

بسم الله الرحمن الرحيم



HOSSAM MAGHRABY



شبكة المعلومات الجامعية التوثيق الالكتروني والميكرو فيلم



HOSSAM MAGHRABY

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
على هذه الأقراص المدمجة قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

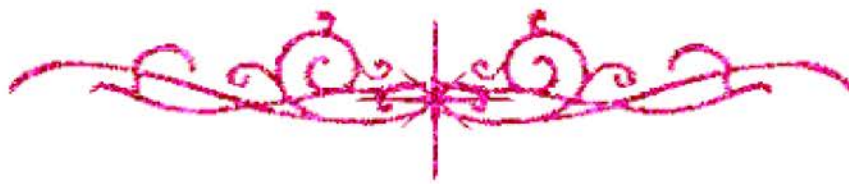


A red decorative flourish or signature line.

HOSSAM MAGHRABY



بعض الوثائق الأصلية تالفة



HOSSAM MAGHRABY



بالرسالة صفحات

لم ترد بالأصل



HOSSAM MAGHRABY

B 14119

Intrusion Detection Using Distributed Agents

By

Ahmed Shaaban Abd El Alim

A Thesis Submitted to the
Faculty of Computers & Information
Cairo University

In Partial Fulfillment of the
Requirements for the degree of
Master of Science

In
Information Security

Under the Supervision of

Prof. Sanaa El Ola Hanafi Ahmed

Head of
Information Technology Dept.
Faculty of Computers & Information
Cairo University

A.Prof. Imane Aly Saroit Ismail

Information Technology Dept.
Faculty of Computers & Information
Cairo University

FACULTY OF COMPUTERS & INFORMATION
CAIRO UNIVERSITY-EGYPT
2004

Admission

I certify that this work has not been accepted in substance for any academic degree and is not being concurrently submitted in candidature for any other degree.

Any portions of this thesis for which I am indebted to other sources are mentioned and explicit references are given.

Student Name: Ahmed Shaaban Abd El Alim.

Intrusion Detection Using Distributed Agents

By

Ahmed Shaaban Abd El Alim

A Thesis Submitted to the
Faculty of Computers & Information

Cairo University

In Partial Fulfillment of the
Requirements for the degree of
Master of Science

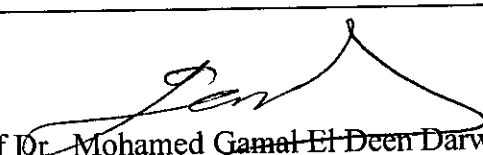
In

Information Security

Approved by the Examining Committee


Prof Dr. Yosri Saber Al Gamal

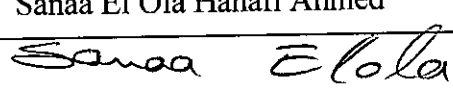
(Judge)


Prof Dr. Mohamed Gamal El Deen Darweesh

(Judge)

Prof Dr. Sanaa El Ola Hanafi Ahmed

(Supervisor)


Dr. Imane Ali Saroit Ismail

(Supervisor)

FACULTY OF COMPUTERS & INFORMATION
CAIRO UNIVERSITY-EGYPT

2004

To my parents and my fiancée.

Acknowledgements

First I would like to thank God that gives me the ability to do this work. I thank Dr. Sanaa El Ola about her continuous guidance and care.

I would like to thank my supervisor, Dr. Imane Ali. Her invaluable help and useful directions were the primary reasons this work being in this shape.

I am very grateful for my parents for their continuous support and prayers, especially my father who insisted and pushed me to prepare for the master degree.

And finally, but most importantly, I would like to thank my fiancée. Her encouragement and continuous support, made it possible for me to finish this work. She patiently helped me a lot in printing and formatting this thesis, and preparing for the master presentations.

Really words cannot express how much I am grateful for these people.

