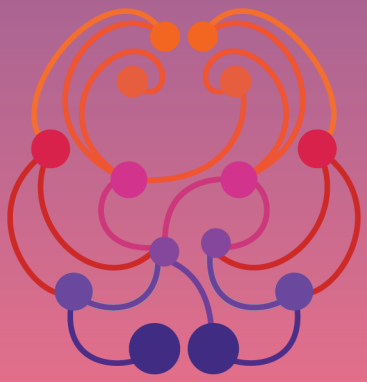

BOSTON UNIVERSITY
MACHINE INTELLIGENCE COMMUNITY

We are an organization focused on providing opportunities for students to learn about machine intelligence in a community environment.

Boston University Machine Intelligence Community
mic.bu.edu
bumic@bu.edu
bumic
@bumic_
@bumic_

MACHINE INTELLIGENCE COMMUNITY

Boston University Machine Intelligence Community
Secure Machine Learning Series

Time: 3:30 - 4:30 PM
Location: Center for Integrated Life Sciences and Engineering (CILSE) Seminar Room 101

This series will cover the burgeoning field at the intersection of cyber security and machine learning. Each seminar will cover different attacks or cryptographic techniques at the bleeding-edge of machine learning security and highlight the urgency for further research as intelligent systems increasing pervade society.

Topics	Date
1. Introduction to Secure Machine Learning	1.29.2018
2. Stealing Machine Learning Models via Prediction APIs	2.5.2018
3. Real-world Adversarial Examples Guest speakers: LabSix (https://goo.gl/MiqwMr)	2.19.2018
4. Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures	2.26.2018
5. Certified Defenses for Data Poisoning Attacks	3.19.2018
6. Deep Learning with Differential Privacy	4.2.2018
7. CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy	4.16.2018
8. Practical Secure Aggregation for Privacy Preserving Machine Learning	4.23.2018
9. Secure Multi-Party Learning	5.7.2018