INTRUSION DETECTION IN DISTRIBUTED MULTIMEDIA APPLICATIONS

Regina Awor Komakec
Research Number: 571

Abstract

Over the past few years, distributed multimedia systems and applications have experienced an increase in popularity. However, there are growing security concerns as growth in internet use has led to rise to internet-based attacks. With the increasing attacks on internet-based applications, intrusion detection systems play an important role in providing warnings indicating possible security breach.

The aim of this research is to investigate, using Bayesian statistics, how well intrusion detection systems can be used to secure internet-based telephony, vis-à-vis teleconferencing systems. We hypothesize that the exchange of information between IDSs, by setting them in sequence, can improve the effectiveness of intrusion detection in a real-time scenario. To examine this notion, we tested two different intrusion detection systems, with varying specifications, in turn against VoIP-based traffic containing a pre-determined number of attacks. We also investigated the possibility of applying the two IDSs in sequence, where the information output from one IDS acts as input for the second IDS.

The main contribution of this thesis is its demonstration of how varying intrusion detection systems (IDSs) complement each other. In addition, we demonstrate how Bayesian network classifiers can be used to evaluate, as well as to predict IDS performance.