ANATOMY, DISSECTION, AND MECHANICS OF AN INTRODUCTORY CYBER-SECURITY CLASS'S CURRICULUM AT THE UNITED STATES NAVAL ACADEMY

Christopher Brown, Frederick Crabbe, Rita Doerr, Raymond Greenlaw,
Chris Hoffmeister, Justin Monroe, Donald Needham, Andrew Phillips, Anthony Pollman,
Stephen Schall, John Schultz, Steven Simon, David Stahl, Sarah Standard
United States Naval Academy

Abstract

Due to the high priority of cyber security education, the United States Naval Academy rapidly developed and implemented a new cyber-security course that is required for all of its first-year students. During the fall semester in 2011, half of the incoming class (about 600 students) took the course through a total of 31 sections offered by 16 instructors from a variety of disciplines and backgrounds. In the following spring semester, the remaining half of the first-year students will take the course. This paper explains the motivation that instigated and drove course development, the curriculum, teaching mechanics implemented, personnel required, as well as challenges and lessons learned from the first offering of the course. The information contained in this paper will be useful to those thinking of implementing a technical course required of all students at the same level in an institution (in our case first-year students) and particularly those interested in implementing such a course in cyber security.

Introduction

In May 2009, President Obama's Cyberspace Policy Review included an action item to "expand and train the workforce, including cyber security expertise in the Federal government" [1]. In response to this charge, the United States Naval Academy's (USNA's) Academic Dean & Provost created a Cyber Warfare Ad Hoc Committee. This committee was comprised of faculty and staff members with broad representation from across the campus. Their charge was to explore and define the scope of understanding of cyber security needed by Midshipmen (undergraduate students at USNA), as future naval officers. The committee consulted with the Office of the Chief of Naval Operations and Commandant of the Marine Corps staffs, and sought their input and perspectives on the education USNA's graduates should receive to help address the needs of the Navy and Marine Corps. The committee also analyzed the other service academies' inclusion of cyber-warfare concepts in their curricula, and examined graduate-level programs to determine the foundational education and skills necessary for entry into their cyber-warfare-related curricula.

In August 2009, USNA's Cyber Warfare Ad Hoc Committee delivered its Initial Report that included a recommendation to create a required core course providing a technical foundation for undergraduate cyber-warfare education for all students regardless of academic major [2]. The unanimous view of the committee was that the course be technically oriented, focused on naval applications and case studies, and delivered in a hands-on, lab-based format. This course was intended to form the technical basis for continued cyber-security education that could be expanded upon as appropriate within the various majors. In the spring semesters 2010 and 2011, a prototype course based on the Cyber Warfare Ad Hoc Committee's recommendations was developed, delivered, and refined by USNA's Computer Science Department.

In April 2010, USNA's Academic Dean & Provost formed an Ad Hoc Committee on Cyber-Security Curriculum Options. This committee, comprised of three senior professors from the Divisions of Engineering & Weapons, Humanities & Social Sciences, and Mathematics & Sciences, was charged with examining a variety of approaches for integrating cyber concepts in the core curriculum. Ultimately, the committee recommended a two-course, technically-oriented sequence: the first to be taken by all students during their initial year and the second, providing more technical depth, to be taken by all students during their third year. This paper focuses on the development of the content of the first in that sequence of two cyber core courses. And while the term "cyber" is currently used in many ways, for the purposes of this paper, we use it to refer to the totality of the space in which new kinds of computer crime, terrorism, espionage, and warfare are taking place.

Although USNA settled on one course in the first year and a second course in the third year, numerous other options were considered. No option was deemed easy to implement; in fact, at the time the options were formally presented (February 2011), the general consensus of the Committee, and all others who had been involved as well, was that the earliest possible implementation date for any option selected would be August 2012. In February 2011, the Committee's recommendation was approved, but the implementation date was to be August 2011—a mere six months later. There were many "roadblocks" to overcome to meet this deadline, some that would be typical of any academic campus (such as faculty-led, curriculum-review processes and faculty-senate votes and recommendations). In this instance, the ground rules usually applied at USNA were modified given the short deadline and the importance of the initiative. USNA leadership made two things clear from the outset: the implementation deadline of August 2011 was immovable, and the inclusion of the new cyber course as a first-year, lab-oriented, technical-core course was non-negotiable. Other than that, all other specific details from course content to faculty development to assessment measures were left up to the faculty to debate and decide. So, in that context and with only six months to act, all faculty approval processes were conducted in parallel with course development and implementation planning. Figure 1 summarizes some of the key dates and events in planning, development, and rollout of the cyber-security course.

May 2009	President Obama's Cyberspace Policy Review released
August 2009	USNA Cyber Warfare Ad Hoc Committee Initial Report delivered
January 2010	First prototype course commenced
April 2010	USNA Ad Hoc Committee on Cyber Security Curriculum Options formed
January 2011	Second prototype course commenced
February 2011	Cyber-security course options formally presented
Spring/summer 2011	Recruiting of instructors to teach the course conducted
Spring/summer 2011	Course content developed
August 2011	Instructors' two-week "boot camp" provided
August 2011	Cyber-security class for half of the first-year students rolled out
December 2011	First offering of cyber-security class successfully completed

Figure 1. Timeline indicating key events in the successful rollout of the cyber-security course.

There were many other significant challenges as well, ranging from determining what technical content to teach, to who would teach the course and how USNA would identify and prepare those faculty members within a six-month time frame. Perhaps the greatest challenge of all, though, was how to teach this technical course to a new class of 1,200 first-year students (600 each semester) in a way that did not simply add more work to an already very busy schedule for the first-year students. The phrase "very busy" is used because students at the service academies have many demanding military obligations that are not common at other institutions and classroom attendance is required. At USNA, all first-year students take the same "core" of courses in their first year, an academic workload that amounts to 11 courses consisting of 35 credits over two semesters. To make room for the new cyber-security course, one of the existing core courses was moved to the sophomore year (which itself resulted in additional curriculum changes and shifts) thereby resulting in only a single hour increase in course time. While finding the "slot" in the first-year schedule was challenging, a greater challenge was how to teach another technical subject (in addition to the required science-and-engineering-focused calculus and chemistry core courses) in such a way that the students would be engaged in the material sufficiently so that the difficulty associated with the technical nature of the content would be compensated for by the motivation of learning about the practical aspects of both offensive and defensive cyber security. The mantra was “Make it Navy relevant and make it exciting!” That outcome was considered essential; in a technical course involving two lecture hours and two lab hours per week, the end result needed to be that the students really enjoyed and learned the content, and that their day-to-day behavior regarding the use of social media, the Internet, wired and wireless networks, and so on, would now be much-better informed and positively affected by their new understanding of the risks and threats associated with cyber security.

The remainder of this paper is as follows. Section 2 provides a discussion of related work. Sections 3 and 4 are focused on course content and course mechanics, respectively. In section 5 personnel requirements are described. Section 6 covers student, faculty, and administrators’ perspectives of the course. In section 7 lessons learned and numerous recommendations are given for others facing a similar challenge. Finally, a summary is given in section 8.

