Earlence Fernandes – Teaching Statement

The opportunity to help students achieve their educational and professional goals is a key reason why I am interested in an academic career. I greatly enjoy interacting with students, helping them learn about computer science and research, and helping them learn how to solve problems. As a security researcher, I am grateful for the opportunity of introducing the *security mindset* to students who will build the systems of tomorrow.

My teaching experience spans research mentoring of undergraduate and graduate students, teaching graduate courses, and guest lecturing for outreach activities. I've published peer-reviewed papers with two Master's students, an undergrad, and a high-school student. I am committed to engaging undergraduates in research because it gives them an opportunity to see how CS research is done, and potentially opens up a new career path as well. I recently wrote a proposal on defending voice assistants from voice-based confusion attacks, and was awarded $10,000 to employ an undergraduate student.

I was a primary instructor for EECS 588 (graduate computer security) at Michigan, and the main instructor for CSE 590Y (adversarial deep learning) at Washington. Student evaluations of the courses were consistently high. As a future faculty member, I look forward to teaching security, systems, and introductory CS courses.

Teaching philosophy and experience. I have a holistic view of teaching and tailor my lecturing to the requisite discipline and to the audience at hand. For classroom teaching, I take a practical approach and prefer explaining concepts through many carefully chosen examples and hands-on projects before introducing a principle. Being an experimental computer scientist, this is generally the method that I follow in my research and I find it to be a valuable tool to learn the "what" and more importantly the "why" about a given principle. I have taught EECS 588, a graduate course in computer security at Michigan in the Winter of 2017 with the above precepts. For example, a component of coursework was to replicate recent attacks. I recently organized and led a graduate seminar on adversarial deep learning at UW. The challenge here was to create a common platform where people of different research backgrounds can participate. Because adversarial ML is an inter-disciplinary topic, I structured sessions to first explain ML or security ideas (through small examples) relevant to that paper, before diving into the details.

Courses I can teach. I am able to teach introductory and advanced computer security courses, and undergraduate courses on operating systems, networks and distributed systems. I am also interested in leading a graduate level seminar on security for emerging technologies to identify opportunities for collaboration with students and to educate them on the latest challenges in this space. Because my general approach to computer security research is to quickly adapt to new domains, I am also able to adapt my teaching interests to focus on courses depending on the needs of the department.

Course material development. I am currently engaged in developing course material for undergraduate students to help them learn about smart home security. This material is designed as a lab, where students will compromise physical devices like a router, microwave, and door lock. All these devices are simulated in a realistic network setting that is likely to be found in homes today. The learning objectives are to introduce students to the new ways of thinking about hacking homes. One example is the idea of compromising a single device, and using that to escalate privileges to other devices. While this is a standard concept in network security, a new aspect in smart homes is that such escalations can occur due to logic errors in simple rules that connect devices in the home. Another interesting aspect is helping the students explore the new privacy implications of smart home devices. Our vision is to release this lab to the greater community of educators in the hope of helping students at many universities learn about smart home security.

Mentoring experience. I've served as a bachelor thesis technical advisor for two students. My role was to provide assistance on technical topics in mobile systems security. One student has a full-time position in data analysis for security, and the other went on to earn a Master's degree at Harvard. I mentored two Master's students and published peer-reviewed papers with both students. The Master's students went on to full-time positions at VMWare and Google. I'm also currently mentoring a graduate student at UW on ML security, and four undergraduates on topics ranging from end-user programming for IoT to ML security. While working with undergraduate students, the main challenge I faced was scoping the research task and breaking it down into manageable parts. Helping the student on managing work in well-defined pieces helped bring results. Similarly, while mentoring graduate

students, the main challenge was that they get bogged down in detail and hence lose focus of the problem we are trying to solve. My strategy here was to continually help them understand how tasks they are doing at that moment contribute to the overall picture. I found that writing about the problem and submitting for peer-review helps in this process. Based on this experience, my mentoring revolves around two principles:

- *Precisely characterizing the problem:* I like to help students learn how to carefully vet an idea for scientific merit and for motivation. I believe in well-motivated impactful research output and in my experience, having in-depth discussions that question assumptions before diving deep into prototyping systems or attacks leads to such kind of work. Furthermore, one of my first questions to students with research ideas is "How will you evaluate this?". The evaluation forms an important part of characterizing a problem and assessing its merit. While this is a general idea I try to implement in my mentoring, I am careful to also encourage students and their ideas, especially those who are new to research, because coming up with ideas and talking about them can be a daunting experience.
- *Writing early:* I encourage my students to write workshop papers or "mini-proposals." I find that writing about research often helps make concrete the core principles of the work, its contributions, and helps weed out unfruitful paths of investigation. Furthermore, this builds confidence in students, and helps them build ties with the community early on in their careers.

Outreach activities. I regularly conduct guest lectures and seminars at my undergraduate institution in India on pursuing higher-level education, including careers in research in the hope of encouraging more students to take up computer science research. I've also guest lectured on the topic of machine learning security at UW for the CSE 484 undergraduate security course. I served on a panel that explained Internet of Things security to engineers and scientists in the Ann Arbor area (SUMIT 2016 conference). Most recently, I participated in a roundtable discussion organized by Congressperson Pramila Jayapal on policy issues regarding IoT. Furthermore, I am interested in engaging K-12 students in CS through various programs that universities generally have with local schools. I believe that the tangible nature of smart home devices makes for a fertile domain to engage young students in CS.