THE EFFECTIVENESS OF DETECTION METHODS IN INTRUSION DETECTION SYSTEMS

HAFIZ BIN MOHD SARIM

Disertasi yang diserahkan untuk memenuhi keperluan bagi Ijazah Sarjana Teknologi Maklumat

Mac 2002
**Abstrak**

Mekanisma kawalan capaian yang diberikan bersama-sama sistem pengendalian komputer kurang berkesan dalam menahan pencerobohan dari pengguna luar. Sistem Pengesa Pencerobohan adalah sejenis perisian keselamatan komputer yang boleh mengesahkan pencerobohan yang sedang berlangsung dan juga mampu mengelakkan kerosakan sistem dari berlaku. Pengesanan yang dilakukan ini bergantung kepada metodologi pengesanan yang digunakan oleh Sistem Pengesa Pencerobohan. Dari berbagai jenis metodologi pengesanan yang ada, empat jenis metodologi dipilih disini. Setiap metodologi pengesanan dibincangkan dan juga ditaksirkan dari segi keberkesanannya dalam menangani pelbagai jenis pencerobohan, kesilapan klasifikasi, dan juga dari aspek perlaksanaan sebenar. Beberapa cadangan dikemukakan untuk memperbaikan lagi metodologi pengesanan. Cadangan-cadangan ini termasuk menggabungkan metodologi pengesanan yang ada, memproses jejak audit bagi mengelakkan input yang rosak, dan juga menyertakan mekanisma pencegahan kerosakan sistem akibat dari pencerobohan. Metodologi pengesanan yang digunakan juga perlu mampu ditingkatkan lagi untuk mengikuti perkembangan infrastruktur. Pengesanan pencerobohan secara am boleh, juga dipertingkatkan lagi dengan menguatkuasakan polisi keselamatan, mengawal masa capaian, dan juga menghadkan hak-hak kakitangan pentadbiran untuk mengelakkan penyalahgunaan hak-hak yang diberikan.
Abstract

Access control mechanisms included in operating systems are not very effective in preventing intrusions by the most determined of attackers. An Intrusion Detection System (IDS) is a security software that is able to detect an intrusion when it occurs and can potentially prevent a system compromise from being completed. The actual detection is done by the detection method used by the IDS. Four detection methods are discussed and assessed in terms of their effectiveness in repelling intrusion types, vulnerability to classification errors; and also performance in practical implementation. Recommendations are made to improve the general effectiveness of the detection methods in use. They include combining detection methods, pre-processing audit logs to prevent bad input, and including mechanisms to preempt intrusions from completing. The method must also be scalable to accommodate infrastructural growth. Intrusion detection can also be improved by careful enforcement of security policy, adding access time limitations, and also limiting administrative privileges to prevent abuse of the powers entrusted upon them.
Acknowledgements

This dissertation was written to fulfill the requirements of the Masters of Information Technology program at Universiti Malaya. As the author, I would like to extend my gratitude and appreciation to the people who made this research report possible: the Masters of IT Class of 2002, faculty and administrative staff of the Faculty of Computer Science and Information Technology, and the entire administration of the University. Special thanks goes out to Mrs. Miss Laiha Mat Kiah, a lecturer in the faculty specializing in computer networks and computer security, and also the Masters Dissertation Supervisor for this research. Thank you for your priceless guidance and assistance in making this research report a reality.

This dissertation was written by Hafiz bin Mohd Sarim and is the rightful property of University Malaya.
# Table of Contents

**ABSTRACT** ........................................................................................................ III

