Design and Development of Cybersecurity Concentration Courses and Laboratory Experiences for Undergraduate Students

Dr. Nikunja Swain P.E., South Carolina State University

Dr. Swain is currently a Professor at the South Carolina State University. Dr. Swain has 30+ years of experience as an engineer and educator. He has more than 60 publications in journals and conference proceedings, has procured research and development grants from the NSF, NASA, DOT, DOD, and DOE and reviewed a number of books on computer-related areas. He is also a reviewer for ACM Computing Reviews, IJAMT, CIT, ASEE, and other conferences and journals. He is a registered Professional Engineer (PE) in South Carolina and ETAC of ABET reviewer for Electrical Engineering Technology and Computer Engineering Technology.

Dr. Biswajit Biswal, South Carolina State University

Biswajit Biswal, Ph.D.

Biswal is working as Assistant Professor of Computer Science at South Carolina State University, Orangeburg, SC, USA since January 2017. He holds Ph.D. in Computer and Information Systems Engineering from Tennessee State University, M.S. in Electrical Engineering form NYU Tondon School of Engineering, and B.E. in Medical Electronics Engineering from India. His research interests are machine learning, data mining, cyber security, cloud computing, RF signal detection (Drones), IOT, and big data analysis. He has more than 10 technical papers published in conferences and journals. He is also a member of IEEE.

Design and Development of Cybersecurity Concentration Courses and Laboratory Experiences for Undergraduate Students

Abstract

Information and Communication Technologies (ICT) have become increasingly important for US citizens, who are becoming dependent on the use of information networks and services in their daily lives. Yet, while uptake of new technology among citizens is high, a large portion of the population remains unaware of their exposure to risks from security breaches and "cyber-abuse" in the form of network disruptions, malicious code, criminality and hackings, as well as hardware and software failures. There is an urgent need for the development and implementation of awareness-raising campaigns targeted at the safe and responsible use of ICT.

The demand for cybersecurity experts in both the public and private sectors is far outpacing the development of the talent pool, making for a hyper-competitive labor market. Against ever evolving cyber-threats the need to graduate students skilled in the concepts and technologies of cybersecurity is becoming a critical responsibility of academic institutions in order to help preserve the sovereignty of the US and her allies. Roughly two-thirds of security practitioners indicate that their organization does not invest enough in security awareness training. Professionals in the field consider it imperative for academic institutions to increase course development in computer security to make students both knowledgeable and technologically prepared for future challenges in this field. Knowledge about ongoing and planned activities will help the institutions to design and develop effective programs individually and in collaboration with others. Universities are only beginning to catch up.

The objective of this paper is to describe our experiences in the design and development of cybersecurity courses and laboratory exercises for a cybersecurity concentration for our computer science majors. The findings presented in this paper may be used by interested parties in cybersecurity curriculum and course development.

Introduction

Information and Communication Technologies (ICT) have become increasingly important for US. The 2005 U.S. President's Information Technology Advisory Committee (PITAC) report *Cybersecurity: A Crisis of Prioritization* included statistics on attacks and vulnerabilities. Data from this report shows that the total number of attacks – including viruses, worms, cyber fraud, and insider attacks in corporations – is rising by over 20 percent annually, with many types of attacks doubling in number [1]. In November and December 2015, ISACA and RSA Conference conducted a global survey of 461cybersecurity managers and practitioners. The report data reveal that almost 60 percent of respondents experienced a phishing attack in 2015 and in 30 percent of these organizations, it is occurring on a daily basis. In addition, 20 percent are dealing with insider damage and theft of intellectual property at least quarterly [2].

High-profile data breaches have become all too common in recent years with companies such as Target Home Depot and Anthem forced to own up to and handle PR nightmares following large-scale hacks. As a result, security has become a major priority for businesses both big and small -- but hackers always

seem to be one step ahead. This is especially problematic for many organizations that are simultaneously unable to hire or retain technical talent. Results indicate that cybercrime is a credible threat to enterprise resiliency as are advanced persistent threat (APT) and traditional attack vectors. The demand for Cybersecurity experts in both the public and private sectors is far outpacing the development of the talent pool, making for a hyper-competitive labor market [3, 4].

