UNIVERSITI PUTRA MALAYSIA

DETECTING COORDINATED DISTRIBUTED ATTACKS USING MOBILE AGENTS WITH ASSOCIATED MANAGERS ARCHITECTURE

ALI JAVAN

FK 2011 78

DETECTING COORDINATED DISTRIBUTED ATTACKS USING MOBILE AGENTS WITH ASSOCIATED MANAGERS ARCHITECTURE

By

ALI JAVAN

© COPYRIGHT UPM

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

June 2011

DEDICATION

*This thesis is dedicated to my beloved mother **Maryam Rezaei** and the memory of my father **Mohammad Ali Javan**, those who gave me the love of studying and respect for education, and to my dear uncle **Mohammad Javan**, who has been my greate source of support and inspiration.*

© COPYRIGHT UPM

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master.

DETECTING COORDINATED DISTRIBUTED ATTACKS USING MOBILE AGENTS WITH ASSOCIATED MANAGERS ARCHITECTURE

By

ALI JAVAN

June 2011

Chair: Khairulmizam Samsudin, PhD

Faculty: Engineering

Technological advances have led the modern world to a global network ecosystem. More complex threats including coordinated distributed attacks have flourished against the vital services and priceless resources stored on the omnipresent networks, compels companies to resort to numerous security measures to defend against outsiders and even legitimate insiders of their networks. Attacks that have already penetrated through the first shield of defense (i.e. firewall) should be detected with automatic intrusion detection systems (IDS). Existing detection models together with other Internet services have suffered from common deficiencies historically inherited during the creation of the networking and the Internet. Several models have been proposed which emphasized on reducing these deficiencies in some aspect; though, introducing different drawbacks altogether on the network. Distributed intrusion detection system based on mobile agents has attracted the most attention due to their reliability and ability to recognize variety of distributed attacks with minimum burden on available resources. In this thesis we have introduced a distributed architecture based on autonomous mobile agent that relies on Associated Managers (AM) strategy. Associated Managers in charge of managing distinct virtual territories

© COPYRIGHT UPM

in a large network may remove the single point of failure, improve the performance and decrease the overhead load imposed by distributed IDS architecture on the network. Unlike existing proposed distributed mobile agent IDS, AM architecture has led to improved stability and reliable IDS with less severe bottlenecks. In this thesis the design and implementation of simulated AM using JADE (Java Agent DEvelopment framework) framework, are presented in detail. Performance of AM architecture, facing coordinated distributed attacks in different phases, is presented. Comparisons are made with proposed distributed IDS architecture based on mobile agents from the literature. Upon designing and developing a simulation test bed, an evaluation strategy based on simulated coordinated attacks is devised to clearly illustrate the performance of each architecture. Various aspects critical for a distributed IDS in detecting coordinated attacks are thoroughly assessed and advantages of AM over the other architecture are presented.

The results indicates that in comarison with the other mobile agent based model, the performance of AM in terms of time of detection and bandwidth usage is less affected by the number of infected hosts and correlation method and correlation time. As such, AM could finish the detection faster by consuming less amount of bandwidth in case of wide-spread distributed attacks. The performance of AM is more stable in the event of increasing overwhelmed hosts in the network. Overall, using AM model is beneficial for detecting the coordinated distributed attacks and improved the performance of detection in every phase of coordinated distributed attacks.

© COPYRIGHT UPM

Abstrak ini dibentangkan kepada Senat Universiti Putra Malaysia bagi memenuhi salah satu syarat untuk bergraduat Ijazah Master Sains

MENGESAN SERANGAN SEBARAN TERKOORDINASI MENGGUNAKAN EJEN MOBILE SERTA SENIBINA *ASSOCIATED MANAGERS*

Oleh

ALI JAVAN

Jun 2011

Pengerusi: Khairulmizam Samsudin, PhD

Fakulti: Kejuruteraan

Kemajuan teknologi telah membawa dunia moden kepada rangkaian ekosistem yang global. Kesannya ialah ancaman bertambah rencam termasuk serangan sebaran terkoordinasi terhadap perkhidmatan yang sangat penting terdapat dalam rangkaian, menjadikan syarikat terpaksa membina langkah balas untuk menyangkal godaman dari luar atau dalam rangkaian mereka. Serangan yang telah menembusi *firewall* harus dapat dikesan melalui *intrusion detection system* (IDS). Model pengesanan sedia ada yang disediakan oleh perkhidmatan internet tidak dapat menampung lagi serangan tersebut. Banyak model telah dicadangkan bagi menampung kelemahan dalam sesetengah aspek; walaupun ia menimbulkan kelemahan yang berbeza sama sekali pada rangkaian. *Intrusion detection system* yang mobil, menarik perhatian kerana kehandalan dan kemampuan untuk mengenalpasti serangan dengan beban minimum pada sumber yang sedia ada. Dalam tesis ini kami telah memperkenalkan satu rekabentuk berasaskan ejen mobile autonomous yang bergantung kepada strategi *Associated Managers* (AM). *Associated Managers* bertanggung jawab menguruskan beberapa daerah dalam rangkaian yang besar, dan membuang poin gagal (*failure*

