Building a Cyber Security Engineering Program? Begin by Cloning Your Computer Engineering Program

Dr. Douglas W. Jacobson, Iowa State University

Doug Jacobson is a University Professor in the Department of Electrical and Computer Engineering at Iowa State University. He is currently the director the Iowa State University Information Assurance Center, which has been recognized by the National Security Agency as a charter Center of Academic Excellence for Information Assurance Education. He teaches network security and information warfare and has written a textbook on network security. For a non-technical audience he co-authored a book on security literacy and has given numerous talks on security. His current funded research is targeted at developing robust countermeasures for network-based security exploits and large scale attack simulation environments and is the director of the Internet-Scale Event and Attack Generation Environment (ISEAGE) test bed project. He has given over 75 presentations in the area of computer security and has testified in front of the U.S. Senate committee of the Judiciary on security issues associated with peer-to-peer networking. He has served as an ABET program evaluator representing IEEE for five years. He is a Fellow of IEEE and received the IEEE Educational Activities Board Major Educational Innovation Award in 2012 for his work in teaching information assurance to students of all ages.

Dr. Julie Ann Rursch, Iowa State University

Julie A. Rursch is an Associate Teaching Professor in the Department of Electrical and Computer Engineering at Iowa State University. Her focus is on secure and reliable computing. She has been an integral part of onboarding the B.S. in Cyber Security Engineering and the minor in Cyber Security Engineering.

Building a Cyber Security Engineering Program?

Begin by Cloning Your Computer Engineering Program

Abstract

Introduction

The nation is facing an increasing need for a workforce trained in elements of cyber security. The demand for workers in computer and information technology occupations is well-documented. The Bureau of Labor Statistics has projected a 12 percent growth in the number of job offerings from 2018 to 2028[1]. This is much faster than the average for all other occupations. And while this number is staggering and leaves us to wonder how to fill the gap of general technology workers, the growth expected in the more specialized information security subsector is projected at a whopping 32 percent growth during the same period[2]. Clearly, there is a need for colleges and universities nationwide to begin programs or fortify existing programs to produce graduates with cyber security skills.

However, building a new major focused on cyber security engineering is a daunting task for any size institution, whether the largest public or the smallest private. As always, it behooves us as educators to make the most of existing resources. This is why we propose the best way to begin a cyber security engineering program is not to start from scratch, but to start with cloning your computer engineering program. Begin by keeping the best of your existing program that already fulfils the accreditation requirements and build a solid cyber security core to compliment those technical computer engineering skills.

Why should we clone the computer engineering program? A cyber security engineering program that has its foundation in computer engineering combines a strong engineering perspective, a solid knowledge of computers, and the core elements of cyber security. Engineers are problem-solvers at heart. And, there are no bigger problems that need robust solutions than security issues in cyberspace. From desktops to cell phones, from wired to wireless networks, from cyber physical to Internet of Things devices, cyber security engineers who have a solid background in computer engineering are well-positioned to tackle the security challenges of today and tomorrow.

This paper discusses the process we used to leverage the existing faculty, classrooms, courses, and knowledge to build our cyber security engineering degree. The focus of this paper is on the design of the curriculum and the new cyber security core courses that were developed to provide those foundational elements of cyber security to the students. Additionally, the outreach and co-curricular activities used for recruiting and retaining students in the major are addressed.

New Cyber Security Engineering Degree: The Path to Getting Here

As background, the computer engineering degree at Iowa State University was created in 1977 by faculty in the electrical engineering department. The program has remained housed in the same department as electrical engineering, with only the name being changed to the department of electrical and computer engineering to represent the duality of the department. Additionally, the department added a degree in software engineering jointly administered with the department of computer science in 2007. At the graduate level the electrical and computer engineering department has been teaching cyber security courses since 1995 and created a cyber security

graduate degree in 2000. The computer engineering curriculum offers focus areas in software systems, embedded systems, networking, information security, computer architecture, and VLSI. Students also may take elective courses in control systems, electromagnetics, microelectronics, VLSI, power systems, and communications and signal processing. However, there was only one undergraduate course in cyber security.

Since our graduate classes were available to undergrads as technical electives many students interested in cyber security took the one undergraduate cyber security course and two or three graduate level courses to meet graduation tech elective requirements. Some remained at the university and completed a master's degree in cyber security. This was a viable pathway that seemed to meet the student demand until approximately 2012. The increased demand by employers for computer engineers with cyber security knowledge and our outreach and co-curricular actives (described below) began to drive interest in cyber security as an undergraduate focus. Being a victim of our own success, in 2015 we elected to create a minor in cyber security. The minor consisted of 15 credits, of which nine could not be counted toward their bachelor's degree. The minor was designed for students studying computer engineering, software engineering, computer science, or management information systems. For the minor we introduced three undergrad courses in cyber security which were to be used as the nine standalone credits. The focus of the three new undergraduate courses was hands-on, active learning labs and are the core of the new cyber security major. (Details on the courses are included below.)