The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million, stated Michael Brown, CEO at Symantec, the world's largest security software vendor. Not long before Brown's statement, the Cisco 2014 Annual Security Report warned that the worldwide shortage of information security professionals is at 1 million openings, even as cyberattacks and data breaches increase each year. In order to solve for the severe shortage in cyber security talent around the globe, cyber security education needs to be overhauled and reprioritized and women must be encouraged to enter this largely male dominated field. This indicates a clear need to increase awareness training for employees as phishing and social engineering attack success is dependent on humans [6].

Experts agree that there is a growing need for cybersecurity professionals and universities across the country haven't caught up to the needs of the corporations. Against ever evolving cyber-threats the need to graduate students skilled in the concepts and technologies of Cybersecurity is becoming a critical responsibility of academic institutions in order to help preserve the sovereignty of the US and her allies. Universities are only beginning to catch up [3, 5].

Security programs, security tracks and certificates in information security exist, but often these courses are available only for computer science majors or majors in computer related disciplines [9]. Breaches in cyber infrastructure impact everyone, not just computing professionals. It is crucial that more undergraduate majors receive education and training that deepens their conceptual and practical understanding of issues in Cybersecurity [7, 8]. Professionals in the field consider it imperative for academic institutions to increase course development in computer security to make students both knowledgeable and technologically prepared for future challenges in this field. As a result, we should all recognize the importance of cybersecurity in the undergraduate curriculum. Our graduates must have security skills in addition to communication, critical thinking and analytical skills. This additional skill will offer our majors the opportunity to extend the security focus beyond the departments, to raise awareness outside of the computer science community, and provide a path for further studies and employment in Cybersecurity [7-15].

To address the problem of the lack of awareness and participation in Cybersecurity, we plan to use a multi-tier approach to increase capacity in cybersecurity education, training, and awareness in the undergraduate curriculum by creating a successful model of Cybersecurity education; and this reform will be based on our prior experience with the introduction of innovative teaching modules in a number of science, mathematics, and engineering Technology courses, faculty student seminar series, working in teams, use of simulation and K-17 student competitions.

Education

Almost every career path open to a bachelor's degree student encompasses some aspect of security. System administrators must be able to properly configure and maintain a system; programmers must know how to build secure software from the bottom up; web development personnel must understand the risks involved and how to best reduce the potential impact of these risks; and project managers must understand the cost/benefit tradeoffs involved with implementing secure systems. The field of security is large and rapidly changing, and one could easily offer multiple courses on computer security. As a result, we should all recognize the importance of cyber security in the undergraduate curriculum. Our graduates must have security skills in addition to communication, critical thinking and analytical skills. This additional skill will offer our majors the opportunity to extend the security focus beyond the department, to raise awareness outside of the computer science community, and provide a path for further studies and employment in cyber security. Our concentration on cybersecurity is designed to provide our students with the knowledge and skills necessary to contribute this important field and help preserve the sovereignty of our Nation. This concentration contributes to the mission of the Department, College and University as it provides education and skills to students, faculty and staff to live productively in a dynamic, global society. The primary objective of this concentration is to provide a strong foundation in cybersecurity principles, as well as practical hands-on experience. Successful students would have tools to become cybersecurity/information assurance professionals.

Cybersecurity Concentration Courses

We are of the belief that cybersecurity courses will require computing background and therefore, we decided to embedded our cybersecurity concentration courses to our CAC of ABET accredited Computer Science Program. Our Computer Science curriculum requires 124 credit hours of course work with 9 credit hours CS Advanced Electives and 9 hours general electives. We decided to use these 18 elective hours for our cybersecurity concentration curriculum courses without increasing the graduation/degree requirement of 124 credit hours. With this curriculum structure, our cybersecurity concentration graduates have a solid background both in Computer Science and Cybersecurity.

