A Capstone Design Project for Teaching Cybersecurity to Non-technical Users

Tanya Estes, James Finocchiaro, Jean Blair, Johnathan Robison, Justin Dalme, Michael Emana, Luke Jenkins, and Edward Sobiesk
United States Military Academy
West Point, New York 10996 USA
firstname.lastname@usma.edu

ABSTRACT

This paper presents a multi-year undergraduate computing capstone project that holistically contributes to the development of cybersecurity knowledge and skills in non-computing high school and college students. We describe the student-built Vulnerable Web Server application, which is a system that packages instructional materials and pre-built virtual machines to provide lessons on cybersecurity to non-technical students. The Vulnerable Web Server learning materials have been piloted at several high schools and are now integrated into multiple security lessons in an intermediate, general education information technology course at the United States Military Academy. Our paper interweaves a description of the Vulnerable Web Server materials with the senior capstone design process that allowed it to be built by undergraduate information technology and computer science students, resulting in a valuable capstone learning experience. Throughout the paper, a call is made for greater emphasis on educating the non-technical user.

Categories and Subject Descriptors

K.6.m [**Miscellaneous**]:
Security
K.3.2 [**Computer and Information Science Education**]:
Information systems education, Computer science education, Computer literacy
K.4.2 [**Social Issues**]:
Abuse and crime involving computers

General Terms

Security, Management

Keywords

Cybersecurity education; cybersecurity general education; multi-discipline cybersecurity education

1. INTRODUCTION

This paper presents a multi-year undergraduate computing capstone project that holistically contributes to the development of cybersecurity knowledge and skills in non-computing high school and college students. The student-built Vulnerable Web Server application is a system that packages instructional materials and pre-built virtual machines, created using Oracle VirtualBox, into interactive cybersecurity lessons. The lessons cover the following topics: introduction to cyber, law/ethics, Linux, cross-site scripting, SQL injection, and remote file inclusion. Defensive techniques are covered throughout most lessons, and the three attack lessons also include appropriate reconnaissance concepts. The lessons allow non-technical students to quickly and safely experience a technical but multi-disciplinary introduction to computer security that captures their imagination. The Vulnerable Web Server materials have been piloted at several high schools and are now integrated into multiple security lessons in an intermediate, general education information technology course at the United States Military Academy.

In 2001, Maconachy et al [17] published a seminal model for information assurance (see Figure 1). In their paper, they describe *People* as "the heart and soul of secure systems" and they state that *People* "require awareness, literacy, training and education in sound security practices in order for systems to be secured" [17]. Despite this emphasis and need, properly training and educating people appears to us to be one of the weakest aspects of modern society, and this weakness is especially prevalent among the younger generation, for whom the use of information technology is now almost ubiquitous.

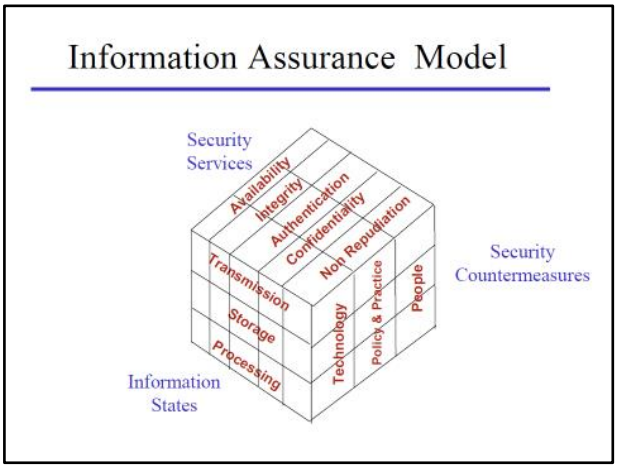

Figure 1. Maconachy et al's seminal model for information assurance [17].

Based on this motivation, the driving force of this project is to help non-technical students gain interest and knowledge in computers and computer security by providing a unique resource and experience. Vulnerable Web Server combines free software and curriculum designed to be used by educators to teach the basics of

SIGITE'16, September 28–October 1, 2016, Boston, MA, USA.

ACM 978-1-4503-3835-6/15/09…$15.00.
http://dx.doi.org/10.1145/2656450.2656478

cybersecurity. We intend that this software will ultimately motivate students to obtain degrees and jobs in cybersecurity – jobs that are desperately required to meet the security needs of our Nation in the private sector, government, and military. We think any motivated high school or college teacher can use the Vulnerable Web Server software and curriculum with an existing computer lab classroom to teach and inspire students about basic cybersecurity concepts.