**ACKNOWLEDGEMENTS** .................................................................................... IV

**TABLE OF FIGURES** ....................................................................................... VII

**GLOSSARY OF TERMS** ..................................................................................... VIII

**PART 1: INTRODUCTION TO INTRUSION DETECTION SYSTEMS (IDS)** ............. 1

1.1 OVERVIEW OF SECURITY ................................................................................. 2

1.1.1 Security in Computing .................................................................................. 2

1.1.2 The Need for Additional Security ................................................................. 3

1.2 INTRODUCTION TO INTRUSION DETECTION SYSTEMS ............................. 5

1.2.1 Definition of Intrusion Detection Systems (IDS) ......................................... 5

1.2.2 Limitations of Computer Systems ................................................................. 5

1.2.3 Elements of an Intrusion Detection System ............................................... 7

1.2.4 Management of Intrusion Detection Systems ............................................. 9

1.3 FOCUS OF RESEARCH ................................................................................... 10

**PART 2: IDS PERFORMANCE MEASUREMENTS** ........................................... 13

2.1 INTRUSION TYPES AND INTRUDER PERSONALITIES ............................... 14

2.1.1 Intruder Types ............................................................................................. 14

2.1.2 Intruder Personalities and Categorization .................................................. 18

2.2 ERROR TYPES ............................................................................................... 20

2.2.1 Classification Errors .................................................................................... 20

2.2.2 False Positive ............................................................................................. 20

2.2.3 False Negative ............................................................................................ 22

2.3 PRACTICAL CONSIDERATIONS .................................................................... 25

2.3.1 Restriction of User Activity ........................................................................ 25

2.3.2 Suspension of Supervision ......................................................................... 27

2.3.3 Response to Suspected Intrusions .............................................................. 28

2.4 DEFINITION OF EFFECTIVENESS ............................................................... 31
PART 3: ANALYSIS OF IDS DETECTION METHODS .................................................. 35

3.1 BEHAVIOR-BASED INTRUSION DETECTION BY OBSERVING THE SEQUENCES OF SYSTEM CALLS ................................................................. 38

3.1.1 Description of Methodology .................................................................. 38
3.1.2 Effectiveness of Detection Method against Intrusion Types ..................... 46
3.1.3 Capacity of Detection Method in Overcoming Error Types ....................... 53
3.1.4 Performance and Impact of Detection Method in Practical Implementation .... 56

3.2 BEHAVIOR-BASED INTRUSION DETECTION THROUGH FILE INTEGRITY CHECKING .......................................................... 59

3.2.1 Description of Methodology .................................................................. 59
3.2.2 Effectiveness of Detection Method against Intrusion Types ..................... 67
3.2.3 Capacity of Detection Method in Overcoming Error Types ....................... 74
3.2.4 Performance and Impact of Detection Method in Practical Implementation .... 77

3.3 KNOWLEDGE-BASED INTRUSION DETECTION USING STATE TRANSITION ANALYSIS .. 80

3.3.1 Description of Methodology .................................................................. 80
3.3.2 Effectiveness of Detection Method against Intrusion Types ..................... 90
3.3.3 Capacity of Detection Method in Overcoming Error Types ....................... 97
3.3.4 Performance and Impact of Detection Method in Practical Implementation .... 100

3.4 KNOWLEDGE-BASED INTRUSION DETECTION USING PATTERN-ORIENTED MODELING ..

.......................................................... 103

3.4.1 Description of Methodology .................................................................. 103
3.4.2 Effectiveness of Detection Method against Intrusion Types ..................... 113
3.4.3 Capacity of Detection Method in Overcoming Error Types ....................... 120
3.4.4 Performance and Impact of Detection Method in Practical Implementation .... 123

3.5 SUMMARY OF IDS DETECTION METHOD EFFECTIVENESS ....................... 127

PART 4: RECOMMENDATIONS AND CONCLUSION ............................................... 131

4.1 OBSERVATIONS FOR IMPROVEMENTS IN GENERAL DETECTION METHODOLOGY .... 132
4.2 OTHER CHANGES NECESSARY FOR EFFECTIVE INTRUSION DETECTION ............. 140
4.3 CONCLUSION ....................................................................................... 145

BIBLIOGRAPHY ......................................................................................... 148
Table of Figures

