#### **Analytical Project Assignment**

Team L

Detecting network intrusions

## Associated data sets

network\_traffic.csv

Data Description.doc

# Data description

XYZ Bank is a large and profitable bank in Saint Louis, Missouri. Like any large corporation, XYZ Bank has a very large and intricate infrastructure that supports its networking system. A Network Analyst recently discovered unusual network activity. Then, pouring over year’s worth of logs, their team of analysts discovered many instances of *anomalous* network activity that resulted in significant sums of money being siphoned from bank accounts. The Chief Networking Officer has come to your group for help in developing a system that can automatically detect and warn of such known, as well as other unknown, anomalous network activities.

The network\_traffic.csv file is a synopsis of logged network activity. It contains labeled examples of benign network sessions as well as examples of sessions involving intrusions. It is important to note that it is likely that there exist many different intrusion types in the data. The data\_description.txt file provides explanations of each of the attributes found in the network\_traffic dataset.

### Your tasks

1. Determine if it is possible to differentiate between the labeled intrusions and benign sessions.
2. Is it possible to identify different types of intrusions? If so, which values of which attributes in data correlate with the specific types of intrusions?
3. Develop and implement a systematic approach to detect instances of intrusions in log files. Your system will need to be able to take a new network\_traffic log file and determine the existence of known patterns of intrusions as well as anomalies which may be indicative of new and unknown intrusion patterns.
4. Evaluate detection power of your system.
5. Can your intrusion detector be used in real-time? It would need to be able to receive data about a current session, and in seconds determine if it is likely to be and intrusion of previously seen type or an anomaly potentially signifying an unseen yet intrusion mode. What information should be exchanged via the user interface of such system?