Shortly after inception of the minor, the cyber security external advisory board challenged the department to create an undergraduate degree in cyber security, while maintaining the qualities of engineering we instill in our graduates. The advisory board wanted employees with the problem-solving abilities of a computer engineer coupled with the knowledge of cyber security problems. In other words, they did not want an "IT" only focus to the degree; they wanted an engineering focus. Additionally, one of the authors of this paper was part of the IEEE group looking at the proposed ABET cyber security engineering criteria. The participation in the IEEE group also helped shape the conversation around the creation of a cyber security engineering degree at our institution.

We are often asked, "Why engineering?" and, "What are the differences between cyber security engineering and cyber security degrees?" In the early days of work with cyber security, systems tended to be fairly isolated and designed to solve a particular problem. Over the past 15 years, cyber systems have become highly interconnected and highly interdependent. In addition there are now billions of devices connected to the network that do not receive users input through the traditions keyboard and display. This has made the internet the most complex system ever created and, therefore, the protection of the internet is a complex system problem.

Engineers, by training, are well suited to work on complex system level problems. The use of formal lab experiments, critical system thinking, and team based approaches to problem solving enable engineers to solve complex problems. This is not to say that "IT" focused programs are not needed, but as we start to look at computers controlling the physical world and our critical infrastructure, it is clear we need a systems approach on top of the "IT" focused approach. The tiered approach is also a feature of our new degree as described below. We do need to teach engineering fundamentals, systems thinking, as well as the tools and methods used in "IT" focused security.

BS in Cyber Security Engineering

When we were planning for the new cyber security degree, we wanted to start with computer engineering as the core building block for the new degree. However, starting with a degree that already contained 127 hours meant we had to look at what was critical and what could be removed to make room for cyber security courses. At Iowa State University the college of engineering has a common first year experience which left us with only three years that could be modified to accommodate the new cyber security courses. It was a fairly clear cut decision to keep all required computer engineering and computer science courses to ensure none of the rigor of the computer engineering degree would be lost. This would also reduce the number of additional courses to be developed and allow for an easier startup on the institution. To add the cyber security focus, eight cyber security courses were included in the degree curriculum. Half of the eight are required courses, the other four are electives. Again, this decision not only made logical sense, but it provided a solid basis in cyber security while maintaining the computer engineering core. As was mentioned earlier one of the authors participated in the approval process for the new ABET Cyber Security Engineering criteria. [3]. The new cyber security engineering degree was designed to meet the new ABET criteria.

Fig. 1 depicts the course subject matter over the four year curriculum plan for a cyber security engineering student compared to a computer engineering student. The red text represents the content removed from the computer engineering degree and the black text is what was added. In the second year the second physics (commonly known as physics 2) and the required electronic circuit courses were removed. They were replaced by three required cyber security courses. In the third year we removed an electrical engineering elective and replaced it with a fourth required cyber security course. Additionally, we modified the requirements of the tech electives in the degree. Rather than continuing to allow any computer engineering electives, the requirement was change to require cyber security electives. Finally, cyber security is now integrated into the existing capstone design course. This is discussed further later in the paper.