Related Work

Teaching cyber security to computer science and related majors is not a particularly new idea; many higher-education institutions offer courses in computer/network security, and a few even offer full degree programs in cyber security. Finding undergraduate, graduate, and even certification courses in cyber security is not especially challenging. However, the Naval Academy was in search of a stand-alone, technical, hands-on course with a broad range of cyber-security content that could be taught to every first-year student, regardless of their intended major or computer knowledge/skills, and further which served to significantly enhance the student’s awareness and understanding of the risks and threats associated with cyber security, especially those that are relevant to the U.S. Navy and Marine Corps. As Tikekar discusses in [3], a hands-on approach in cyber security for undergraduate students already is recognized in some undergraduate Computer Science Departments. However, no institution appears to either require or even offer as an elective option a single cyber-security course for all students, and no single textbook exists that presents technical content with practical case studies and hands-on lab experiences that is accessible to students outside of a computer science (or related) major. For this reason, a conglomeration of parts of four textbooks [4-7] was used, but as described in the next section, much of the content was developed in-house and most students in the course rarely used their textbooks.

In our comprehensive review of relevant work done at other universities, we found that in 2003, Syracuse University, in partnership with the Air Force Research Laboratory in Rome, NY, developed an advanced cyber-security elective aimed at third- and fourth-year students [8]. The course has now evolved into a paid internship with the Air Force Research Lab in Rome, NY, and focuses not only on the technical aspects of cyberspace, but also on leadership challenges faced when securing a domain [9]. In addition, although not yet a common trend, some high schools are creating cyber-related curricula, as is the case at the Rome Catholic School in Rome, NY. Rome Catholic School offers K–12 cyber education, focusing on computer security and prevention of cyber-bullying [10].

Furthermore, while numerous universities have Computer, Network, or Information Security undergraduate programs, the courses in these programs are not required for all first-year students, usually have several prerequisites, and are typically not even available to first-year students as a result. For example, according to the Seattle Times, in the University of Washington (UW) Computer Science and Engineering Department, “This year, record numbers have swamped the UW’s beginning computer classes—nearly 2,000 students—eclipsing even the dot-com boom in the `90s. Yet the department has trimmed faculty and has not expanded the number of degrees it awards, due to state budget cuts. As a result, the department now turns away four out of every five who want to go on to major in computer science" [11]. While some universities are cutting their faculty due to funding constraints, many academic institutions are now recognizing the need to increase the amount of students enrolled in computer-related courses [12]. Although UW offers various CSE classes to non-CSE majors, a review of the online courses for non-majors demonstrates that none of the classes offered teach cyber security. And we have found similarities to this situation with many other programs.

Before launching our first-year, cyber-security course, we contacted the two other major military service academies to determine what cyber-security education was provided to their students. The United States Air Force Academy (USAFA) requires an introductory computer-systems and information-technology course that includes five lessons focused on the fundamentals of computer security. In the summer of 2011, USAFA rolled out an elective two-week, full-time program to about 90 cadets that provides them with a hands-on experience in cyber security. The content of the elective course has perhaps a 40% overlap with the content of the USNA first-year course [Gibson, personal communication]. Similarly, the United States Military Academy's curriculum includes an information-technology-related course, but the focus is not in computer or network security [13].

Course Content

Introduction

In this section we delve into the specific goals of the course, its hands-on aspects, the course components and premise, and an outline of the course.

The Cyber Warfare Ad Hoc Committee's Initial Report describes Cyber Warfare as "... a technical academic core of tightly inter-related subject matter, as well as a wide range of important topics that, while dependent on the technical core for fullest appreciation, are not dependent on each other. Stated another way, cyber warfare is comprised of, first, a foundational component, dealing with a set of interconnected fundamental technical concepts, and second, a wide range of interdisciplinary topics, touching upon the areas of law, political science, strategy and tactics, policy, ethics, and the study of foreign languages and culture" [2]. The Initial Report also includes a recommendation to create a required core course providing the technical foundations of Cyber Warfare; a course that is technical in nature, relevant to naval officers, and delivered in a hands-on and engaging manner.

The required cyber-security course now offered at the Naval Academy was designed as an academic, technical, hands-on, and engaging course on the technical foundations of cyber security. The fundamental goals for the course are that students acquire:

- an understanding of the basic physical and virtual architecture of cyberspace, including: the individual computer and program, the physical components and protocols of a network and the Internet, and the distributed client-server system that is the world wide web,
- hands-on experience with basic components of the physical and virtual architecture of cyberspace and the ability to relate that experience to the larger system,
- an understanding of the Department of Defense's pillars of Information Assurance (availability, integrity, authentication, confidentiality, and non-repudiation), the inherent vulnerabilities of information systems that endanger these properties, defensive measures to ensure that information systems retain these properties, and offensive measures that can be used to violate these pillars, and
- hands-on experience with some basic defensive and offensive practices in cyberspace, and the ability to relate that experience to new or more sophisticated attacks and defenses.

Hands-on Aspects

The hands-on element of the course is crucial to delivering a meaningful academic, technical, and engaging experience. It provides students with concrete experiences that they can relate to new or more-complex situations and/or technologies they encounter in order to make sense of them. For example, the lessons devoted to computer programs look at the source code of only simple programs, but as a hands-on exercise, the students are asked to provide unexpected input that crashes these programs or that make them behave in unintended ways (for example, text where numbers were expected). The lessons ask students to modify these simple programs to deal gracefully with bad input so that they get concrete hands-on experience with "patching" these kinds of coding errors, and thus see firsthand how hard it is to anticipate all the ways that input might be problematic. This same concept reoccurs in the section on attacks against network services. A network service is simply a program that sits and waits for input from a network connection rather than a keyboard or mouse. If an attacker can send that program input that the programmer did not anticipate and deal with gracefully, the service can be made to crash or do unintended things. Because this experience is similar to the one that the students engaged in with simple programs, even though the students are not in a position to understand complex programs such as web servers or DNS servers, the students can still understand, more than superficially, how those programs might be induced to do unintended things if fed cleverly crafted input by attackers. Through careful design, almost every class meeting involves hands-on activities. These activities provide students with concrete experiences from which to reason and to generalize, as well as a strong foundation for critical thinking and problem solving.

Course Components and Premises

The cyber-security course is divided into three modules: the Cyber Battlefield, Models and Tools, and Cyber Operations.

One cannot begin to instruct students in cyber attack and cyber defense until students actually understand the space in which these actions take place, so the first part of the course introduces students to the "Cyber Battlefield": digital data, computer hardware, operating systems, programs, the web, networks, wireless networks, and the Internet. By covering these elements of cyberspace, students get hands-on experience with them and also see a variety of "bad things" that can happen (for example, clicking on a hyperlink to some innocuous site but instead being sent somewhere else, crashing programs with bad input, injecting malicious code into a website to crash it, stealing user names and passwords with malicious e-mail attachments, and so on). The students not only see how systems are supposed to work, but also understand how malicious actions break them.

The second section of the course is "Models and Tools." In this section students learn formal models of "security" and "risk" for information systems. To make concrete and compelling what could be abstract and lacking motivation, these models are related back to the "bad stuff" that the students saw happening in the first part of the course. For example, we show how an injection attack that redirects one website to some other site is an attack on availability. The models are then used to understand and reason in a principled way about new situations. With this new-found understanding of what security really means for an information system (that is, what things we are really trying to protect) we look at some of the fundamental tools used to provide security: firewalls, symmetric encryption, cryptographic hashing, authentication, asymmetric encryption, and digital certificates.

