Chapter 9
Contextual Anomaly Detection Methods for Addressing Intrusion Detection

Florian Gottwalt
University of New South Wales, Australia

Elizabeth J. Chang
University of New South Wales, Australia

Tharam S. Dillon
University of New South Wales, Australia

ABSTRACT

One promising method to detect cyber-crime is anomaly detection, which enables one to detect new, unseen attacks. Despite this ability, anomaly detection methods only have limited utilization in practice, due to the high number of false alarms generated. Recent research has shown that the number of false alarms can be reduced drastically by considering the context in which these alarms occur. However, important questions include, What does context mean in the realm of anomaly detection? and How can it be incorporated to identify potential cyber-crime? To address these questions, this chapter provides novel definitions of context and contextual anomaly detection methods. Based on these, a new taxonomy is proposed for contextual anomaly detection methods, which organizes the methods by the specific problems they address. Further, the chapter highlights the potential of contextual anomaly detection for the reduction of false alarms, particularly for network anomaly detection and provides an introduction and holistic overview of the field for professionals and researchers.

DOI: 10.4018/978-1-7998-5728-0.ch009

INTRODUCTION

Cyber-crime is a continuously growing threat for individuals and organizations alike resulting in a high demand for novel approaches to detect and reduce the number of cyber-crimes. For organizations, one common method to detect and mitigate cyber-crime are intrusion detection methods. Intrusion detection methods utilize either signature detection methods, which allow to identify pre-defined, known attack signatures or anomaly detection methods, which allow to detect new, unseen attacks.

While anomaly detection methods are promising to detect novel types of attacks, their biggest problem is the large number of false alarms generated due to the difficulty of defining normal behaviour in a constantly changing environment. This particularly applies to network anomaly detection (NAD) methods, which often are not enabled in practice due to the overflowing of security analysts with alarms, false alarms (Chandola, Banerjee, & Kumar, 2009).

One way to reduce the number of false alarms in anomaly detection methods is to incorporate context into the process to, "put alarms into context". But what does context mean in the realm of anomaly detection and how can it be considered and incorporated into the process? Context is an ambiguous term, which has been interpreted and used in various ways, all under the umbrella of contextual anomaly detection (CAD). The lack of distinction between different areas of CAD has led to some extensively studied areas overshadowing other areas of anomaly detection methods utilizing context.

Considering this neglect of distinction and the aim of reducing the number of false alarms for network anomaly detection and cyber-crime detection, this chapter:

- Highlights the biggest challenges NAD methods are facing due to the nature of network traffic and network attacks
- Analyses how context has been used in the network anomaly detection process
- Proposes novel definitions and a new taxonomy for CAD methods to resolve the ambiguity of the term context and its usage in anomaly detection
- Discusses and highlights opportunities for future research for the incorporation of context into the anomaly detection and cyber-crime detection process

In the following section, a brief background of network anomaly detection and the challenges traditional NAD methods are facing are highlighted. This is followed by a survey on how context has been used in the NAD process. Subsequently, the term context and its previous usage in anomaly detection is discussed, followed by a proposal of new definitions and a new taxonomy for contextual anomaly detection. Afterwards, the branches of the newly proposed CAD taxonomy are summarized. Before concluding this chapter, opportunities and challenges for the application of contextual anomaly detection in intrusion detection are discussed.

BACKGROUND AND CHALLENGES FOR TRADITIONAL NETWORK ANOMALY DETECTION

The field of network anomaly detection has been researched over a considerable time and due to the large corpus of work and surveys conducted, only challenges current state of the art network anomaly detection techniques face are summarized, without elucidating all the specific techniques in detail.