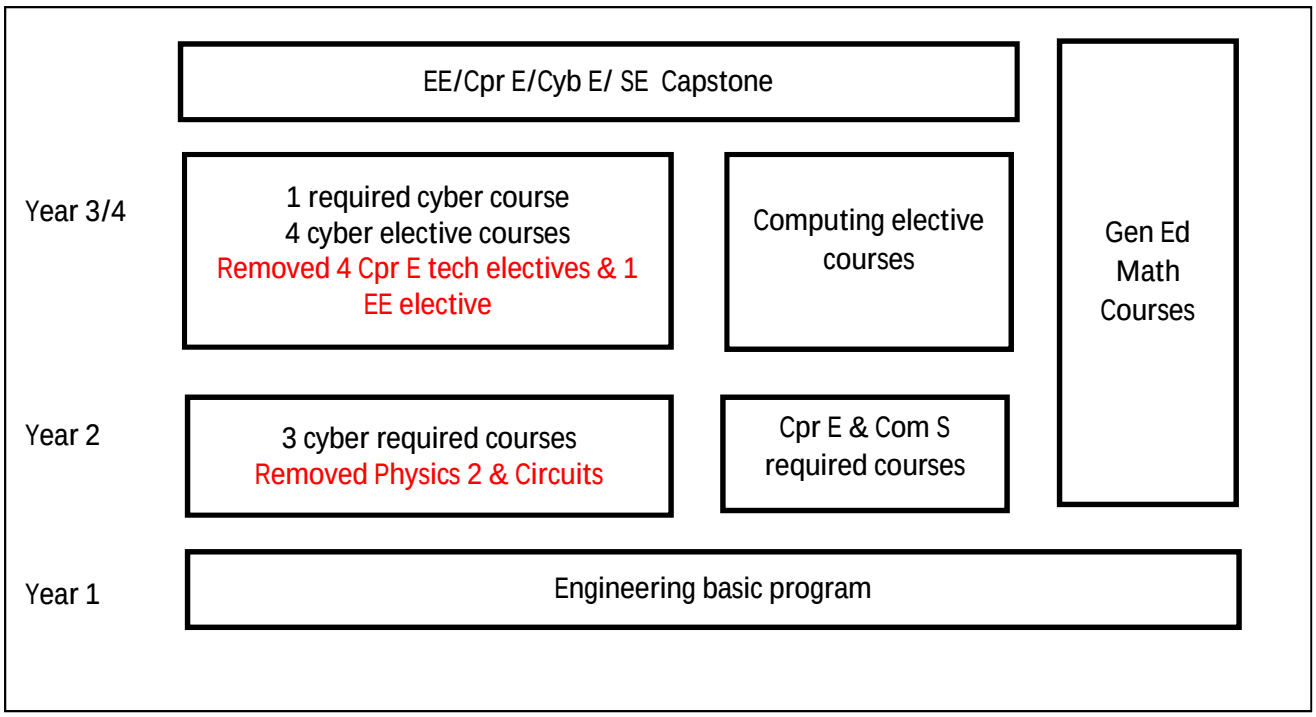

Fig. 1 Comparison of cyber security engineering degree with computer engineering degree

One of the interesting, hard problems in teaching a hands-on cyber security engineering program is that we need to teach "everything" before we can teach anything. So we had to design a curriculum that started with a broad set of learning objectives to teach students enough networking, operating systems, applications, infrastructure, and basic security that they could then be taught cyber security engineering. The previous work completed on courses for our cyber security minor provided us a baseline from which we could start the development of the cyber security major courses. The approach was to use the first "foundational" courses (230/231) to provide "enough" content to give students the breadth of knowledge to move into the "systems" approach to cyber security engineering. The higher level courses were developed to allow students to go into depth and develop their knowledge in more focused and systems approaches to cyber security. Fig. 2 below provides an overview of cyber security courses.

