Procedia Computer Science
Volume 80, 2016, Pages 1940–1946

ICCS 2016. The International Conference on Computational Science

Enhancing Computational Science Curriculum at Liberal Arts Institutions: A Case Study in the Context of Cybersecurity

Paul Y. Cao[1, 2] and Iyad A. Ajwa[2]
[1]University of California San Diego, San Diego, CA, U.S.A.
[2]Ashland University, Ashland, OH 44805, U.S.A.
yic242@eng.ucsd.edu, iajwa@ashland.edu

Abstract

Computational science curriculum developments and enhancements in liberal arts colleges can face unique challenges compared with larger institutions. We present a case study of computational science curriculum development at a medium sized liberal arts university in the context of cybersecurity. Three approaches, namely a cybersecurity minor, content infusion into existing courses, and a public forum are proposed to enrich the current computational science curriculum with cybersecurity contents.

Keywords: Computational Science, Cybersecurity, Liberal Arts, Curriculum Enhancement

1 Introduction

Computational Science is a very dynamic field spanning across many disciplines. Cybersecurity is a computing-based field that aligns network resources, human resources, and processes to ensure “assured operation” in the presence of adversaries and risks [1]. This area has become one of the most serious economic and national security challenges. The number of cyber-attacks continues to grow each year, and cyber threats are becoming more diverse, disruptive, and damaging. With several initiatives attempting to address critical cybersecurity workforce development, an expansion of cybersecurity related education is one of the most important steps to secure the cyberspace. A rigorous technical training and certification process should be an integral part for students majoring in technical fields such as computer science or information systems. A framework to develop and retain talents should also be a necessary aspect in workforce development. Also, fundamental training on cybersecurity topics would be extremely valuable to students who may become personnel with non-technical roles in the cybersecurity industry, or who may work with information systems in government or business [2, 3].

Many universities and colleges have responded to the unprecedented demand by implementing courses, programs and tracks in cybersecurity or information assurance [1]. Curriculum development

Selection and peer-review under responsibility of the Scientific Programme Committee of ICCS 2016

doi:10.1016/j.procs.2016.05.510

usually involves in new course developments and security content infusion [4]. Institutions with significant human and financial resources can build up a cybersecurity program relatively fast. Smaller liberal art institutions usually lack the expertise in cybersecurity, have limited resources, and need to deliver content in a short timeframe. Thus, liberal arts colleges usually start with one or two new courses in information assurance, hacking, or network security. Ashland University offered courses on network security and gray hat hacking in spring 2015 before a comprehensive minor was proposed [5]. This strategy provides valuable leads into further program development and allows faculty members to gain training and experience in offering a more comprehensive cybersecurity curriculum.

One potential pitfall of cybersecurity program development is the overwhelming focus on technical training in specific courses and focus only on Information Systems or Computer Science majors. In addition to educating technologically competent professionals in cybersecurity, we also need, for example, managers with both knowledge of cybersecurity concepts and a useful framework for developing an organizational culture that will rapidly identify and eliminate mistakes. Managers with a cybersecurity training can make companies less vulnerable to cyber-attacks. Thus, a comprehensive curriculum update involving related programs and departments should be implemented if possible. Students in these related programs, such as business, criminal justice, and law, will benefit from exposure to cybersecurity topics.

This paper is organized as follows. Section 2 discusses related work in cybersecurity curriculum development. In Section 3, we present a case study of computational science curriculum enhancement in the context of cybersecurity. Three major venues of curriculum enhancement: cybersecurity minor, cybersecurity content integration, and cybersecurity awareness are discussed in details in this section. In Section 4, we provide descriptions of newly created courses as well updates made to existing courses related to cybersecurity. Section 5 concludes the paper.