We used evidence based practices such as review of existing cybersecurity curriculum in other academic institutions, discussion with our industry partners and scholarly literate to develop courses for this concentration. We discussed the findings from all these sources and came to conclusion that our cybersecurity curriculum courses must address the following topics:

1. Security Literacy: a basic understanding of security terms
2. Security risks: a basic understanding of what is at risk (confidentiality, integrity, availability) and threat sources (such as connectivity, physical threats, etc.)
3. Spoofing: email and IP address spoofing
4. Reconnaissance software: packet sniffers and port scanners
5. Encryption: types, limitations, and uses
6. Operating system vulnerabilities: buffer overflow conditions, supplied daemons, flaws/patches
7. Denial of service: email and network attacks
8. Viruses and worms: construction and protection
9. Remote monitoring programs: basic configuration and purpose
10. Trojan horses: mechanisms and common attacks

11. Secure email: filters and hoaxes
12. Firewalls: tasks and implementation
13. Mobile code: usefulness and potential for malicious code

After number of discussions with our partners in academia and industry, we came up with six courses for our cybersecurity concentration courses as describe below:

CS 225 - Introduction to Cybersecurity
This course provides a comprehensive, trustworthy framework of practices for assuring information security. The content of the course will be based on the Department of Homeland Security and Department of Energy's Essential Body of Knowledge (EBK) for IT Security. Course includes hands-on laboratory exercises.

CS 325 - Computer Forensics
This course introduces students to computer forensics and cyber-crime scene analysis. The various laws and regulations dealing with computer forensic analysis will be discussed. Students will be introduced to the emerging international standards for computer forensic analysis, as well as a formal methodology for conducting computer forensic investigations. Course includes hands-on laboratory exercises.

CS 335 - Cryptography and Network Security
This course provides an introduction to the fundamental components of encryption. Topics include the history of cryptography, public key and private key systems, hashing and digital signatures. Topics also include the development of the Advanced Encryption Standard (AES), the use and functionality of Pretty Good Privacy (PGP) and the Secure Socket Layer (SSL). Course includes hands-on laboratory exercises.

CS 425 - Application and Data Security with Privacy
This course focuses on application and data security provides students a look at how malware infects computers, how SQL injections and DNS injections work, as well newer topics such as healthcare information systems data security and industrial control systems security.

CS 435 - Management of Information Security
This course focuses on the analysis and management of information and information systems security including processes, technology, and facilities.

CS 489 – Cyber Security Capstone
Students will be required to complete a practical project on Cyber Security. Students will use their knowledge from previous courses to complete this project. The project topics will be decided in consultation with DOE labs, federal agencies and others. Students will be required to submit a final project report and present their project findings in class. The presentations may be conducted in a virtual environment to allow participation of members at a distance. Instructor will provide guidelines for the project.

Concentration Learning Outcomes

Upon completion of the Cyber Security Concentration, graduates will have the ability to:

- Discuss in depth the origins, nature, and current issues in cybersecurity and its related activities using precise terminology
- Apply a range of cybersecurity concepts to mitigate risks in cybersecurity operations
- Develop solutions for networking and security problems, balancing business concerns, technical issues and security.
- Effectively communicate technical information verbally, in writing, and in presentations.
- Use appropriate resources to stay abreast of the latest industry tools and techniques analyzing the impact on existing systems and applying to future situations.
- Explain the concepts of confidentiality, availability and integrity in Information Assurance, including physical, software, devices, policies and people. Analyze these factors in an existing system and design implementations.

These concentration outcomes enable CAC of ABET learning outcomes for computer science and cybersecurity. Some of the practices that are used in these courses are team work, term paper and presentations, simulation exercises, hands-on activities, and guest speaker series. These activities are well liked by students and it helps them in their understanding of the subject matter and helps them in summer internships.

The Concentration Approval Process – The approval process for course/minor/concentration/degree programs consists of the following six (6) sequential steps: (a) Approval by the Department/College Curriculum Committee, (b) Approval by the ED. Policy Council, (c) Approval by the Faculty Senate, (d) Approval by the Board of Trustees and President, and Approval by the South Carolina Commission of Higher Education (CHE) and SACSCOC if needed.

