Chapter 10
Anomaly-Based Intrusion Detection:
Adapting to Present and Forthcoming Communication Environments

Jorge Maestre Vidal
https://orcid.org/0000-0002-4131-5100
Indra, Spain

Marco Antonio Sotelo Monge
Universidad Complutense de Madrid, Spain

Sergio Mauricio Martínez Monterrubio
https://orcid.org/0000-0002-1520-1249
Universidad Complutense de Madrid, Spain

ABSTRACT

Anomaly-based intrusion detection has become an indispensable player on the existing cybersecurity landscape, where it enables the identification of suspicious behaviors that significantly differ from normal activities. In this way, it is possible to discover never-seen-before threats and provide zero-day recognition capabilities. But the recent advances on communication technologies are leading to changes in the monitoring scenarios that result in novel challenges to be taken into consideration, as is the case of greater data heterogeneity, adversarial attacks, energy consumption, or lack of up-to-date datasets. With the aim on bringing the reader closer to them, this chapter deepens the following topics: evolution of the anomaly definition, anomaly recognition for network-based intrusion detection, outlier characterizations, knowledge acquisition for usage modelling, distances and similarity measures for decision-making, anomaly recognition and non-stationarity, metrics and evaluation methodologies, and challenges related with the emergent monitorization environments.

DOI: 10.4018/978-1-5225-9611-0.ch010

INTRODUCTION

The preliminary research in the Intrusion Detection Systems (IDS) field focused on monitoring and analyzing the protected environment looking for previously known patterns of malicious actions, which was typified as Signature-Based (SB) intrusion detection. But although nowadays this paradigm still playing an essential role in the cybersecurity landscape, the rapid proliferation of malware and related threats eventually encouraged the design of novel approaches, which were able to deal with never-seen-before threats (Maestre Vidal, Sandoval Orozco, & García Villalba, November 2017). This resulted in a wide variety of Anomaly-Based (ABS) Intrusion Detection Systems, that typically attained to recognize attacks by distinguishing the normal and habitual protected system usage (hypothesized as legitimate) form discordant (hypothesized as malicious). This modus operandi involves the adoption of knowledge acquisition and modelling capabilities that for the sake of effectiveness, should be adapted to the evolution over the years of the monitoring environments.

Consequently, the emergent communication ecosystem entails a brand-new change for researchers on anomaly-based intrusion detection, where environments like Internet of Things (IoT), Edge computing, the fifth generation of cellular mobile communications (5G), smart cities or Software-Defined Networks (SDN), lead to multiple and dynamic data sources, and more heterogeneous traffic with non-stationary features (Sotelo Monge, Maestre Vidal, & García Villalba, 2017). Another difficulty inherent to the new communication enablers is the constraint of computing resources, which is particularly present in ubiquitous computing and wearable devices. Due to this, the anomaly-based detection algorithms should not only be effective, but efficient.

With the aim on bringing the reader closer to these concerns, this chapter has the main objectives of reviewing and discussing the principal aspects of anomaly-based detection applied to intrusion detection and deepening in the challenges posed by the emerging communication technologies. The chapter is organizing into nine sections, being the first of them the present introduction. The second section defines the anomaly conceptualization and introduces the main lines of research related to this term; the third section reviews the different anomaly characterizations; the fourth section provides an overview of the knowledge acquisition strategies applied to the identification of anomalies; the fifth section introduces the different measures of similarity that are usually taken into account for their identification; the sixth section discusses the problem of detecting anomalies in non-stationary scenarios; the seventh section outlines their evaluation criteria; the eighth section describes the challenges faced by anomaly-based intrusion detection at the forthcoming communication scene; and the last section presents the conclusions and future research trends.

Anomalies and Conceptualization

The problem of identifying anomalies has been object of study for decades, as it can be observed in publications like (Edgeworth, 1887), where instead of the term “anomaly” the expression “discordant observation” was considered. As pointed out by (Chandola, Banerjee, & Kumar, 2009), the word anomaly has been replaced by equivalent concepts over the years, being also referred to as: outliers, isolated parts, exceptions, aberrations, surprises, peculiarities or polluting elements. The use of each of these tags usually varied according to the domain in which it has been used, just as it happened with their definition. In order to familiarize the reader with the evolution of this concept, the following discusses some of the most popular anomaly conceptualizations and the research topics directly related with their study.