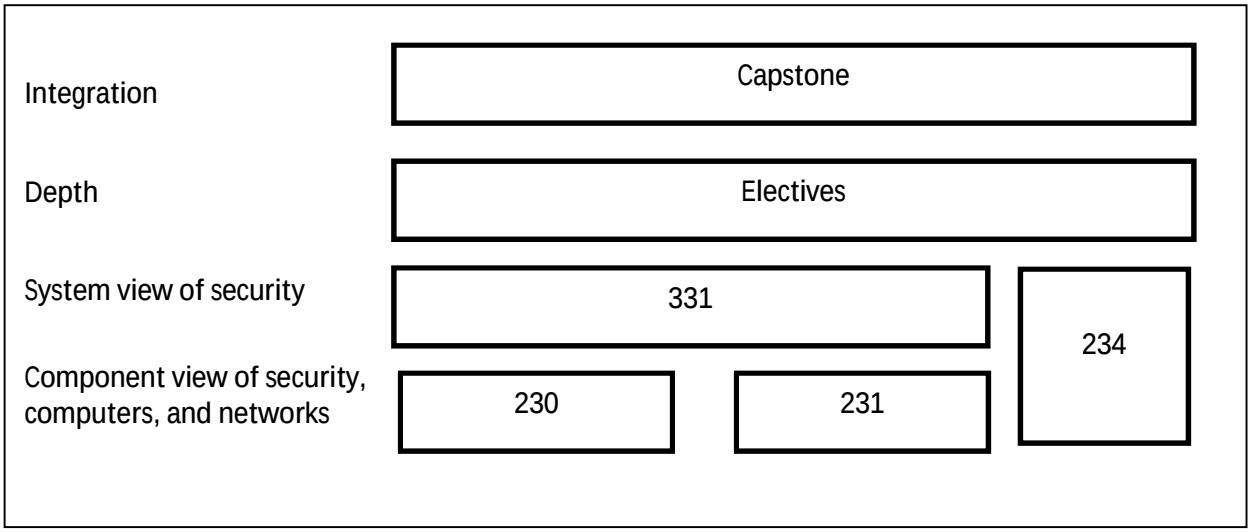

Fig. 2 Overview of the cyber security engineering degree

As we can see from the figure above there are two courses that teach "the everything" (230, 231) and one required course that ties it all together (331). In addition, we have a legal and ethical issues course (234) that also help tie things together through examining non-technical issues that effect cyber security. These four courses are then followed by cyber security and computing electives that go into more depth on particular aspects of cyber security. Then, as with any engineering degree, there is a capstone experience that brings everything together.

Required Cyber Security Courses

Below is a brief description of the four required courses, as well as a description of the virtual laboratory in which all labs for the three core technical courses are run. Several of the electives and graduate courses also are implemented in the environment. More details about the courses including a recent syllabus can be found on the Iowa State University Information Assurance website [4]

Virtual Laboratory – ISELab

The ISELab virtual laboratory provides a real world networking environment for students. The ISELab provides 120 publicly addressable IP ranges "borrowed" from the Internet. These IP ranges are connected to the backbone "Internet" network within the ISELab to allow students to work in or run their own "corporate" network. ISELab is air-gapped for most protocols, however, there is a proxy that allows http, https, and ftp traffic into the environment for the purpose of updating operating systems, installing packages, or reading additional information from the web. [5]

Each student in the course is given their own "public" IP range. To the student it appears he/she is working within their own network directly connected to the Internet. However, all traffic is contained in ISELab by an air-gap. This prevents beginner mistakes such as misconfiguration

from affecting others in the class, others on the campus network, or others on the Internet. Each student has their own subdomain that is maintained in the internal ISELab DNS server.

ISELab is built upon a testbed (ISEAGE) developed at Iowa State University. The testbed provides core networking and routing functionality on a single VMWare ESXi server. Additional information about the testbed can be found on the ISERink website [6

Course #1 - Cpr E 230 Cyber Security Fundamentals

The first course in the three course required series focuses on teaching students the fundamentals of operating systems, networking, and cyber security in a hands-on, lab-focused course. Students are required to have at least one basic programming course prior to taking this course. At our institution, students will have had both an introductory C course as part of the freshman experience and a Java course as their required computer science introductory object oriented course. In this first cyber security course, students must learn basic information about Linux operating systems as many of them have never touched a machine outside of a Windows GUI environment or a Java IDE. Low level topics such as how operating systems work, what packages are, how packages are installed, how to create and manage users, as well as what permissions are and how to manage them are covered. Students are also introduced to networking including the OSI and TCP/IP models, the basics of routing and network equipment, firewalls, and virtual private networks. The topics of web applications and web servers and the security surrounding those are also included in the course. In weekly labs, students implement services in a secure manner in their own network. Example services include DNS, email, directory services, TLS web traffic, SSH, firewalls, VPN, and more. At the end of the semester, a final project is given where the students are provided a single server that they have to evaluate in terms of security, noting what has been configured incorrectly and propose a way to fix the problems.

By the end of the 16-week course, students can explain basic cyber security terms and concepts. They are able to design basic computer and network defenses, as well as install systems in virtual environment. They have honed their troubleshooting skills to cover basic networking, operating system, application, and security problems.

Course #2 - Cpr E 231 Cyber Security Concepts and Tools

Cpr E 230 is a prerequisite for this course. Students must come with basic computer competencies from that course such as operating systems, networking, and cyber security knowledge. The course revolves around the concepts found in being a penetration tester and evaluating systems, networks, software, and physical locations for vulnerabilities, as well the countermeasures for each potential attack vector. During the first few weeks of lab, students focus on the process an attacker goes through such as reconnaissance, scanning and enumeration, gaining access, maintaining access, and covering their tracks. Students are each given a "corporate" network where they have a desktop machine, but know nothing other than the IP range that they are to evaluate. Each week they take the steps an attacker would take if they were conducting an active attack. Students scan the network for potential targets and open ports, determine vulnerabilities, exploit those vulnerabilities, gain a foothold on the servers, learn about

the users and administrators, use that information to pivot to another network, and then leave a backdoor to which they return at a later date to continue activity. The emphasis in the course is on using tools to evaluate a network, systems, and software, as well as securing these systems. They also work with authentication and access control methods, as well as common web attacks, including social engineering and malware. For their final project each student is given a new "corporate" network where they complete three phases: evaluation of the "corporate" network for vulnerabilities, remediation of those vulnerabilities, penetration testing of two other classmates' "corporate" networks. As part of the final phase, they write a penetration testing report for their classmate "client" listing vulnerabilities and remediations.

