How Do We Teach Cybersecurity?: Cybersecurity as an Interdisciplinary Study at the University of Virginia

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Samuel Y Ahn

Spring, 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Kent Wayland, Department of Engineering and Society

How Do We Teach Cybersecurity?: Cybersecurity as an Interdisciplinary Study at the University of Virginia

CS4991 Capstone Report, 2024

Samuel Youngjin Ahn
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
sya5jv@virginia.edu

ABSTRACT

Cybersecurity is a growing and increasingly important discipline in computer science, but it is notoriously difficult to teach at an undergraduate level as technologies constantly change, the prerequisite requirements are dense, and the field is heavily based on deep understanding and application skills. To work around these difficulties and better teach cybersecurity at UVA, I recommend changes to the UVA CS department to teach cybersecurity skills and knowledge more effectively to prospective CS engineers by addressing curriculum and teaching ideologies and methodologies, with the goal of improving education, retention, and real-world applicability. I also recommend changes to the UVA B.A./B.S. CS cybersecurity policy such that students will be able to utilize their time and training in academia as credible and valuable credentials after graduation to bolster and accelerate applications of taught skills in future occupations. In this way, students of the new curriculum will better learn cybersecurity in greater depth, benefit from acquiring a real-world applicable skill set, and gain proper recognition and qualification for time spent training at university. To address flaws in the current curriculum and brainstorm potential solutions, further work is needed for detailed analysis and implementation of these ideas.

1. INTRODUCTION

As it currently stands, the cybersecurity courses offered as a part of the CS curriculum sufficiently teach the general theory and elementary understanding of common topics in cybersecurity, but leave room for improvement, as there remains inefficiency and untapped potential for a greater depth of learning within the curriculum. Inefficiencies in current courses are present in the form of overlapping curriculum, methodology of teaching, and the structuring of cybersecurity courses as standalone, supplemental elective courses as opposed to a series of connected but independent courses.

The undergraduate CS curriculum does not train its students for more “real-world” or “on-site” applications in post-education opportunities. Instead, it teaches students the ability to quickly grasp and learn ideas in computer science through classes that teach the fundamentals in-depth and the learning process for diverse topics. For example, a Data Structures and Algorithms class may not exhaustively teach data structure and algorithms but, instead, would teach essential topics such as binary search trees or Dijkstra’s shortest path algorithm along with how to approach problems with algorithmic thinking and an understanding of how to apply a data structure for a given problem.

The cybersecurity classes within the UVA CS curriculum also follow this ideology of courses within the department, focusing more on teaching students the general outline of important topics with a strong emphasis on learning the surface-layer content of cybersecurity. However, this leaves a few areas recognized as important but left only briefly covered within the curriculum, such

as how to approach problems from an attacker or defender point-of-view. To address this issue, I recommend altering the curriculum slightly to rebalance priority and give enough attention to critical cybersecurity skills to ensure that students graduate with a stronger start in developing their skills in the field.

Inefficiencies in teaching methodologies within the cybersecurity courses also exist. This element usually relies heavily on course professors and their personal methods of teaching cybersecurity. It is worthwhile to determine which methods make for the most effective teaching of knowledge, skills, and intuition in cybersecurity. We will investigate specific methods that are most successful in achieving the goals of the new curriculum in which lecture delivery methods, course assignments, examinations, and overall curriculum design are critical elements.

Another problem with the curriculum is the availability of courses. This problem is multifactorial, with problems relating to a lack of staff to teach the courses, a lack of course variety to instruct students, a lack of space in the currently offered courses, and competition for schedule space with other classes. Some of these problems are harder to address than others, such as adequate staffing and space, but we can address the other issues through changes in the curriculum.

The large scope and wide variety of topics necessary to cover cybersecurity strains the structure of the courses. Currently in the new curriculum (2019 onwards), only two courses exist in the cybersecurity focal path. The issue with the information required to teach cybersecurity is that there are too many topics to cover to put into a small number of classes; however, if addressed separately, these topics are often not broad enough to take up an entire semester-long course.

Another issue within the larger scope of cybersecurity is a student population that is diverse and has wide-ranging familiarity with topics. Some students come into the program with little to no experience, learning the contents for the first time. Other students come in with specific and selectively specialized information in some topics, leaving them with the need to take a class for which they already have sufficient knowledge in order to gain credit enabling them to move on to a post-requisite class. Their options are to take the class in order to gain the credit needed to complete the cybersecurity focal path; or not take the class to avoid wasting valuable schedule space and opting to take other courses instead.

2. BACKGROUND

UVA's cybersecurity courses themselves are a mix of core classes and additional special topics courses; core classes being Introduction to Cybersecurity (ICS) and Defense Against the Dark Arts (DADA) (a lower-level look at cyberdefense. Previously taught special curriculum courses include Network Security, Hardware Security, Privacy in the Internet Age, AI-Powered Cybersecurity, Data Privacy, Cybersecurity and Elections, Cyber Forensics, Penetration Testing, and more.

