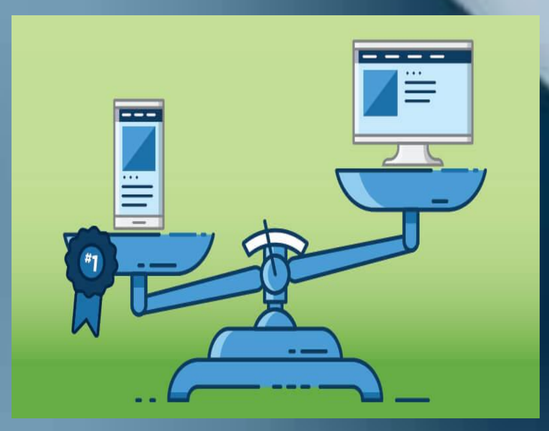
ARIEL UNIVERSITY
Department of Computer Science

Classifier System for Application-Level Mobile Traffic

Yair Ivgi and Johann Thuillier
Supervisor : Dr. Dvir Amit

Background

With the increasing proliferation of smartphones, the amount of sensitive data increased drastically. Numerous studies have shown that encryption isn't enough to protect entirely confidentiality. In fact, Machine Learning techniques can classify user's parameter like OS, browser and application. However, most of these studies deals with Computer traffic. This, raises a fairly critical question:
"What about Mobile traffic Classification?"



Objective

We're interested in developing and expanding a machine learning classification algorithm for application-level mobile traffic identification We will probably not be able to achieve a perfect identification. we will try to reach a 70 percent classification at this initial stage of the device type and application.

System overview

The system consists of three main parts:

Network trace capture

- The recording of mobile network traffic and arranging the data.

The Classifier

- Turn each flow of recorded data into vector of features, then analyze it with the hybrid algorithm consists of The k-nearest neighbors and The k-means algorithms.

App Identification

- There are two phases:
- The first is the training of the algorithm and actually create a fingerprint for the applications.

- The second phase is the classification phase which we try to identify the new records.

System diagram