A second important aspect of this work is to demonstrate an example of a computing capstone project that contributes to society and to the profession while also focusing on the emerging topic of cybersecurity. Development of the Vulnerable Web Server application took place over the past two years. The consecutive student development teams consisted of senior level information technology and computer science majors who were advised by faculty members from multiple computing and non-technical disciplines.

2. RELATED WORK

Previous literature related to various aspects of the Vulnerable Web Server project is mixed and diverse.

The most successful relevant initiatives involve extracurricular cybersecurity competitions. For K-12, the CyberPatriot program [8] now includes thousands of high school and middle school teams, and the National Collegiate Cyber Defense Competition [20] and National Cyber League [21] are providing similarly positive impact at the college level. Programs such as these are extraordinarily important and deserve our strongest support. However, these programs go beyond the non-technical user (although they may allow the non-technical user to become a technical user). Our Vulnerable Web Server project does not compete against these programs, but rather supports and complements them by inspiring non-technical users to seek out and participate in competitive cyber environments.

Several excellent papers and reports address needs for cybersecurity and computing education at the K-12 and college levels. These works address various aspects of the topic such as what should be included in a college-level general education course devoted solely to cybersecurity [5, 19], how to integrate "cyber throughout an institution's entire curriculum including within the required general education program, cyber-related electives, cyber threads, cyber minors, cyber-related majors, and cyber enrichment opportunities" [26], and what are some of the needs and solutions to cybersecurity (and computing) instruction at various levels of education [9, 12, 13, 16].

Key articles and guidelines exist (and are continuing to be developed) that address the addition and integration of cybersecurity to computing curriculums, such as into the disciplines of computer science, information technology, and information systems [1-4, 25]. In general, these works present cybersecurity best practices as well as knowledge, skills, and abilities that an undergraduate computing program should enable.

More narrowly, articles, initiatives, and guidelines now exist for an undergraduate program(s) that specifically focuses on cybersecurity [7, 18, 19, 22, 24]. This emerging field of study is formally developing curriculum guidelines under the purview of the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers, and accrediting bodies such as ABET are giving serious consideration to the development of cybersecurity accreditation program criteria.

More generally, many fine works describe computing capstone projects [6, 11, 14, 15, 29, 30]. These papers cover best practices and pedagogy for a culminating computing project and span topics that include technical skills, team work, and communication.

Several frameworks and documents also now exist providing competencies and goals for the cybersecurity work force across the domains of the military, government, and private sector [23, 27, 28]. These frameworks are mostly focused on the cybersecurity professional, and not on the non-technical worker, student, or professional.

Finally, a well-known tool in cybersecurity instruction is the Damn Vulnerable Web Application (DVWA) [10]. DVWA teaches cybersecurity through the use of a software generated computer, or virtual machine (VM) that provides a PHP/SQL application. A VM is able to effectively replicate a physical computer with some added benefits, particularly the ability to take a snapshot of the virtual machine. DVWA does not provide instructions for the setup of the VM. Instead, educators or students must utilize outside sources for a tutorial. Although the use of a virtual machine is optional for installing DVWA, we would not advocate installing DVWA on an existing hardware operating system. Those not familiar with VMs may find them more confusing than helpful. DVWA also assumes the user has fairly strong knowledge of programming and web technologies. DVWA does not provide a walkthrough or lesson plan for their product, nor do they address ethical instruction.

3. CAPSTONE PROJECT BACKGROUND

One of the unique aspects of the Vulnerable Web Server package is that it was iteratively designed, built, and fielded by undergraduate information technology and computer science majors for their two-semester senior capstone design project. To provide some additional context on this, we will briefly present some background on this capstone experience, during which the Vulnerable Web Server materials were constructed.

A two-semester team capstone project is the culminating experience of our information technology and computer science majors. These projects are completed during senior year by teams of generally 3-6 students. Significant effort is made to have teams consist of students from different disciplines, and all projects involve multi-disciplinary considerations. Each project has at least one faculty advisor, and students are required to seek out advisors from different disciplines as needed. The projects often have external, real-world customers, and all projects require tangible deliverables. Any software construction that is part of the project is conducted using the agile development methodology, and particular care is given to address both the technical and non-technical requirements of a project.