2 Related Work

Cybersecurity related curriculum development has many focuses and variations. One group of work focuses on a single aspect of the curriculum development. For example, Brown *et al.* [6] reported their experience with the development of a single introductory cyber-security course in the US Naval Academy. Their experience report covered many challenges with the development of a cybersecurity course, such as the shortage of faculty expertise, technical content selection, and the need for short turnaround time. Greenlaw *et al.* [7] discussed their experience in building a lab course in network reconnaissance, attack and defense. Their work shares valuable curriculum development experiences and contributes to an ever-increasing content pool necessary for any successful cybersecurity program. However, their work lacks the global view on what a complete cybersecurity curriculum would be composed of.

Another group of existing curriculum development efforts stresses on the integration of cybersecurity topics into the overall CS curriculum. For example, Bratus *et al.* [8] integrated hacking principles into the undergraduate curriculum at Dartmouth College. Authors in [9] proposed a system approach that incorporates both hardware and software in cyber assurance education. The authors build a complete Information Assurance B.S. curriculum at the University of South Alabama and the paper included a comparison of two cybersecurity B.S. degrees at the University of Maryland University College and at Louisiana Technical University. This group of work offers a complete curriculum development experience, mostly on the technical contents of a cybersecurity degree. However, most of the work lacks broader collaborations with other departments or programs.

Two existing experience reports focus on the development of a cybersecurity minor. Dardick *et al.* [10] discussed a minor in digital forensics, and Katz [11, 12] shared experience in building up a cybersecurity minor at the Armstrong Atlantic State University. A minor in cybersecurity requires fewer resources and may achieve targeted cybersecurity education goals through innovative curriculum design and inter-program collaborations.

3 Enhanced Undergraduate Curriculum

This section addresses the enrichment of Ashland University's computational science curriculum in the context of cybersecurity. The primary goal of the enhancements we have made to our curriculum is to formally train technical professionals in the area of cybersecurity. Another goal is to educate business professionals about the risks involved in cybersecurity. To achieve these goals, we had identified three objectives: establish a new cybersecurity minor, integrate cybersecurity content into existing courses, and increase the awareness and understanding of cybersecurity on campus and in the local community. Strategies we have followed to achieve these goals are detailed in the following sections.

3.1 Cyber Security Minor

The Cyber Security Minor at Ashland University integrates cybersecurity topics such as fundamentals of computer security, computer networks, penetration testing, information and network security, public-policy, security policy analysis and implementation, and law that are taught by various programs including computer science, information systems, and criminal justice. The minor aims at providing our students with formal training in a career path that is in high demand.

Our first strategy to develop the minor consisted of two steps. The first step was to identify existing courses that are related to cybersecurity and taught by the above-mentioned programs. We also examined and adopted existing courses taught by other programs such as accounting and supply chain management. The second step was to identify topics relevant to cybersecurity that we do not have courses for. As a result, several new courses had been developed and included in the minor. A list of newly created courses and their contents is provided in Section 4.1. We then constructed a new minor in cybersecurity following the traditional paradigm that consists of required and elective courses in addition to a required internship.

The second strategy was to form and enhance partnerships with associate degree schools that currently offer programs in cybersecurity or related areas. Ashland University has existing articulation agreements with three such schools. Moreover, there are only a few community colleges in Ohio that offer a degree in cybersecurity [14]. Our next goal is to partner with these community colleges so that we could provide a clear education path for associate-degree cybersecurity students to bachelor degree professionals. Their BS education in computer science focuses knowledge and expertise on how to protect and defend our information from malicious cyber-threats. It will further enhance their critical thinking skills, technical skills, and business management skills. We believe this strategy on one hand will significantly benefit society by producing students capable of contributing to the improvement of information security in their government and business organizations [18]. On the other hand, graduates from this program, equipped with a strong skill set in both technical and managerial areas, will be very attractive candidates for employment.

Our third strategy has been the establishment of relevant internship opportunities. As mentioned above, students enrolled in the cybersecurity minor are required to complete an internship or a work experience relevant to cybersecurity. Ashland University has established an articulation agreement with a private firm on security in Ohio where our students can complete the required internship.

