Chapter 6
Classifying Host Anomalies: Using Ontology in Information Security Monitoring

Suja Ramachandran
Bhabha Atomic Research Centre, India

R.S. Mundada
Bhabha Atomic Research Centre, India

A.K. Bhattacharjee
Bhabha Atomic Research Centre, India

C.S.R.C. Murthy
Bhabha Atomic Research Centre, India

R. Sharma
Bhabha Atomic Research Centre, India

ABSTRACT

In this chapter, the authors propose an ontology based approach to classify the anomalous events occurring in a number of hosts, thus filtering the interesting or non-trivial events requiring immediate attention from a set of events. An ontology is developed to structure the domain of anomaly detection. It expresses the semantic relationships among the attributes of an anomaly detection system and events collected by it. The system harnesses the reasoning capability of ontology and that of inference engine to make meaningful assumptions about anomaly events. This enables automatic classification of the reported anomalies based on the functionality and significance of the originating host as well as the associated system resource or parameter.

1. INTRODUCTION

Security is a fundamental issue of concern in computing systems. With the recent trends in distributed computing and the emergence of World Wide Web as a universal medium for conducting business, security has become critical in IT architectures.

With the proliferation of computer systems and networks, security problems such as unau-

DOI: 10.4018/978-1-60960-123-2.ch006

thorized access of data, tampering of information systems etc. have turned into a major concern for all organizations. In maintaining secure computer networks, much of the difficulty can be attributed to the lack of proper information management: the amount of information at hand is enormous, much of it changes rapidly, and the relevant information is difficult to identify. The limitations of each security technology combined with the growth of cyber attacks impact the efficiency of information security management and make the network administrator's job tedious. Therefore, there is a need for automated information security monitoring systems that can manage themselves given high-level objectives from administrator.

The focus of modern information systems is moving from data-processing towards concept-processing, that is, the basic unit of processing is becoming more a semantic concept which carries an interpretation and exists in a context with other concepts. (Brank, Grobelnik and Mladenic, 2005). An ontology can be defined as a "formal, explicit specification of a shared conceptualization" (Gruber, 1993). It is a formal representation of a set of concepts within a domain and the relationships between those concepts. Ontological analysis clarifies the structure of knowledge. For a given domain, its ontology acts as a structure that captures and represents the knowledge on that domain. Ontologies are used in artificial intelligence, the Semantic Web, software engineering, biomedical informatics, library science, information architecture etc. as a form of knowledge representation about the world or some part of it.

In this chapter, we are proposing an information security monitoring system which is a combination of an anomaly detection system and an ontology based reasoning mechanism. In a diverse and complex network set-up, it is nearly impossible for the administrator to keep track of the activities and events occurring in each and every servers and devices. In our view, a comprehensive information security monitoring system must not only provide alarms on possible intrusion attempts, but it should be able to capture all the events of interest occurring in a network, thus providing a complete overview of system security. Such a system should be capable of analyzing the obtained data and presenting meaningful information to the system administrators.

The proposed system looks for anomalous behaviors of a host which might include security breaches, performance bottlenecks, resource misuses or configuration problems. Such a strategy of extensive event collection provides the administrator with a complete picture of what is happening in the network. Also, it improves the possibilities of real time detection of an attack taking place against the network. But, at the same time, this approach leads to a situation where the system administrators are flooded by the torrent of events to be able to understand the significance of each of them. In such cases, the events are usually just stored for future reference without any analysis or correlation; hence intrusion attempts might go unnoticed.

At this point, a matter of prime concern is that the significance/criticality of the reported anomalies varies from each other. Every host has a precise behavior in terms of its system resources and services running on it, hence what is considered normal/ trivial in one host's environment could be different in another. For example, an activity that can be ignored in a web server may be considered crucial when occurred in a mail server.

In this work, we attempt to categorize the obtained anomaly events based on their originating host and associated system resource or parameter, thus essentially filtering and reducing the amount of events requiring further analysis. Our idea is to develop an ontology to express the semantic relationships among attributes of the anomaly events, thus structuring the domain of anomaly detection. The power of ontology is used in expressing relationships between collected data, and its reasoning capability to categorize the events into predefined compartments.