Philosophy. My previous teaching experience helped me realize that no one learns in the same way. Therefore, I would like to teach students based on their personalities and backgrounds. I ever used the rusty steel to explain the program vulnerability to my uncle, a construction project manager. He immediately understood that our jobs are similar: while I care about the security of computer programs, he manages the quality of buildings.

I like to apply this philosophy in my teaching activities. First, I will set proper goals for teaching students in different levels: helping undergraduate students understand the underlying principles of real-world techniques, like how compiler works; mentoring graduate students to develop their interests and skills in finding and solving problems, like proposing defenses. Second, I plan to mentor students based on their characteristics. For students expecting actionable tasks, I will first ask them to follow my schedule, gradually let them maintain the schedule and finally help them manage research independently. For students with strong motivations, I will advise them on high-level ideas and leave them to find projects and make progresses. With different teaching strategies, I can cover everyone in the class and help students build their own strengths in research.

Teaching Experience. My informal teaching experience started very early. My mother, a primary school teacher, told me that teaching not only helps others learn new concepts, but also enhances her understanding. Therefore, I always like to teach others and even stayed late at school to answer questions from my classmates.

During the study in National University of Singapore (NUS), I served as a teaching assistant and lab instructor for three modules: CS4239 Software Security, CS5231 Systems Security and CS4238 Computer Security Practice. Together with the professors, I designed the homework, graded assignments for about 180 students, hosted office hours and gave lectures during the lab experiments. For CS4239, I introduced the fuzzing tool *American Fuzzy Lop (AFL)* to the class, designed the homework and gave the lab lecture of the fuzzing logic. For CS5231, the most interesting work is to customize our ongoing research into class projects, which should reflect the cutting-edge research but with moderate challenges for students to finish in time. Prof. Zhenkai Liang, my Ph.D. advisor and the lecturer of CS5231 and CS4238, won the *Annual Teaching Excellence Award* of NUS two times, and I fortunately participated in the teaching for both of them.

Mentoring Experience. I have been fortunate to mentor several talented undergraduate and graduate students from Georgia Tech (three graduate students) as well as NUS (three undergraduate and one graduate student). My mentoring experience mainly involves thee activities: First, I help students approach security problems like a researcher: for a security issue, what are the current progress and the remaining challenges; for a new solution, what are the strengths and the limitations. Second, I help them understand the challenges of security research, tell them the way to accept the disappointed results and motivate them to keep working. Third, I like to help students on concrete problems, which are usually related to programming with LLVM, performing binary analysis, or setting up servers. With my mentoring, Jinho Jung has published two papers on top-tier conferences, one about hindering malicious fuzzing activities (Security'19) and another about finding performance regression bugs in database management systems (VLDB'20). Chenxiong Qian completed his first paper on reducing program's attack surface (Security'19). Ren Ding built a platform to automatically triage program crashes from coredumps and measure potential privacy leakages (under submission).

Teaching Plans. I am interested in teaching any class of computer science to undergraduate students and teaching advanced security classes to graduate students, like system security and software security. Due to the active confrontation in security research, I believe the best way to understand various attacks and defenses is to use them in practice (in a safe way). Therefore, I would like to design the class with multiple security tasks, and set students into two groups: attackers and defenders. For each task, the students as attackers will try to hack the devices of another team; while the students as defenders will protect their system from attacks. Students change their roles in the middle the task so that everyone has the chance to apply both attack and defense knowledge. I believe this will attract students to understand the taught security mechanisms and even explore new attacks and defenses beyond the class materials in order to win the competition.