Technische Universität München
Lehrstuhl für
Netzarchitekturen & Netzdienste
Prof. Dr. Georg Carle

Thesis (MA/BA/IDP)

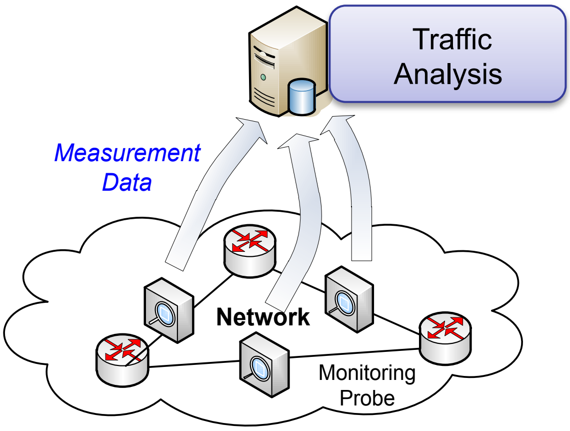
Configuring Attack Detection Algorithms

Motivation

Malicious activities are common in today's Internet. Scanning, spamming, or infections of computers can be observed many times throughout a single day. Operators and administrators are interested in identifying such events in order to warn users or in order to implement countermeasures.

Many malicious activities leave footprints in the network traffic, which can be detected by Intrusion Detection Systems (IDS). A lot of different IDS and traffic analysis methods exist, but neither of them is able to perfectly detect all security related incidents. an IDS can make two kinds of errors: It can flag innocent traffic as attack traffic (false positive), or it can fail to detect malicious traffic (false negative).

Both types of errors are undesired from an operator perspective. False negatives can lead to undetected system compromise, false positives lead to wasted time as a human operator needs to investigate the cause of the alarm. False positives are often seen as the bigger problem by operators, due to the additional work load that is required to analyze the alarms.



Many algorithms use parameters which help to control to the sensitivity of the analysis. Adjusting these parameters is essential for configuring such algorithm for practical use. Failure to find good parameters can result in either high rates of false positives or false negatives. Finding good parameters is often an time-consuming task, which needs to be performed separately for each network.

Your Task

Your task is to implement and evaluate methods for configuring known attack detection algorithms that have been presented in intrusion detection research in the past years. This configuration process involves the automatic identification of good parameters for the selected intrusion detection algorithm.

Contact

Lothar Braun <braun@net.in.tum.de> Tel.: 289-18010

Felix von Eye <felix.voneye@lrz.de> (LRZ)