2009

An agent-based framework for distributed intrusion detections

Dayong Ye

University of Wollongong

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author.

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
An Agent-Based Framework for Distributed Intrusion Detections

A thesis submitted in fulfillment of the requirements for the award of the degree

Master by Research

from

UNIVERSITY OF WOLLONGONG

by

Dayong Ye

School of Computer Science and Software Engineering
May 2009
© Copyright 2009

by

Dayong Ye

All Rights Reserved
Dedicated to
Zhen Ye and Tonghua Wang
Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Dayong Ye
May 25, 2009
Abstract

Network application has become a part of our everyday life. With the increasing of convenience and popularity of network, more and more malicious users utilize network to obtain their vicious intentions. In order to protect network users’ information security and privacy, various intrusion detection systems were proposed and developed in the last decade. Intrusion detection as an emerging technology has made great achievements in theory and practice, whose aim is to protect the confidentiality, integrity or availability of a system or resource. As a complex system, the development of an intrusion detection system includes many aspects, such as system architecture design, design and implementation of system components, system test in real cases, and so on.

Though many intrusion detection systems have been presented, most of them mainly focus on one or two aspects of intrusion detection systems. This thesis aims at providing a rudimentary solution for an agent-based Peer-to-Peer distributed intrusion detection framework. The major contributions of this thesis include the following five aspects.

1. Introducing a novel Peer-to-Peer framework which involve different agents on different peers;

2. Designing functionalities of each agent in the framework by using JACK/UML approach;

3. Representing knowledge of each agent about intrusion and detection according to employing ontology;

4. Developing an efficient task allocation protocol which is used to coordinate different hosts in the system to collaboratively detect distributed attacks;

5. Implementing and testing the framework in a reasonable manner by utilizing an agent development environment, i.e. $JACK^{TM}$.

In summary, this framework integrates agent technology, Peer-to-Peer architecture, ontology technique and a task allocation protocol. Implementation and experiments
show the potential applicability of this framework to real cases. In addition, this framework could help in development of a good intrusion detection system in open and complex environments.
Acknowledgements

Studying abroad is a tedious and tired journey. Without the help and support of many people, I cannot complete my research.

I am indebted to my supervisors, Associate Professor Minjie Zhang and Dr. Quan Bai. Their constant commitment and guidance was instrumental in the completion of this thesis, and in making it a fulfilling experience. I am grateful to Dr. Quan Bai for his kind help, encouragement and patient proofreading my thesis and research papers. I am also delighted for Associate Professor Minjie Zhang’s enthusiasm for my everyday life. Furthermore, I thank the School of Computer Science and Software Engineering and the University of Wollongong for the financial support of conference attendance.

My thanks are extended to Mr. Shaojie Yuan, who often discusses with me in the lab and enriches my knowledge; and Mr. Guohua Yao, my house mate, who chats with me during our dinner time everyday and brings me a lot of fun.

I would like to express my deepest gratitude to my parents, Zhen Ye and Tonghua Wang, who always make their financial support, encouragement, understanding and love. Without their help, this thesis would not be finished. Thanks too, to my wife, Yun, for her constantly tolerating my selfishness and her delicious food. I hope she could forgive me for what I have done. I have dedicated this thesis to my parents and my wife for their patience, understanding and unconditional love.

Finally, thanks to all the anonymous reviewers of my research papers, and all my other dear friends and relatives who have supported me.
Publications

The followings are list of my research papers that have been already published during my Master study that is to be ended by the completion of this thesis.


## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>v</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>vii</td>
</tr>
<tr>
<td>Publications</td>
<td>viii</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Intrusion and Intrusion Detection</td>
<td>2</td>
</tr>
<tr>
<td>1.1.1 Intrusion</td>
<td>2</td>
</tr>
<tr>
<td>1.1.2 Intrusion Detection</td>
<td>7</td>
</tr>
<tr>
<td>1.2 Agent-Based Intrusion Detection Systems</td>
<td>9</td>
</tr>
<tr>
<td>1.3 Research Concerns</td>
<td>12</td>
</tr>
<tr>
<td>1.4 Thesis Structure and Outcomes</td>
<td>14</td>
</tr>
<tr>
<td>2 Related Research and Literature Review</td>
<td>16</td>
</tr>
<tr>
<td>2.1 Architecture and Design of Agent-Based Intrusion Detection Systems</td>
<td>16</td>
</tr>
<tr>
<td>2.2 Intrusion Detection Language</td>
<td>18</td>
</tr>
<tr>
<td>2.3 Task Allocation Protocols and Resource Search Mechanisms</td>
<td>23</td>
</tr>
<tr>
<td>2.3.1 Task Allocation in Distributed Environments</td>
<td>23</td>
</tr>
<tr>
<td>2.3.2 Resource Search in P2P Environments</td>
<td>25</td>
</tr>
<tr>
<td>2.4 Summary</td>
<td>27</td>
</tr>
<tr>
<td>3 A Novel P2P Agent-Based Framework for Distributed Intrusion De-</td>
<td>28</td>
</tr>
<tr>
<td>tections</td>
<td></td>
</tr>
<tr>
<td>3.1 Framework Architecture</td>
<td>28</td>
</tr>
<tr>
<td>3.1.1 Monitor Agent</td>
<td>28</td>
</tr>
<tr>
<td>3.1.2 Analysis Agent</td>
<td>29</td>
</tr>
<tr>
<td>3.1.3 Executive Agent</td>
<td>29</td>
</tr>
<tr>
<td>3.1.4 Manager Agent</td>
<td>30</td>
</tr>
</tbody>
</table>
List of Tables

3.1 UML High Level Stereotypes for JACK\textsuperscript{TM} ............................. 34
3.2 UML Association Level Stereotypes for JACK\textsuperscript{TM} ............................. 34
4.1 An Example of N-Triples ................................................................. 47
4.2 N-Triples Notation for Suspicious Doorknob-Rattling Attack ................. 51
4.3 Query for Suspicious Doorknob-Rattling Attack ..................................... 52
# List of Figures

1.1 Attack Classification with Ontology ........................................... 4
1.2 A Paradigm of Doorknob-Rattling Attack .............................. 6
1.3 A Paradigm of Chain/Loop Attack ............................................. 7
1.4 A Paradigm of Mitnick Attack .................................................. 8
1.5 A Standard Architecture of IDS ................................................ 10

3.1 Architecture of the Framework ..................................................... 29
3.2 Retrieval Process ................................................................. 32
3.3 A Simple Example of Designing JACK$^TM$ Agent with UML ...... 35
3.4 Design of Monitor Agent with JACK/UML ............................... 35
3.5 Design of Analysis Agent with JACK/UML ............................... 37
3.6 Design of Executive Agent with JACK/UML ............................. 38
3.7 Design of Manager Agent with JACK/UML ............................... 40
3.8 Design of Retrieval Agent with JACK/UML ............................. 42
3.9 Design of Result Agent with JACK/UML ................................. 42

4.1 RDF relationship graph ........................................................... 44
4.2 Ontology representation of agent knowledge in each peer .......... 45
4.3 Monitor Agent Knowledge ..................................................... 46
4.4 Analysis Agent Knowledge .................................................. 48
4.5 Executive Agent Knowledge .................................................. 49
4.6 Manager Agent Knowledge .................................................. 50

5.1 Interaction Process Between Initiator and a Participant ............. 56
5.2 Performance of different protocols on distinct average number of neighbors 62
5.3 Performance of different protocols on distinct TTL value .......... 63
5.4 Performance of different protocols on distinct number of agents .. 64
5.5 The performance of ETAP with different number of walkers ........ 66
6.1 An example P2P network which has been attacked by Doorknob-Rattling 69
6.2 Detection of Doorknob-Rattling Attack with different mechanisms . . . 70
6.3 An example P2P network which has been attacked by Chain/Loop . . 72
6.4 Detection of Chain/Loop Attack with different mechanisms . . . . . . 73
6.5 An example P2P network which has been attacked by Mitnick . . . . 74
6.6 Detection of Mitnick Attack with different mechanisms . . . . . . . . 76