Announcement of student job (HiWi) in Cooperation with Fraunhofer AISEC, Garching

A Framework to Adversarial Machine Learning

Motivation
Machine learning and deep learning are widely applied in many domains, such as autonomous car, medical diagnosis and e-commerce recommendation systems. However, the current learning models rely heavily on the quality of training data to produce reliable Intelligence, which on the other hand exposes vulnerabilities to adversaries who intend to manipulate the learnability of state-of-art intelligent systems. Adversarial machine learning investigates thus the vulnerabilities of machine learning, and offers deeper insights of the learning models, further proposes secure and robust machine learning algorithms, which are resilient to malicious data manipulation.

Task Description
In this project you will be actively involved in designing and developing a framework for adversarial machine learning. You will get familiar with different machine learning algorithms in depth, and learn how to reverse engineering the algorithms, further evaluate their robustness against adversarial attacks. You will then be required to develop simple front-end for reporting, and a dashboard to compare different learning models and benchmark different datasets systematically.

Requirements
- Strong programming skills in Python
- Experience with frameworks of machine learning and deep learning, e.g., scikit-learn, tensorflow
- Experience with data visualization, e.g., matplotlib, Bokeh, D3js
- Good knowledge of machine learning and deep learning
- Experience with version control system and good team work, e.g., git
- Basic knowledge and interest in IT Security is a plus
- Experience with numerical programming is a plus

Contact
Dr. Huang Xiao
Telefon: +49 89 322-9986-149
E-Mail: huang.xiao@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Cognitive Security Technologies (CST) Research Group
Parkring 4, 85748 Garching (near Munich), Germany
http://www.aisec.fraunhofer.de

Date of publication: 19. Juni 2017