Yicheng Zhang web: https://yichez16.github.io/yicheng.github.io/ yichez16@uci.edu

Statement of Purpose

of Yicheng Zhang (ECE PhD applicant for Fall—2021)

After conducting a series of fancy attacks on hardware, for instance, GPU and FPGA accelerators, I discovered I was enthusiastic about investigating security issues in computer systems. Thus, my first academic objective is to pursue a doctorate in computer engineering to effectively pursue my research interests and effectively attain my professional goals.

At the University of California, Irvine, I worked with Prof. Zhou Li and Prof. Mohammad Al Faruque and wrote a paper[1] to exploit GPU side-channel information to extract the structural secret of a neural network model under their supervision. I also developed a remote power side-channel attack on FPGA to reconstruct machine learning model structure under the guidance of Prof. Zhou Li and Prof. Mohammad Al Faruque. After these two works, I got interested in architecture and systems security had plenty of future study ideas.

I want to work with Prof. G. Edward Suh on the design of secure computing systems or with Prof. Zhiru Zhang on the design of faster and more efficient computing systems(Especially FPGA accelerators) or with Prof. José F. Martínez on microarchitectures and embedded systems. My future advisor could assume, among other things, my familiarity with the following areas: GPU security, side-channel attack, and machine learning security.

Leaky DNN: Stealing Deep-learning Model Secret with GPU Side-channel

To better prepare for rigorous doctoral study, I accumulated skills and knowledge that will aid my doctoral studies and research over the course of my involvement in various research projects. For example, one of the hardware security studies I was involved in is leaky DNN [1], written under the supervision of Prof. Zhou Li and Prof. Mohammad Al Faruque. In this work, the key question we ask and aim to answer is: **can an adversary infer DNN structural secrets like layers and their hyper-parameters by exploiting the GPU side-channel?**

As the first step, I revisited the existing GPU side-channel [2] but found it insufficient for our goal. Their attack exploits an Nvidia GPU feature named Multi-Process Service(MPS), which allows the attacker's kernel (called spy) to stay in the same GPU cores as a victim kernel. The spy observes the victim kernel's resource usage by taking samples through CUPTI (Nvidia performance counters). However, due to MPS' unbalanced scheduling, the spy is allowed to collect only one sample at the end of one training iteration, which is too coarse-grained to reveal the DNN structure.

Comparing to the previous work [2], we pursue the **opposite direction**. We let MPS be switched off (the default setting) and run a spy concurrently with the victim's DNN to force context switching. This time, the time-sliced scheduler ensures spy and victim kernels to take fair shares of execution time. Therefore the spy can achieve a much higher sampling rate through CUPTI.

Still, another challenge has to be addressed to recover the model structure. The execution time for different ops varies significantly, resulting in an uneven number of samples among different layers. To address the issue of unbalanced samples, we design the inference model on top of the Long Short-Term Memory (LSTM) model, capable of handling complex time-series and utilizing the layer contextual information.

My experience with this project contributed greatly to my ability to carry out independent research and a deep interest in hardware security areas. I enjoyed the challenging process of exploring hardware "bugs" of computer systems since these "bugs" can not be easily fixed like software "bugs." For example, a software "bug" can be fixed by releasing a patch. However, hardware " bugs" sometimes can only be solved by the new generation of architecture instead of software support.

Stealing Neural Network Structure through Remote FPGA Side-channel Analysis

I started my second project under the guidance of Prof. Zhou Li and Prof. Mohammad Al Faruque. In this work, I found the model secret is vulnerable to when a cloud-based FPGA accelerator executes it. When I first started working on this project, I found many works demonstrating the possibility of using local side-channel attacks on CPU, GPU, microcontroller, and FPGA to infer the model secret. However, their works assume the attacker has complete control of or physical access to the deep-learning model accelerator, not the real case for cloud computing. In our attack, we extend the attack to a more realistic and challenging scenario, which is on the cloud. The attacker can only measure the victim's DNN execution passively(no control of input) and covertly(no physical access to FPGA instance). I remotely programmed a ring oscillator (RO) power sensor on the

same FPGA accelerator with other tenants processing their deep-learning models. By leveraging the power side-channel information collected by the ring oscillator (RO) sensor, I can reconstruct the model sequence with over 90% accuracy. My hardware security interests evolved further during this project, where I deployed remote power side-channel attacks in cloud computing. Also, in this project, I served as the leader of the whole project. It provides me with a valuable chance to learn how to communicate with all team members and manage the project.

Teaching Experience I have served as Teaching Assistant at the University of California, Irvine, for three courses, i.e., Continuous-Time Signals and Systems(EECS150), System Software(EECS111), and Object-Oriented System Programming(EECS40). Such experience provides me the chance to learn how to mentor students and how to do good presentations. In Object-Oriented System Programming(EECS40), I led four projects designed to let students practice java programming. By making well-crafted slides and recorded videos, I tried to make every student feel their programming skills improved. The warm feedback from students makes me feel satisfied with my work, and it also spurs me to pursue my dream to become a good professor, not only good at research but also instructing students.

The reason why I choose Cornell University

The Ph.D. program in Electrical Engineering at Cornell University is the ideal program to prepare me with the knowledge and skills needed to accomplish my academic goals: to become a professor. What sets this program apart from many others is the breadth and depth of training that allows students to pursue their research interests and career goals. The program offers a larger selection of computer architecture and embedded system courses. I was also excited to learn that students in this program can also take classes in the Department of Computer Science further enhance their understanding of system security. Besides, after communicating over email with Dr. G. Edward Suh and his Ph.D. students, I learned that the mentoring model in the program creates an environment where professors care about their students and encourage students to collaborate with multiple professors in the program and scholars from across the university. These factors ultimately benefit students in the program by gaining different perspectives and valuable research experience. I can truly make a difference in the hardware security field with the training I will receive at Cornell University.

References

[1] Junyi Wei, Yicheng Zhang, Zhe Zhou, Zhou Li, and Mohammad Abdullah Al Faruque. Leaky dnn: Stealing deep-learning model secret with gpu context-switching side-channel. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 125–137. IEEE, 2020.