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 Inference 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 inference 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.