Some of the projects, including the Vulnerable Web Server, continue for multiple years. This creates the added challenges and opportunities of ensuring all artifacts are properly documented and preserved; any preliminary fielding results and insights are consolidated for the next iteration; and that some sort of hand-off occurs between the incoming and outgoing project teams. All multi-year projects continue to extend and improve on the project, they do not simply repeat the project.

The Vulnerable Web Server capstone project was particularly challenging from a requirements analysis perspective because there were so many different aspects to consider. As example, they needed to consider a user to be both the non-technical high school or college students who would take the lessons as well as the non-technical high school or college teacher who would teach them. Besides researching and implementing the virtual technologies, our students also had to become knowledgeable on pedagogy as well as cybersecurity. Finally, they needed to ensure that they gave

perspective students the proper ethical, legal, and technical backgrounds before they got to the formal cybersecurity lessons.

4. VULNERABLE WEB SERVER (VWS)

4.1 VWS Overview

The software and curriculum of VWS is available as a free download from on our website, http://vwseducation.weebly.com/. Perspective instructors are able to download the network setup guide, the required virtual machines (VMs), and the VWS curriculum. Instructors start by setting up the network. The network setup guide provides step-by-step instructions with screen shots on how to create a wireless network in the classroom, configure each of the physical machines, and establish the virtual machines, which include 17 client machines (Kali Linux 2.0) as well as the vulnerable web server itself (Ubuntu Desktop). VWS is composed of two phases, *Building a Knowledge Base* and *Creating Understanding through Practical Exercises*, both of which we will cover in more depth below. A diagram of the phases and respective lessons is shown in the VWS interface pictured in Figure 2. The selection of lessons for the VWS was inspired by the NICE framework [23].

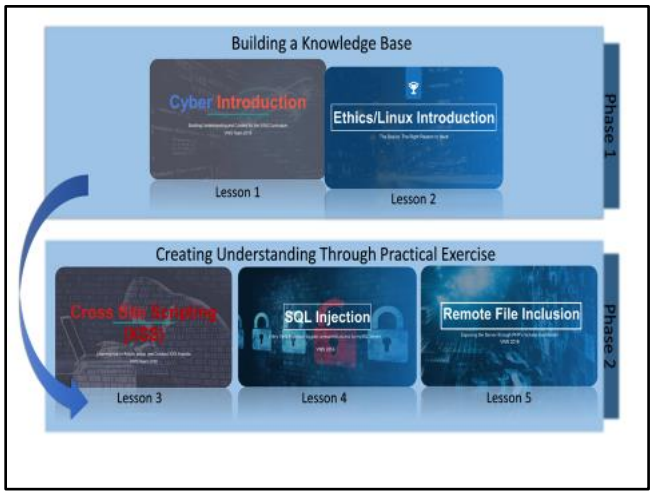

Figure 2. The Vulnerable Web Server lesson interface.

As seen in Figure 2, the VWS materials are divided into multiple lesson topics, each of which is discussed in greater detail below.

4.1.1. Phase I: Building a Knowledge Base

The intent of *Phase I: Building a Knowledge Base* is to better educate students on the cyber domain itself as well as provide them with (1) the basic skills that will allow them to complete the VWS practical exercises and (2) the legal / ethical foundation needed to safely study attack techniques.

4.1.1.1. Cyber Introduction

The Cyber Introduction lesson defines cyberspace and the operations that take place in it as well as providing an overview of the VWS content and the specific attacks covered in the materials. These include SQL injection, Cross-Site Scripting, and Remote File Inclusion. The *Cyber Introduction* lesson also covers how cyber operations affect all aspects of our lives, including personal security, organizational security, and military security. This lesson's materials are presented in a 55 minute block of instruction that may include the use of multimedia tools, such as YouTube videos, that help explain basic concepts in a fun and engaging fashion. Overall, this lesson provides a global context for the entire program.

4.1.1.2 Ethics/ Linux Introduction

This lesson includes a PowerPoint slide presentation that explains what a hacker is (black hat, white hat, and gray hat) as well as why organizations may use a white hat hacker to find weaknesses in a computing system in order to shore it up against possible exploitation by black hat hackers. Great care is taken to discuss the legal and ethical consequences of hacking a system without written consent and of taking on unauthorized privileges. The 1st, 2nd and 3rd order effects of actions are treated as well. Students additionally learn the best ways to protect their personal information when operating on the Internet.