Our cybersecurity concentration proposal went through all these processes successfully except SACSCOC and we started offering the curriculum courses from 2015.

Laboratory Modules

Laboratory modules are used for teaching, research and outreach, and the design of laboratory modules reflect these uses. We use two different laboratory settings for our cybersecurity concentration courses – virtual and face-to-face.

The virtual laboratory is from the NDG NetLAB+ (*https://www.netdevgroup.com/content/cybersecurity*). This platform provides our students with laboratory experiences on number of cybersecurity and computer science topics in an online environment. Our students conduct experiments in *NISGTC Security+*, *NISGTC Network Security*, *NISGTC Forensics*, *NISGTC Ethical Hacking*, *CSSIA CompTIA Security+*. This laboratory is also used by our academic partners at a distance.

The face-to-face to laboratory is designed with laboratory units/workstations from Marcraft (https://tech-labs.com/products/marcraft-cyber-security-essentials-concepts-practices). We use these workstations/units to provide our students with hands-on laboratory experiences on *application security*,

medical security, enterprise security, network security and ethical hacking. Both NDG labs and Marcraft labs are easy to use and pre-designed labs with instructions.

Professional Development and Awareness

We have conducted number of Cybersecurity outreach activities for our students and students from K-17 schools during last five years. Some of these activities are hands-on activities on physical security, summer workshops on Linux and Raspberry PI, Thunderbird cup competition through Sandia National Lab, Raspberry and Lego activity through Lawrence Livermore National Lab, Introduction Digital Forensics, Cyber patriot competition, and cryptography. Our students have participated in cybersecurity competitions such as Palmetto Cyber Defender Competition and hackathon events. We have provided workshops in Cyber Security for selected faculty and staff members from SC State and local K-12 schools. The workshops are usually conducted during each summer.

Since an early infusion of the STEM concepts into the young minds can increase the enrollment, we plan to conduct K-17 outreach program. One of the key objectives of this outreach program is to expose students to cybersecurity concepts especially Cybersecurity fundamentals, cryptography, ethical hacking and computer forensic. Our cybersecurity experience will help us in designing hands-on activities suitable for K-17, especially 6-12 grade classrooms.

These activities engage students in solving a given problem or implementing a certain task, thereby enhancing their imagination ability and creativity. In our K-17 outreach programs, our objective will be to enable students in bringing their ideas into life. Educating teachers is a vital component in this outreach program. This is because it is the K-17 teachers who can provide students an everyday experience of computing/cybersecurity concepts through afterschool programs or by infusing the concepts in the curriculum.

In order to educate the K-17 teachers we plan to host workshops and training programs for teachers. The workshop will include lectures on various Cybersecurity concepts and instructive sessions on pedagogical teaching tools and methods. The workshops will also include sessions that aim at changing the perception of teachers and discussing the potential benefits of STEM infusion in school. The K-17 outreach program also helps to develop a bond and familiarity between students and STEM faculty in SC State and hence it is easier to recruit them into the STEM discipline. Each teacher completing the workshop will be provided with a free Raspberry PI kit to pursue their interest in their classrooms and schools.

Outreach activities

Three faculty and ten students of the Department of Mathematics and Computer Science are currently involved in a project dealing with K-12 outreach activities in local schools. The department is also working on arrangements to extend these activities to other local schools. The central theme of this K-12 outreach is “Computational Thinking Using Hands-On Activities” such as introduction to Excel, PowerPoint, Robotics, and Visual Programming. These K-12 outreach activities are supported through a project titled - STARS (Students & Technology in Academia, Research & Service) Alliance. The primary objective of the STARS project is the broadening of participation in computing through best practices and community building. Provisions will be made for **v**isits to these and other K-12 schools to

advertise the program and make presentations on Cyber Security. We plan to make few of the Cyber Security courses and modules online to K-12 school teachers, local two year and four year college teachers and others interested in Cyber Security education and awareness.

