Challenge 9

Android is the most popular mobile operating system worldwide. As Android apps could be downloaded and installed from various places, including third-party app stores, they have been an appealing target for malicious actors to deliver their attacks. Along with this, various malware detection and characterization methods have been proposed by both academia and industry that rely on different range of features.

In this challenge, you are provided with a dataset of malicious and benign Android apps and their network layer features collected by analyzing their network traffic. This dataset contains 7,845 applications, each with 12 different features. Read this dataset and shuffle its rows. Then, select 6,276 applications for training, and 1,569 apps for testing.

Prepare a report and submit a PDF file by Tuesday (**12/15/2020 before 6 pm**) considering the below details:

1. Train an SVM classifier using the training data (i.e., 6,276 apps).
2. Test the trained SVM classifier on the testing data (i.e., 1,569 apps).
3. Calculate and report the accuracy of the trained classifier on the test data.
4. Create an adversarial test data from the original test data by relying on the UniversalPerturbation attack. Use the Adversarial Robustness Toolbox (ART), supported by DARPA, to deliver this attack and create a perturbed test dataset.
5. Calculate and report the accuracy of the trained classifier on the perturbed test data and compare it with the one obtained from Step 3.