Finally, once the students understand the battlefield, what they are trying to defend (or attack), and what defenses they can employ (or must defeat), we move to the third and final module of the course: "Cyber Operations." In this section of the course, we look at cyber reconnaissance, attack (including malware), defense, forensics, and case studies. The course culminates in a capstone experience which includes a series of three hands-on labs in which each section of students is divided into two teams, with each team responsible for their own network. Teams reconnoiter their opponent's network, attack their opponent's network, and finally defend (that is, harden) their own network and re-attack their opponent's hardened network. These activities occur on virtual hosts and networks served from a system that is:

a. completely isolated from the Naval Academy’s public network,
b. able to be reset in seconds to its initial configuration following each lab period,
c. indistinguishable from a real physical network.

Course Outline

The outline shown in Table 1 provides an overview of the specific topics covered in the course, broken down into the three fundamental sections previously discussed. More specific detail on course content can be found at http://www.usna.edu/cs/si110/.

Course Mechanics

Introduction

In this section we discuss the “mechanics” involved in teaching the first-year, cyber-security course: the assumed background of the incoming students; the lecture and lab delivery (as well as the rigor of the material); homework and exams; the student and instructor communication mechanisms during the semester; and the means by which additional tutoring and review were available.

Student Background

Realizing that the cyber-security course was required for each student entering their first year at USNA, it was anticipated that there would be a wide variety of backgrounds encountered with first-year students. USNA is a highly selective institution. For the class of 2015 there were 19,145 applicants and only 1,426 were offered appointments (offered admission) [14]. There are 993 men and 236 women in the class, or roughly 19% female [14]. The students come from all 50 states, U.S. territories, and several foreign countries. Over 50% of the class of 2015 ranked in the top 10% of their high school class, and 50% of the students scored from 590–720 on the SAT Verbal and 50% scored from 610–730 on the SAT Math [14]. We assumed that each first-year student had some (though not much) computer experience along with a basic understanding of the Windows™ operating system and its associated applications. But given the first-year nature of this course there could be no prerequisites.

Table 1. Course Topic Outline.
(Minutes Dedicated to the Topics)

Module	**Topic (Minutes spent in class on topic)**
The Cyber Battlefield	Digital Data 1 & 2 **(100)**
	The Physical Computer **(50)**
	PC Vivisection Lab **(50)**
	Operating Systems 1 & 2 **(100)**
	Programs Parts 1–5 **(250)**
	Web: Servers, Browsers, and HTML **(50)**
	Web: Build Your Webpage Lab **(100)**
	Web: Client-Side Scripting: Non-event Driven, Event Driven, and Forms **(200)**
	Web: Server-Side Scripting **(50)**
	Web: Injection Attacks and Cross-Site Scripting **(100)**
	Networks, Protocols, and the Internet: Parts 1–4 **(200)**
	Networks: Build-a-LAN Preparation **(50)**
	Networks: Build-a-LAN Lab **(100)**
	Networks: Wireless Networking **(50)**
	Networks: Build-a-Wireless-Network Lab **(100)**
Models and Tools	Information Assurance **(50)**
	Firewalls **(50)**
	Authentication/Crypto 1: Symmetric Encryption **(50)**
	Authentication/Crypto 2: Cryptographic Hashes **(50)**
	Authentication/Crypto 3: Digital Cryptography and Tools **(50)**
	Authentication/Crypto 4: Asymmetric Encryption **(50)**
	Authentication/Crypto 5: X.509 Certificates Lab **(100)**
Cyber Operations	Forensics Lab **(100)**
	Phases of a Cyber Attack /Recon **(50)**
	Network Attack **(50)**
	Network Defense **(50)**
	Malware **(50)**
	Case Studies **(50)**
	Cyber Recon Lab **(100)**
	Cyber Attack Lab **(100)**
	Cyber Defense Lab **(100)**

Course Delivery

As noted earlier, instructors taught material through both lecture and lab format. Online student lecture or lab notes, as appropriate, were available for each of the 41 lessons. Both internal (available only on campus) and external (http://www.usna.edu/cs/si110/) websites were created. The course policies, support materials, and supplemental resources were also available on both websites. The internal website contained links to all software resources needed for the course; however, not all these resources were available on the external site. The external site existed so that students could access course material when travelling for an athletic or extra-curricular event. Additionally, there was a website accessible only to instructors to provide lesson plans, laboratory guides, and homework solutions. All of the lectures included a link to a homework assignment that was due the next class period. Every instructor also used an in-class, individual message board for sharing links and demonstrating some web-based activities.

Following customary procedure at USNA, there were three exams administered for the course. The exams tested material taught during that portion of the course and were 50 minutes in duration. The final exam was cumulative, covering material throughout the entire semester. Students were given three hours in which to complete the final exam. In order to standardize exam grading across sections, a rubric was provided in order to determine the amount of partial credit to be awarded for wrong answers. Due to the labor-intensive nature of producing such a rubric and the short time period during which the cyber-security course was developed and offered to all first-year students, no such rubrics were provided for grading homework assignments; however, answer keys were provided for homework assignments.

Communication

Offering a new, required, cyber-security course to first-year students with a newly-indoctrinated set of instructors, some who did not have a computer-science background and/or had never taught at USNA before, meant that communication (constant, consistent, and concise) was paramount. An email alias was created for each of the 31 course sections which were further grouped into an overall course email alias. Instructors regularly used their section's email alias for specific class updates, while the course coordinator (see section 5 for more details of the role of course coordinator at USNA) was the primary user of the overall course alias for more-global course announcements. An instructor-email alias (consisting of the 16 course instructors) was also created and used for a wide variety of purposes: from finding another instructor to cover one's section, to discussing ways in which to present lecture and lab material, to pointing out relevant research articles. Those instructors teaching labs later in the day could often benefit from comments sent through the instructor-email alias by instructors who had taught labs earlier that same day. Since lab participation was a vital part of the overall course-learning experience, the instructor-email alias was also used to identify students in each of the 31 sections who missed a given lab and schedule a consolidated make-up session.

While instructors maintained almost daily email contact, mandatory weekly instructor meetings were held to review the previous week's classes, as well as to prepare for the upcoming week's material. These meetings were also used to gauge the overall progress of the students, as well as to discuss any content issues for the course. Typical examples of content issues were discussions about the arrival of new hardware/software or how a lecture/lab could be better presented next semester. When a particularly involved lab was forthcoming, the weekly instructor meetings were devoted to stepping through the lab. Aside from preparing the instructors to lead their class through the lab, these exercises resulted in a plethora of feedback, which was then used to improve the lab activity and the wording of its instructions. The nature of the setup and specific software used for some labs meant that it was not possible for instructors to practice those labs on their own time in their own offices.

Additional Instruction

Since this cyber-security course had never been taught at USNA before, a support structure for student learning was critical. The offering of any required college-level course comes with the responsibility of providing tutoring, additional review, and outside of class extra instruction. USNA's cyber-security course offered all three. Using the model of other USNA technical core courses, an evening, group-study program was instituted. This Midshipmen Group Study Program (MGSP) was available Sunday–Thursday evenings, led by junior- and senior-year computer science and information technology majors selected by USNA's Center for Academic Excellence and the Computer Science Department. These popular sessions provided students an opportunity to receive supplemental instruction, homework assistance, and review of hands-on classroom activities. Attendance was taken so that instructors were aware which of their students were seeking extra assistance, but attendance was not required. MGSP was augmented with special review sessions for each of the 6-week, 12-week, and final exams. These well-attended sessions, held during the MGSP timeframe on a Sunday evening prior to the exam, reviewed key learning objectives and homework exercises while also answering student questions. For these reviews, numerous instructors and rooms were used. Some instructors supplemented exam reviews by offering evening online instruction using an online-meeting tool. If one-on-one tutoring was needed, students were encouraged to contact their instructor for additional help.

