As an undergraduate at the University of Texas, I co-founded and co-led an outreach program called the Computer Science Roadshow. Working with other CS students, I created a presentation for the area's middle and high schools to explain what Computer Science is, introduce some perhaps non-intuitive areas within Computer Science, debunk stereotypes about the field, and outline how to prepare to later pursue a CS degree and career. These presentations were well received by both students and teachers, and they piqued the interest of students who perhaps had not previously considered Computer Science. We often opened the Roadshow presentations by asking the students how many computers they owned, and as expected, they counted only personal computer like desktops and laptops. We then explained how computers surround us and impact our lives – in cell phones, music players, medical devices, and even cars. This realization, as embodied in the feedback from the students, also fuels my own research interests: security and privacy for these embedded systems is critical – both because these devices are increasingly integrated into people's lives, and because many people are unaware that there are computers in these devices, let alone security and privacy risks.

My initial concern as an undergraduate was to understand how computers worked: once I was able to write interesting programs, I still lacked an understanding of how it is that a program actually executes. In my sophomore year I took both a digital logic design course and an introductory computer architecture course; these courses began to answer my questions about the previously mysterious lower-level foundations of computing. The professor of this latter course, Professor Doug Burger, became my undergraduate research advisor. Under his supervision, I worked on computer architecture research for the next two years, focusing specifically on memory disambiguation. My experience with undergraduate research left me with an understanding of the research process, both as an individual and as part of a larger research initiative, and it also prepared me with a solid technical understanding of how computers work at the lowest levels.

Beginning my PhD this fall with Professor Yoshi Kohno at the University of Washington, I have shifted my research focus to computer security and privacy. Security-related research appeals to me for two main reasons. Most importantly, security is a broad topic relevant at each layer of abstraction and to every emerging technology. Each area of Computer Science that we introduced in the Roadshow—robotics, computational biology, the Internet, embedded systems, artificial intelligence, cognitive science, and medicine—all have important security and privacy concerns. Security thus has a direct relevance to our lives. It is important to me to both address these concerns and to reach out to the broader community to raise awareness of them.

Second, I believe the security mindset—viewing designs skeptically—to be a critical part of any design process. While other areas in Computer Science strive to get things to work better, faster, and smarter, security requires decomposing an existing or emerging design from a different angle in order to improve the final product. I often find myself thinking this way in day to day life when I encounter a new technical design or business idea. As computers become more commonplace in all aspects of our lives, it is crucial to both our personal and national safety to develop frameworks in which new computer designs ensure privacy and security. The combination of my broad interests across the applications of computer science and my lower-level understanding of computing positions me to make contributions to these areas.

This past summer, I interned on the security engineering team at Amazon.com. It solidified my interest and gave me concrete experience with security in a leading technology company whose success depends on building and securing customer trust. Mimicking what the security team does on a day to day basis, I conducted security reviews for almost every one of

the 150 intern projects across the company. I learned how to quickly assess a project design, ask the right questions to uncover potential security issues, and address those issues. I also learned that even at a company like Amazon, many developers are not sufficiently trained in security issues. Indeed, another aspect of my internship consisted of giving security training classes to other interns in order to provide them with specific skills to understand and fix some of the most prevalent web security vulnerabilities such as cross-site scripting and cross-site request forgery.

Security and privacy issues are faced not only by Amazon and other web-based companies, but across all industries that are increasingly using computers as a core part of their business. Though a team of security experts can help to mitigate some of these issues, there remain fundamental challenges to adequately securing many systems. During my internship at Amazon, I was often frustrated with the ad-hoc way in which security features are tacked on to existing designs, giving best programming practices rather than a framework for understanding and solving security problems in a more fundamental and rigorous way. I am drawn to a research career by the hope to go beyond simple security enforcement, instead creating new frameworks and paradigms to more fundamentally *ensure* security.

If even developers at Amazon have a difficult time recognizing and resolving security and privacy issues, how can teenagers, like those to whom we presented the Roadshow, be expected to do so? These students are often the early adopters of new technologies, and combined with their lack of expertise, this makes them more vulnerable to potential threats. I intend to continue the type of outreach I did with the Roadshow now that I am a graduate student at the University of Washington. In particular, I am interested in outreach activities targeted at middle and high school students that (1) broaden their understanding of and participation in Computer Science and (2) help teach them how to be safe and secure users of technology. Because of the early-adopter status of this age group, observing their interactions with technology may also help generate new research ideas.

My interest in education and outreach is deeply related to the technical concerns of computer security: I am invested in raising awareness of these issues among the broader community. I found it rewarding to give the security training classes to interns at Amazon, especially when I could see tangible results in how these interns then approached potential security issues in their projects. One of my most fulfilling experiences in college was watching a high school girl who I tutored in math/science grow both personally and academically over the years. These experiences, combined with the Roadshow, solidified my desire to have impact via education, teaching, and outreach in addition to research.

My career goals are to research the security and privacy issues associated with the ubiquitous use of computing across a wide variety of areas, to develop frameworks to systematically ensure security in these systems, and for my work to be meaningful beyond technology to society at large. I am interested in computer security because I believe it is fundamentally important for society: without prioritizing security considerations in new technologies, we risk building our world on a fragile foundation. I will address this concern in my research by focusing on security and privacy for cyber-physical systems, systems that have tightly integrated physical and computational components and are becoming more commonplace in our world. My previous research, internship, and teaching experiences put me in a position to achieve these goals, and the NSF fellowship will give me the freedom to pursue them.