Machine Learning (ML) Security Workshop

Course Objectives

At the end of the course, participants will:

- Understand the security threat landscape
- Understand the top security issues revolving around machine learning
- Understand how to take preventive measures
- Learn about the Secure Development Lifecycle (SDL) for machine learning products
- Gain knowledge on the security considerations when deploying production models

Course Overview

With the explosive growth of machine learning applications and products, the question of their security touchpoint is becoming a major interest area for many organizations. Machine learning security covers both how such products affect the security posture of the organization, and what threats they bring to such a system, as well as how to protect such systems from adversaries. This course outlines the state-of-the-art in machine learning security and how the topic has evolved. It is intended for developers and managers to make strategic decisions for their machine learning products as both a vendor and a customer.

Course Duration

2-day instructor-led training

Course Outlines

- Understanding the ML development flow
- Understanding the difference between training and inference, and the security paradigm for each eco-system
- Understanding ML System Risks & Challenges
- Reviewing the top 10 security threats for ML systems
- Understanding Challenges of ML security

Subjects

- Threat analysis for a machine learning systems
- Security issues in deploying machine learning systems
- IP protection of ML systems
- Weaknesses of machine learning systems
- Current attacks on machine learning systems
- Active areas of ML security research, future, and Q&A session