We believe our new minor enjoys several features and has several benefits to offer. The new minor is interdisciplinary and, as such, it creates a powerful learning experience for the students and emphasizes critical thinking through integrative learning. In addition, the new minor provides computer science students with key coverage of business applications and concepts. Moreover, it provides business students with essential knowledge and skills to better understand the importance of protecting key information system assets with cybersecurity techniques. Furthermore, the internship agreement provides students enrolled in our program a guaranteed opportunity to complete a real-world work experience relevant to cybersecurity.

3.2 Cybersecurity Content Integration

We have adopted the philosophy that security issues should be addressed in all aspects of computational education curriculum. Security components to be included in our existing computer science courses had been identified and are being infused. These courses include introductory programming, web programming, computer algorithms, computer architecture, operating systems, computer networks, and software development. Detailed cybersecurity content integration into these courses is provided in Section 4.2.

The cybersecurity content infusion also focuses on courses from other majors such as business. For example, the commercial Enterprise Resource Planning (ERP) software has been integrated into several business courses at Ashland University providing students with hands-on experience to use the software, including how to protect ERP systems from cyber-attacks [14].

In addition to the enhancements being made to courses, faculty knowledge and skills relevant to cybersecurity needed to be enriched as well. Cybersecurity knowledge and skills of the faculty are deepened through professional development activities. This will increase faculty capacity to deliver an upgraded curriculum to a wide range of students, including multiple enhancements in existing courses and programs. Professional development opportunities that our faculty have started pursuing include attendance at national conference workshops (Association for Computing Machinery Conference (ACM) on Computer and Communications Security and the IEEE Security and Privacy Conference) as well as industry training (SANS Institute and COMPTIA).

3.3 Cybersecurity Awareness

Promoting the awareness and understanding of cybersecurity is very important in today's world. To achieve this goal, we have adopted the following strategies.

Students enrolled in our cybersecurity minor are encouraged to compete in cybersecurity contests such as the Midwest Regional Collegiate Cyber Defense Competition. We believe that increased student involvement in cybersecurity-related issues promotes awareness of cybersecurity, both within various academic constituencies and within the local community. Participation in contests also promotes our cybersecurity minor and supports our marketing and recruitment efforts [14].

We are in the process of forming a local chapter of a Network Defense Security club. The Network Defense club will be established based on the model we currently utilize for the local student chapter of the ACM. This new student-run organization will hold regular meetings of the club members, where students have an opportunity to further develop cybersecurity skills beyond what is taught in formal coursework. Topics to be explored during club meetings will include assembly of cybersecurity hardware, hands-on experience in securing various network layers from malicious access, use of software packages related to cybersecurity, minimizing human error as a contributing factor in cyber-attacks, and career exploration in the field.

The establishment of a seminar series to promote awareness of cybersecurity on Ashland University campus and in the local society of the City of Ashland is our next strategy. Guest speakers, who are experts in cybersecurity topics, will be invited to talk about their field of expertise and state of the art techniques used in securing computers and network infrastructure.

Our last strategy is to establish professional development opportunities for K-12 teachers in the area to heighten their awareness and understanding of cybersecurity. We are planning to offer these teachers the opportunity to participate in summer workshops. In addition, we plan to invite local high-school students, counselors, mathematics and science teachers, and other interested K-12 constituencies, to participate in our seminar series. While seminar topics might be dealing with complex issues related to cybersecurity, our plan is to make most presentations accessible to wider audiences.

4 Course Development and Update

This section provides details of newly created courses as well as updates made to several existing courses related to cybersecurity curriculum development. We have developed these courses based upon recommendations of the ACM-IEEE Task Force, who stated in their CS2013 Final Report that the "importance of security concepts and topics has emerged as a core requirement in the Computer Science discipline, much like the importance of performance concepts has been for many years" [13].

4.1 New Course Developments

The following is a list of new courses developed to incorporate cybersecurity in various programs and departments. These courses introduce students to concepts where the depth is unique to information security. Thus, these courses conform to ACM-IEEE Task Force curriculum guidelines for Group 1 of the Information Assurance and Security Knowledge Area [13].

