



Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Intrusion Detection Correlation in Computer Network Using Multi-Agent System

A Dissertation

Submitted in Partial Fulfillment of the Requirements of the
Degree of Doctor of Philosophy in Electrical Engineering
Computer and Systems Engineering Department

Submitted by

Ayman Elsayed Elsayed Taha

M. Sc., Electrical Engineering
(Computer and Systems Engineering)
Ain Shams University, 2002

Supervised by

Prof. Dr. Hani M. K. Mahdi

Prof. Dr. Ismail Abdel Ghafar Farag

Assoc. Prof. Dr. Ayman Mohamed Bahaa

Cairo, Egypt

May, 2011

جامعة عين شمس - كلية الهندسة

قسم هندسة الحاسبات والنظم

ترابط اساليب اكتشاف الاختراق فى شبكات الحواسب باستخدام نظام العملاء المتعدون

رسالة

مقدمة للحصول على درجة الدكتوراه فى الهندسة الكهربائية

(هندسة الحاسبات والنظم)

مقدمة من

أيمن السيد السيد طه

ماجستير الهندسة الكهربائية

(هندسة الحاسبات والنظم)

جامعة عين شمس - 2002

تحت اشراف

أ.د. هانى محمد كمال مهدى

أ.د. اسماعيل عبد الغفار فرج

د. أيمن محمد بهاء الدين

القاهرة - مصر

يوليو - 2011

Abstract

Ayman Elsayed Elsayed Taha
Intrusion Detection Correlation in Computer Network
Using Multi-Agent System
Doctor of Philosophy Dissertation
Ain Shams University, 2011

Alert and event correlation is a process in which the alerts produced by one or more intrusion detection systems and events generated from different systems and security tools are analyzed and correlated to provide a more succinct and high-level view of occurring or attempted intrusions. Current correlation techniques improve the intrusion detection results and reduce the huge number of alerts in a summarized report, but still have some limitations such as a high false detection rate; missing alerts in a multi-step attack correlation; alert verifications are still limited; Zero Day attacks still have low rates of detection; Low and Slow attacks and Advanced Persistent Threats (APTs) cannot be detected; and some attacks have evasion techniques against IDSs. Finally, current correlation systems do not enable the integration of correlations from multiple information sources and are limited to only operate in IDS alerts. Agents and multi-agent systems have been widely used in IDSs because of their advantages.

The thesis purpose is to prove the possibility of improving both IDS Accuracy and IDS Completeness through reducing either False Positive or False Negative alerts using correlation between different available information sources in the system and network environment. The dissertation presents a modular framework for a Distributed Agent Correlation Model (DACM) for intrusion detection alerts and events in computer networks. The framework supports the integration of multiple correlation techniques and enables easy implementation of new components.

The framework introduces a multi-agent distributed model in a hierarchical organization; correlates alerts from the IDS with attack signatures from information security tools and either system or application log files as other sources of information. Correlation between multiple sources of information reduces both false negative and false positive alerts, enhancing intrusion detection accuracy and completeness. Each local agent aggregates/correlates events from its source according to a specific pattern matching. The integration of these correlation agents together forms a complete integrated correlation system.

The model has been implemented and tested using a set of datasets. Agent's proposed models and algorithms have been implemented, analyzed, and evaluated to measure detection and correlation rates and reduction of false positive and false negative alerts.

In conclusion, DACM enhances both the accuracy and completeness of intrusion detection. DACM is flexible, upgradable, and platform independent. It decreases the audit load and the time cost required to obtain effective situational understanding; increases the coverage of the attack space and forensics; and improves the ability to distinguish the serious attack from the less important ones or identify the kind of needed reaction. DACM can also be used to enhance the early detection capability of APT. Finally, DACM can be used as a real time system with minor modifications. We think that this is a promising approach successfully combining correlation techniques with agent technology in intrusion detection systems in order to provide higher security for computer networks and internet services.

Keywords:

Intrusion Detection, Alert Correlation, Multi-Agent Systems, Learning Agent, Reduction Rate

Acknowledgements

First, thanks to Allah (God) who made me able to accomplish this work, I sincerely express my deepest gratitude to my thesis supervisors, **Dr. Hani Mahdi**, Professor of Computer Engineering, Faculty of Engineering, Ain Shams University, and **Dr. Ismail Abdel Ghafar**, Professor of Computer Engineering, Military Technical College, and **Dr. Ayman Bahaa**, Associate Professor of Computer Engineering, Faculty of Engineering, Ain Shams University. I was fortunate to have met such outstanding scholar supervisors. I like to express my thankfulness for their kind supervision and offering unfailing support, invaluable advices and comments and helpful and useful discussions in selecting the interesting point and during the preparation of this thesis. I owe a special acknowledgment to them for giving me a lot of their time during the years of preparing this thesis. I could never had done it without their support, technical advice and suggestions, thorough reading of all my work.

