**Teaching experience and interests.** I have been the teaching assistant for the graduate-level Network Security class twice during my PhD study at Georgia Institute of Technology. I have experience in creating class projects, teaching project sessions in classes, grading homework and projects, and holding office hours to help students review material and make progress in projects. During my time at Georgia Institute of Technology and Columbia University, I have presented papers I have read, in a way that teaches the materials from the papers, and hosted discussions among PhD students in group seminars. I will be interested in teaching Network Security, Introduction to Computer Security, and special topics in security such as Machine Learning Security.

**Mentoring experience.** I have mentored two master's students, three undergraduate students, and four PhD student collaborators. Students at different stage of their academic study need different kinds of guidance.

For undergraduate students and master's students I have worked with, they are curious about what is research and want to have some experience in doing research. Therefore, I worked with them on well-defined problems that can be parts of a bigger research project, so they can have short-term positive feedback about doing research. For example, I worked with Weifan Jang, a master's student from Columbia University, on designing new attacks using mixed integer linear programs to evaluate the robustness of tree models. His work was used as one evaluation technique in our USENIX Security'21 paper [1]. After we published that paper together, I helped him with his PhD application materials, and now he is a PhD student at Harvard University. One of my undergraduate students, Zeyi Liu, also became more interested in doing research after I worked with her on using Generative Adversarial Networks to evaluate the robustness of PDF malware classifiers [4]. I am currently mentoring her with applying to PhD programs.

For the PhD students I have collaborated with, I have been mentoring them to become more rejection proof. It is a common struggle for almost all PhD students to face rejection. Research studies have shown that it is not intelligence that predicts how students successfully overcome challenges and achieve their long-term goals, but it is grit [2]. Grit is perseverance and passion for long-term goals despite failure and adversity. I have used both research results and different kinds of real-life stories to motivate the students when they fail. I often encourage students to look for internal motivation of solving interesting problems that matter, instead of only relying on external feedback from whether some papers get accepted immediately.

I have mentored PhD students to read more broadly and encouraged them to come up with their own ideas. Good ideas often come from discussions, and possibly after refining the initial ideas for many times. I have encouraged students to share their thoughts at the early stage, even if they do not think these are good enough to write papers on. I have also encouraged students to do experiments at the early stage, because even if the experiments did not work out, they would have learned something new to help them think about the problems. Mentoring students is also a process for me to learn from the students. To make real progress in science, we need ideas from different kinds of people.

**Approach to teaching.** My goal of teaching is to let students have the tools and skills to become independent learners, and be interested in lifelong learning. My approaches include teaching students to develop critical thinking skills, teaching underlying structure of the problems and solutions, and creating supportive environment for different students.

**Critical thinking skills.** I believe that students need to learn arguments from different sides, be open-minded, and form their own opinions. For example, in computer security, detecting vulnerability at the system level vs at the network level has pros and cons from each side. At the system level, we have the opportunities to collect rich information about the program behaviors, but we cannot detect threats that are only visible from a global perspective. At the network level, it is the reverse. I will teach students that different techniques are preferred for solving different problems, and it might be worthwhile to combine the techniques to utilize the strengths from both depending on the situations. I will teach students to be skeptical about absolute arguments.

**Underlying structure.** Learning to identify common underlying structure of different problems and solutions

is important for students to become independent learners. If seemingly-different problems have the same underlying structure, we can try existing solutions first, to avoid re-inventing the wheel. On the other hand, some solutions proposed for different problems have the same underlying structure. If we already know the benefits and shortcomings of an existing solution, these properties likely apply to another solution with the same structure. For example, in the paper "A Sense of Self for Unix Processes", the authors proposed to use sequences of system calls to detect anomalous program behaviors, which indicate potential network intrusion attacks. Researchers have shown that attackers can mimic the behaviors of normal programs to generate benign-looking system call sequences to evade the detection. Since then, different papers have proposed to use sequences of Android API calls to detect malware, sequences of domain name lookups to detect malicious domains, and sequences of user clicks on social networks to detect click fraud, etc. Because these solutions have the same structure, they are subject to the same kinds of evasion attacks.

**Supportive environment.** One out of every two or three people is an introvert. Introversion is about how a person responds to stimulation, including social stimulation. Extroverts crave large amounts of stimulation. For example, I had a collaborator who likes to write papers at a noisy restaurant. On the contrary, introverts are most capable when they are alone or in a quiet environment. Unfortunately, modern learning and working environment are mostly designed for extroverts. We need a much better balance to encourage collaboration between students and to give different students the best environment that can bring out their full potential. I will make classes work well for both introverts and extroverts. I will assign both group projects with pairs and individual projects to students. I will encourage more independent work, which has been shown by research studies from psychologists to help students master knowledge and skills [3, 5]. Class participation such as addressing the whole class with comments is beneficial for extroverted students, but I also want to allow introverts opportunities to express their thoughts. For example, students could submit a short paragraph in writing to demonstrate their thoughts on the reading assignments, especially if they do not want to speak up in classes. I will also make teaching materials such as videos available online if possible, which allows students to learn the materials in environments that are best for them.

## References


[1] Y. Chen, S. Wang, W. Jiang, A. Cidon, and S. Jana. Cost-Aware Robust Tree Ensembles for Security Applications. In *USENIX Security Symposium **(USENIX Security)***, 2021.

[2] A. L. Duckworth, C. Peterson, M. D. Matthews, and D. R. Kelly. Grit: perseverance and passion for long-term goals. *Journal of personality and social psychology*, 92(6):1087, 2007.

[3] G. J. Feist. Autonomy and independence. *Encyclopedia of creativity*, 1:157–163, 1999.

[4] Z. Liu. MalGAN Attack against PDF Malware Classifiers. `https://github.com/lzylucy/Malware-GAN-attack`.

[5] C. J. Nemeth and J. A. Goncalo. Creative collaborations from afar: The benefits of independent authors. *Creativity Research Journal*, 17(1):1–8, 2005.