Abstract:

Recent years have seen the emergence of new kinds of software including deep learning, programmable computer networks, and blockchains. Unfortunately, these systems have been shown to suffer from critical safety and security errors, affecting their wider adoption. The goal of my research is to develop new automated program verification and synthesis techniques which ensure safety and reliability of these systems.

In this talk, I will start by introducing AI2, the first automated verifier for neural networks able to certify large convolutional models. The key idea behind AI2 is to bridge abstract interpretation and neural networks, enabling a sound over-approximation of a network’s behavior in a scalable manner. I will then briefly discuss DL2, a system which enables clean interaction with deep learning models by allowing users to pose queries in a declarative manner. Finally, I will demonstrate how automated program analysis and synthesis can address key security and reliability challenges in domains such as computer networks and blockchains, preventing severe outages and financial losses.

Bio: Dana Drachsler-Cohen is an ETH Postdoctoral Fellow at the department of Computer Science, ETH Zurich. Her research interests span automated reasoning, program synthesis and machine learning. She obtained her PhD from the Computer Science Department at the Technion in 2017.