Course #3 - Cpr E 331 Application of Cryptographic Concepts to Cyber Security
The prerequisites for this course are Cpr E 230 and Cpr E 231. This course provides students with the basic cryptographic underpinnings used in modern cyber security encryption suites. The course starts as all cryptography courses would with basic cryptographic concepts of the CIA model and classic ciphers to provide some background into the common concepts in encryption. The course then focuses on modern cipher suites. Each week a different cryptographic concept is examined both in terms of the mathematical concepts in their algorithms and their uses in protocols. The weekly lab focuses on the hands-on use of that encryption concept to benefit cyber security. Weekly topics in the class include the symmetric stream and block ciphers, asymmetric cipher suites, perfect forward secrecy, elliptic curves, cryptographic random numbers and hash functions, and user authentication and key management including digital signatures. In addition to cryptography, the use of covert channels to deliver messages and malicious code is covered. For the final project in this course, students select a cyber security problem and must formulate a solution to the problem that includes a hands-on demonstration of the problem and solution combination.

Course #4 – Cpr E 234 Legal, Professional, and Ethical Issues in Cyber Systems
This course is not a prerequisite or a co-requisite in the core three series of the cyber security foundational courses. It can be taken at any point in the degree program. However, we have found students hungry to take cyber security courses early in their academic career and that second and third year students are primarily found in the course. The course emphasizes legal, ethical, and professional issues in cyber systems that extend beyond the technical issues covered in Cpr E 230, Cpr E 231, and Cpr E 331. It covers topics such as privacy, government regulation, and compliance as applied to professional practice of cyber security. While the three technical courses focused on weekly lab exercises, this course focuses on giving students contact with guest lecturers from government and industry who work in cyber security. The discussions focus around current legal and ethical issues that face practitioners every day. Students complete weekly reflection writings and in class activities/discussions that focus on current events and/or guest lecturers' materials. In addition to the weekly assignments, students will write a research paper on a cyber security ethical or legal topic of their choosing. It should also be noted the EE and Cpr E programs are discussing adding this course to their curriculum.

Technical Elective Courses
The electives for the cyber security engineering degree are divided into two categories, cyber security courses and computing courses. Currently, there are four cyber security technical

electives offered at the undergraduate (400) level. There are two additional undergraduate cyber security technical electives being designed at the time of this paper being written. Most of these courses would be taught by most cyber security programs and for brevity we will not expand on them other than a one sentence description. Additional information can be found on the Iowa State University IAC website [4]. However, one of the currently offered courses is novel and worth discussing in this paper. It is the cyber security practicum (432)

Currently offered

- Network security: provides students an in depth look at network based attacks and defenses.
- Secure operating systems: provides students a hands-on look at modern secure operating systems and how they enhance overall security
- Cyber security practicum: described in more detail below
- Software analysis and verification for safety and security: looks at formal methods to help create and verify the security of software.

In design

- Wireless security: this course looks at wireless networks from the physical layer up.
- Internet of Things / Cyber Physical Systems security: provides students the opportunity to examine a wide variety of IoT and CPS devices and their insecurity
- Select graduate courses: students are allowed to take selected graduated courses in their senior year.

Novel Technical Elective – Cpr E 432 Cyber Security Practicum

This course focuses on the design and implementation of a secure networked environment that is penetration tested by peers in the course. Evaluations are made of each environment and whether it withstood testing, as well as what vulnerabilities were able to be exploited. After this attack phase, students complete an evaluation of their security plans and take the necessary remediation steps to further harden their networked environment. The lecture targets the tactics needed to be taken by the students in their weekly lab practicum. In addition to using technical skills, students use their technical writing skills in their design documents, implementation plans, and post-mortem security evaluations.

Capstone Integration

The new cyber security degree uses the same senior design course as the computer, electrical and software engineering programs. To ensure the projects have a cyber security focus we have a mixture of cyber security only projects and projects where cyber security plays a critical role in the project. It should be noted this mix was in place before the creation of the BS in cyber security engineering due to the interest of both faculty and students. In addition, we have added cyber security as a constraint that needs to be addressed in the design report for all projects.

Senior design projects are proposed by industry, faculty, or students who are the clients in the year-long project. Each senior design team is advised by an assigned faculty member who may also be the client. The cyber security engineering students are placed on projects that require the analysis, design, and evaluation of cyber security systems, including system integration and implementation.