Personnel Required

Introduction

This section describes the personnel required to develop, teach, and oversee the cyber-security course successfully: the course instructors, course coordinator, course content developers, facilities manager, technical-support staff, and administrators. We describe the contributions and a few of the issues involved with each role, as well as the qualifications and duties required. We needed to expand and to adjust temporarily the responsibilities of many staff and faculty members in order to deliver the course. The Computer Science Department offered 31 sections with an average size of about 18 students: minimum size was 17 and maximum size was 20.

Course Instructors

Having only six months lead time between the decision to deliver the cyber-security course and the start of the fall 2011 semester, there was considerable concern about where to find qualified instructors; hiring enough new faculty members (either part-time or full-time) with appropriate qualifications to teach cyber security is a very difficult proposition due to the high demand for this skill set. So, interested faculty members were sought from other departments, from the campus IT staff, and also from outside of the USNA academic community. As a result of these vigorous efforts, the group of sixteen instructors teaching the initial run of the course included:

- six instructors from the Computer Science Department (three civilian and three military),
- three military instructors from USNA's Center for Cyber Security Studies (CCSS),
- one instructor from the Division of Engineering and Weapons leadership staff (military),
- one instructor from the Electrical and Computer Engineering Department (military),
- one instructor from the Oceanography Department (civilian),
- one instructor from the Mathematics Department (military),
- one instructor from the Physics Department (military),
- one civilian instructor from USNA's Information Technology Services Division (ITSD), and
- one civilian instructor from the NSA on temporary assignment to the CCSS.

Instructor teaching loads varied from one to four sections each. The faculty members who we assembled possessed various levels of technical expertise in cyber security. Some faculty members were active military officers who brought a great deal of relevant operational exposure gained during their previous career assignments. We should note that roughly 50% of the faculty members at USNA are military members who hold at least a Master's degree, and those percentages are the same for the Computer

Science Department. Other instructors had a strong personal technical interest in the subject matter, while some had significant but non-technical experience. We next summarize the qualifications and duties of instructors.

- Key qualifications:
  - Master's Degree or higher in computer science or closely related field.
  - Relevant computer science, networking, and security background.
- Duties:
  - Prepare, teach, and administer sections of the cyber-security course with approximately 20 students per section.
  - Grade all materials, as USNA has no teaching or research assistants.
  - Work closely with the course coordinator and provide feedback on the course.

Regarding the time commitment, if an instructor taught more than one section, each additional section added several more hours of work per week due to in class time (four hours), grading (approximately three hours, including two homework assignments per week, labs every other week, and three exams), and office hours. All of the exams were common exams, so instructors essentially needed to cover the same material, as it was provided by the course coordinator (see the next subsection for more details about the role of the course coordinator).

Course Coordinator

Due to the technical nature of the course and the short timeline for implementation, several faculty members from the Computer Science Department were tasked with forming a course-coordination cadre to flesh out the course details fully. This group had four leaders. One developed much of the overall curriculum for the course, another led the hardware and software analysis and acquisition efforts and assisted with the curriculum development, a third developed much of the lab-focused portions of the course, and a fourth formatted homework and solutions. These development efforts began in earnest in April 2011 and continued full time throughout the summer and into the fall semester concurrent with the running of the cyber-security course. In the following we summarize items relating to the course-coordinator position.

- Key qualifications:
  - PhD Degree in computer science or closely related field.
  - Relevant computer science, networking, and computer security background with an emphasis on cloud computing.
  - Ability to lead, mentor, and motivate other instructors.
  - Significant pedagogical and course development expertise.
  - Capable of responding to a wide range of queries in a timely manner.
- Duties:
  - Lead curriculum development team.
  - Supervise overall course administration.
  - Report course progress and activities to USNA's administration.
  - Maintain email list and conduct weekly meetings of instructors.
  - Develop and administer assessment methods for the course.
  - Prepare mid-term and final exams.
  - Develop and provide course calendar, student and instructor notes, course policy, and syllabus.
  - Maintain course website.
  - Assist and train other instructors.
  - Manage unexpected or last minute issues.

All courses at USNA have a course coordinator, so we did not need to create an entirely new model for developing and teaching this course. This fact helped significantly in that faculty members were used to working together in teams to teach a course. The benefits of a good course coordinator are that less-experienced instructors have a framework from which to deliver a strong class, and the efforts of one are leveraged so that faculty members do not need to duplicate work.

Struggles in coming to total agreement on the initial curriculum were expected, but everyone tried to keep the best interests of the Midshipmen foremost in mind. The natural tensions and the diversity of instructors will undoubtedly help us evolve and improve the course rapidly. In hindsight we probably should have implemented a formal reporting system for providing suggestions about all aspects of the course. This convention would help us keep a better record of suggestions and provide those making suggestions a formal voice.

Course-Content Developers

Section 3 of this paper reviewed the material contained in the course. The course content was developed mostly by the course coordinator, the instructors who taught the prototype of the course, and a small subset of the instructors. We list the qualifications and duties for those developing course materials.

- Key qualifications:
  - Master's Degree or higher in computer science or closely-related field.
  - Relevant computer science, networking, and computer security background with an emphasis on cloud computing.
- Duties:
  - Develop labs and curriculum components as directed by the course coordinator.
  - Test and debug labs.
  - Provide feedback on student and instructor notes.

Facilities Manager

We designated an experienced faculty member, the Chair of the Computer Science Department's Systems Committee, as the course's Facilitates Manager. This faculty member, who also taught the course, served as the main coordinator for hardware and software identification, acquisition and testing. We found that this approach worked well since it allowed the Course Coordinator to focus more fully on the task of developing course content. There were times when technical staff needed to drop everything they were doing to aid the facilities manager in addressing emergent problems with course hardware and software, for example, certain network ports were not available when they were needed or there were problems with resolving IP addresses on student laptops. Our facilities manager had the positional authority to expect immediate assistance from the technical support staff when required. Issues that prevented instructors from teaching the course effectively or prevented students from working on class material were given the highest possible priority, and the facilities manager and technical-support personnel did a good job in fixing any problems that developed unexpectedly. In the following we summarize items relating to the facilities-manager position.

- Key qualifications:
  - Master's Degree or higher in computer science or closely related field.
  - Relevant computer science, networking, and computer security background with an emphasis on cloud computing infrastructure.
- Duties:
  - Identify, acquire, test, and lead the maintenance of the hardware and software systems required to support the delivery of course.
  - Help trouble-shoot and fix problems.
  - Coordinate technical-support staff for the course.

Technical-Support Staff

This course required dedicated technical support. It was important to have technical-support staff available and ready to go to lab rooms to assist instructors with real-time issues. Although, as we noted earlier, instructors practiced the labs during weekly instructor meetings, there were occasions when unexpected problems arose during labs. If instructors were not able to solve such problems themselves, they needed assistance from the technical-support staff, facilities manager, or course coordinator. Running such a course for the first time would be impossible with just faculty members supporting the course, as there are many network issues that need to be addressed.

Our technical-support staff for the course included a contractor who had a high level of proficiency with the computer security and the cloud computing aspects of the course. Additionally, several staff members from the Academy's information technology staff were assigned to assist with the hardware and software support for the course. In the following we summarize items relating to the technical-support positions.