Armed with a legal and ethical foundation relative to hacking, students then move into a block about the basics of Linux, introducing them to the operating system preferred by many cybersecurity professionals. Students are shown both Kali and Ubuntu home screens (Figure 3) and learn about the terminal and how to execute simple Linux commands. Time is also spent covering how a command-line interface compares to what is happening in a Graphical User Interface environment (Figure 4). These basic Linux skills will allow students to comfortably perform the exercises in Phase II.

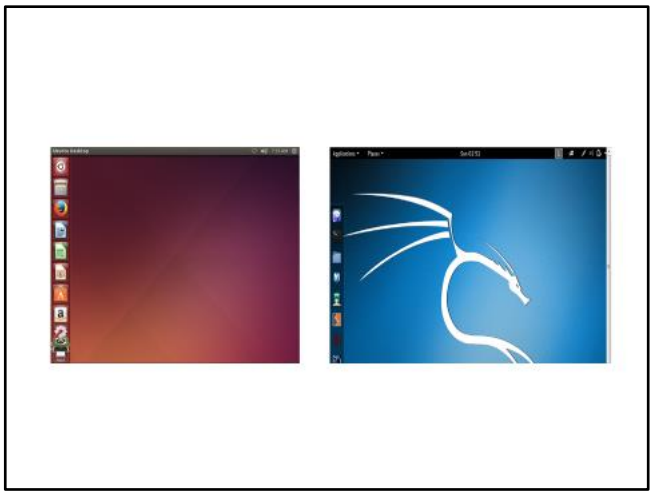

Figure 3. VWS attacker and defender interfaces.

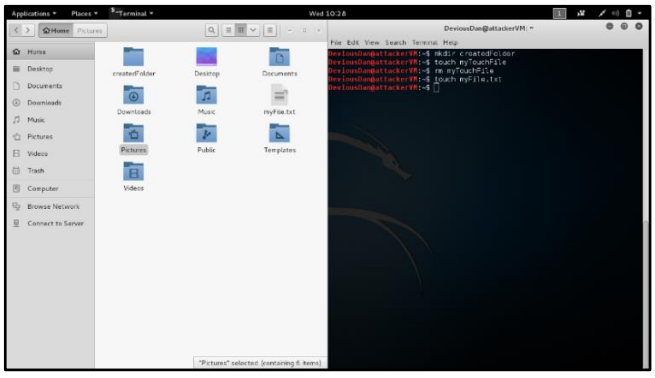

Figure 4. Graphical User Interface and Linux Terminals side-by-side.

4.1.2. Phase II: Creating Understanding through Practical Exercises

Phase II: Creating Understanding through Practical Exercises is designed to allow students to go through hands-on tutorials of three

categories of exploits: Cross-Site Scripting, SQL Injection, and Remote File Inclusion. Each of these lessons include an introduction and information about the attack followed by a guided practical exercise that allows students to conduct reconnaissance to determine if a system is vulnerable to the attack, and then to conduct the exploit in a safe, air-gapped network environment.

4.1.2.1. Cross-Site Scripting

The Cross-Site Scripting (XSS) lesson presents the first of three exploit categories to students. They learn how to: set up basic HTML and PHP form pages; explain what an XSS is and how hackers use it; and generate a basic XSS attack. Students also learn some simple techniques to defend against XSS attacks. The attack lessons emphasize the practice of reconnaissance prior to any attack, and how hackers seek to determine the level of protection and vulnerabilities on a site (see Figure 5).

Figure 5. VWS explaining Cross-Site Scripting.

4.1.2.2. SQL Injection

Students next learn about SQL Injection. This lesson begins with a high level introduction to databases and data-driven applications as well as the language SQL. Four examples of how SQL injections have been used in the past are discussed to demonstrate the real-world dangers of this exploit. The lesson activity that accompanies this instruction has students conduct an SQL injection attack showing the need for database security measures.

4.1.2.3. Remote File Inclusion

This lesson begins with an explanation of Remote File Inclusion (RFI). Reconnaissance is again reinforced in this lesson by explaining how hackers find a site that is vulnerable to an RFI attack. The lesson emphasizes the dangers posed by remotely controlled executable files. Students learn how PHP vulnerabilities allow an attacker to gather victim information. This lesson also gives a good overview of Linux and LAMP services. As with all of the lessons in VWS, students are shown techniques to defend against the given attack.

