ADWAIT NADKARNI - TEACHING STATEMENT

I consider teaching as a crucial and inseparable part of being an academic. As an educator, my lifelong goal is to pass onto students the motivation, excitement, and curiosity that inspired me to choose a career in Computer Science. In the short term, my objective is to inculcate a security-aligned mindset in students from various backgrounds within computer science, such as operating systems, networking, software engineering, and application development.

Teaching Philosophy

Students are naturally curious about the subjects that relate to their daily lives. They also internalize concepts when they impact reality. My teaching philosophy embodies these two truths. I take the approach of engaging students in broad, open-ended discussions that make them realize the impact of the topic. Not only is this approach ideal for teaching computer science, where most concepts are inspired by real-world problems, but more importantly, it inspires creativity and curiosity in students, and motivates learning.

In my classes, I employ a lecture-based but interactive style of teaching. The focus of my lectures is to motivate students to question the design of existing and proposed computer systems, by asking *why* certain design choices were made in the past, and why alternate designs may have failed. Every component of the class, including the lectures, homework assignments, course projects, and quizzes, has a considerable portion dedicated to improving the students' understanding of design-level concepts. Further, I employ in-class exercises to enable students to take positions on the concepts they have just learned, and often lead the discussions with existing real-world problems to which the concepts may be applied. I believe that a good mix of conceptual learning, in addition to practical exposure to the field, is an essential ingredient in the student's holistic growth as a confident computer scientist and professional.

Finally, I believe that a firm course structure helps students fully focus on learning the subject at hand. In my classes, I provide students with a precise syllabus, with the following aspects planned and described to a significant level of detail: (1) overall course structure and expected learning outcomes, including grade distribution for different course components, (2) the course project split into different components with individual deadlines, (3) the nature and characteristics of the exams (e.g., sample exam questions), (4) homework assignments and submission policies, (5) integrity, accommodations, and other policies, and finally, a detailed lecture schedule which includes assigned readings, holidays, and all deadlines. I also regularly remind students of upcoming deadlines, add/drop dates, and important readings for upcoming classes. This planning on my part helps students gauge the workload beforehand, removes their focus from the grading entirely, and allows them to fully enjoy the class. Indeed, in my seven classes taught at William & Mary, I have only had one student come to me for grade adjustment, which I attribute to this structure.

Teaching Experience

As an Assistant Professor of Computer Science at William & Mary, I have taught the following computer science courses over a span of ten semesters, namely (1) CSCI-680 Computer and Network Security (Fall'17), (2) CSCI-445 (*CSCI-420 prior to Fall'20*) Mobile Application Security (Spring'18, Fall'18, Spring'20, Fall'20, Fall'21), (3) CSCI-667 Concepts of Computer Security (Spring'19, Spring'22), and (4) CSCI-680 IoT Security & Safety (Fall'19, Spring'21).

CSCI 680 - Computer & Network Security (Fall'17): When I joined William & Mary in Fall'17, I noticed the lack of a conceptual computer security course at the graduate level. To fill this gap, I introduced a Computer & Network Security class (CSCI 680) for MS and PhD students in computer science. The objective of this class was to provide a graduate-level introduction to computer and network security. Successfully completing the class would allow students to evaluate works in academic and commercial security, and gain rudimentary skills in security research.

CSCI 667 - Concepts of Computer Security (Spring'19, Spring'22): After petitioning the relevant committees, I was successful in getting a version of my Fall'17 CSCI 680 class formally incorporated into the Arts & Sciences Graduate Curriculum, as a new *CSCI-667 Concepts of Computer Security* course. This new course focuses on two primary learning objectives for graduate students in CS: (1) being able to understand concepts in computer security, apply them to solve real-world problems, and evaluate security research,

Table 1: Teaching Evaluation scores for classes taught, from Fall'17→ Spring'22.

