Masters Project titled “Behavior Based Network Analysis Tool”

San José State University
A Project Report

Presented to

The Faculty of Department of
General Engineering
San Jose State University
In Partial Fulfilment
Of the Requirements for MS Degree

Team #12

Dec 11, 2009

Industrial Advisor: Prof Morris Jones
Technical Reader: Prof. Harry Li

Members:

Aggarwal, Anupa(GE)

Kakuru, Sindhu(EE)

Shah, Ravi(GE)
APPROVED BY THE DEPARTMENT OF GENERAL ENGINEERING

Dr. Leonard Wesley  
Associate Professor, Department of Computer Engineering, San Jose State University  
Master of Science in Engineering (MSE) Director  
Graduate & Extended Studies  
College of Engineering  
San Jose State University

iii
APPROVED BY THE DEPARTMENT OF GENERAL ENGINEERING

Morris Jones
Professor, Department of Electrical Engineering, San Jose State University
College of Engineering
San Jose State University
APPROVED BY THE DEPARTMENT OF GENERAL ENGINEERING

Dr. Harry Li
Professor, Department of Computer Engineering, San Jose State University
College of Engineering
San Jose State University
Abstract

Information is the asset for every enterprise today and researchers are working vigorously to develop top most software that are capable enough for providing cent percent security to the Enterprise Network. Varieties of security software are invented daily with each possessing some peculiarity. Examples include Norton Anti Virus, Firewalls, Intrusion Detection System, Intrusion Detection Expert System and many more. All these software have their advantages and disadvantages. But security being the most important criteria there can be no room for ignorance. Hence a new technology called Network Behavior Analysis is stepping into the security globe that not only incorporates positives of already prevailing software but even improves upon their shortcomings to provide better network security.

For the major project, our team is aiming to deploy a behavior based network analysis tool that will identify the user on to the network. The main advantage of USER IDENTIFICATION would be enhanced security and most importantly it will save the time of network administrators in troubleshooting.

In order to understand the ins and outs of the technology literature review was done extensively. Market/Economic Analysis clearly states the success of the technology in the upcoming years. As far as architecture implementation is concerned, the front end of the software tool has been designed in PHP while the back end is My SQL Database Server. The Programming Language used for Data Extraction is Perl while the data was collected with the help of Wireshark Network Analysing Tool.
Acknowledgement

We wish to express our deep gratitude to everyone who made a tremendous effort to make this project successful. In particular, I would like to express the deepest appreciation to Prof. Morris Jones who has the attitude and substance of genius. He continually and convincingly conveyed the spirit of appreciation in regard to our work. Without his support and motivation we would not have been able to reach up to the department expectations.

We would like to thank Prof Harry Li, Prof Frank Lin who had always been there to provide us technical guidance. In addition we would like to thank Prof. Michael Jennings who had always given us the heads up for the preparing project part B.

Last but not the least we would like to thank Prof. Wesley for guiding us during second half of the Masters Project Journey. We are sure this experience would be an added asset in our career flights.

- Aggarwal, Anupa
- Shah, Ravi
- Kakuru, Sindhu
# Table of contents

1. **Introduction** .................................................................................................................. 1  
   1.1 Project Scope .................................................................................................................. 1  

2. **Project Description** .................................................................................................... 3  

3. **Literature Review** ....................................................................................................... 4  
   3.1 Detailed Description of technologies ............................................................................ 5  
      3.1.10 Network Behaviour Analysis .............................................................................. 5  
      3.1.11 Learnt Model ....................................................................................................... 6  
      3.1.12 Rule Based Systems ............................................................................................ 6  
      3.1.13 Model Based Systems .......................................................................................... 7  
      3.1.14 Data Mining ........................................................................................................ 7  
      3.1.15 Neural Networks ................................................................................................ 8  
      3.1.16 Pattern Matching ................................................................................................ 8  
      3.1.17 Statistical Models ................................................................................................. 8  
      3.1.18 Specification Based Models ................................................................................. 9  
      3.1.19 Protocol Based Models ....................................................................................... 9  
      3.1.20 State Based Models ............................................................................................. 9  
      3.1.21 Transaction Based Model ................................................................................... 9  
      3.1.22 Firewall Technologies ........................................................................................ 10  
      3.1.23 Intrusion Detection Systems ............................................................................... 13  
      3.1.24 ANTI-VIRUSES ................................................................................................. 14  

4. **Design Description** ..................................................................................................... 16  

5. **Project Architecture** .................................................................................................. 16  
   5.1 Specifying Dynamics .................................................................................................... 18  

6. **Economic Justification** ............................................................................................... 22  
   6.1 Executive Summary ...................................................................................................... 22  
   6.2 Problem Statement ....................................................................................................... 25  
   6.3 Solution and Value Proposition .................................................................................. 26  
   6.4 Market Size .................................................................................................................. 27  
   6.5 Competitors ............................................................................................................... 28  
   6.6 Industry Ratings ......................................................................................................... 29  
   6.7 Customers .................................................................................................................... 30  
   6.8 Cost Profile ................................................................................................................. 30  
   6.9 Break Even Analysis .................................................................................................... 37  
   6.10 P & L Statement ........................................................................................................ 38  
   6.11 SWOT Analysis ......................................................................................................... 38  
   6.12 Business and Revenue Model ................................................................................... 39  
   6.13 Norden-Rayleigh Model ........................................................................................... 39
List of Figures

Figure 1: Project Development Life Cycle .................................................. 2
Figure 2: Network Security development phases ....................................... 4
Figure 3: Taxonomy of Anomaly Detector Behavioural Model .................... 6
Figure 4: Layers of Network Security .......................................................... 14
Figure 5: Architectural View of NBA ........................................................... 17
Figure 6: Activity Diagram ........................................................................ 20
Figure 7: Market Survey for NBA ................................................................. 27
Figure 8: Workbook Screenshot ................................................................. 31
Figure 9: Per PC Implementation Costs ....................................................... 33
Figure 10: IT Labor Cost ............................................................................. 34
Figure 11: Revenue Growth ....................................................................... 36
Figure 12: Cost vs Benefit .......................................................................... 37
Figure 13: Break Even Analysis .................................................................. 37
Figure 14: P&L statement ........................................................................... 38
Figure 15: SWOT Analysis ......................................................................... 38
Figure 16: Norden Rayleigh Probability Density Function Graph ............... 40
Figure 17: Cumulative Costs in Norden Rayleigh ....................................... 41
List of Tables

Table 1: Competitors Details.................................................................28
Table 2: Competitors Rankings............................................................29
Table 3: Hardware Cost.................................................................31
Table 3: Software Costs.................................................................32
Table 4: One time Implementation Labor/Services............................32
Table 5: Cost Summary......................................................................33
Table 6: Cost of Savings.................................................................34
Table 7: Business Value of Productivity Benefit...............................35
Table 8: Revenue Margin.................................................................35
Table 10: Return on Investment.........................................................36
Table 11: Norden-Rayleigh Calculations.............................................41