- Key qualifications:
  - Significant work experience with computer networks, computer security, and cloud computing infrastructure.
  - Experience with UNIX and Windows™ operating systems.
  - Good problem solving skills.
  - Excellent communication skills.
- Duties:
  - Create, support, and maintain computer networks and cloud computing infrastructure for SI110.
  - Be on call during class and lab times.

Administrators

From the Superintendent to the Academic Dean & Provost to the Math & Science Division Director to the Computer Science Department Chair, administrators played a vital role in the successful rollout of the cyber-security course. (Note that at USNA the Academic Dean & Provost position is equivalent to the Vice President for Academic Affairs, and a Division Director is equivalent to a college level Dean.) They had to have vision; they had to instill the belief that this project could and would be implemented; they had to encourage faculty and set milestones; they had to provide resources and strong support for all personnel involved. And, most importantly, they had to remain flexible and keep expectations realistic. Our administration formed the appropriate committees, sought appropriate input for the course, listened to the feedback that they received, and helped guide the course through appropriate USNA approval channels. The administrators acted quickly in terms of hiring instructors and replacing lost technical staff. They helped as much as possible in expediting hardware and software requests which often can be notoriously slow in large organizations. And, they found creative ways to free up instructors to teach the course. When tension on the instructor team emerged, administrators worked to keep that tension in check. Cohesion was helped by the weekly meetings and by encouraging open communication. The course received a great deal of media attention [15-21], and administrators worked on promoting the course both internally and externally. Without such a strong and dedicated administrative team, the course could never have been implemented. The challenge would simply have been too great for a department to take on alone.

Perspectives on the Cyber-Security Course

In this section we take a look at perspectives of the course from the student, faculty, and administrative points of view.

Student Perspectives

Our information regarding the student perspective comes from two in-class surveys administered at 6 and 16 weeks, course evaluations, and discussions with students. We administered the 6-week survey to all of the nearly 600 students in the course, and 435 students responded. We present a few of the items from that survey in Figures 2 through 5.

Student feedback regarding course workload was an important element to evaluate. As depicted in Figure 2, at the 6-week point, only 3% of the students indicated that they spent more time on the cyber-security class than they did on either their chemistry or calculus classes (both also required classes for all students), and 29% indicated that they spent similar amounts of time on these three courses. We felt reassured that the new course did not turn out to be more time-consuming than other USNA technical core courses.

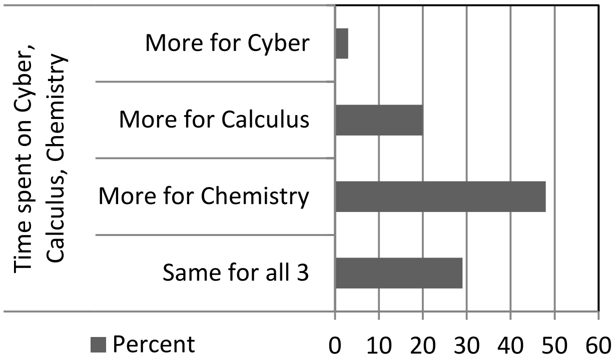

Figure 2. 6-Week Survey – Workload Comparison

In addition, a majority of students felt that the student-learning support structure afforded opportunities for extra help, opportunities that were on par with those provided for the well-established chemistry and math classes that also use the MGSP system described earlier. Roughly 94% of the students felt that the hands-on activities were helpful, as displayed in Figure 3. While Figure 4 demonstrates that about two-thirds of the students indicated that they truly enjoyed the hands-on activities, while almost all of the remaining third indicated that they enjoyed the hands-on activities somewhat.

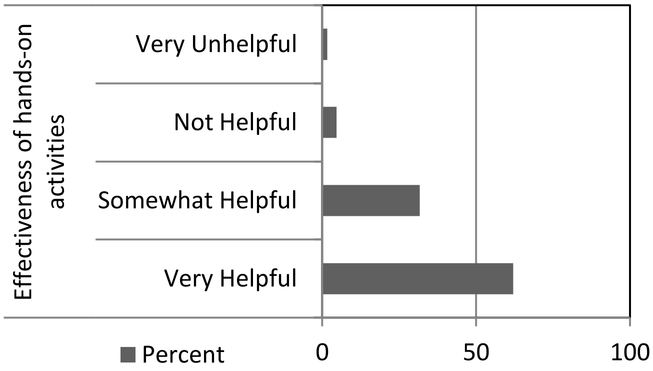

Figure 3. 6-Week Survey –
Hands-on Activity Effectiveness.

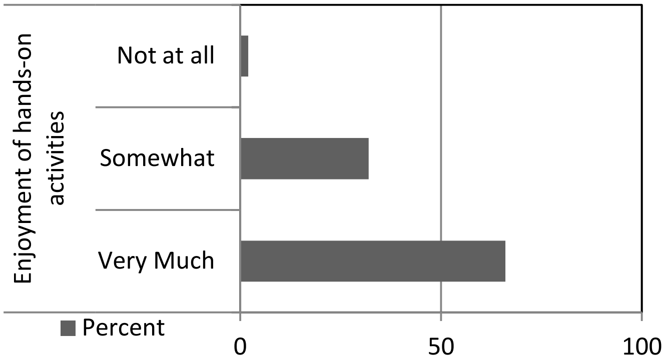

Figure 4. 6-Week Survey –
Enjoyment of Hands-On Activities.

Roughly 27% of the students felt the course assumed at least some knowledge/skills that they did not already possess, but of those just 13% felt that this deficiency was a problem. The others were able to adjust, as presented in Figure 5.

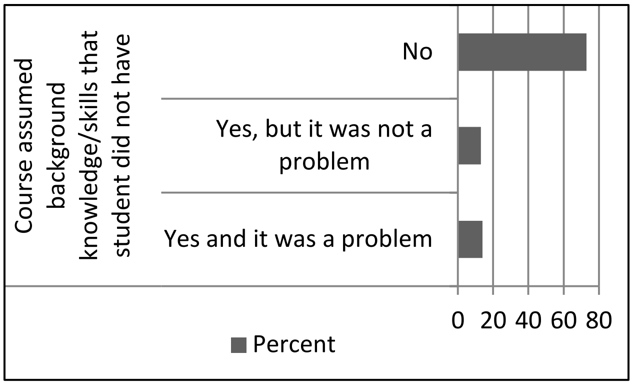

Figure 5. 6-Week Survey –
Computer Skills Assumed.

Regarding the 16-week survey, there were 504 responses. The focus of this survey was to determine what labs students most enjoyed or felt were useful, and how much the students felt they learned about threats and the concepts in the three modules presented throughout the course. Figures 6 through 11 display the results of the 16-week survey.

The final three labs, Cyber Reconnaissance, Cyber Attack, and Cyber Defense were intended to pull the concepts from the entire course together as the students apply what they learned in the virtual environment. 82% of the students felt the final three labs were at least somewhat useful (Figure 6).