	Questions	**Receptive to questions**		**Prepared for class**		**Knew the subject**		**Overall effectiveness**		**Course difficulty**	
Term	***Class* (# of Responses/Class Size)**	**My Avg**	**Dept Avg**	**My Avg**	**Dept Avg**	**My Avg**	**Dept Avg**	**My Avg**	**Dept Avg**	**My Avg**	**Dept Avg**
Fall'17	*CSCI 680: Comp. & Network Security* (5/5)	5.0	4.46	5.0	4.58	4.8	4.74	4.8	4.15	3.2	3.69
Spring'18	*CSCI 420: Mobile App Security* (20/21)	4.89	4.49	5.0	4.51	5.0	4.74	4.6	4.16	3.65	3.7
Fall'18	*CSCI 420: Mobile App Security* (12/12)	4.58	4.37	4.83	4.39	4.83	4.66	4.67	4.07	4.0	3.8
Spring'19	*CSCI 667: Concepts of Comp. Security* (7/7)	4.86	4.48	5.0	4.49	5.0	4.73	4.43	4.13	3.86	3.6
Fall'19	*CSCI 680: IoT Security* (4/4)	5.0	4.57	5.0	4.65	5.0	4.82	4.75	4.24	4.0	3.62
Spring'20	*CSCI 420: Mobile App Security* (17/26)	4.76	4.43	4.88	4.55	4.88	4.78	4.47	4.17	3.71	3.59
Fall'20	*CSCI 445: Mobile App Security* (21/24)	4.76	4.54	4.9	4.59	5.0	4.77	4.57	4.22	4.0	3.58
Spring'21	*CSCI 680: IoT Security* (6/8)	5.0	4.41	5.0	4.48	5.0	4.73	4.83	4.18	3.67	3.63
Fall'21	*CSCI 445: Mobile App Security* (19/34)	4.58	4.45	4.84	4.42	4.95	4.72	4.21	4.18	3.63	3.47
Spring'22	*CSCI 667: Concepts of Comp. Security* (11/12)	4.73	4.5	4.82	4.57	4.82	4.75	4.64	4.26	3.64	3.56

and (2) performing basic security research. The course has a semester-long research project, composed of multiple milestones that teach students how to do research, such as coming up with a project proposal, surveying related work, planning experiments and forming a research plan, and finally, writing a conference-style research paper. This model has so far been successful in getting students involved in research; three of my PhD advisees were recruited from this class, and research projects from the class have been published in top security [1, 2] and SE [3] venues.

CSCI 445 - Mobile Application Security (Spring'18, Fall'18, Spring'20, Fall'20, Fall'21) (*taught as CSCI-420 prior to Fall'20*): Computer Science majors generally take up application/software development positions upon graduation. To teach future application developers the fundamentals of application security, including best-practices and application security analysis techniques, I created the Mobile Application Security course in Spring 2018. This course is split into two phases, each with a dedicated project. In the first phase, students learn about the security-design aspects of building mobile applications, such as the best-practices for storage, network communication, and application interactions. Students apply what they learn to design a mobile application that is graded for both functionality and security. The second phase teaches students the basics of application security analysis. Students perform a large-scale analysis of Android applications with fixed analysis/security goals as the project for this phase, and are graded on the depth and robustness of their analysis and findings. While this class is one of the more difficult ones at William & Mary, my interactions with students have led me to confirm that they enjoyed its practical nature. After petitioning the relevant committees, I was successful in getting this course permanently added to the Arts & Sciences Graduate Curriculum as CSCI 445 in Fall 2020.

CSCI 680 - IoT Security & Safety (Fall'19, Spring'21): The security architectures of operating systems (OSes) are continuously evolving, and the security and safety challenges in consumer IoT environments such as automated homes have motivated OS designers to re-think key security decisions. To introduce students to this exciting research domain, I created the graduate IoT Security & Safety class in Fall 2019. The class is lecture-based, but with a heavy focus on readings from top-tier security venues. Students are expected to write at least one paper review one a published work every class, which performs three essential functions. First, reading close to 23 papers in-depth (i.e., since they have to be reviewed as well), and discussing the paper at the end of each class, allows students to learn this domain at an agile pace. Second, by reviewing published work as if it was under review, students learn to identify research challenges from literature, and develop new research ideas, which is critical for developing a successful research agenda. Finally, this approach also allows graduate students to polish their peer-review skills (i.e., as the reviews are graded on factuality, detailed comments for authors, and helpfulness as well).

In the course of my teaching, I have been able to add one graduate (CSCI 667) and one undergraduate (CSCI 445) class to the permanent curriculum at W&M, and have generally received positive feedback on my teaching from both students and colleagues. Whenever I have received constructive comments on improving certain aspects (e.g., more clarity in grading), I have immediately incorporated them. The average teaching evaluation scores for my graduate and undergraduate classes are shown in Table 1.

Student Mentoring

I consider mentoring students to be my key responsibility and privilege as a teacher. In my five years at William & Mary, I have established the Secure Platforms Lab (SPL) within the CS department, and have been fortunate to mentor several graduate and undergraduate students. I am currently advising four PhD students, Sunil Manandhar (expected graduation: Summer 2022), Kaushal Kafle (expected graduation: Spring 2023), Amit Seal Ami (expected graduation: Spring 2024, co-advised with Prof. Poshyvanyk), and Prianka Mandal (expected graduation: Spring 2024). I previously co-advised another MS/PhD student, Richard Bonett, who is currently on medical leave. Additionally, I have supervised a Masters student, Brian Burns, who completed his Masters project in Spring'19. I am also advising one undergraduate student, Sayyed Razmjo (**Charles Center Summer Research Scholar 2022**). My research with W&M graduate students has produced top-quality conference publications [1, 2, 4, 5, 6, 7, 3, 8, 9].