ICS serves as a general introduction to many topics in cybersecurity for the other classes in the curriculum. DADA serves as a more in-depth class that further explores topics from ICS. While these classes cover a decent portion of cybersecurity, they are too tightly scheduled to explore their topics deeply and do not cover specialized topics that would be found in special topics courses that should be fundamental.

As a student of the pre-2019 curriculum cybersecurity focal path, as well as a teaching assistant for ICS and Network Security for over a year, I lay out specific issues to improve the program from both a student and teaching perspective. I also provide insights from members of the cybersecurity faculty and national award-winning UVA cyberdefense team members.

3. RELATED WORKS

Existing literature specifically on an undergraduate cybersecurity focus within a computer science major is mostly limited to the curriculums and ideologies of college and university programs. Works for specific curriculums that balance between a general computer science program with a cybersecurity focus, instead of programs that are exclusively

cybersecurity, certification-only, or continuing education, including the Virginia Tech College of Engineering's B.S. Computer Science—Major in Secure Computing curriculum, Carnegie Mellon School of Computer Science's Undergraduate Concentration in Security & Privacy, and Georgia Tech College of Computing's School of Cybersecurity and Privacy.

Undergraduate programs that also provide certification include George Mason University College of Engineering and Computing's B.S. Computer Science program's undergraduate certification, Rochester Institute of Technology School of Individualized Studies program's certification policies, and the University of Arizona College of Applied Science and Technology's interdisciplinary certificate program.

4. PROPOSAL DESIGN

UVA classes can cover more depth, correct inefficiencies in teaching methodologies, address issues in availability, scope, and schedule, and accommodate students who have differing skills and needs from the curriculum. Many of the topics in the cybersecurity classes cover its contents at a very general level. UVA cybersecurity courses often only theoretically introduce security topics and only explain the content, provide examples through assignments that explore the concept simply, and make memorizing and understanding theory the main goal of the class. Although this appears sufficient, due to the brevity and generality of the content, students only know the gist of the main ideas, and find themselves unable to retain and apply their knowledge from these classes. This problem stems from a combination of limited class time, a theoretical-based teaching approach, and a scope that is too broad to cover in one or two semester-long courses.

The first solution to alleviate these problems would be the restructuring of cybersecurity classes by segregating topics into their own semester-long courses. An approach to this solution may be to keep ICS as is as a general introductory course that serves as the class that teaches the base knowledge for each course that sets up deeper learning for other classes but specializes DADA into a cyberdefense course that specializes in low-level and memory defense instead of general defense. Other topics that can be taught as specialized classes might include a web security class teaching database security, web server protection, and web programming vulnerabilities; a networks security class different from the existing class that focuses on primarily networking protocols at different layers and protection of traffic through tools like firewalls and other software; a memory persistence course that focuses on highly specific information in memory hardware, vulnerabilities, and exploits; a class on computer and internet privacy like CMU's Engineering Privacy in Software course (CMU, n.d.); or even sociopolitical cybersecurity with cybersecurity in cyberwarfare, social engineering, and the sociopolitical and ethical implications in applications of cybersecurity in the modern world of cyber illiteracy like UArizona's National Security Policy course (UArizona, n.d.). Professors can work together to ensure that courses work well together separately and do not overlap while also not being overly dependent on one another.

This solution solves a myriad of the aforementioned problems, allowing more students to enroll for these classes, teaching students cybersecurity topics more in-depth to better provide fundamental knowledge, and giving professors more time to teach course content without feeling pressured to cram too much information into one class and rush its conveyance.

Another solution in conjunction with the previous one that addresses this problem would be to stray away from a majorly expository, theory-based teaching methodology and balance education with more application, reverse-engineering, and attacker/defender perspective not only to develop essential knowledge, but also independent logical and systematic thinking that can be applied to current and future problems, and develop more hands-on experience. In cybersecurity, simply understanding the problems and their solutions is not enough. Students will be more successful if they are able to understand the application and thought process of cyber offense

and defense. One way to develop an understanding of the process would be to teach students guidelines for thinking, and then encourage them to innovate and plan ways to execute an original attack, given the conditions of vulnerable software. Another way would be the incorporation of applied cybersecurity in capture-the-flag work, creating and maintenance of systems, and red-team (offensive) and blue-team (defensive) practices within classes. Approaching cybersecurity education from this perspective teaches students to understand the theory better through application, strengthens retention, provides basic experience, and prepares an inquisitive cybersecurity mindset that is imperative for success in the field.

Accessibility and accommodations for students in cybersecurity classes are limiting factors to enrollment numbers, interest, and opportunities. The diversification and specialization of class subjects help give students more opportunities to learn what they do not know while not redundantly teaching them what they already know. More can be done to better ease the problem of requisite classes discouraging students from taking cybersecurity classes. To accommodate students with prior experience in cybersecurity, the CS department should offer better testing opportunities to give students prerequisite or corequisite credit for classes without the need to take the course, thus allowing students to progress through the curriculum without redundancy.

