

# An Undergraduate Cyber Operations Curriculum in the Making: A 10<sup>+</sup> Year Report

Shiva Azadegan, Michael O'Leary  
Towson University  
{sazadegan, moleary}@towson.edu

**Abstract**— In fall 2002, Towson University launched an undergraduate computer security track within its computer science program. This program was the first undergraduate program in the state of Maryland with a strong and technical computer security focus and among the first in the country addressing the shortage of skilled cybersecurity professionals. Since its inception, this program has gone through several assessment cycles and curricular revisions to stay current with the demands of ever-evolving cybersecurity discipline. These revisions allowed the program to meet the rigorous requirements of the NSA Cyber Operations program, and in 2014, Towson University was designated as one of fourteen National Centers of Academic Excellence in Cyber Operations. This paper describes the current curriculum for the track and discusses lessons learned and challenges faced during the past fourteen years. We believe our undergraduate cyber operations program, developed, evolved and tested at a large public institution with students with widely-differing academic and socio-economic backgrounds provides a valuable model for adopting and adapting at other institutions interested in starting such programs.

**Keywords**— Computer Science Education, Cybersecurity Education, Cyber Operations.

## I. INTRODUCTION

The lack of trained and educated cybersecurity workforce is a serious challenge facing our nation. The demand for cybersecurity professionals far exceeds the supply and is expected to continuously rise globally [1] for the foreseeable future. Cybersecurity education has never been as important as it is today and plays a crucial role in addressing the need for the skilled cybersecurity workforce. This need has been clearly recognized at the highest levels of government, as evidenced by the number of Presidential Executive orders and government programs [2,3,4,5] aimed at increasing the number of information assurance and security professionals.

Towson University, a pioneer in cybersecurity education and a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) since 2002, launched an undergraduate computer security track [6] within its computer science program in Fall 2002. This program was the first undergraduate program in the state of Maryland with a strong and technical computer security focus and among the first in the country addressing the shortage of skilled cybersecurity professionals. The security track was added to our ABET accredited Computer Science program which provides the theoretical and mathematical foundation for the security courses. Over the past 14 years, the track has gone through several assessment and revision cycles to stay current with the

demands of ever-evolving cybersecurity discipline and to meet the rigorous requirements of the NSA Cyber Operations program [5]. In 2012, TU received a \$2M CyberCorps Scholarship for Service [4] grant providing support for qualified students in this program, and in 2014, TU was designated by the NSA as a National Center of Academic Excellence in Cyber Operations.

In this paper, first we describe the current curriculum for this program; second, we discuss the resource requirements for offering and managing such programs; third, we highlight some the outside the classroom activities that have enhanced the quality of and attracted students to this program; and last, we share some of our challenges faced during this period.

## II. THE TRACK

Cybersecurity programs are widely varied in content and program intent. The main objective of our program was to develop a technical undergraduate security program that builds upon the core computer science courses, allows students to complete their degree in four years, and provides students with ample opportunities to work on applied and hands-on projects to equip them with the skills needed to join a highly demanding cybersecurity workforce. The difference between our general CS program and the CS with a track in computer security program is that the breadth provided by the upper-level CS elective courses in the former was replaced with the depth provided by the security courses in the latter. The original list of security track courses was [6]:

1. Computer Ethics
2. Introduction to Computer Security
3. Introduction to Cryptography
4. Network Security
5. Application Software Security
6. Operating Systems Security
7. Case Studies in Computer Security

This program has evolved over time. The computer ethics course is now a required course for all our computing majors and the introduction to Cryptography course satisfies an upper-level math requirement for our CS majors. The original Introduction to Computer Security course was taken by both security and non-security students as was designed to provide students with a broad overview of technical and human components of information systems security. The security track students found much of that material redundant and covered in

