

UNIVERSITY OF OKLAHOMA
GRADUATE COLLEGE

**EVOLUTIONARY COMPUTATION
APPLIED TO
INTRUSION DETECTION**

A Thesis
SUBMITTED TO THE GRADUATE FACULTY
in partial fulfillment of the requirements for the
degree of
MASTER OF SCIENCE

By
Pedro A. Diaz-Gomez
Norman, Oklahoma
2004

**EVOLUTIONARY COMPUTATION
APPLIED TO
INTRUSION DETECTION**

A THESIS APPROVED FOR THE
SCHOOL OF COMPUTER SCIENCE

By

Dr. Dean F. Hougen – Chair

Dr. John Antonio

Dr. Changwook Kim

© by Pedro A. Diaz-Gomez 2004
All Rights Reserved.

Dedication

This thesis is dedicated to my parents, brothers and sisters, parents and brothers in law, El Bosque University staff, principally Ing. Jairo Barragan; My wife Emiliana, that is always in my heart, and my kids: Pedro Arturo, Ana Maria, Carolina y David. Emy, sons and daughters: you are my life, you encourage me to accomplish great projects, I love all your effort to be the best!. Did you remember my goals? to be the best ... and to all the American People, but specially to those that devote their life to “giving”...Yoana, Emily, Millie, Ron, Bud, Dee, ...

Acknowledgments

I would like to thank Dr. Dean Hougen, Dr. John Antonio, Dr. Lakshmivarahan, and Dr. Kim, for their teaching and patience. From all of you, I learned not only in the classroom, but with your example, the way to do science and be better. Thanks a lot.

Contents

Dedication	iv
Acknowledgments	v
List Of Tables	vii
List Of Figures	viii
Abstract	ix

List Of Tables

List Of Figures

Abstract

One of the most important goals of every company is to preserve the integrity, confidentiality, and availability of its data and information. Many efforts have been made to accomplish that goal: security policies, firewalls, Intrusion Detection Systems (IDSs), anti-virus software, and standards to configure services in operating systems and networks. This thesis focuses on one of those topics: Intrusion Detection Systems, following the guidelines of a new approach: evolutionary computation. In this sense this thesis presents principally the use of genetic algorithms to develop IDSs and shows an example of a tool for audit trail analysis.