# Malware Detection and Prevention System Based on Multi-Stage Rules

*Ammar Alazab, School of Information Technology, Deakin University, Burwood, VIC, Australia*

*Michael Hobbs, School of Information Technology, Deakin University, Burwood, VIC, Australia*

*Jemal Abawajy, School of Information Technology, Deakin University, Burwood, VIC, Australia*

*Ansam Khraisat, Ballarat University, Mt Helen, VIC, Australia*

## ABSTRACT

*The continuously rising Internet attacks pose severe challenges to develop an effective Intrusion Detection System (IDS) to detect known and unknown malicious attack. In order to address the problem of detecting known, unknown attacks and identify an attack grouped, the authors provide a new multi stage rules for detecting anomalies in multi-stage rules. The authors used the RIPPER for rule generation, which is capable to create rule sets more quickly and can determine the attack types with smaller numbers of rules. These rules would be efficient to apply for Signature Intrusion Detection System (SIDS) and Anomaly Intrusion Detection System (AIDS).*

*Keywords:* *Anomaly Intrusion Detection System (AIDS), Attack, Intrusion Detection System (IDS), Malicious, Malware, Signature Intrusion Detection System (SIDS), Zero Day Attacks*

## 1. INTRODUCTION

Intrusion detection is the method of recognizing user activities that may possibly steered a computer system from a secured state to an unsecure state. Since the quantity of attacks against computer systems increases regularly, it is very important for IDS to be effective; that is means, it should detect known and unknown attacks with minimum false alarms. However, Most of the IDS designed have problem in efficiently detecting all the attacks attempts and need a quantity of computational overhead, making it challenging to create real-time IDS.

There are two approaches to analysing events using IDSs. These are Signature based Intrusion Detection Systems (SIDS) and Anomaly based Intrusion Detection Systems

DOI: 10.4018/jisp.2013040102

(AIDS) .At an earlier time of intrusion detection techniques mostly rely on signatures patterns of well-known Malware and take decisions by match up to signatures. This style of detection strategy is usually known as (SIDS). Nevertheless, it is very hard for SIDS to detect zero attack with unidentified signatures (Alazab, Abawajy, & Hobbs, 2013; Alazab, Alazab, Abawajy, & Hobbs, 2011). AIDS use a model of the normal system behavior and try to find important features from this model in the data achieved through the real behavior of the system (Spathoulas & Katsikas, 2010). However, (AIDS) has attracted the interest of many researchers to overcome the disadvantage of SIDS. AIDS detects users' activities that are not the usual behaviour on a computer network. According to this approach, the assumption is that attacker behaviour deviates from normal user behaviour. Thus, AIDS involves the training stage and a testing stage. In the training stage, the normal traffic profile is labelled by using data that is accepted as normal behaviour; in the latter, the testing stage is applied to new data set. The result from this, the AIDS have ability to monitors the activities of new users and compares the new data with the obtained profile and tries to detect deviations. Those different from normal behaviour are considered as attacks (Alazab, Hobbs, Abawajy, & Alazab, 2012).

AIDS is categorized into many sub-kinds in the literature such as statistical techniques, data mining, artificial neural networks, and genetic algorithms and so on. The main benefit of an anomaly-based scheme is the power to detect zero days Malware. The reason for that, the AIDS does not depend on signatures database. It is used a model describing the normal user behavior, and any abnormal behavior that deviates from the model is identified. Thus, AIDS has many advantages. First, they have the ability to find insider attacks. Second, the AIDS relies on the users profiles. Thus it is extremely hard for an attacker to identify what the normal user activity without generation an alarm (Patcha & Park, 2007). The reason for that the AIDS uses machine learning techniques in order to build user profiles. Unfortunately, making a user profiles is a challenging task because AIDS looking for unusual activity rather than actual malicious (Patcha & Park, 2007).

As discussed above Independent approach for (AIDS) and (SIDS) will not be as effective as collaborative approach to detect known and unknown attacks at the same time. As Intrusive activity does not match with anomalous activity every time. Though, there are five probabilities as shown in Figure 1. To address this problem, we present a Multi stage Rules to create robust model, which can reveal behaviors of attackers. The central idea is to apply sequential multi stage rules to learn rules that accurately capture the behavior of intrusions and normal activities. If user activity instance doesn't satisfy any of the normal profile rules, then it is considered as new attack .These rules can then be applied for signature detection and anomaly detection. Our approach can give an accurate boundary between normal activities and intrusion.

*Figure 1. Probability to identify the intrusion and normal*