Distributed Anomaly-based Intrusion Detection System

Judit Gyimesi

Budapest University of Technology and Economics

Intrusion Detection Systems (IDS) are software or hardware systems, which automatically monitor network traffic looking for suspicious signs of intrusions. Their aim is to recognise already on-going attacks, and possibly block them, in co-operation with other tools like firewalls, as well. According to data processing, one family of IDS-s is anomaly based intrusion detection systems, which assume that an attack causes abnormal behaviour, which can be detected. Thus they log user profiles, and if the difference of stored and monitored behaviour exceeds a threshold, an alarm is generated and other steps can be taken. The greatest advantage of anomaly detection is the ability of recognising new, unknown attacks. Though it is advisable not to use it as a stand-alone system, only with other security tools, for it can easier be eluded than other IDS-s.

Deploying more than one IDS-s in a distributed environment can give solutions to numerous problems, which I will discuss. More detailed, I will describe a particular case showing my algorithm for detecting the spreading of Internet worms, and bounding them. Effectiveness is demonstrated by mathematical analysis. According to the analysis, the second phase of the infection can be warded off and in many cases, significant fraction of the first phase as well.