The senior (capstone) design experience occurs during the student's last year in the program via the two-semester sequence of courses EE/Cpr E/SE 491: Senior Design Project I and Professionalism and EE/Cpr E/SE 492: Senior Design Project II. The two senior design courses heavily emphasize design under constraints, problem solving, technical writing, oral presentations, project planning, economic analysis, professional issues, and contemporary issues. Typical capstone projects require students to use a variety of engineering tools and engineering standards, while integrating knowledge from many of their courses.

The first semester course (491) focuses on various aspects of engineering design, with input from outside speakers (faculty and local engineers). Student teams meet weekly with their faculty advisor. At the end of the semester, a design document is developed and a design review is conducted by a 4-5 member faculty team.

During the second semester course (492) the team implements their design, as well as communicates, their project client, objective, constraints, budget, approach, deliverables, relevant standards, and results to peers in the class as well as a final oral presentation to an industry panel comprised of four industry engineers. Additionally, the students present a poster session with demonstrations in the afternoon following their morning industry panel review.

ABET Integration

One difficult aspect of standing up a new program is ABET accreditation and the assessment process. We chose to integrate the cyber security engineering program assessment into the ECE department's process. This allows us to share assessment data and processes. An overview if the department's assessment process and how the new degree is integrated is provided below.

The Department of Electrical and Computer Engineering has implemented a multilevel assessment process for measuring student attainment of outcomes for the Electrical and Computer Engineering programs. A summary of the approach was presented at the 2013 ASEE Annual Conference [7]. The new cyber security engineering program will also use the same process. The multilevel assessment process for measuring student attainment of outcomes as described below and summarized in table 1 and 2 below:

1. Level 1 assessment uses high-level information from a cross-section of students in the program that can be used to identify trends and potential problems. Level 1 information corresponds to student competencies observed by supervisors (employers) in the workplace during student internships. The results of the surveys are mapped to ABET student outcomes 1-7; all outcomes are assessed at level 1.
2. Level 2 assessment is finer grained and more specific than level 1. Level 2 information corresponds to student performance as demonstrated through work submitted during the senior year in the senior design class (CPRE/EE 491 and CPRE/EE 492) and in the portfolio class (CPRE/EE 494). The student work consisting of various design project deliverables and portfolio items are reviewed and scored by faculty. Rubrics are used and cover all ABET student outcomes (a) – (k) except outcome (b), which is given special attention using level 3 assessment. The senior year is an opportune time to assess student learning in a summative manner.
3. Level 3 is finer grained and more specific than the other levels. It provides more in-depth examination of a student outcome earlier in the program at the time the student is

learning about it. Level 3 information corresponds to student achievement on specific assignments in selected courses. The courses and assignments are selected based on their appropriateness to measure a particular student outcome. Student work is scored by the instructor using rubrics. Table 2 shows which courses are used by the 3 programs.

As shown in Table 1 below, data are collected from three types of measurements (direct, indirect, and informal) and at three different levels (1: program, 2: demonstration and 3: learning). The indirect and informal methods are based on student input from surveys, student forums, and informal feedback from faculty and students. Direct measurements are obtained from four sources: senior design, the required portfolio class, selected required courses before the senior year, and workplace competency assessments completed by employers.

Table 2 shows the assessment of student outcomes and as can be seen the cyber security engineering program uses many of the same courses as the computer engineering program. The primary differences are using the 331 course which as discussed above is a course that ties the learnings from the first two required courses together. To measure ABET students outcome 4 in the cyber security engineering program we use the required ethics course.

Table 1: The multilevel Student Outcomes assessment process

	Direct	Indirect	Informal
Program level ***(Level 1)***	Workplace Competency assessment – Employer	Workplace Competency assessment – Student Student forums	Student input Faculty input
Demonstration level ***(Level 2)***	Student Portfolios Senior Design	Student Portfolios	Student input Faculty input
Learning level ***(Level 3)***	Several courses	Student forums	Student input Faculty input

Table 2: Assessment of student outcomes

Direct Assessment tool			**Student Outcomes**						
			1	**2**	**3**	**4**	**5**	**6**	7
Level 1: survey from employers			√	√	√	√	√	√	√
Level 2: Senior design scoring by faculty			√	√	√	√	√		
Level 2: Portfolio assessment by faculty						√			√
Level 3: Course based									
CPRE	EE	Cyb E							
CPRE 281	CPRE 281	CPRE 281						√	
EE 230	EE 230		√	√					
CPRE 288	CPRE 288	CPRE 288		√					
CPRE 381	EE330		√						
CPRE 310	EE332	CPRE 310	√						
CPRE 394	EE394					√			
		CPRE 234				√			
		CPRE 331	√					√	

Recruitment, retention, and outreach

Iowa State University has created multiple programs to increase the number of students interested in cyber security either from high school or students enrolled at the university. We also have activities that provide a venue for students to enhance their cyber security skills. While not a focus of this paper, any successful program will need to develop recruitment, retention and outreach strategies. Below are short descriptions of our three largest activities we use to get and keep students interested in cyber security along with URLs to the programs.