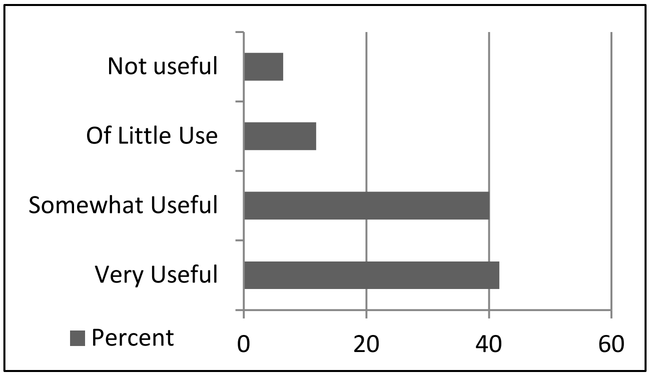

Figure 6. 16-Week Survey –
Usefulness of Final Three Labs
Toward Understanding Attack and
Defense of Information Systems.

Figure 7 exemplifies that the Network Attack Lab was by far the most-liked lab with 35% of the students selecting it. This choice of lab was followed by the Build a Webpage (25%), Network Defense (11%), PC Disassembly (10%), Attack the Message Board (7%), Network Recon (4%), Forensics (3%), Build a Wireless Network (3%), Build a Wired Network (1%), and Certificates (< 1%) labs.

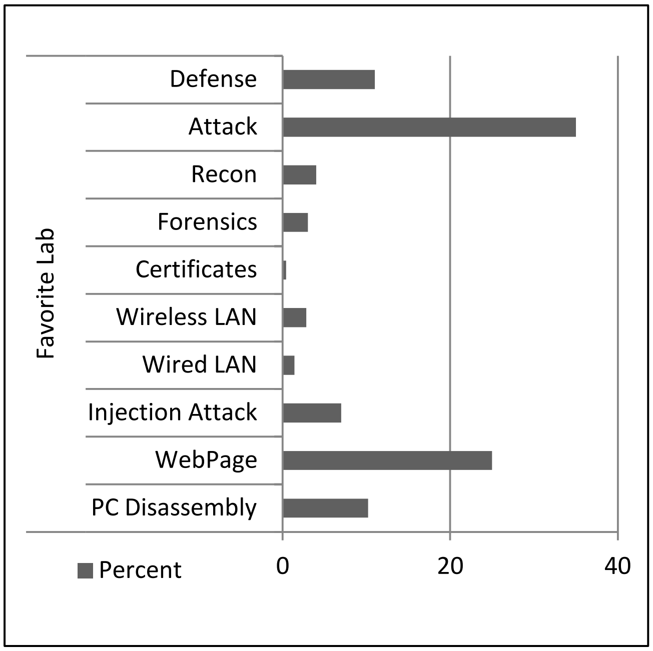

Figure 2. 16-Week Survey - Favorite Lab.

About 95% of the students said that they became more aware of the threats facing their computer than before they started the course, while about 4% indicated they were already highly aware of the existing threats, Figure 8.

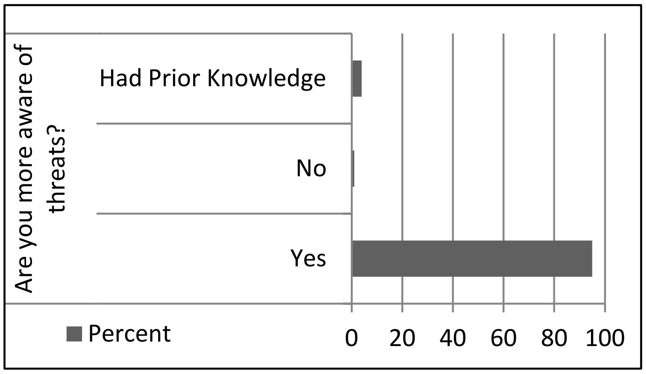

Figure **8**. 16-Week Survey –
Awareness of Threats

For each of the three modules of the course (as described in section 3), between 88–95% of the students indicated that they either had a much-better or somewhat-better understanding of the key issues involved. In other words, as self-reported, the course learning objectives were met by about 90% of the students. Figures 9, 10, and 11 display the student response percentages for each of the three modules. Students provided multiple comments and suggestions for course improvements on the surveys and also on the student opinion forms (end of semester survey required for every USNA course).

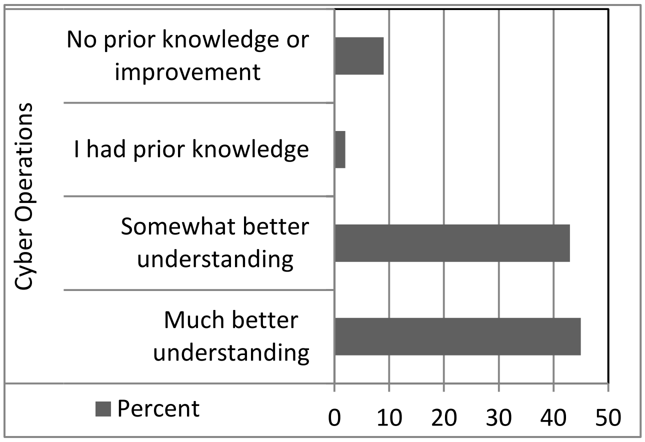

Figure 9. 16-Week Survey –
Understanding of Cyber Operations Concepts.

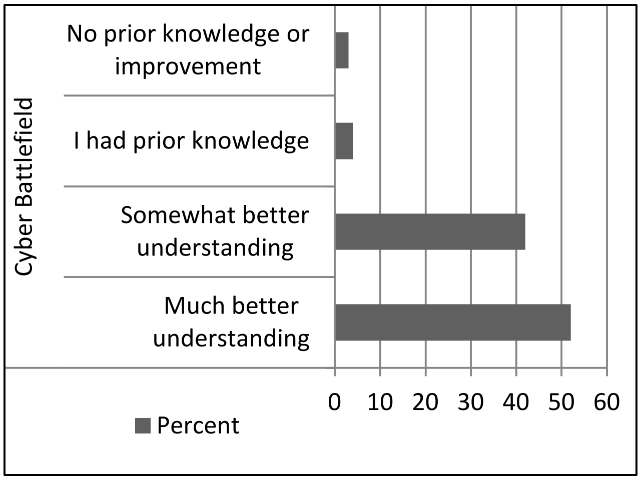

Figure 10. 16-Week Survey –
Understanding of Cyber Battlefield Concepts.

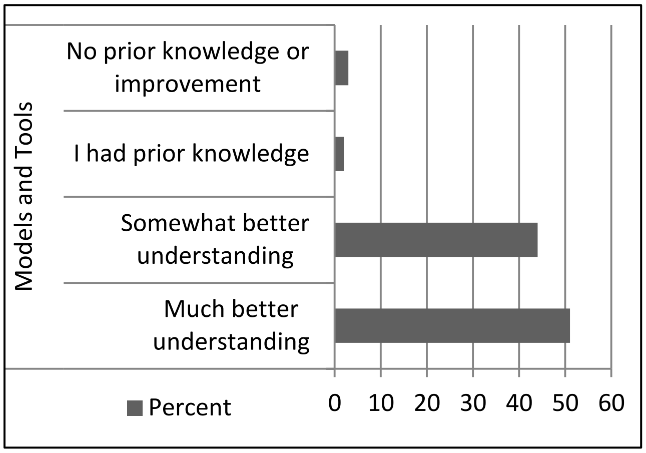

Figure 11. 16-Week Survey – Understanding of Models and Tools Concepts.

