Statement of Purpose

Yuqing Yang
161250179@smail.nju.edu.cn

My objective is to pursue a Ph.D. in Computer Science, and my future career expectation is to become a researcher and professor. Since 2018, I have been actively engaged in three different but related, tough but interesting research projects, and made interesting discoveries of myself. My research interests span in fields of computer security and information retrieval techniques, with a focus on how to make embedded systems, mobile systems, and cloud systems more dependable, and in the future, to lower the overhead of these approaches.

My motivation of doing researches stems from the Network Attack and Defense course, in which I learned novel techniques of exploiting and defending systems through tough and challenging works. I have found that with the rapid development of computer systems and ubiquitous computing, an increasing risk of information leakage is almost inevitable underneath the seemingly inspiring rapid development of computer science technology. As soon as the research and development of cyber and computer technology continues, new channels will be opened for attack, and the war between defenders and attackers will never end.

With such consideration, I started my first research project to make an investigation on the security issue of local DL models in mobile apps. We have found that the users, the developers and the DL framework providers all lack the acknowledgement of such security problem, and their rudimentary obfuscation method to encrypt the model can be easily bypassed by simply slicing and repacking the app itself. The valuable models therefore can be stolen and wrapped for further development, incurring financial losses to companies.

During the research, I found that compared with doing implementational works following certain practices, I enjoy much more in taking an adventure exploring new topics, chasing after state-of-the-art techniques, and make my own contribution that will truly be influential and novel. Although I have spend six tough monthis trying to make the first prototype on my own to prove the feasibility, I am often thrilled by tiny progresses I made, and I kept being confident in myself that my work is of great value and novelty. Before starting the research, I have never experienced feelings like this. That is why I find myself suitable and capable to do and keep doing research.

Research Experiences. I have been engaged in several research projects as a motivated undergraduate, idea proposer and implementer. Except for the DL model stealing project, I found that it will be fancy to combine Information Retrieval techniques to help the detection of intrusions. Therefore since Oct. 2018, I have been doing research utilizing Information Retrieval techniques for Github issue clustering. And I proposed my own workflow to use domain knowledge to cluster and alter, and to evaluate with coherence and distance between clusters.

Moreover, when taking the Mobile Comm. course, I proposed and implemented a new idea to locate APs with signal fingerprint, combined by some certain movement of the phone. This project has been expanded to a research project of locating hidden surveillance webcamera, thereby helping users to identify and locate them, protecting their privacy.

Teaching Experiences. I have been exceptionally appointed as Undergraduate Teaching Assistant for outstanding performance in Network Attack & Defense in 2018 Fall and 2019Fall, and Teaching Assistant of Computer Network in 2019 Spring(The first undergraduate ever to serve as a TA in this course). I have delivered several lectures on CTF crypto and misc topics, and served as committee member of 2nd and 3rd TrinityCTF contest. During all of these experiences I have proved my communication skills of organizing and explaining complicated issues systematically. I regard such communication skill as a must-have in my future research.