the management consulting or compliance side. Or, a third party consulting company will go and do audit engagements. [It doesn't train them overall] in the highly technical side, but it trains them enough, and gives them a background enough and some basic tools so that they could be of interest to such a company if they wanted to become technical the company would then invest the resources to make them more technical.

FJS So, when you say technical, what kind of technical fields do you think of? Is that like penetration testing, or security engineering?

ROBERT I mean, yeah so, I don't give them enough that they could be adequate pen-testers out of the box. I give them rudimentary things to practice on Wireshark, or Backtrack, or I have them practice running things enough, nothing enough that they could just be hired by someone and then just become just their own independent person and run the whole security engagement. They could plan the idea, and practice one, and they could definitely walk through the policies, and [mumble] but not enough where they could technically go and say hey, "let me look at your network and solve all of your issues."

FJS Yeah, um. That's interesting. So my next question, as a follow up to that is, um, where/how do you split your course up between theory and practice? Is it, 50/50, and or why do you do it that way?

ROBERT So my course is divided into 4 major sections. Which usually covers theory and practical at the same time.

[00:04:45]

So every lecture that we have there's a guest lecture that comes in [mumble] and gives a security focused talk and they're usually more practically oriented, they give experiences and stories, and uh, careers, what they do is they will walk, like I have one that was a networking security guy for the government out here, and he walked through their security protocols and what they do to secure their networks. Um, and then I usually we cover people based security management and then in each of those there's 4 units that they have roughly 10–20 hours of technical tool homework. Where I define a certain tool, and say ok, "Here's what you need to go do, and go do it." So the technical, technical training is completely outside of class. [Mumble]

FJS Say that again?

ROBERT I take the technical out of the class, because if I keep it inside of the class I have to go at the speed of the slowest person. And it stops from being "here's how to actually use the tool, and begins to be ok here's steps on the exact way to use the tool, and [mumble, but the idea is that if people get lost at that point then they just have no idea what they're doing]. And it's not learning how to use a tool, it's learning how to follow directions.

FJS So you kind of take the tool out of the course, but you leave it in as an objective? Like, do they get graded on bringing that back?

ROBERT Yeah, it's graded. They have to work on this. They have to do their best work, and they have tools to work on. It's worth um, 20% of the grade is based on these tech things, and then every test they do has half the test grade is application. The application I actually make them say hey, we're doing a network based thing [mumble] and they have to do that. Someone says

how it should be, they need to show me how this bears security. Does that make sense [mumble] networks.

[00:07:00]

FJS That kind of leads into my next question which is how does that mindset of splitting those things up affect how you maintain the course?

ROBERT How does it do what to the course?

FJS How does that affect how you maintain the course or review the course? If you split up assignments how does that affect when you decide to maybe change the assignment or change part of the course? Does that add a significant burden or not?

ROBERT Oh oh it's pretty easy. Every year I've been changing the tools. That's not a big deal.

FJS Um.

ROBERT If it's a technical tool it's taken out of the tests, the lectures, the questions.

FJS Ok.

ROBERT So it's a very modular approach.

[00:07:57]

FJS Um can I ask kind of where you came up with the foundation to make it modular? Was it like that before you came to . . . ? Or was that something you developed on your own?

ROBERT I developed it. The . . . course, when I came, was basically a network security course. And it really wasn't that good. So I developed this [inaudible]. I reached out some of the other colleges and asked what they do. Then it [was a matter] of looking at it and saying "well this works well for me, and this doesn't work well." So I adjusted it every year. This is not like my finalized done course. I've been teaching it for three years now.

FJS The next question I have, is one that I added in. Learning management systems, like Blackboard and Gradebook, those have become really common in education. Could you envision how maybe a security lab assignment be integrated with something like that? And would that be good or bad?

ROBERT Integrated within that actual tool environment?

FJS Yes.

ROBERT I mean, I list all of my assignments on Blackboard, and make them submit things back through blackboard. But, none of these tools that I have are that type of environment. A lot of them are based on the individual computer, and the encryptions ones, they're breaking encryption with a network based tool. And um, you can't run them on Blackboard because it has to be in very controlled environment, or isolated virtual machine. So it's not really well suited to that. Nor is our system administrators willing to administer that in a virtualized lab. I know I could I have cloud space and do it that way, and use it for other classes, but I don't know if that's secured yet.

FJS Um, the question number 5, I'd had just said, what do you rely on to make your course or program flexible in the changes to cyber security in the field. You had mentioned kind of having it being a modular approach. How does that help you adapt to maybe different trends in security?

[00:10:45]

ROBERT First off I have a broad sense of [inaudible] based on physical network people and security of risk management. And it doesn't matter what trend you're talking about. Those are always applying. So when new things come up it's easy to bring them, and I build current events into it so every week they have to submit what they've been reading about security and we discuss it. It's based on current topics and the tool that I update every year, I say these are kind of outdated, let's work with a platform with new ones. Um, and again, the labs are independent for that reason

because I keep upgrading the tools. So, it was made with that purpose in mind, that every year I would have to update it. Well, I've kept it that way because it's very updateable.

FJS How does maintaining this course kind of compare to something else that you teach?

ROBERT Oh this course requires the most work to keep it up to date.

FJS Ok.

ROBERT All the other ones are a lot easier.

[00:11:49]

FJS Ok, so the last question that I'd had is kind of about Bloom's Taxonomy. Are you familiar with that at all?

ROBERT Is that the learning taxonomy?

FJS It's the diagram that talks about the different levels of understanding in teaching. So the first would be remembering, the second is understanding, then there's applying, then there's analyzing, evaluating, and at the top is creating. So, the question kind of just asks, how do you try to implement that kind of philosophy into your course?

ROBERT So, on my test, my application ones are always trying to create something that's based upon the security approach. I try to get to the creating level, but I kind of [inaudible] for that. So usually it's more of the analyzing and evaluating than it is the creation. I give them plenty of things where I say look at this, tell me what's wrong with this. Or, we have speakers come in and they do it all, so. And that's what a lot of these labs are like. If we say here's a password file, you guys break it, and tell me what's there. It's sort of more in the middle to high tier.

FJS When you do like a password breaking lab do you kind of just say, here's the thing, use whatever to do it, or do you kind of give them some directions and say here's a tool, give them options.

ROBERT I say like, here's the tool we're using. Here's where to download it. Here's a link to its fact figures. I usually say here's a few YouTube videos for it. Now here's the file. I don't necessarily make them go and learn everything themselves.

[00:13:58]

FJS I think that's all I have. Do you have any other comments or questions that this has made you think about?

ROBERT Well I mean this is one course, it's an elective in the program. From the overly technically, we have the desire to expand and make it more technical. But we have limited resources here so, it hasn't come about yet. If they ever give more resources, there will probably be more courses and content applied to the [inaudible] but [inaudible] want to take it, so.

FJS Yeah.

ROBERT I'm not expecting people to come out and be an IT expert, that just doesn't happen.

FJS Yeah, and I think that's one thing I've seen at BYU. There's a lot of 400-level security courses across the ISYS program, the IT program, computer science.

ROBERT Yeah, and we have some over in the other schools, and theirs is based more on software security. Frankly, I don't think that they're that good, but they probably think mine aren't that good and that theirs are better.

FJS [laugh]

ROBERT But that's the difference between a computer scientist and a business person, right?

FJS Yeah, exactly.