© COPYRIGHT UPM

point), mempertingkatkan prestasi dan mengurangkan beban yang disebabkan oleh *intrusion detection system* (IDS). Tidak seperti yang disarankan oleh IDS yang sedia ada, senibina AM meningkatan kestabilan dan kebolehpercayaan IDS serta mengurangkan kesesakan . Tesis ini membentangkan reka bentuk pelaksanaan dan simulasi AM menggunakan framework JADE, akan dijelaskan secara terperinci. Prestasi senibina AM, yang menghadapi serangan sebaran terkoordinasi dalam pelabagar fasa juga di jelaskan.

Perbandingan dibuat berdasarkan kepada cadangan senibina IDS berasaskan agen mobile sedia ada. Semasa merancang dan membentuk *test bed* simulasi satu strategi ujian penilaian berdasarkan serangan sebaran terkoodinasi telah disediakan bagi menjelaskan prestasi setiap senibina. Berbagai aspek penting untuk sebuah IDS untuk mengesan serangan sebaran terkoordinasi akan dinilai secara terperinci dan kelebihan AM mengatasi senibina yang lain akan dijelaskan.

Keputusan menunjukkan bahawa perbandingan dengan model ejen lain yang berasaskan mobile, prestasi AM dari segi masa pengesanan dan penggunaan bandwidth kurang terjejas oleh beberapa host yang dijangkiti, begitu juga dengan kaedah dan masa korelasi. Oleh itu, AM dapat menjalankan pengesanan yang lebih cepat dengan penggunaan jalur lebar yang sedikit sekiranya berlaku serangan sebaran terkoordinasi. Prestasi AM juga adalah lebih stabil sekiranya berlaku peningkatan host dalam rangkaian. Secara keseluruhannya, penggunaan model AM dapat mengesan serangan sebaran terkoordinasi dan meningkatkan prestasi pengesanan di setiap fasa serangan sebaran terkoordinasi.

© COPYRIGHT UPM

ACKNOWLEDGEMENTS

At the outset, I am thankful to the Almighty God who is the most beneficent and most merciful, for all his blessings, without which I wouldn't be able to achieve this feat.

I would take this opportunity to thank my thesis supervisor Dr. Khairulmizam bin Samudin of the Department of Computer and Communication System, Engineering Faculty, Universiti Putra Malaysia. His remarkable level of knowledge and support has led me to work confidently and his critical comments and suggestions instructed the study in the right direction. Without his significant assistance and patience, I could not have finished this dissertation.

Special thank goes to my co-supervisors, Associate Professor Abdul Rahman Ramli, who has also markedly helped me to finalize this dissertation.

I am also thankful to all the staff and authorities of the Universiti Putra Malaysia, particularly the Department of Computer and Communication System.

Last but not least, I would like to thank my family and friend. My beloved mother Maryam Rezaei who gave me life and love in the first place; her great trust, dedication and generosity has backed me in my entire life. My late father Mohammad Ali Javan for his unconditional support during his life and his great inspiration, which has led me to pursue my dreams. My dear brother and sister and respected friends, for their incredible support and encouragement.

There are many more who deserve to be thanked whose names I may have forgotten to mention, but their priceless help, friendship and advice are always appreciated.

© COPYRIGHT UPM

I certify that a Thesis Examination Committee has met on **the 3th of Jun, 2011** to conduct the final examination of Ali Javan on his thesis entitled "**DETECTING COORDINATED DISTRIBUTED ATTACKS USING MOBILE AGENTS WITH ASSOCIATED MANAGERS ARCHITECTURE**" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Raja Syamsul Azmir bin Raja Abdullah, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

M. Iqbal bin Saripan , PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Fakhrul Zaman Bin Rokhani , PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Kasmiran Jumari, PhD
Professor
Faculty of Engineering
Universiti Kebangsaan Malaysia
(External Examiner)

_____

BUJANG KIM HUAT, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

© COPYRIGHT UPM

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the **Master of Science**. The members of the Supervisory Committee were as follows:

Khairulmizam Samsudin, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abdul Rahman Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

© COPYRIGHT UPM

_____

HASANAH MOHD GHAZALI, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institutions.

_____

ALI JAVAN

Date:3 June 2011

© COPYRIGHT UPM

TABLE OF CONTENTS

© COPYRIGHT UPM

© COPYRIGHT UPM

© COPYRIGHT UPM