- Penetration Testing and Ethical Hacking, a computer science course on commonly used penetration testing techniques and tools. A focus is on exploiting and malware analysis. Ethics and legal system in hacking are also covered. This course should be taken after students have taken the existing computer networks course.
- Foundations of Cybersecurity, a junior level computer science course. Topics taught in this course include network security protocols and design principles, risk management and incidence recovery, application and mobile security, and access control. This course is a follow-up of the Penetration Testing and Ethical Hacking course. and prepares students to pass security+ certification.
- Cisco Networking. The purpose of this technical computer science course is to prepare students to obtain Cisco CCNA certificate. Topics discussed in this course include LAN and VLAN setup, IPv4 and IPv6 routing and services, and troubleshooting network. This course will be a follow up course of the existing computer networks course.

4.2 Existing Curriculum Updates

In this section, we provide descriptions of cybersecurity components that are infused into existing courses. Each of these courses incorporates information security topics that are integrated into other knowledge areas that reflect naturally implied or specified topics with a strong role in security concepts and topics. Thus, these courses conform to ACM-IEEE Task Force curriculum guidelines for Group 2 of the Information Assurance and Security Knowledge Area [14].

- Programming in Java: The current computer science curriculum has two courses in the introductory programming sequence. Computer science majors take them in their first year. Integrated cybersecurity components of these courses include input and output validations, safer array indexes, canonical file path representations, safer random number generator, and software testing.
- Advanced Web Programming, a computer science elective course. It is a continuation of another computer science course on Web Design and Programming. Cybersecurity components that have been added to this course include best practices for securing dynamic websites, SSL and its utilization, including SSL certificate and their installation, security issues with user authorization, database security, OS security, and email security.

- Computer Architecture, a sophomore level computer science course that requires students to complete a data structure course and two courses in discrete mathematics. A unit addressing hardware insecurity including chip vulnerability has been infused into this course.
- Operating Systems, a required senior level computer science course. Units on security and protection have been incorporated.
- Computer Networks, an elective junior/senior level computer science course. Components of cryptography, symmetric-key and public key algorithms, and authentication protocols have been infused.
- Software Engineering, a required senior level computer science course where students complete their capstone project. The course will address common software security practices such as risk analysis, privilege issues, and sandboxing. Potential problems in software design related to security will also be covered.
- Forensic Accounting, a business course that will include coverage of how to detect and prevent accounting fraud via information systems and networks.
- Supply Chain Management, a business course that will enhance existing coverage of supply chain security and risk management, particularly regarding the protection of critical information systems infrastructure, and also risks specific to security in the cyber supply chain.
- ERP Systems, a business course that will include coverage of how to protect ERP systems from cyber-attack.

The following chart illustrates the relationship between courses that are affected in the computer science curriculum. Note that the data structures course is a prerequisite of almost all computer science courses. Thus, it is listed in the figure below though it is not been infused with cybersecurity concepts.

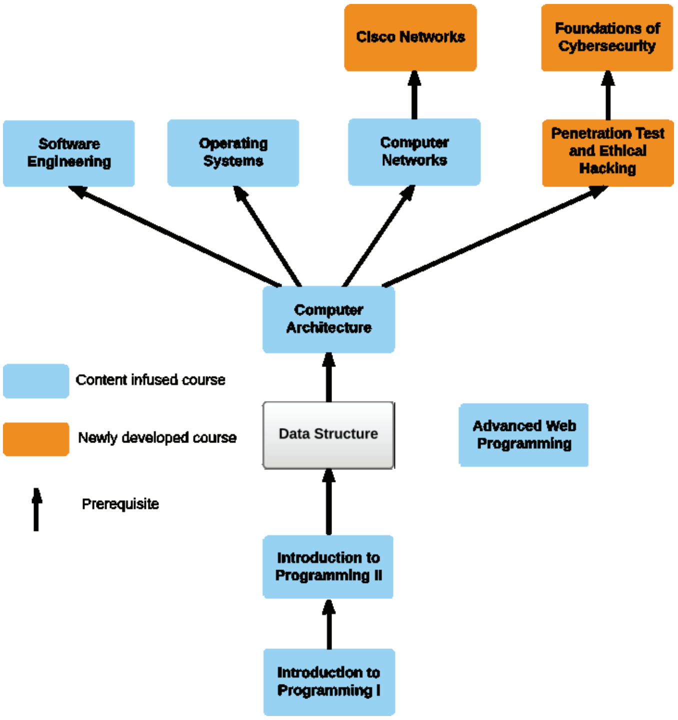

Figure 1. Courses that are either updated or newly developed related to cybersecurity