High school engagement

Iowa State University has been involved in cyber security outreach since 2004 with the goal of increasing interest in cyber security. Lead by Doug Jacobson and Julie Rursch, the faculty and staff at Iowa State University have been pioneers in the effort to encourage high school students to become interested in cyber security.

In 2004 the university offered one of the nation's first high school summer camps focused on cyber security [8]. In fall of 2005 we decided that we wanted to reach more high school students by providing an opportunity for schools to introduce cyber security as an after school program. This led to the nation's first high school cyber defense competition (CDC) in the spring of 2006 (more on the CDC below). Our first year we had 60 students from10 high schools participate and in 2007 it grew to 130 representing 17 high schools. [9]

Based on the success of the high school CDC we decided we should grow the program to help increase the number of students interested in other aspects of computing. In 2008 with funding from the State of Iowa Department of Economic Development and in partnership with the state technology association, we started the IT-Adventures program [10, 11, 12] which was dedicated to increasing interest in and awareness of information technology (IT). Today the IT-Adventures program has three tracks from which students can choose to study: Cyber Security, Smart-IT, and Robotics.

Cyber Defense Competitions

The second major activity is the multiple cyber defense competitions we run each year. Iowa State University began hosting Cyber Defense Competitions (CDC) in 2005. To date Iowa State University has run more than 60 Cyber defense competitions. [13]

In a CDC students design, configure, and maintain a set of servers and a network in a secure manner prior to the competition. Then, during the day long competition, they work to prevent security breaches and to remediate exploits that occur while maintaining a fully functional network for their end users. The program was expanded rapidly and Iowa State now hosts four college level cyber defense competitions and one high school level competition each year. The student club (IASG) (discussed below) is responsible for organizing and running events for Iowa high schools, Iowa community colleges (two-year), our own Iowa State University students, and four-year students from universities across the nation. The CDCs have become a key component in the education of the students interested in cyber security, as well as a recruiting tool for employers nationwide. Our corporate sponsors of the CDCs set up booths at the competitions

and talk with the students providing information about cyber security opportunities within their organizations, as well as general knowledge about the industry.

Student Club

The Information Assurance Student Group (IASG) in the Department of Electrical and Computer Engineering at Iowa State University was started in 2003 as a retention and engagement effort for students who were interested in information assurance and computer/network security [14]. However, it quickly grew into a wholly student run organization that not only focuses on educating its own members, but also runs cyber defense competitions (described above) and works with corporate sponsors and recruiters to provide learning opportunities. The IASG provides weekly active, inquiry-based learning meetings for its membership which focus on developing students' applied and practical security skills. Before the creation of the cyber security minor and then the degree, the IASG provided a way for students interested in security to learn from each other. Today the IASG not only supports the cyber security engineering students, but also opens the door for computer engineering software engineering, management and information systems, computer science, and other degrees who are interested cyber security to gain hands-on experience and real-life security skills.

Issues and Conclusions

At Iowa State University we have successfully built a new cyber security engineering program that has a foundation in key computer engineering concepts. Our employers and our external advisory board have both been very pleased with the final product we have created. However, this new cyber security engineering degree has not come without issues.

One of the biggest obstacles that we have faced is the limited resources at our disposal, both human and equipment. As we all know, hiring new faculty members is a challenge in general, and finding individuals with advanced degrees who know cyber security and aren't lured into industry with high wages and promises of fame and fortune is difficult. We have provided a stop-gap measure to teach cyber security courses by retooling some of our existing faculty members to take a more active role in the delivery of cyber security courses. Additionally, we have hired an adjunct faculty member who is a cyber security practitioner to teach the cyber security ethics class. This is a win-win combination as he provides additional labor in the teaching of one course per semester and he has the day-today experience with current legal and ethical issues in his "daytime" job.

We are fortunate at Iowa State University that our dean and our provost have been very supportive of the new cyber security engineering degree. When the cyber security minor was under development the department received funding for new hardware to support the virtual laboratory environment. The technical support for the new equipment has been given to our existing support group for the department. And, the department has funded a small lab support team that includes one graduate student and one undergraduate student to help develop, deploy,

and keep labs up-to-date. However, we believe the demands on the virtual laboratories and the support teams will continue to grow as the student numbers increase.

