Intrusion Detection System to Protect Network Resources

Prepared by

P.P.D.S.C.Weeraratne

MSc 08/10012

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirements of the Degree of the Master of the Science in Information Technology.

Declaration

I am declare that this thesis is my own work and have not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of Student Signature of Student

Date:

Supervised by

Name of Supervisor Signature of Supervisor

Date:

Acknowledgements

First of all, I thank my wife and my parents for their tireless and invaluable help and encouragement and patience. Without their continuous support, I would not have been able to write this dissertation. Similarly I thank my friends for providing me with their tremendous support. Moreover I gratefully acknowledge my friend, Mr.Suresh Wijesinghe (Network Security consultant and Certified Ethical Hacker) who gave me the idea of this research project.

Special thank for my University Supervisor Mr. Saminda Premaratne, who supervise and drive me towards the goal. Constantly he advises me about objective of this project. That is very helpful to me on the track towards my goal.

This research project is implemented and tested at my office, Research and Development Lab. I would be thankful to my team leader Mr. Eranga Wickramasinghe who gave me permissions and resources to make this project a success.

Abstract

The rapid proliferation of Information System networks and IS an application has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. There are several kinds of intruders that can affect to company information system. They may be inside or outside users. Sometimes it may be authorized or unauthorized users. These intruders slow down high-speed internet connection as well as high performance and expensive IT resources. Because they are looking around the world for idle IT resources for running their processor inside others resources. The network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defence. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective.

In this research, examine the vulnerabilities of networks and say that we must include intrusion detection in the security architecture for computing environment. We have showed such architecture and evaluated key mechanisms in this architecture such as applying sensors to intrusion detection, anomaly detection and misuse detection for ad-hoc networks.

Contents

List of Figures

List of Table