Machine Learning+Security+Verification Workshop 2019

Vijay Ganesh
University of Waterloo, Canada

Monday Aug 26th, 2019

CONTEXT AND MOTIVATION FOR THIS WORKSHOP

Machine Learning

and

Applied Logic

(verification, analysis, synthesis, security, software engineering)

MACHINE LEARNING FOR SOFTWARE ENGINEERING AND SECURITY

- ML applied to logic, software engineering, and security (broadly construed) tools/algorithms
  - ML-based program analysis: Mayur Naik, Prateek Saxena
  - ML-based logic solvers: Vijay Ganesh, Elias Khalil, Kshitij Bansal, Antonina Kolokolova
  - ML-based verification and invariant synthesis: Arie Gurfinkel
  - ML for physics and mathematics: Craig Larson, Sebastian Wetzel
  - ML-based fuzzers: Joe Scott (poster)
  - ML-based runtime verification: Reza Babaee (poster)

SECURITY OF ML

- Logic, verification, analysis, and security tools/algorithms as applied to ML
  - Introduction to reinforcement learning and robustness issues: Pascal Poupart
  - Adversarial attacks: Nicolas Papernot, Yaoliang Yu
  - Adversarial robustness: Alexander Madry, Alexey Kurakin, Bo Li, Florian Kerschbaum, Dirk Nowotka
  - Verification of DNNs: Nina Narodytska, Yichen Yang, Kuldeep Meel, Gagandeep Singh
  - Verification and analysis of systems that use ML as a component: Krzysztof Czarnecki
  - Logic Guided ML: Joe Scott (poster)
  - Bias in ML: Haobei Song (poster)
  - Causes of Adversarial Vulnerability: Angus Galloway (poster)

THANKS TO OUR SPONSORS!

- Waterloo Cybersecurity and Privacy Institute
- Waterloo AI Institute
- Vector Institute
- Waterloo Electrical and Computer Engineering Department