For outreach and professional development activities, the participants evaluate all program activities regarding the relevance and presentation of information, pointing out the program's strengths and weaknesses. Of course, they are also provided with the opportunity to write or discuss additional comments or concerns. These findings are analyzed and used to improve the activities such as reducing the presentation time and devoting more time to hands=on activities.

Assessment and Evaluation

The assessment of our cybersecurity concentration courses are primarily through student evaluation of courses. These evaluations are conducted by our university assessment center and the results are shared with the responsible faculty and the department chair. The results are analyzed by the department and used for continuous improvement. Also, we receive feedback from student summer internship mentors and use this information to improve our curriculum and teaching methodology. Table 1 shows course evaluation results for our cybersecurity courses during the last three years. The evaluation results for each course is above 90% and therefore, needs no improvement.

Table 1. Cybersecurity Course Evaluations during last three years

Course Number	Number of Students Responding to Survey	Average Score (Out of 5)	Does the course meet the performance measure score (85%)?
CS 225	10	4.80 (96%)	Yes
CS 325	17	4.63 (92.6%)	Yes
CS 335	2	4.91 (98%)	Yes
CS 425	7	4.98 (99.6%)	Yes
CS 435	3	4.85 (97%)	Yes
CS 498	4	4.95 (99%)	Yes

Summary and Conclusions

Our cybersecurity activities have been possible because of generous grant from National Nuclear Safety Agency (NNSA). Our cybersecurity concentration program has 35+ majors, and we have graduated 3 students from this concentration, and we will be graduating at least 5 students from this concentration in May, 2019. Some of our concentration majors have summer internships in cybersecurity with Lawrence Livermore National Laboratory (LLNL), US NAVY/SPAWAR, Norfolk State University, and others. They have participated with hackathons, and cybersecurity competitions such as Southeast Collegiate Cyber Defense Competition (SECCDC) and Palmetto Cyber Defense Competition (PCDC). Participation in these activities along with summer internships have provided them with knowledge to address real life cybersecurity issues and threats.

We are in the process of completing our application to NSA Center of Academic Excellence program (CAE) (https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae). We have completed mapping our cybersecurity course content to the cybersecurity Knowledge Units (KUs) and we collecting documents for the other criteria elements. We plan to complete this process within the next 2 months and submit our application to NSA for the CAE designation. Table 2 shows the draft mapping of our courses to the knowledge units (KU) of NSA CAE designation. Table 3 summarizes our cybersecurity activities before and after 4 years of the

Table 2 – Draft KU Mapping (CAE-CD Application)

Knowledge Unit (KU) Type	No.	Knowledge Unit (KU)	Computer Science/Cybersecurity Courses
Foundational	1	Cybersecurity Foundations	CS 225, CS 435, CS 425
	2	Cybersecurity Principles	CS 435, CS 401, CS 335
	3	IT System Components	CS 225, CS 335, CS 425
Technical Core	4	Basic Cryptography	CS 335, CS 225
	5	Basic Networking	CS 420, CS 335, CS 225
	6	Basic Scripting and Programming	CS 151, CS160, CS 170, CS 260, CS 318
	7	Network Defense	CS 335, CS 325, CS 225
	8	Operating Systems Concepts	CS 401, CS 225
Optional	9	Advanced Cryptography	CS 335, CS 420
	10	Advanced Network Technology and Protocols	CS 420
	11	Cyber Crime	CS 225, CS 325, CS 435
	12	Data Structure	CS 280
	13	Digital Forensics	CS 325
	14	Host Forensics	CS 325
	15	Media Forensics	CS 325
	16	Network Forensics	CS 325, CS 335
	17	Network Technology and Protocols	CS 420
	18	Operating Systems Theory	CS 401
	19	Penetration Testing	CS 425
	20	Vulnerability Analysis	CS 425, CS 225
	21	Web Application Security	CS 425
	22	Algorithm	CS 280, CS 320

Table 3 below summarizes our cybersecurity activities before and after 4 years of our K-20 cybersecurity workforce development grant form National Nuclear Security Agency (NNSA) grant.