Table of Contents

Acknowledgements	v
List of Tables.....	x
List of Figures	xi
List of Abbreviations.....	xiii
Abstract	xiv
Chapter 1: Introduction	1
Chapter 2: Information Security	4
2.1 Introduction	4
2.2 Information System Security Components	6
2.2.1 Information Systems Resources	7
2.2.2 Information Security functional areas	10
2.2.3 Threats and Risks	12
2.2.4 Information Security Measures	19
2.3 Security Policies.....	19
2.3.1 Program Policy	20
2.3.2 Issue-Specific Policy	21
2.3.3 System-Specific Policy	22
2.4 Information security risk management.....	24
2.4.1 Risk Assessment.....	24
2.4.2 Risk Mitigation.....	27
2.4.3 Uncertainty Analysis.....	29
2.5 Computer Attacks and Vulnerabilities	30
2.5.1 Types of Computer Attacks	30
2.5.2 Types of Computer Vulnerabilities	32
2.6 Attack Life-Cycle.....	35
2.6.1 Attack Stages.....	36
2.6.2 Attacker Behavior	37
2.7 Summary	38

Chapter 3: Intrusion Detection	39
3.1 The Seriousness of Cyber Attacks	39
3.2 Concepts and Definitions	41
3.3 Why Using Intrusion Detection Systems?	42
3.4 Attacker and Victim Perspectives on Intrusion.....	45
3.5 Generic IDS Model	47
3.5.1 Audit Source.....	47
3.5.2 Data Collector	48
3.5.3 Classification and Analysis Engine.....	48
3.5.4 Knowledge Database.....	48
3.5.5 Response Unit	48
3.6 Desirable characteristics of an intrusion detection system	49
3.7 Main features of an Intrusion Detection System.....	50
3.7.1 Processing and analysis of data.....	51
3.7.2 Target System.....	53
3.7.3 Detection Methods	57
3.7.4 Audit Source.....	59
3.7.5 Usage Frequency	60
3.7.6 Behavior on Detection.....	61
3.8 Techniques used for intrusion detection	63
3.8.1 Rule-based Expert Systems.....	63
3.8.2 State transition analysis.....	65
3.8.3 Statistics	66
3.8.4 Neural networks	66
3.9 Intrusion Detection Challenges.....	67
3.10 Summary	68
Chapter 4: IDSUDA Design &Architecture	69
4.1 Introduction to Software Agents Technology	69
4.2 Software Agents Types	70
4.2.1 Collaborative agents.....	72

4.2.2 Interface agents	73
4.2.3 Mobile agents	74
4.2.4 Information/Internet Agents.....	75
4.2.5 Reactive Agents	76
4.2.6 Hybrid Agents	76
4.3 Using Distributed Agents in Intrusion Detection.....	76
4.4 Related Work	77
4.5 IDSUDA Design	84
4.5.1 Common System Design Specifications	84
4.5.2 Agent Design Specifications	85
4.5.3 IDSUDA Agent Type.....	86
4.5.4 Communication Model Design Specifications.....	87
4.6 IDSAUDA Architecture.....	87
4.6.1 Agent Architecture	88
4.6.2 Sub-Agent (Resource Monitor) Architecture.....	90
4.6.3 Communication Server Architecture.....	91
4.7 Comparing IDSUDA with the prior systems	92
4.8 Summary	95
Chapter 5: Implementation	96
5.1 Implementation platform and development languages	96
5.2 IDSUDA Features	97
5.3 IDSUDA Intrusion Detection Rules.....	98
5.4 Agent Internal Events (the main data units).....	99
5.5 Agents Implementation	100
5.5.1 Resources monitors (sub-agents)	100
5.5.2 Agent Controller.....	111
5.5.3 Communication Server.....	113
5.5.4 Other Components	115
5.6 IDSUDA Assessment.....	117

5.7 Summary	119
Chapter 6: Tests and Results	120
6.1 Testing IDSUDA	120
6.1.1 Test Scenario 1: Scanning.....	120
6.1.2 Test Scenario 2: Penetration	122
6.1.3 Test Scenario 3: Persist.....	125
6.2 Performance	130
6.3 Disadvantages of IDSUDA.....	131
6.4 Summary	132
Chapter 7: Conclusion and Future Work.....	133
7.1 Summary	133
7.2 Conclusion	133
7.3 Future work.....	138
References.....	139
Output From The Thesis.....	146

List of Tables

Table 2.1: Information System threats	5
Table 3.1: Centralized versus Distributed IDS	52
Table 4.1: Comparing IDSUDA with prior systems	94
Table 5.1: Comparison Between IDSUDA and two Commercial IDSs	118
Table 6.1: Test scenario 1 results	122
Table 6.2: Test scenario 2 results	125
Table 6.3: Test scenario 3 results	129
Table 6.4: Testing IDSUDA performance (Network Watcher module is not enabled)	130
Table 6.5: Testing IDSUDA performance (Network Watcher module is enabled) ...	131
Table 9.1: Summary of IDSUDA Tests	131
Table 9.2: Performance tests summary	131