Abstract

Deploying Intrusion Detection Systems (IDS) inside a company or institution’s network is becoming a common practice these days to prevent or mitigate the possibly devastating effects of worms, Distributed Denial-of-Service (DDoS) or any other attacks launched against them.

To improve its response time and allow for better communication and cooperation between network security experts about eminent or ongoing attacks it has been suggested to move IDS to the core of the network - the Internet backbone infrastructure. However, current IDS solutions are hardly scalable and cannot sustain the high volume levels of network traffic in realtime.

The implementation of sampling mechanisms has been regarded as a possible solution to that problem, but investigation is still ongoing about which sampling methods and which detection metrics provide the best compromises in terms of improved performance at multi Gigabit speeds while having low error rates at detecting attacks. This thesis addresses these and other aspects of high speed intrusion detection, namely using the two most common approaches: signature detection and anomaly detection.

The study is initiated with a survey of the current state of the art and enhanced with the creation and development of a framework specifically aimed at simplifying the comparison of different sampling methods and detection algorithms. It is also designed to allow the quick introduction of new methods and more complex algorithms.

Regarding anomaly detection, the preliminary tests show that different sampling methods affect detection in a similar way and that conservative sampling rates provide good results when using the entropy of the destination port as main metric. However, more aggressive sampling rates are not suitable for use with this metric and would need more complex algorithms.

Signature detection is not compatible with sampling, however, as its effectiveness drops sharply even with very modest sampling rates.