Table 3 – Summary of Activities

Summary of Activities – Before and After "K-20 Cybersecurity Workforce Pipeline Development" Grant		
Before Grant	After 4 years of the	Planned/On-Going
• 1 Introductory course • Limited offering • No formal labs • Limited K-12 outreach activities • No faculty/staff hires for cybersecurity • Limited research activities (3 cybersecurity related external funding proposals submitted) • No cybersecurity Internships • 10 students	• Concentration in Cybersecurity for CS Majors with 6 course sequence • CHE approved curriculum • Courses offered during each semester and summer • 2 new Cybersecurity Labs • New faculty and staff hires (2 faculty and 1 staff) for CS and Cybersecurity • Student Summer Cybersecurity Internships at LLNL & NASA (3 students) • Student internships with faculty at SC State • Enhanced grant writing activities (8 proposals with cybersecurity components) • Enhanced K-12 outreach activities – Summer workshops and Weekend School visits • 35+ new students at different stages of the concentration program • Minor in Cybersecurity for all majors with 5 courses • Student participation in Cybersecurity Competitions (SECDC, PCDC) and Hackathons (SODACITY HACKATHON BY CAPGEMINI 2018 - 1st prize; CUHACK by Clemson University, January, 2019 – 2 first	• Center of Excellence in Cybersecurity Proposal – Spring 2019 • Center of Academic Excellence (CAE) Application to NSA/DHS, May 2019 • Student Participation in SECDC, PCDC, and Digital Forensics Competitions (Feb – April, 2019)

	place Awards) • World of Microcontrollers – Hands on session to juniors and Seniors at the South Carolina Governors School of Science and Math (SC GSSM), January 12, 2019.	

Acknowledgement

The cybersecurity activities described in this paper are supported by grant from NNSA/DOE (DE-NA20002686) and Subaward number (F1040061-14-10). The authors wish to acknowledge this support and thank NNSA for this grant.

References

[1]. President's Information Technology Advisory Committee (PITAC), Cyber Security: A Crisis of Prioritization (Feb. 2005).

[2]. State of Cybersecurity: Implications for 2016 - An ISACA and RSA Conference Survey. Retrieved from https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

[3]. Top U.S Universities failing at Cybersecurity Education. Retrieved from https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html

[4]. Can higher education fix the cybersecurity shortfall? – Retrieved from http://www.schools.com/articles/cybersecurity-shortfall

[5]. D. Rowe, B. Lunt, J. Ekstorm, "The Role of Cyber-Security in Information Technology Education" - *SIGITE'11*, October 20–22, 2011. 3

[6]. Cybersecurity job market to suffer severe workforce shortage. Retrieved from *https://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html*

[7]. L. Clinton (2009). "Education's Critical Role in Cybersecurity" - *EDUCAUSE Review*, vol. 44, no. 5, 60–61.

[8]. R. Raj, S. Mishra, C. Romanowski, T. Howles (2008), "CyberSecurity as General Education", 15th Colloquium for Information Systems Security Education (CISSE 2011), Fairborn, Ohio, June 2011. 5

[9]. G. Meiselwitz, Information Security across Disciplines - *SIGITE'08*, October 16-18, Cincinnati, Ohio, USA.

[10]. Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, (4), 3–4.

[11]. Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber Education: A Multi-Level, Multi-Discipline Approach. In *Proceedings of the 16th Annual Conference on Information Technology Education* (pp. 43–47). ACM.

[12]. Cahoun (2017). Incorporating Blended Format Cybersecurity Education into a Community College Information Technology Program, Community College Journal of Research and Practice ,Vol. 41, Iss. 6.

[13]. Yang and Wen (2017). Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States, Journal of Education for Business Vol. 92 , Iss. 1.

[14]. Developing a Comprehensive Cybersecurity Curriculum with a Collaborative Learning Environment, National Cybersecurity Institute Journal, 2(2), 5-15.

[15]. Cybersecurity Outreach for Underrepresented Minorities, National Cybersecurity Institute Journal, 2(2), 17-28.