Finally, the new cyber security major did not kill the cyber security minor. We continue to offer the minor for computer engineering, software engineering, computer science, and management information systems students. We believe the cyber security void is so large that each of these kinds of students can help fill the gaps we are positioned to see in the next 20 years.

Footnote: For those who are interested, all laboratories used in the three core technical courses have been included in the National Security Agency's National Cybersecurity Curriculum Program [15]. Additionally, the ISELab is freely available by request at the ISERink web site [6]

Lessons learned and future work

The program started May of 2019 without much advertisement. During the summer 2019 orientation we had about 30 incoming freshman that transferred from another major into cyber security engineering. We had an additional 50 current students transfer to the new degree. This large transfer was unexpected, even though in hindsight it should have been anticipated. The large number of transfer students forced us to try to create cyber security technical electives sooner than we expected.

The biggest issue we have with is the first three cyber security courses offered (CprE 230, 231, 331) are very lab intense and allow students to work with fully functional clients and servers that they configure, test for vulnerabilities, exploit, and secure. These labs do not follow a cookbook approach and do not give students every answer because we are trying to teach problem-solving and troubleshooting skills, as well as thinking outside of the box, in security. However, that means these classes have a very high dependence on the undergraduate TAs providing support both during the 2-hour lab and also during online office hours that happen throughout the week.

We are working to come up with ways to steam line the lab setup and support along looking at how we can use dedicated TA support to keep the lab current and to make sure the labs are functional as technology changes. We are also working to increase the number of technical electives.

Another effort is to look at recording the lectures in 230 and 231 not only to help deal with the shortage of faculty to teach these two courses, but also to provide modules that students in the follow on course can review. Again, going back to the "we need to teach everything before we each anything" concept we believe that be providing modules for the "everything" part students will be more successful in the follow on courses.

References

[1] (2019). *Occupational Outlook Handbook*. Available: https://www.bls.gov/ooh/computer-and-information-technology/home.htm

[2] (2019). *Fastest Growing Occupations*. Available: https://www.bls.gov/ooh/fastest-growing.htm

[3] ABET Cyber Security Engineering criteria. Available: https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2020-2021/

[4] ISU course listing. Available: http://www.iac.iastate.edu/courses/

[5] J.A. Rursch and D. Jacobson. "When a testbed does more than testing - The Internet-Scale Event Attack and Generation Environment (ISEAGE) - providing learning and synthesizing experiences for cyber security students," Frontiers in Education, Oklahoma City, OK, Oct. 23-26, 2013.

[6] ISERink testbed. Available: http://www.iserink.org/

[7] Diane T. Rover, Douglas W. Jacobson, Ahmed E. Kamal, Akhilesh Tyagi, "Implementation and Results of a Revised ABET Assessment Process", 2013 ASEE Conference, Atlanta, GA. June 23-26, 2013

[8] Doug Jacobson, "Computer Security Summer Camp for High School Students", Proceedings of the 2006 American Society for Engineering Education, Chicago, June 18-21 2006.

[9] J.A. Rursch and D. Jacobson. "This IS child's play - Creating a playground (computer network testbed) for high school students to learn, practice and compete in cyber defense competitions," Frontiers in Education, Oklahoma City, OK, Oct. 23-26, 2013.

[10] Rursch, J., Jacobson, D.W., "IT-Adventures: Turning High School Students "ON" to Information Technology", *Proc. Frontiers in Education* (San Antonio, TX, Oct. 18-21, 2009).

[11] Julie Rursch, Andy Luse, and Doug Jacobson, "IT-Adventures -- A Program to Spark IT Interest in High School Students using Inquiry-Based Learning with Robotics, Game Design, and Cyber Defense", IEEE Transactions on Education, Vol. 53, Issue 1, pages 71-79, 2009. (IEEE Education Society 2011 Transactions on Education best paper award 2011)

[12] IT-Adventure program descritption. Available: http://www.it-adventures.org/

[13] Iowa State Cyber Defense Competitions. Available: http://www.iac.iastate.edu/get-involved/cyber-defense-competitions/

[14] J.A. Rursch, D. Jacobson and M. Sullivan, “Information Assurance Student Group: How to Turn a Club into a Valuable Learning Experience for Students,” 2012 ASEE Annual Conference, San Antonio, TX, June 10-13, 2012.

[15] NSA Clark Center. Available: https://www.clark.center/home