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 المتعددون

رسالة

مقدمة للحصول على درجة الدكتوراه فى الهندسة الكهربية

(هندسة الحاسبات والنظم)

مقدمة من

أيمن السيد السيد طه

ماجستير الهندسة الكهربية

(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

List of Figures

LIST OF TABLES

List of Algorithms