A Study of the Low-level Network Data

Iosif-Viorel Onut and Ali A. Ghorbani
({onut.viorel, ghorbani}@unb.ca)

Abstract

One of the most important phases of implementing an intrusion detection/prevention system is to identify the set of features that the system is going to use. Based on our already proposed feature classification schema for network intrusion detection, we present the design of a feature extractor that extracts and statistically analyze features with respect to attacks. The presented system extracts and analyzes in real time a total of 613 different features. The system uses Chebyshev's Inequality to detect any deviation between the expectation of the normal behavior (i.e., mean) and the value of the feature while under attack. The experimental results, conducted on DARPA dataset, statistically highlight the importance of each proposed feature category, as well as identify some of the most sensitive features to attacks.

.