I would like to thank the Center for Education and Research of Information Assurance and Security (CERIAS), Purdue University, USA. I appreciate the valuable support of the CERIAS executive director **Prof. Eugene Spafford**, the generous effort of his staff especially Information Assurance Research Engineer **Keith Watson**, for their cooperation during my scholar visit to the Center. They provided me with great resources to capture and collect the data needed for this work. Special Thanks to my friend Glenn Glover who guided me to that center.

I appreciate the assistance and input from my colleagues in ORC and their support during this work, special thanks to **Ahmed Abdel Sabour** and **Galal Mohamed** for their help during implementing the proposed model.

I will never be able to thank my mother and my family enough for supporting me during my whole life. I tried to accomplish this work to make them proud of me. Finally, I am very grateful to my wife **Dalia**, and my lovely two kids, **Asser** and **Sama**, for their patient support especially during my scholar visit, sacrifices, sustained moral support, and encouragement. I always thank my God for blessing me with such a wonderful family. I would like to dedicate this work specifically to them and my mother and my whole family.

Statement

This dissertation is submitted to Ain Shams University for the degree of Doctor of Philosophy in Computer and Systems Engineering Department.

The work included in this thesis was carried out by the author at Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : 07 / 07 / 2011

Signature :

Name : Ayman Elsayed Elsayed Taha

Table of Contents

Abstract	i
Table of Contents	v
List of Figures	ix
List of tables	xii
List of Algorithms.....	xiii
List of Abbreviation	xiv
Chapter One: Introduction	1
1.1 Intrusion Detection and Response Systems	1
1.1.1 IDS Terminology and Parameters	1
1.1.2 IDS Limitations	2
1.1.3 Intrusion Detection Alerts Correlation	2
1.1.4 Agents in IDS	3
1.2 IDS Correlation Problem Definition	3
1.3 The Proposed Model.....	4
1.4 Methodology	5
1.5 Contributions.....	5
1.6 Dissertation Organization	6
Chapter Two: Literature Survey and Related work	7
2.1 The Importance of Security and Intrusion Detection	7
2.1.1 Security Mechanism	8
2.1.2 Intrusion Detection Systems	9
2.1.3 Intrusion Detection Correlation Systems	14
2.1.4 Recent Cyber Security Attacks.....	15
2.2 Basic Concepts of Data Correlation	19
2.2.1 Alert normalization.....	23
2.2.2 Alert aggregation and Fusion	24
2.2.3 Alert verification and Prioritization.....	26
2.3 Alerts Correlation Techniques	28
2.3.1 Correlation of Attack Scene	29
2.3.2 Correlation of Pre and post conditions	31

2.3.3	Casual analysis Correlation based on Statistical Techniques ..	33
2.3.4	Distributed Correlation	34
2.4	Alert Correlation Limitations	36
2.5	Agents in IDS and Correlation	37
2.6	Comprehensive Approach Model for IDS Alert Correlation...	39
Chapter Three: Distributed Agent Correlation Model		43
3.1	Distributed Agent Correlation Model Description	43
3.1.1	IDSs Correlation Agents	44
3.1.2	INFOSEC Tools Agents	46
3.1.3	System and Application Logs Agents.....	48
3.1.4	DACM Central Agent	50
3.1.5	Formal Description for Central Agent	51
3.1.6	Response Agent	52
3.1.7	Learning Agent	52
3.1.8	The Knowledge Base and Security Policy	53
3.2	DACM Components	54
3.3	DACM Knowledge Base	55
3.3.1	System Parameters and Role Base Tables	55
3.3.2	Alerts Table	56
3.3.3	Vulnerability Scanner	56
3.3.4	Performance Monitors Tables	57
3.3.5	Firewall Log Files Tables	57
3.3.6	System Audit Files Tables	58
3.3.7	Services Log Files Tables	58
3.3.8	Output Tables:	58
3.4	DACM Features	59
3.5	Implementation Scope and Performance Enhancement	61
Chapter Four: DACM Design and Algorithms		63
4.1	IDS Alert Correlation	63
4.1.1	IDS Alert Correlation Performance Analysis.....	63
4.2	Modified CAM Time	64