Faculty Perspectives

On the whole, faculty members felt the course was successful while also challenging to teach. The course contained a lot of technical material. Even experienced computer-science faculty members needed to do a lot of preparation and learn new material. After having reviewed the course materials, Dr. Mark Burge, a research scientist at MITRE Corp. and a former Associate Professor of Computer Science, said, “I would have to do a huge amount of preparation to teach that course” (Mark Burge, Personal Communication, November 2011). Instructors (see section 5 for a list of their backgrounds) who taught the course but were not computer science faculty members did a tremendous amount of preparation for the course. Nevertheless, faculty members all agreed that it is critically important to teach all Midshipmen about the cyber-security domain.

Administrative Perspectives

A great deal of resources and effort went into delivering the course, and from the administrative point-of-view due to the great success of the course and the importance of this topic to national security, these resources were well spent. Given the diversity of the current instructors, the administration is hopeful that more faculty members will become involved in cyber-security research and that USNA will see more interdisciplinary research conducted due to the cross-fertilization that the course essentially forced. In addition, expectations are that we will see an increase in the number of students majoring in computer science and information technology. Many parents of Midshipmen commented that they were pleased their sons and daughters were learning about cyber security at USNA.

Lessons Learned and Recommendations

In this section we describe some of the lessons learned, not previously mentioned, and make some recommendations about offering such a cyber-security course. We also describe some ideas for improvements to the course.

Since many of the instructors were new to the course material, possessed varying levels of technical exposure to cyber security, and in some cases had never before taught at an undergraduate institution, USNA offered a two-week hands-on summer preparatory “boot camp” in August 2011. During this session, the entire course was presented and Beta tested. The “boot camp” gave the instructors the opportunity to familiarize themselves with the content and provided the course coordinators the feedback necessary to refine material and test the support equipment. Fortunately, all instructors taught for the full semester without any emergency departures. Nevertheless, one recommendation is to train and maintain a list of possible replacement instructors in the event of an unexpected departure.

Section 4 discusses the weekly instructor forum which was conducted in one of the student classrooms for faculty to discuss successes, challenges, and upcoming content. These meetings, together with the instructor-email alias, provided additional opportunities to test and improve upcoming labs and lectures. Such email aliases were key to communicating successfully and efficiently. The instructor alias facilitated an ongoing exchange of ideas and a venue for capturing experiences and challenges encountered during the course. The section email aliases and in-class message boards were broadly used and considered very helpful. The course-wide email alias was valuable for pushing out important, class-related information in a timely manner, including new versions of available software, homework availability, scheduled times of review sessions, exam-schedule information, etc.

As discussed in the *Course Delivery* subsection, the primary reference for students was the course website, which was a very successful tool for students and instructors. Students routinely requested that the online lessons (for example, lecture notes) be made available prior to or during the actual lecture. Provided with the course notes in advance, students would be able to answer the majority of the questions posed by their instructor throughout a given class by simply reading from the notes rather than engaging in critical thought about the material discussed in the lecture. Therefore, this student recommendation will not be implemented. As an alternative, we may try to develop pre-reading content to introduce the terminology in advance to students. A pre-read could enhance the student's lecture comprehension and engagement, without revealing the critical thinking aspects of the material. The technical orientation and dynamic nature of the course necessitated the robustness and currency of the website, as it was the primary source of lesson material for the students. A secondary source of information was the required course textbook; however, most students never used their textbooks for this course, and therefore the textbook requirement needs to be reassessed. A textbook that meets the desire for pre-reading material would certainly be preferred but is not currently available.

The previously discussed student-learning support structure with MGSP, exam reviews, and extra instruction were extremely popular among the students, and the student opinion forms highlighted that fact. As expected, the sessions dedicated to exam review were the best attended with about 50% of students attending. For MGSP sessions, between 10–20% of the students attending was more typical. USNA will soon offer evening cyber-security tutors in its Center for Academic Excellence, and this service is seen as a necessity for the course. The speed with which this new core course was implemented limited the ability to staff the academic center tutors in time for the fall semester. Additionally, an "extra-help" non-credit class is being offered starting with the spring 2012 course. This "extra help" period is available to students that anticipate needing additional assistance and study time for most of the first- and second-year technical core courses at USNA.

A key miscalculation when developing the content for this course was the expectation that students would have a certain level of basic computer skills at the start of the course. The reality was that while students were adept end users of computer technology, they superficially understood the concepts and practical applications of computer technology and basic user security. As a result of this realization, future iterations of this cyber-security course will likely be adapted to take the lack of basic skills into account. One possible approach is to assess the level of basic computer knowledge during the summer orientation before the beginning of the academic year. For those students without requisite computer skills, a short remedial course could be offered to bridge the knowledge gap. This assessment could also provide a baseline to measure knowledge transfer during and after the delivery of the course. All first-year students are issued laptops at USNA and make heavy use of those machines in the fall. For this reason we expect the 600 students taking the course during the spring will not be burdened by a similar lack of basic computing skills. Furthermore, in course evaluations, many students suggested incorporating a weekly quiz into the course to provide an opportunity for students to gauge their retention of the concepts. Quizzes would encourage repetitive learning and build student confidence leading up to the exams, both of which the students needed due to their knowledge and skills gaps. Including quizzes will be examined in subsequent semesters; however, finding the class time to incorporate an additional, non-trivial assessment element to the course will be a significant challenge.

While the cyber-security course was technically oriented and hands-on, it can benefit from real-world contextual reinforcement of the technical concepts discussed in the classroom. USNA's Center for Cyber-Security Studies sponsors seminars and a lecture series with top-level, subject-matter experts discussing cutting-edge, cyber-security topics. And although these sessions were available to the student body at large and well attended, the incorporation of these events into the classroom may have provided an additional avenue for the needed contextual reinforcement. Additional contextual material will likely be integrated directly into course material. Since the required course textbook was insufficient at providing up-to-date content, online cyber-security articles may hold the key to delivering current and relevant supplemental and pre-read materials.

The weekly use of hands-on laboratory exercises were instrumental in creating knowledge transfer and widely enjoyed by the majority of students, as indicated in course-wide evaluations. One downside to the exercises was the lack of laboratory assistants. Frequently, during the labs, the exercise was interrupted with competing individual technical issues or student questions. While the lab objectives were usually met, having (dedicated) assistance during the lab would have facilitated more-effective knowledge transfer for the class as a whole while providing the ability to address individual concerns.

Clearly, not all institutions can or would necessarily devote this amount of energy and resources to introducing an institution-wide course in cyber security. However we encourage other institutions to take some steps toward preparing students to handle emerging cyber-security threats. These steps might be any one of the following: the introduction of a non-technical, elective, cyber-security course that has no prerequisites, the introduction of a technical cyber-security course in a specific department such as information technology or computer science, the introduction of a short course on cyber security, or perhaps the incorporation of more cyber-security material into existing courses.

Summary

By all measures the cyber-security course was successful. The course was implemented and provided to nearly 600 first-year students in the fall semester with only six months notice. Overall, the learning objectives of the course as designed were met. The course was technically oriented with hands-on activities designed to reinforce the learning objectives. Although most of these students will not pursue careers in cyber security, they will graduate with a better understanding of its fundamentals. Throughout this work we have highlighted many of the difficult challenges that were overcome to make the course a success. Finding qualified staff to teach/develop such courses and allocating the necessary resources are possibly the greatest challenges that an institution intending to design and implement a new curriculum will face.

References

1. B. Obama, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, May 2009, (accessed December 19, 2011).

2. D. Needham and P. Vincent, "Initial Report of the Dean's Cyber Warfare Ad Hoc Committee," USNA-CS-TR-2011-02. U.S. Naval Academy Computer Science Department, Annapolis, MD, 2011.