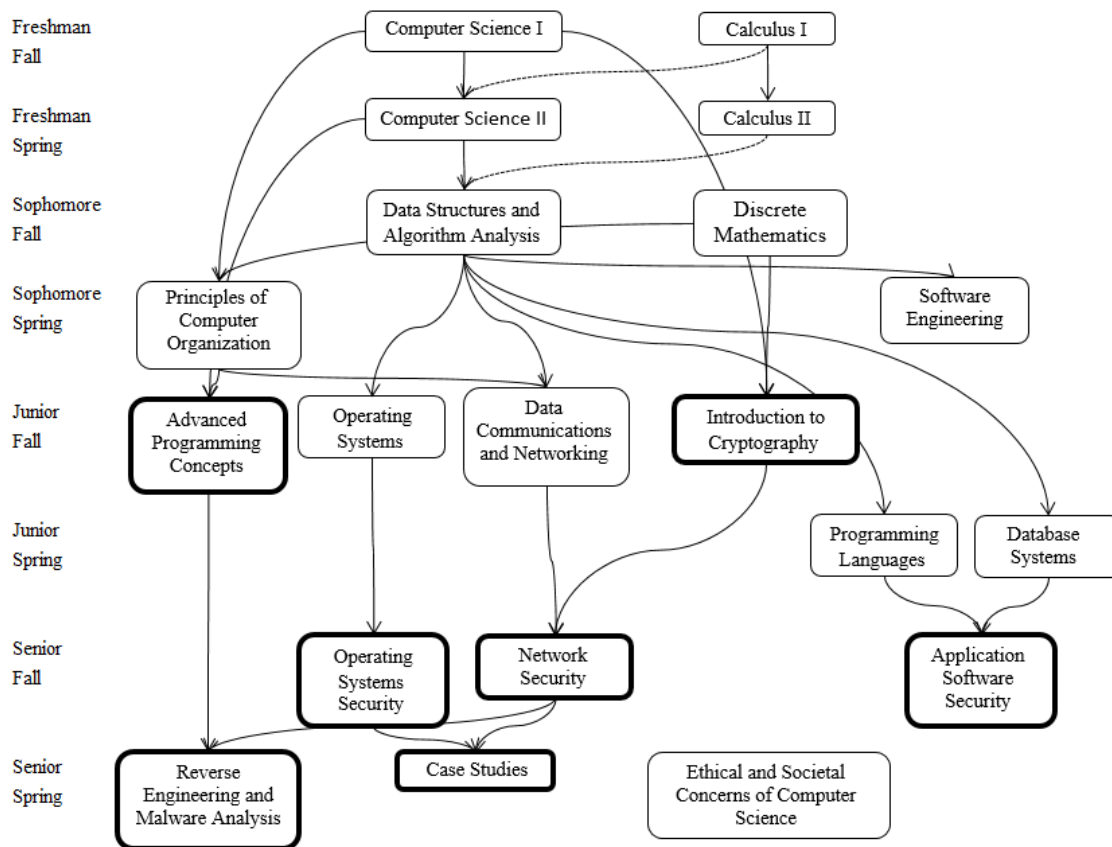


Figure 1: Typical sequence of courses

more detail in other courses. In 2012, that requirement was dropped from the track.

Instead, to better meet the more rigorous requirements of the Cyber Operations designation, two new courses were developed and are now required. The first course is Advanced Programming Concepts. Our CS1/CS2 sequence is taught in Java; these programming courses are taken by all of our majors. Cyber security students also need to be proficient in C and assembly language; these are the topics covered in this course. Moreover, to promote secure coding principles from the very beginning, we have been using Security Injection modules [7,8] in our CS0, CSI and CSII courses since 2008.

The second major change was the addition of a course in malware analysis and reverse engineering; this has as prerequisite the Advanced Programming Concepts course. Students in this course do more than learn the basics; their final project involves the reverse engineering of live malware.

This course is now a partner to our capstone course, Case Studies. In this course, students are broken into teams of 3-6 that build progressively more sophisticated business networks. During three live fire exercises each team attempts to defend their network while trying to attack the networks of other teams.

A Red Team of program graduates and other industry and government professional friends of the program come in and attack all of the student teams. Once the live fire exercise concludes, the student teams perform forensic analyses on their systems and write a report detailing what worked, what didn't, how they were attacked and identify the attacker(s). A textbook, *Cyber Operations* [9] has been written for the course that shows students how to set up, defend, and attack networks. The current state of the curriculum is summarized in Figure 1 that shows a typical path through the program including course prerequisites. Security track courses are depicted in bold. University core requirements and some math and science courses are not included.