I have also had the fortune of working with several skilled and motivated undergraduate students, through independent research credits, the Charles Center scholarship, and honors research opportunities. In the past, five undergraduate students have graduated from my group: Ruhao (Tony) Tang (graduated Spring'19), Rozda Askari (graduated Spring'19), Caleb Atkins (graduated Spring'20), and Hanqiu Peng (graduated Spring'20), and Kunyang Li (graduated Spring'22). My undergraduate students have been able to actively contribute to research in my lab. Specifically, Ruhao worked with me since he took my CSCI 420 class in Spring'18, and has made sufficient contributions to be a co-author on our paper [6] published at IEEE S&P 2020, a top venue for security research. Ruhao won the **W&M CS Stephen K. Park Award for Undergraduate Research Excellence** for this work, completed his MS in cybersecurity from Georgia Tech, and landed his first job at the MIT Lincoln Laboratory. Further, both Ruhao and Kunyang won the **Charles Center Summer Research Scholarship** to work with my lab over the summer (2018 and 2021 respectively), and completed their honors theses with me.

I was recently awarded the ***2021 Graduate Faculty Mentoring Award*** by the College of Arts & Sciences in recognition of my graduate mentoring efforts. My lead graduate student, Sunil Manandhar, was simultaneously awarded the **S. Laurie Sanderson Award for Excellence in Undergraduate Mentoring**, which is a testament to the positive culture of mentoring in my research group. My experience mentoring undergraduate and graduate students at W&M has been rewarding to say the least, and has taught me many valuable lessons. I have learned that being approachable and providing unbiased advice encourages students to talk freely in my presence. This in turn has helped me anticipate and address problems before they become serious. Moreover, my experience has taught me the value of bringing a diverse group of individuals with different personalities, goals and aspirations together as one research lab. Through teaching computer security classes tailored to meet both academic and practical requirements, and recruiting and mentoring highly motivated graduate and undergraduate students in my research lab, I hope to build a lasting computer security presence at William & Mary.

References

[1] R. Bonett, K. Kafle, K. Moran, A. Nadkarni, and D. Poshyvanyk, "Discovering Flaws in Security-Focused Static Analysis Tools for Android using Systematic Mutation," in *Proceedings of the 27th USENIX Security Symposium*, Baltimore, MD, USA, Aug. 2018.

[2] A. Ami, K. Kafle, K. Moran, A. Nadkarni, and D. Poshyvanyk, "Systematic Mutation-based Evaluation of the Soundness of Security-focused Android Static Analysis Techniques," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 15, Feb. 2021.

[3] A. S. Ami, K. Kafle, K. Moran, A. Nadkarni, and D. Poshyvanyk, "Demo: Mutation-based Evaluation of Security-focused Static Analysis Tools for Android." in *Proceedings of the 43rd IEEE/ACM International Conference on Software Engineering (ICSE'21), Formal Tool Demonstration Track*, May 2021.

[4] K. Kafle, K. Moran, S. Manandhar, A. Nadkarni, and D. Poshyvanyk, "A Study of Data Store-based Home Automation," in *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Dallas, TX, USA, Mar. 2019, Best Paper Award.

[5] S. A. Gorski III, B. Andow, A. Nadkarni, S. Manandhar, W. Enck, E. Bodden, and A. Bartel, "ACMiner: Extraction and Analysis of Authorization Checks in Androids Middleware," in *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*, Dallas, TX, USA, Mar. 2019.

[6] S. Manandhar, K. Moran, K. Kafle, R. Tang, D. Poshyvanyk, and A. Nadkarni, "Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses." in *Proceedings of the IEEE Symposium on Security & Privacy (S&P)*, May 2020.

[7] K. Kafle, K. Moran, S. Manandhar, A. Nadkarni, and D. Poshyvanyk, "Security in Centralized Data Store-based Home Automation Platforms: A Systematic Analysis of Nest and Hue," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol. 5, no. 1, Dec. 2020.

[8] A. Ami, N. Cooper, K. Kafle, K. Moran, D. Poshyvanyk, and A. Nadkarni, "Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques," in *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, Apr. 2022, accepted, to appear.

[9] S. Manandhar, K. Kafle, B. Andow, K. Singh, and A. Nadkarni, "Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage," in *Proceedings of the 31st USENIX Security Symposium (USENIX)*, Boston, MA, USA, Aug. 2022, accepted, to appear.