5 Conclusion and Future Work

This paper presents a case study on enhancing the computational science curriculum in a medium-sized liberal college in the context of cybersecurity. We presented the limitations of cybersecurity curriculum development in liberal arts colleges and proposed three approaches to enhance the curriculum. We provided a list of courses that are either newly proposed or with new security topics infused. In the future, we will report on the assessment of the cybersecurity minor at Ashland University including course enrollments, student responses, and industry feedback. We will also report on other enhancements made to the program including the plan to expand the internship to a full semester (12 credit hours) instead of the current requirement of 3 credit hours.

References

[1] J. M. Richards and J. J. Ekstrom, “The Cyber Education Project and IT IAS Curriculum,” pp. 173–178, 2015.

[2] A. Mcgettrick, “Toward curricular guidelines for cybersecurity: Report of a workshop on cybersecurity education and training,” pp. 1–33, 2013.

[3] D. Inserra and S. P. Bucci, “Cybersecurity Challenges and Cyber Supply Chain Security,” vol. 20002, no. 2880, 2014.

[4] A. Siraj, B. Taylor, S. Kaza, and S. Ghafoor, “Integrating security in the computer science curriculum,” *ACM Inroads*, vol. 6, no. 2, pp. 77–81, 2015.

[5] “Ashland University Catalog.” [Online]. Available: https://www.ashland.edu/admissions/majors-programs/course-catalog.

[6] C. Brown, S. Schall, J. Schultz, S. Simon, D. Stahl, S. Standard, F. Crabbe, R. Doerr, R. Greenlaw, C. Hoffmeister, J. Monroe, D. Needham, A. Phillips, and A. Pollman, “Anatomy, dissection, and mechanics of an introductory cyber-security course’s curriculum at the United States naval academy,” *Proc. 17th ACM Annu. Conf. Innov. Technol. Comput. Sci. Educ. - ITiCSE ’12*, p. 303, 2012.

[7] R. Greenlaw, A. Phillips, J. Schultz, D. Stahl, and S. Standard, “Network reconnaissance, attack, and defense laboratories for an introductory cyber-security course,” *Proc. 51st ACM Southeast Conf. - ACMSE ’13*, vol. 4, no. 3, p. 1, 2013.

[8] S. Bratus, A. Shubina, and M. E. Locasto, “Teaching the principles of the hacker curriculum to undergraduates,” *41st ACM Tech. Symp. Comput. Sci. Educ.*, pp. 122–126, 2010.

[9] T. R. Andel and J. T. McDonald, “A Systems Approach to Cyber Assurance Education,” *Proc. 2013 InfoSecCD ’13 Inf. Secur. Curric. Dev. Conf. - InfoSecCD '13*, pp. 13–19, 2013.

[10] G. S. Dardick and L. K. Lau, “Interdisciplinary Minor in Digital Forensics, Security and Law,” p. 371, 2005.

[11] F. H. Katz, “Curriculum and pedagogical effects of the creation of a minor in cyber security,” *2010 Inf. Secur. Curric. Dev. Conf. - InfoSecCD ’10*, p. 49, 2010.

[12] F. H. Katz, “The creation of a minor in cyber security,” *Proc. 2012 Inf. Secur. Curric. Dev. Conf. - InfoSecCD ’12*, pp. 75–81, 2012.

[13] ACM-IEEE Joint Task Force, "Computer Science Curricula 2013, Final Report," December 2013.

[14] I. Ajwa, R. Jacobs, P. Cao, and S. Lowes, "Integration, Collaboration & Partnerships: Building a Multidisciplinary Cybersecurity Program", Ashland University, December 2014.