Personal Narrative

Zheng Li

zheng.li@mail.sdu.edu.cn, Shandong University, P.R.China

I am a third-year Master student (expected June 2020) in the School of Computer Science & Technology from Shandong University. I am supervised by Shanqing Guo, the Professor and Doctoral Supervisor at the School of Cyber Security & Technology, Shandong University. I received my B.S in Computer Science & Technology from Shandong University in 2017.

Machine learning techniques have witnessed tremendous development during the past decade, and are adopted in various fields ranging from computer vision to natural language processing. However, they are facing serious deep learning privacy and security problems. My research interests include the security and privacy of machine learning (ML), especially the analysis and application of backdoors in ML models. I am actively working on protecting the intellectual property of machine learning models, e.g., injecting a backdoor as the basis of claim ownership.

Fortunately, I have had two papers accepted by the Information Security Conference for half a year. In particular, my recent paper titled "How to Prove Your Model Belongs to You: A Blind-Watermark based Framework to Protect Intellectual Property of DNN" was accepted by ACSAC 2019, which made me very excited, encouraged, and honored. Therefore, I am very much looking forward to the conference and hope to consult some famous professors about information security. Further, I will continue my Ph.D. study in the field of information security. I hope to become a corporate expert or university professor in the security field in the future.