Our current curriculum is now well aligned with the CERT approach to Cybersecurity workforce development [10]; the computer science core courses provide the necessary knowledge building, the junior level security courses develop skills, while the capstone courses (Case Studies; Reverse Engineering and Malware Analysis) give student the necessary experience.

### III. RESOURCES

The success of our program is in large measure due to our dedicated and outstanding faculty. We have sixteen faculty members in our department who are conducting research in

information assurance related areas, with ten of them intimately involved in teaching the security track courses and managing the program. Computer security is a rapidly evolving field, with new attacks and new defensive techniques being developed daily. Cyber security faculty need to keep current, and as such none are expected to teach more than one undergraduate security course per year. It is important for schools considering starting a new cybersecurity program to recognize that a large core group of faculty with diverse research areas is needed to support a cybersecurity program.

All our security classes are conducted in an isolated security laboratory; it was originally funded by a grant from the National Science Foundation and was designed based on the Information Warfare Analysis and Research (IWAR) laboratory [11] at West Point. A dedicated isolated laboratory is an integral and vital part of any cybersecurity program. Moreover, due to the participatory and active learning methods used in our security courses, small class size has been proved essential and necessary for effective and quality instruction. We maintain an enrollment cap of thirty students for these classes.

Another key factor for maintaining an up-to-date cybersecurity program is a commitment by the institution to provide adequate funding for professional development opportunities, as well as continued effort by the faculty to apply for external funding for capacity building and curriculum development. During the past fourteen years, our faculty have regularly published and participated in information assurance conferences and summer workshops, have been at forefront of cybersecurity education initiatives, and have secured over \$1 million in external funding for capacity building and curriculum development projects.

Connections with industry practitioners are vital. They provide feedback on the curriculum and help us keep it current and meet industry needs. The Case Studies course requires a talented group of volunteers to act as Red Team; these industry professionals also help the students' professional development through mentoring and help in job placement.

#### **IV. LEARNING OUTSIDE THE CLASSROOM**

What takes place outside the classroom is often as important or more important as what happens inside the classroom. We have developed a vibrant and active Computer security club. This past winter, a group of students ran a wildly successful workshop for students interested in cyber security. The organizers developed a range of challenges from password hacking to network traffic analysis to simple devices (Raspberry PI) to a more complex attack on a live system. Experienced students sat with the newcomers to provide guidance and assistance. The event was so successful that the room ran out of chairs and an emergency pizza run had to be made.

We have also participated extensively in various collegiate cyber defense competitions; student teams won the Maryland Cyber Challenge in 2011, and the mid-Atlantic Collegiate Cyber Defense Competition in 2010, 2012, and 2014. The team

meets and practices regularly throughout the year. The number of available competitions continues to increase, and there are now competitions at a variety of skill ranges from novice to expert. Coupling this with increased student interest, we have found it necessary to split our efforts into two teams, a novice team that focuses on the lower level competitions, and an advanced team for the more sophisticated competitions.

Trips to information assurance conferences contributes significantly to students' experience, motivating them to take a more active role in their professional societies and introduce them to new ideas. Within the past five years our students have presented the results of their undergraduate research projects at Security BSides conferences, attended Women in CyberSecurity conferences (WiCys), and enjoyed BlackHat conferences. Attending WiCys Conferences has been an empowering experience for our female students, as they have an opportunity to connect with and be a part of a much bigger community of women in cybersecurity. We have used this conference as a means of recruiting more female students to our program by encouraging our freshman and sophomore students to attend the conference. Registration fee and hotel expenses are fully covered and partial travel grants are offered by the conference organizers and sponsors.

We host a vibrant monthly cybersecurity seminar series throughout the academic year, allowing students to hear from and interact with cybersecurity experts and practitioners from industry and federal agencies. The seminars have been extremely well attended and well received with standing room only at some. They provide spaces for exposure to real-world cybersecurity topics, attacks and vulnerabilities; hearing about cybersecurity careers and internship opportunities; mentoring and networking, as well as, recruiting. We have also noticed a much more diverse audience in these seminars than we see in our classrooms. We are hoping that these seminars will motivate and attract more minority students to our CS with a security track program.