FIGURE 1: A SAMPLE WORKING ARCHITECTURE OF AN INTRUSION DETECTION SYSTEM .......... 10
FIGURE 2: HOW THE IDS IS USED TO DETECT ANOMALOUS SEQUENCES ........................................ 43
FIGURE 3: BASIC STRUCTURE OF AN IDS TOOL THAT OBSERVES THE SEQUENCES OF SYSTEM CALLS .................................................................................................................. 44
FIGURE 4: BASIC STRUCTURE OF AN IDS TOOL BASED ON THE FILE INTEGRITY CHECKING METHOD ................................................................................................................. 61
FIGURE 5: COLLISION FREQUENCIES OF VARIOUS SIGNATURES USED IN A TEST OF THE FILE INTEGRITY CHECKING METHOD ....................................................................... 64
FIGURE 6: SAMPLE REPORT FROM THE FILE INTEGRITY CHECKER .............................................. 65
FIGURE 7: A SAMPLE OF A STATE TRANSITION DIAGRAM ......................................................... 81
FIGURE 8: A STATE TRANSITION DIAGRAM USED TO DISSECT A KNOWN INTRUSION INTO RECOGNIZABLE STATE ASSERTIONS ........................................................................ 84
FIGURE 9: BASIC STRUCTURE OF AN IDS TOOL BASED ON THE STATE TRANSITION ANALYSIS DETECTION METHOD .................................................................................. 87
FIGURE 10: A SAMPLE OF AN INFEERENCE ENGINE TABLE .......................................................... 88
FIGURE 11: SHAPES USED TO REPRESENT THE ELEMENTS OF A PROTECTION GRAPH ............... 105
FIGURE 12: SIMPLE EXAMPLE OF 4 DIFFERENT AND BASIC PROTECTION GRAPHS ................. 107
FIGURE 13: THE FOUR INFEERENCE RULES USED IN THE PATTERN-ORIENTED MODELING INTRUSION DETECTION METHOD AS SEEN IN A PROTECTION GRAPH ......................... 109
FIGURE 14: A BREAK DOWN OF THE DEMONSTRATION OF AN INTRUSION TECHNIQUE AS SEEN IN A PROTECTION GRAPH .............................................................................. 111
FIGURE 15: BASIC STRUCTURE OF AN IDS TOOL BASED ON THE PATTERN-ORIENTED MODELING METHOD ........................................................................................................... 112

TABLE 1: EFFECTIVENESS OF DETECTION METHODS AGAINST INTRUDER TYPES .................. 127
TABLE 2: EFFECTIVENESS OF DETECTION METHODS AGAINST CLASSIFICATION ERRORS ........ 129
TABLE 3: EFFECTIVENESS OF DETECTION METHODS IN PRACTICE ............................................. 130
Glossary of Terms

Anomaly – Deviation from a known behavior or characteristic.

Audit logs – Computer records that historically lists the activity performed by a user or system process.

Audit preprocessing – Activity done to remove irrelevant or erroneous data found in audit logs.

Back doors – Computer programs that are written to bypass the access control mechanisms of an operating system.

Behavior-based – A category of detection methods used in an Intrusion Detection System.

Buffer overrun – A condition that occurs as a result of the memory or buffer space used by a process exceeding its limits or boundaries.

Classification errors – Mistakes done by the Intrusion Detection System in its detection process.

Cracker – A category of attacker whose intent is usually to compromise or cause damage to a computer system.

Detection methodology – Method used by an Intrusion Detection System to detect intruders.

False positive – A misidentification of an intrusion.

False negative – A failure to identify an intrusion.

finger – A UNIX program that generates a list of users currently connected to a computer system.


IDS administrator – The person directly responsible for the configuration and maintenance of an Intrusion Detection System. Also responsible to respond to alerts given by the IDS. Usually the system administrator.

IMS – Intrusion monitoring system. Same as IDS. See Intrusion Detection System below.

Intruder – Person or process that attempts illegal access to system, or compromise of a computer system or its contents.
Intrusion Detection System – A security software that is used to detect intrusions and alert the IDS administrator of the intrusion. It might also preempt the intrusion from completing.

Knowledge-based – A category of detection methods used in an Intrusion Detection System.

lpr – The printing program used in the UNIX operating system.

passwd – The name of the password file used in the UNIX operating system.

Preemption – A process of interfering with an intrusion attempt to prevent it from successfully completing.

Privilege – Access or rights given to users or processes.

RTID – Real-Time Intrusion Detector

Scanners – A type of Intrusion Detection System that attempts to locate intruders offline. It does not operate in real-time.

sendmail – The program that allows the sending, receiving, and managing of E-mail used in the UNIX operating system.

Superuser – A level of privilege that allows unlimited and unrestricted access to the computer system.

System objects – primitive and most basic commands used by a particular operating system to complete a process.