4.2 VWS Fielding

Towards the end of each two-semester development cycle, the VWS materials were piloted at several high schools and one college. At the college, it is now the center piece in three security lessons in an intermediate, general education information technology course. Over the two years that these pilots were conducted, the capstone project teams gained real-world insights on various challenges involved in having a conceptual idea meet the reality of a classroom (see Figure 6 for pictures of this experience). The insights resulted in numerous VWS improvements and truly gave our students the opportunity to identify and account for user needs as well as to integrate IT-based solutions into a user environment.

Figure 6. Piloting the Vulnerable Web Server at high schools.

4.3 VWS Limitations

Although the VWS materials provide some great opportunities for students, there are currently still some limitations.

The current implementation of VWS is focused more towards educating students on offensive, as opposed to defensive, techniques. The goals of VWS are: (1) to capture the student's imagination, (2) to inspire further study, and (3) to teach cybersecurity awareness and fundamentals. Based on these goals, as VWS evolved, design choices were made that supported ease of implementation involving attack demonstrations instead of solely defensive actions. We felt that demonstrating attacks is essential to capturing imagination and inspiring action. Current lessons include some defensive actions in the intro lesson and at the end of each attack lesson. Future lessons in VWS will include more defensive-focused actions.

Concern has sometimes been expressed that teaching high school students about hacking and specific computer exploits is risky. We had individuals tell us that high school students did not have the maturity to treat such dangerous information and skills with the proper respect. We disagree with these statements. We feel it is essential that younger students be exposed to the needed ethical foundation in the cyber domain as early as possible and in conjunction with learning some of the captivating attack techniques. The cyber ethics lesson also covers some of the laws regarding hacking so that students understand the potential consequences of their actions. VWS does teach some basic concepts and tools that could be used maliciously, however these are all drawn from information that is already available on the Internet. Students will not be technical experts leaving this course. VWS compiles the information into one source so that educators can easily learn and then teach their students some basics of cybersecurity. We believe it is paramount for students to know and understand cybersecurity risks and vulnerabilities, whether they go on to become cybersecurity experts or just general users in the cyber domain.

The final challenge with the current design of VWS is that students may have difficulty fielding these materials on their own. In preliminary versions of VWS, students had a vulnerable server installed on their computer which they could practice on. In the current VWS version, students do not have the vulnerable server

installed on their computer. This is both a feature and a flaw. We do not advocate encouraging students to try this on their own without instructor (and ethical) supervision. Students learning outside of the classroom is beyond the scope of this project. Much outside the classroom material exists on the topic and is widely available on YouTube and other video sites. The VWS walkthrough manual provides links to outside sources which can instruct students, but exposure to this possibility is at the instructor's discretion.

5. FUTURE WORK

Future updates to the VWS curriculum may include an introduction to scripting in python, introduction to networking, introduction to social engineering, a separate lesson on cyber laws, specific lessons targeting defense, and a methodology for dynamically updating lesson materials based on evolving threats. We would like to field VWS to more classrooms in order to obtain further feedback to understand what high school teachers need, and how students learn with the VWS materials. Ultimately, this was not a project focused solely on pedagogy, but a project on packaging cybersecurity materials for secondary education and college general education in the United States.

6. CONCLUSION

Vulnerable Web Server provides packaged materials on computer security which can be taught by high school and college educators who have little experience with computers, networks, or cybersecurity. The curriculum includes several lessons with hands-on labs teaching some basics of cybersecurity. All VWS content is free of charge, and it builds on other open-source software. Schools must provide their own computer and network hardware. VWS allows the schools to provide cybersecurity education and allows students to gain cybersecurity experience, hopefully generating further study, enthusiasm, and awareness. We believe the experience gained will encourage more students to study cybersecurity in the future and bring more technology professionals into the workforce to make our country's national infrastructure more secure.

In addition to this work describing the contributions and capabilities of VWS, it also demonstrates an example of a senior capstone design experience that combines many of the best practices of previous capstone pedagogy to produce meaningful artifacts in the emerging cybersecurity domain. As we discussed in the introduction, the education of *People* must be a central aspect of any security system. This project allowed our students to see how much of a challenge accomplishing that education can be.

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the United States Government.