#### **V. CHALLENGES**

One of our main challenges, which sadly is not unique to our program, is to attract and recruit more students from underrepresented groups. The percentage of students from the underrepresented groups for this program has been consistently lower compared to that of our computer science program. From the one hundred and forty students who have graduated in this program, 10% have been female students, 3% were African American students and less than 2% were Hispanic students. For the first eight years, the track attracted only white male students. This year, however, we had six female students (27%) in the capstone class which has been the largest cohort of female students, thus far. A trend that we hope continues to grow!

To date, we have offered one section of each security track course per year. With the continued growth and popularity of the security classes, we have reached our enrollment capacity

and are forced to offer multiple sections, which require additional resources and qualified faculty.

Cybersecurity is a relatively new and emerging area and there is a huge demand in the government, industry and academia for the PhD graduates in this field. Another challenge that we have faced during the past several years is recruiting and hiring qualified tenure-track faculty in cybersecurity. It is difficult to recruit faculty with applied and practical experience.

Faculty supporting the program need to have sufficient time to (1) keep up with current trends and developments in the field, (2) maintain their professional connections with industry and practitioners, and (3) work with students outside the classroom, especially in time consuming endeavors like coaching the cyber defense teams.

## VI. CONCLUSION

In this paper we described the current curriculum of and the revisions made to the undergraduate security track embedded within our ABET accredited computer science program. The track was designed with a strong technical focus, which was retained and enhanced throughout the several revision cycles during the past fourteen years. The program provides fundamental and theoretical computer science and mathematics through its computer science curriculum and its required thirty credits of math and science courses; provides cybersecurity related skill building courses through four junior level project-based security courses; and provides experiential cybersecurity skills through its two capstone courses. Our graduates have been in demand and actively recruited by the federal and government agencies as well as the private sector.

We believe our program provides a viable undergraduate cybersecurity education model for addressing the shortage of cybersecurity skilled professionals. The program developed and assessed and evolved at a large public institution with a diverse student body, and it can be easily replicated at other institutions with a strong computer science program.

Next year, we are planning to pilot a research-based course for our advanced students who like to learn about emerging security topic areas.

## ACKNOWLEDGEMENT

This work was supported by the National Science Foundation under grant No. DUE-0113783.

## REFERENCES

- [1] K. Evans, and F. Reeder, "A Human Capital Crisis in Cybersecurity, Technical Proficiency Matters." Center for Strategic & International Studies, November 15, 2010.
- [2] Homeland Security. National Strategy to Secure Cyberspace. Retrieved June 3, 2016 from <https://www.dhs.gov/national-strategy-secure-cyberspace>
- [3] NICSS. National Centers of Academic Excellence (CAE). Retrieved June 3, 2016 from <https://nics.us-cert.gov/education/national-centers-academic-excellence-cae>
- [4] US Office of Personnel Management. CyberCorps: Scholarship for Service. Retrieved June 2, 2016 from <https://www.sfs.opm.gov/>.
- [5] National Centers of Academic Excellence in Cyber Operations. Retrieved June 2, 2016 from <https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/>
- [6] S. Azadegan, M. Lavine, M. O'Leary, A. Wijesinha, and M. Zimand, "An Undergraduate Track in Computer Security". Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education, Vol. 35, No. 3, June 2003.
- [7] B. Taylor, and S. Kaza, "Security Injections: Modules to Help Students Remember, Understand, and Apply Secure Coding Techniques." Proceedings of the ACM Conference on Innovation and Technology in Computer Science Education, June 27-29, 2011.
- [8] Security Injections @Towson – Cybersecurity Modules for Computer Science Courses. Retrieved June 3, 2016 from <http://cis1.towson.edu/~cssecinj/>
- [9] M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, Apress, October 2015.
- [10] M. Baker, "State of Cyber Workforce Development." Software Engineering Institute, Carnegie Mellon University, August 2013. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=83504>
- [11] J. Schafer, D. Ragsdale, J. Surdu, and C. Carver, "The IWAR range: a laboratory for undergraduate information assurance education." Journal of Computing Sciences in Colleges, Volume 16 Issue 4, 2001.