Network Based Distributed Intelligent Intrusion Detecting System

A PROJECT REPORT PRESENTED BY

RK. AHMADH RIFAI KARIAPPER

to the Board of Study in Statistics and Computer Sciences of the

POST GRADUATE INSTITUTE OF SCIENCE

in partial fulfilment of the requirement

for the award of the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

of the

UNIVERSITY OF PERADENIYA

SRILANKA

2010

Network Based Distributed Intelligent Intrusion Detecting System

RK. Ahmadh Rifai Kariapper
Department of Physical Sciences & Technology
Sabaragamuwa University of Sri Lanka

The breach of security barriers of the computer systems has always been a greater concern in the information technology era. The Intrusions and Attacks seem to come from different angles and in different types everyday. It has been a critical battle to keep phase with the ever increasingly mounting threats to the computer Systems. Intruders or attackers analyze the computer systems or computer networks for any possible loop-holes and vulnerabilities.

The existing Intrusion Detection Systems (IDS) are not efficient and intelligent enough to detect the new types of attacks. The signature based IDSs only detect the known type of intrusions where as the misuse detection based IDSs producing a huge amount of false alarms. Traditional intrusion detection systems are increasingly limited by their need of an up-to-date and comprehensive knowledge base.

The PEARL coding is used to detect the intrusions since it is having graphical user interface to develop GUI part and as well it can be used to create common gateway interfaces. I used WinDump within the program code and the output was diverted to route back to the input of the PEARL code. Because of anomaly detection on clustering technology the system showed positive results and good in detecting. Another important stage is good scalability as well performance of the proposed system. Meanwhile method of capturing data packets, the activity of central anomaly processing unit and GUI console are very rebellious challenges.

The proposed Network-Based Distributed IDS is having the capability to learn and detect the new type of attacks. This IDS is not the ultimate Intrusion Detection Software but it will focus on overcoming the most prominent drawback of the existing systems and may be a new step toward a better IDS.