7. REFERENCES

[1] *ACM Inroads*. March 2014. Volume 5, No. 1.

[2] *ACM Inroads*. June 2015. Volume 6, No. 2.

[3] Association for Computing Machinery and IEEE Computer Society. 2013. *Computer Science Curricula 2013 Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. http://www.acm.org/education/curricula-recommendations.

[4] Association for Computing Machinery and IEEE Computer Society. 2008. *Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*. http://www.acm.org/education/curricula-recommendations.

[5] Brown, C. et al. 2012. "Anatomy, Dissection, and Mechanics of an Introductory Cyber-Security Course's Curriculum at the United States Naval Academy." *Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education*.

[6] Chard, S. and Lloyd, B. 2014. "The Evolution of Information Technology Capstone Projects into Research Projects." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[7] Cyber Education Project. 2016. http://www.cybereducationproject.org.

[8] CyberPatriot – The National Youth Cyber Education Program. 2016. http://cybereducationproject.org/.

[9] Dutta, S., and Mathur, R. 2012. "Cybersecurity-An Integral Part of STEM." *Proceedings of the IEEE Conference on Integrated STEM Education Conference*.

[10] DVWA. Accessed 2016. http://www.dvwa.co.uk/

[11] Fedoruk A., Gong, M. and McCarthy, M. 2014. "Student Initiated Capstone Projects." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[12] Google. 2015. "Searching for Computer Science: Access and Barriers in U.S. K-12 Education." https://services.google.com/fh/files/misc/searching-for-computer-science_report.pdf.

[13] Google. 2014. "Women Who Choose Computer Science -- What Really Matters." http://static.googleusercontent.com/media/www.wenca.cn/en/us/edu/pdf/women-who-choose-what-really.pdf.

[14] Hislop, G. et al. 2012. "Panel: Capstone Experiences for Information Technology." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[15] Jonas, M. 2014. "Capstone Experience – Achieving Success with an Undergraduate Research Group in Speech." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[16] Klaper, D. and Hovy. E. 2014. "A Taxonomy and a Knowledge Portal for Cybersecurity." *Proceedings of the 15th Annual International Conference on Digital Government Research*.

[17] Maconachy, W. et al. 2001. "A Model for Information Assurance: An Integrated Approach." *Proceedings of the IEEE Workshop on Information Assurance and Security*. http://grothoff.org/christian/teaching/2009/3704/w2c3.pdf.

[18] McGettrick, A. et al. 2014. Panel: "Toward Curricular Guidelines for Cybersecurity." *Proceedings of the ACM Special Interest Group for Computer Science Education Conference*.

[19] Military Academy CYBER Education Working Group. 2015. *Draft Cyber Body of Knowledge*. http://computingportal.org/sites/default/files/CEWG%20-%20Draft%20Body%20of%20Knowledge.pdf.

[20] National Collegiate Cyber Defense Competition. 2016. http://www.nationalccdc.org.

[21] National Cyber League. 2016. http://www.nationalcyberleague.org.

[22] National CyberWatch Center. 2016. http://www.nationalcyberwatch.org.

[23] National Initiative for Cybersecurity Education (NICE) Careers and Studies. Accessed 25 May 2015. *DRAFT National Cybersecurity Workforce Framework Version 2.0*. http://niccs.us-cert.gov/research/draft-national-cybersecurity-workforce-framework-version-20.

[24] National Security Agency and the Department of Homeland Security National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). Accessed 2015. https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

[25] Rowe, D., Lunt, B., and Ekstrom, J. 2011. "The Role of Cyber-Security in Information Technology Education." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[26] Sobiesk, E. et al. 2015. "Cyber Education: a Multilayer, Multidiscipline Approach." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[27] United States Department of Energy. Accessed 25 May 2015. *Essential Body of Knowledge – A Competency and Functional Framework for Cyber Security Workforce Development*. http://energy.gov/cio/downloads/essential-body-knowledge-ebk.

[28] United States Department of Labor. Accessed 25 May 2015. *Cybersecurity Competency Model*. http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx.

[29] Zhang, C. and Wang, J. A. 2011. "Performance on Successful IT Capstone Projects: A Case Study." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.

[30] Zheng, G., Zhang, C., and Li, L. 2015. "Practicing and Evaluating Soft Skills in IT Capstone Projects." *Proceedings of the ACM Special Interest Group for Information Technology Education Conference*.