ANALYSIS OF AN INTRUSION DETECTION SYSTEM BASED ON IMMUNILOGY

MOHAMMED HUSSEIN SAEED AL-AMOUDI

A project report submitted in partial fulfillment of the
Requirements for the award of the degree of
Master in Information Security

Faculty of Computer Science and Information System
Center of advance software engineering (CASE)
University Technology Malaysia

November 2008

ABSTRACT

It is believed that many of the mechanism covered in the biological immune system are adapted to the field of computer intrusion detection within “LISYS”. In this report, I went briefly on the mechanisms of the biological immune system, their parallels in LISYS are presented, and how they may operate to intrusion detection in a computer environment is discussed. LISYS is an artificial immune system, which need to be implemented and examine through experiments with variety of challenges in detecting intrusive behaviour in real network with simulated network environment. Components of LISYS need to be challenge also to see wither those mechanisms are really necessary

ABSTRAK

Adalah dipercayai bahawa kebanyakan mekanisma yang terkandung dalam sistem immunisasi (pertahanan) biologikal telah diadaptasikan ke bidang pengesanan ganguan komputer menerusi ‘LISYS”. Dalam laporan ini, saya akan menjelaskan secara ringkas berhubung mekanisma-mekanisma sistem immunisasi (pertahanan) biologikal, membentangkan persamaannya dalam LISYS dan membincangkan bagaimana ia akan beroperasi terhadap pengesanan gangguan di dalam persekitaran komputer. LISYS adalah satu sistem immunisasi (pertahanan) tiruan, yang perlu dilaksana dan dikaji melalui kajian-kajian yang mempunyai kepelbagaian dalam mengesan aktiviti ganguan di dalam jaringan sebenar dengan menggunakan persekitaran jaringan yang telah disimulasi. Komponen-komponen yang terkandung dalam LISYS perlu diuji bagi melihat akan keperluan mekanisma-mekanisma tersebut.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Natural immune system is a source of inspiration for the computer security in the age of the internet, where it is believed that the Immune System solves similar problems that are facing today's most usable security software (IDS). Human immune system is very complex and robust, so does its mechanism can be apply to the technology of computation as a model of intelligence, and show some reliability.

Since 1988, the CERT coordination center (CERT/CC) has been observing computer instructions activities and reports that the number of incidents reported to them has been approximately doubling every year since they started, also Malaysian cert has been reported that in the second quarter of 2006 saw an increased in intrusion incidents with a total of 227 incident (the reported one), which is more than two folds from the previous quarter.

1.1 MOTIVATION

The problem of network intrusion has been there for some time, but with much of services from the ISPs as high speed broadband involve, that provides us the capabilities for video conferencing, VOIP, Video on demand, and on-line gaming etc, in-return, the internet has become ubiquitous in all societies. On the other hand, the internet intrusion of all types have become one of the most important and challenging

problems faced by computer experts. In today world, Worms and Viruses are capturing most of the attention and are responsible for much of the damage. And if we look to the view years back, Viruses and Worms delayed airline flight, infected wireless printer, disrupted cash-dispensing machines, and hijack modems to make long distance phone calls, and it's going to get worse (Secrets and Lies, 2000, p. 45).

Given the sophisticated and speed of propagation of today's attacks, the defenses system in place that are tailored to particular attack signatures is unlikely to keep pace as so called Zero-day attacks become prevalent. A successful defense system must achieve one goal, must be able to respond to wide range of attacks, including those not seen before.

1.2 CONTRIBUTION

Presented in this report is the LISYS approach an example of many other AISs have been developed to replace or solve the problem facing the current computer network intrusion detection. Further, the implementation of an AIS known as LISYS (Lightweight intrusion detection system), with more realistic environment and data to produce a fine result from the experiments and deeply analyze LISYS to see wither it achieves the principle of AIS.

1.3 OVERVIEW

The rest of this written paper structured as follows. The following Chapter "2" I focus in some related background. Follow up with Research Methodology in Chapter "3". In Chapter "4", I went through related work, and describe LISYS in detail. In

Chapter “5”, I report experimental results and experience in running LISYS. In Chapter “6”, I discuss a direction of future work in this area.

REFERENCES

Balthrop, J., Forrest, S., and Glickman, M. (2002b). Revisiting LISYS: Parameters & normal behavior. CEC-2002. Proceeding of the congress on evolutionary computing.

Bruce Scneier. Secret and Lies. Indianapolis, Indiana: Wiley publishing, 2000.

CERT Coordination centre 2002, April. "CERT/cc statistics 1988-2002." Technical report, Carnegie Mellon University.

Dasgupta, Dipankar. (1999). Immunity-based intrusion Detection System: A General (NISSC). Virginia/United state: National Institute of standards and technology and national computer security center,

Forrest, S., Perelson, A. S., Allen, L., and Kuri, R. C. (1994). Self –Non self discrimination in a computer. In proceedings of the 1994 IEE Symposium on research in security and privacy, Los Alemitos, CA.IEEE computer society press.

Forrest, S., Hofmeyr, S. A., Somayaji, A., and Longstaff, T. A. (1996). A sense of self for Unix processes. California. United state: IEEE Computer Society press.

Forrest, S., Hofmeyr, S. A., and Somayaji, A. (1997). Computer Immunology. Communication of the ACM.

Glickman, M. Balthrop, J. Forrest, S. (2003). A Machine Learning Evaluation of an Artificial Immune system. Massachusetts Institute of Technology.

Hofmeyr, S. (1999). An immunological model of distributed detection and its application to computer security. University of New Mexico: PhD thesis.

Hofmeyr, S., and Forrest, S. (2000). Architecture for an artificial immune system. Evolutionary computation Journal.

Kim, J. and Bentley, P. (1999). The artificial immune model for network intrusion detection. Aachen, Germany: in 7th European Conference on Intelligent Techniques and Soft computing.

Parham Peter. (2000). The immune System. New York: Garland Publishing.

Percus, J. K., Ora E. P., and Perelson A. S. (1993). Predicting the size of the T-cell Receptor and antibody combing region from consideration of efficient self-non self discrimination. Proceeding of the national academy of sciences of the United State of

America.

Stibor, T., Mohr, P., Timmis, J. (2005). Is negative selection appropriate for anomaly detection?. USA: ACM.

Somayaji, A. Hofmeyr, S. and Forrest, S. (1997). Principles of a Computer Immune System. ACM.

Symantec Norton Antivirus 2005. http://www.symantec.com/nav/nav-9xnt/,2005.

Trend Micro-Trend Micro outbreak management. http://www.trendmicro.com/en/products/global/enterprise.html,2005.

Tizard, I. R., (1992). Immunology. Third edition. Texas: A&M University.

Weir, D. M. and Stewart, J. (1997). Immunology. Eight Edition. New York: CHURCHILL LIVINGSTONE.

Williams, P. Anchor, K. Bebo, J. Gunsch, G. and Lamont, G, (2001). Towards a computer immune system for detecting network intrusion. Berlin, Springer-Verlag.

Nemesis packet injection. http://packetfactory.net/projects/nemesis/ , 2005.