4.2.1	Agent Based Correlation Model.....	65
4.2.2	Dynamic Parallel Correlation Model.....	72
4.3	DACM Individual Agents.....	76
4.3.1	IP Address Normalization.....	77
4.3.2	Firewall Agent.....	79
4.3.3	FTP local Agents.....	81
4.3.4	SSH Agent.....	85
4.3.5	Error Log Agent.....	87
4.3.6	Access log Agent.....	90
4.4	DACM Central Agent.....	95
4.5	Implementation Environment.....	101
Chapter Five:	DACM Results and Analysis.....	102
5.1	CRIAS Data Set.....	102
5.1.1	CERIAS Network Description.....	102
5.1.2	Data Description.....	104
5.1.3	Attacks.....	106
5.1.4	Attack scenarios.....	106
5.2	IDS Alerts Correlation Results.....	108
5.2.1	IDS correlation Model.....	109
5.2.2	CAM Results.....	110
5.2.3	ABCM results.....	112
5.2.4	DPCM Results.....	113
5.2.5	IDS Alert Correlation Techniques Performance.....	115
5.3	DACM Components Results.....	121
5.4	DACM Central Agent Results.....	123
5.5	DACM Evaluation and Assessment.....	132
5.5.1	DACM Limitation.....	132
5.5.2	DACM Assessment.....	133
5.6	Practical Implementation Issues.....	134
Chapter Six:	Conclusions and Future Work.....	135
6.1	Conclusions.....	135
6.2	Future Work.....	138

APPENDIX A	139
Appendix B: DACM Agents Formal Description	157
REFERENCES.....	163

List of Figures

FIGURE 2.1 COMPERHENSIVE APPROACH MODEL FOR IDS ALERT	
CORRELATION	40
FIGURE 3.1DACM BLOCK DIAGRAM.....	44
FIGURE 3.2 IDS CORRELATION AGENTS	45
FIGURE 3.3 IDS ALERTS OUTPUT USING BASE FOR SNORT	45
FIGURE 3.4 FIREWALL ROUTER LOG FILE	46
FIGURE 3.5 INFOSEC TOOLS CORRELATION AGENTS.....	48
FIGURE 3.6 FTP LOG FILES.....	49
FIGURE 3.7 SYSTEM AND APPLICATION LOGS CORRELATION AGENTS.....	49
FIGURE 3.8 STANDARD ALERT ATTRIBUTES	51
FIGURE 3.9 LEARNING AGENTS BLOCK DIAGRAM	53
FIGURE 3.10. DACM COMPONENTS STRUCTURE	54
FIGURE 3.11 IDSS CORRELATED ALERTS TABLE ATTRIBUTES	56
FIGURE 3.12 VULNERABILITY SCANNER ALERT ATTRIBUTES.....	56
FIGURE 3.13 NESSUS OUTPUT FOR VULNERABILITY SCANNER.....	56
FIGURE 3.14 PERFORMANCE MONITOR ALERT ATTRIBUTES	57
FIGURE 3.15 FIREWALL OUTPUT LOG FILE	57
FIGURE 3.16 FIREWALL ALERT ATTRIBUTES	57
FIGURE 3.17 SYSTEM AUDIT ALERT ATTRIBUTES	58
FIGURE 3.18 SERVICES LOG ALERTS ATTRIBUTES	58
FIGURE 3.19 IMPLEMENTATION SCOPE OF DACM COMPONENTS.....	62
FIGURE 4.1 ABCM CORRELATION MODEL BLOCK DIAGRAM	65
FIGURE 4.2 ABCM SEQUENTIAL LEARNING PHASE	67
FIGURE 4.3 ABCM PARALLEL LEARNING PHASE	67
FIGURE 4.4 CERIAS ABCM PARALLEL LEARNING RESULT.....	68
FIGURE 4.5 ABCM CORRELATION PHASE	70
FIGURE 4.6 DPCM BLOCK DIAGRAM	72
FIGURE 4.7 DPCM CORRELATION STAGES	72
FIGURE 4.8 CERIAS DPCM CORRELATION EXAMPLE	74