As for accessibility to classes, the problem stems from a lack of teaching faculty, as well as current cybersecurity classes being limited to inconsistently scheduled special topics courses resulting in a lack of teaching staff. We can improve accessibility by offering more opportunities for students to take existing classes. More sections of a class can be provided through asynchronous enrollment of cybersecurity classes, allowing students to avoid conflicting class schedules that prevent them from enrolling in UVA SIS. Recordings of lectures and from-home attendance are already utilized in the CS department by many classes, so incorporating these as a key feature of classes eliminates physical limitations in class size. More funding for cybersecurity courses, and providing for the hiring of more teaching assistants, can be utilized to help alleviate the staff and infrastructure strain of larger classes, as well.

To make the cybersecurity courses of the class attractive and useful to UVA students, the CS department can also allow the optional opportunity of undergraduate certification. Students can doubly utilize their commitment to the UVA CS cybersecurity program by gaining certification which gets its requirements met with a more thorough program. Schools like GMU provide opportunities for undergraduate certification as an integrated part of their cybersecurity curriculum (GMU, n.d.), while schools like RIT allow students to add cyber certification as a part of their self-planned core curriculum (RIT, n.d.). If the UVA CS department were to allow opportunities for undergraduate certification, we would provide students more incentive to take the courses, career preparation, and official certification that validate the student's experience.

5. ANTICIPATED RESULTS

I anticipate that if these changes are put into effect, students will find themselves learning more content than they do currently, and gaining more experience in cybersecurity, better preparing them to learn on their own and explore for themselves. They will also leave the program better prepared for their future careers. I believe the UVA cybersecurity program will be further enriched and distinguished. Its effectiveness and the resulting increased interest in students will better populate this part of the curriculum and prepare the overall UVA CS department students for cybersecurity in the real world. As these changes are implemented into the current curriculum, enrollment numbers will increase, allowing the program to stabilize in structure, teaching content, and course availability, and also allowing teaching faculty to develop and correct the program more effectively.

6. CONCLUSION

The current cybersecurity curriculum within the UVA CS department leaves much to be desired but has the potential to develop as a program and provide its students with a better opportunity to learn one of the most important aspects of computer science. We can take examples from other colleges and universities to provide a more structured, consistent, accessible, and accommodative program that provides a more thorough program and prepares students with important fundamental knowledge, field experience, and a cybersecurity mindset. This will be achieved through specification and separation of topics, change in teaching methodology, and improved opportunities for students to take cybersecurity classes.

7. FUTURE WORK

This proposal sets up the foundation for multiple solutions that can be used to fix various problems in the cybersecurity curriculum. Future work will primarily focus on the application of these solutions, and further discussion of these solutions and their feasibility in terms of planning, funding, and rollout. If new methodologies are to be used, work will be needed to evaluate and compare the methodologies that are best in practice. If new courses are created around specialized content, further work will be needed to determine which topics will be used to populate a semester-long course. Once these solutions are refined, further specified, and implemented, additional work will be needed to assess improvements in the quality of student education and preparation. Faculty of these courses within the department will have to find and discuss potentially unforeseen issues of a drastically different curriculum.

REFERENCES

Carnegie Mellon University (CMU). (n.d.). Undergraduate Concentration in Security & Privacy - Software and Societal Systems - School of Computer Science. Cms-Staging.andrew.cmu.edu. Retrieved April 26, 2024, from https://s3d.cmu.edu/education/undergrad/secpriv/index.html

George Mason University (GMU). (n.d.). Computer Science Undergraduate Certificate. Catalog.gmu.edu. Retrieved April 26, 2024, from https://catalog.gmu.edu/colleges-schools/engineering-computing/school-computing/computer-science/computer-science-undergraduate-certificate/#text

Georgia Institution of Technology (GT). (n.d.). School of Cybersecurity and Privacy. Georgia Tech Catalog. Retrieved April 26, 2024, from https://catalog.gatech.edu/colleges/computing/cybersecurity-privacy/

Rochester Institute of Technology (RIT). (n.d.). Undergraduate Degrees and Certificates | School of Individualized Study. Www.rit.edu. Retrieved April 26, 2024, from https://www.rit.edu/individualizedstudy/undergraduate-degrees-and-certificates

University of Arizona (UArizona). (n.d.). Cybersecurity (UCERT). Online.arizona.edu. Retrieved April 26, 2024, from https://online.arizona.edu/programs/undergraduate-certificate/online-undergraduate-certificate-cybersecurity-ucert

Virginia Polytechnic Institute and State University (VT). (n.d.). Secure Computing Major. Catalog.vt.edu. https://catalog.vt.edu/undergraduate/college-engineering/computer-science/secure-computing-bs/