3. R. Tikekar, "Teaching Computer Security to Undergraduates: A Hands-On Approach, *Workshop in Education for Computer Security*," in *Workshop in Education for Computer Security*, Naval Post Graduate School, Monterey, CA, July 15–16, 2004.

4. A. W. Conklin, G. White, C. Cothren, D. Williams, and R. Davis, *Principles of Computer Security: CompTIA Security+™ and Beyond*, 2nd ed., McGraw-Hill, New York, 2010.

5. L. I. O'Leary, *Computing Essentials: Making IT Work for You.* McGraw-Hill, New York, 2012.

6. B. Sosinsky, *Programming the Web: An Introduction (Web Developer Series)*, McGraw-Hill, New York, 2004.

7. W. Willard, *HTML: A Beginner's Guide*, McGraw-Hill, New York, 2009.

8. K. Jabbour, and S. Older, "A Learning Community for Developing Cyber-Security Leaders. The Advanced Course in Engineering on Cyber Security," http://www.cis.syr.edu/~sueo/papers/ace-wecs.pdf, 2010, (accessed December 26, 2011).

9. Anon, "Information Assurance Internship," http://iainternship.com/images/IA_ Internship_Flyer_9132011.pdf, Sep. 13, 2011, (accessed December 26, 2011).

10. Rome Catholic School, Diocese of Syracuse, "Cyber Security K–12 Curriculum," http://www.romecatholic.org/elementary /cyber-security-k-12-curriculum, 2010, (accessed December 26, 2011).

11. D. Westneat, *The Seattle Times*, "UW Service Gap Does Not Compute," http://seattletimes.nwsource.com/html/dannywestneat/2016987078_danny11.html, Dec. 10, 2011, (accessed December 11, 2011).

12. J. Johnson, *The Washington Post*, "Why So Few Computer Science Majors?" http://voices.washingtonpost.com/campusoverload/2011/03/why_so_few_computer_science_ma.html, Mar. 7, 2011, (accessed December 26, 2011).

13. Office of the Dean, United States Military Academy, West Point, New York, "Academic Program: Curriculum and Course Descriptions," http://www.dean.usma.edu/sebpublic/curriccat/static/index.htm, 2011, (accessed February 15, 2011).

14. Office of Admissions, United States Naval Academy. "Class of 2015 Profile," http://www.usna.edu/ admissions/ USNA%202015%20Class%20Portrait.pdf, 2011, (accessed January 3, 2012).

15. M. H. Brown, *Baltimore Sun*, "Naval Academy Preparing Officers for Cyberwarfare," http://www.Baltimoresun.com/news/maryland/education/bs-md-naval-academy-cyber-security-20111019,0,2371754.story, Oct. 19, 2011, (accessed January 4, 2012).

16. C. Carroll, *Stars and Stripes*, "Cyberwarfare Joins the Curriculum at Service Academies," http://www.stripes.com/news/cyberwarfare-joins-the-curriculum-at-service-academies-1.158642, Oct. 24, 2011, (accessed January 4, 2012).

17. E. Kelly, *Capital Gazette Communications*, "Naval Academy Adds Cyber security Courses," http://seclists.org /isn/2011/Mar/ 23, Mar. 8, 2011, (accessed January 4, 2012).

18. E. Montalbano, *Information Week*, "Navy Adds Cybersecurity Academy Requirements," http://www.information week.com/news/government/security/229300570, Mar. 8, 2011, (accessed January 4, 2012).

19. Anon, *The Daily Record*, "Naval Academy to Add Cyber-Security Classes," http://thedailyrecord.com/2011 /03/07/naval-academy-to-add-cyber security-classes/, Mar. 7, 2011 (accessed January 4, 2012).

20. Anon, *Defense Systems*, "Naval Academy Weaves Cybersecurity into Curriculum," http://defensesystems.com/articles/2011/03/08/naval-academy-adds-cybersecurity-courses.aspx, Mar. 8, 2011, (accessed January 4, 2012).

21. A. Riveracorrea, U.S. Navy, "Naval Academy Expands on Cybersecurity," http://www.navy.mil/search/display.asp?story_id=62579, Sep. 6, 2011, (accessed January 4, 2012).

22. B. Witte, *Navy Times*, "Military Academies Teach More Cyberwarfare," http://www. navytimes.com/news/2010/03/ap_cyberwarfare_030810/, 2010, (accessed January 4, 2012).

Biographical Information

Chris Brown is an Associate Professor of Computer Science at the U. S. Naval Academy. His research focuses on symbolic computing and intelligent tutoring systems, and he has a strong interest in computer science curriculum design and development.

Frederick Crabbe is an Associate Professor of Computer Science at the U.S. Naval Academy. His research interests are in intelligent mobile robotics and machine learning.

Rita Doerr is assigned to the Technology Directorate of the National Security Agency as a Computer Science Researcher. She is currently on a Joint Duty Assignment at the U.S. Naval Academy teaching Introduction to Cyber Security, Technical Foundations.

Raymond Greenlaw is the RADM Frank T. Leighton Class of 1948 Distinguished Visiting Professor of Information Technology at the U.S. Naval Academy and the Distinguished Professor of Computer Science at Chiang Mai University in Thailand.

Chris W. Hoffmeister is a Lieutenant Commander Surface Warfare Officer assigned to the Computer Science Department at the U.S. Naval Academy, where he is a Military Instructor. His teaching and research interests include cyber security and protocol analysis.

Justin Monroe is an Ensign in the U.S. Navy with a specialty in Information Warfare. He is currently stationed at Navy Information Operation Command at Fort Meade, MD.

Donald Needham is a Professor of Computer Science at the U.S. Naval Academy. His teaching and research interests are in software engineering and computer security.

Andrew Phillips is the Academic Dean and Provost at the U.S. Naval Academy, and a Professor of Computer Science. His teaching and research interests are in computer security and computer organization.

Anthony Pollman is a Captain in the U.S. Marine Corps. He is currently serving as the Deputy Marine for Research at the Naval Postgraduate School, where he also teaches as part of the Cyber Academic Group.

Stephen Schall is a Lieutenant in the U.S. Navy Submarine Force assigned to the Computer Science Department at the U.S. Naval Academy, where he is a Senior Military Instructor. His teaching and research interests are in computer and network security, as well as algorithms.

John Schultz is a Lieutenant in the U.S. Navy Submarine Force assigned to the Computer Science Department at the U.S. Naval Academy, where he is a Senior Military Instructor. His teaching and research interests are in computer and network security and vulnerability analysis.

Steven Simon is a Captain in the U.S. Navy and Director for the Center for Cyber Security Studies at the U.S. Naval Academy. He has held positions including Deputy CIO, Office of Naval Research/Naval Research Labs; Chief Information Officer, US Strategic Command Center for Combating Weapons of Mass Destruction; and Commanding Officer, Naval Communications Material System.

David Stahl is a Professor of Practice in Computer Science at the U.S. Naval Academy. His teaching interests are in computer graphics and mathematics.

Sarah Standard is a Captain in the U.S. Navy Reserves assigned to the Center for Cyber Security Studies at the U.S. Naval Academy where she is an Instructor of Mathematics and Cyber Security. She is an Information Professional, and her teaching and research interests are in computer security, operations research, and applied mathematics.