FIGURE 4.9 DACM INDIVIDUAL AGENTS	76
FIGURE 4.10 FIREWALL ROUTER LOG CONTENTS	79
FIGURE 4.11 FTP LOG FILE EXAMPLE	81
FIGURE 4.12 FTP TRANSFER LOG FILE EXAMPLE.....	83
FIGURE 4.13 SSH LOG FILE “INETDLOG” EXAMPLE	85
FIGURE 4.14 ERROR LOG CONTENTS	88
FIGURE 4.15 HTTP ACCESS LOG FILE.....	91
FIGURE 4.16 ACCESS LOG TABLE.....	92
FIGURE 4.17 OSHTTP ERROR LOG FILE.....	92
FIGURE 4.18 MISSING EXAMPLE.....	94
FIGURE 4.19 DACM CENTRAL AGENT RESULTS	96
FIGURE 5.1 CERIAS NETWORK BLOCK DIAGRAM.....	103
FIGURE 5.2 SNORT IDS ALERTS	108
FIGURE 5.3 IDS ALERT CORRELATION INTERFACE	109
FIGURE 5.4 AF CORRELATION RESULT	110
FIGURE 5.5 TR CORRELATION RESULT	111
FIGURE 5.6 FINAL CAM CORRELATION RESULT ⁸	111
FIGURE 5.7 ABCM LEARNING PHASE.....	112
FIGURE 5.8 ABCM’S CORRELATION PHASE RESULTS.....	113
FIGURE 5.9 DPCM CORRELATION STAGES RESULT	114
FIGURE 5.10 DPCM FINAL CORRELATION RESULT	115
FIGURE 5.11 REDUCTION RATES COMPARISON OF IDS CORRELATION TECHNIQUES	117
FIGURE 5.12 CORRELATION TIMES COMPARISON OF IDS CORRELATION TECHNIQUES	120
FIGURE 5.13 CORRELATION TIMES COMPARISON OF IDS CORRELATION TECHNIQUES	121
FIGURE 5.14 SSH AGENT RESULT	122
FIGURE 5.15 ABCM RESULT FOR SPECIFIC IP AS PART OF DACM ¹³	122
FIGURE 5.16 DACM DAILY RESULTS.....	123

FIGURE 5.17 DACM IP REPORT FORM ABCM IDS CORRELATED ALERTS ...	125
FIGURE 5.18 DACM IP REPORT FORM HTTP ATTACK ¹⁵	125
FIGURE 5.19 DACM MAXIMUM PRIORITY REPORT	126
FIGURE 5.20 LOW AND SLOW ATTACK SUMMARY	127
FIGURE 5.21 LOW AND SLOW ATTACK FOR 192.160.165.222 ¹⁷	127
FIGURE 5.22 LOW AND SLOW ATTACK FOR 216.129.119.45	128
FIGURE 5.23 DACM SUMMARY REPORT ¹⁸	128
FIGURE 5.24 DACM SUMMARY RESULTS CHART	131
FIGURE 5.25 DACM PERCENTAGE SUMMARY RESULTS CHART.....	132

LIST OF TABLES

TABLE 2.1 CYBER ATTACKERS COMPARISON 19

TABLE 2.2 SOURCES OF INTRUSION DETECTION DATA CORRELATION 21

TABLE 2.3 CAM COMPONENTS REDUCTION RATE FOR DIFFERENT
DATASETS 41

TABLE 4.1 FIREWALL ATTACK TABLE 80

TABLE 4.2 FTP ATTACK TABLE..... 83

TABLE 4.3 FTP TRANSFER ATTACK TABLE 85

TABLE 4.4 SSH TRANSFER ATTACK TABLE 87

TABLE 4.5 HTTP ATTACK TABLE RECORD 90

TABLE 4.6 DAILY REPORT TABLE ATTRIBUTES 98

TABLE 5.1 SNORT IDS ALERT ATTRIBUTES 109

TABLE 5.2 ALERT CORRELATION REDUCTION RATES COMPARISON 116

TABLE 5.3 CORRELATION TIME COMPARISON FOR IDS ALERT
CORRELATION MODELS ORDERED BY DATE OF ALERTS 118

TABLE 5.4 CORRELATION TIME COMPARISON FOR IDS ALERT
CORRELATION MODELS ORDERED BY ALERTS COUNT 119

TABLE 5.5 DACM SUMMARY RESULT 129

TABLE 5.6 DACM PERCENTAGE SUMMARY RESULT 130

List of Algorithms

ALGORITHM 4-1 LEARNING PHASE69

ALGORITHM 4-2 ABCM CORRELATION PHASE 71

ALGORITHM 4-3 DPCM ALGORITHM 75

ALGORITHM 4-4 SAVE IP FUNCTION 78

ALGORITHM 4-5 FIREWALL AGENT.....80

ALGORITHM 4-6 FTP AGENT 82

ALGORITHM 4-7 FTP TRANSFER AGENT 84

ALGORITHM 4-8 SSH AGENT 86

ALGORITHM 4-9 HTTP AGENT..... 89

ALGORITHM 4-10 ACCESS LOG AGENT 93

ALGORITHM 4-11 MISSING LOG AGENT..... 95

ALGORITHM 4-12 DACM CENTRAL AGENT 97