Chapter 108
Adaptive Intrusion Detection Systems: The Next Generation of IDSs

Hassina Bensefia
Mohamed El Bachir El Ibrahimi University, Algeria

Nassira Ghoualmi-Zine
Badji Mokhtar University, Algeria

ABSTRACT

This chapter deals with a challenging issue in intrusion detection research field, which is IDS adaptability. First, it introduces the intrusion detection concepts, then presents with details the two existing generations of IDSs and addresses their major problem: permanent coverage of new attacks patterns in a dynamic changing environment. Thereafter, it evokes the requirement of adaptability in IDS as a mean to remedy this deficiency. Later, it explores the most eminent approaches that are proposed for IDS adaptability. It describes their functional architecture and discusses their strong aspects and weaknesses. At the end, new trends toward the intrusion detection adaptability problematic are mentioned and followed by a conclusion.

1. INTRODUCTION

The intrusion detection field is characterized by two generations of Intrusion Detection Systems (IDSs). The first IDSs generation is conceived by an ad hoc manner and depends on human expertise. This classical generation presents limited performance related to the IDS target environment which is becoming increasingly changing complex with growing amount of traffic. As a result, new attack patterns arise and remain undetected. In order to remedy these deficiencies and remove the ad hoc and manual elements from intrusion detection system design, intrusion detection research is oriented toward the data mining approaches. This attractive paradigm, notably machine learning approaches leads the intrusion detection to a second generation of IDSs called data mining based IDSs. This generation provides more effective intrusion detection models which are automatically built by using learning algorithms. They are endowed with a generalization capacity which covers the

DOI: 10.4018/978-1-4666-9562-7.ch108

new unknown patterns of attacks. However the generalization power reaches its limits through time because of the new attack methods and the emerging attacks which differ significantly from already learned attacks. Then permanent coverage of new attack patterns remains an unreachable goal for the existing IDSs which become progressively inefficient through time. This challenge is closely related to information technology evolution which brings permanent variations in network environments and attacks strategies.

The current network environments are dynamic and changing so that the intrusions occur constantly. For this reason, The IDS must adapt itself to every change in its target environment to be able to detect any new attack pattern and improve its detection performance. The IDS adaptability refers to the ability of continuous automatic incremental learning of the intrusive and normal behaviours. Then the IDS becomes a learning system in relation to its target environment.

2. GENERALITIES AND BASIC CONCEPTS

2.1 Intrusion Detection Concept

The intrusion detection concept was founded by James Anderson in 1980(Anderson, 1980). In his report entitled "Computer Security Threat Monitoring and Surveillance," Anderson states that it is possible to characterize normal use of a computer system thanks to statistical parameters in the records of users' habitual activities, called audit trials. He demonstrates that the audit trials contain the relevant information to reconstitute user's activities. Their analysis enables retracing and understanding the user's behaviour. It identifies the abusive use of the computing resources, the privilege abuse, the excessive use of computer, and may reveal the ongoing and completed attacks. In this way, Anderson plants the original idea of intrusion detection, which was firstly focused on the mainframe environments. In 1986, Dorothy Denning concretised the ideas of Anderson by developing a prototype for Stanford Research Institute which was baptized « Intrusion Detection Expert System (IDES) ». It was destined to analyze audit trials of government systems and inspect user's activity. In 1987, Denning published the foundations of IDES prototype in a paper entitled « An Intrusion Detection Model » (Denning, 1987). This publication was the beginning of the intrusion detection era. By the IDES, Denning proposed not only the first IDS but a methodological model revealing the necessary knowledge for the intrusion detection. This concept reaches thereafter a blossoming in research field and technology, thanks to the American government considerateness and financing granted to the research projects.

The intrusion detection is closely linked to the audit mechanism which is an ubiquitous functioning option in the modern operating systems (Mé, 1997) that records the events occurring in a computer system. An event may be any undertaken action in a computing system such as logging session, program execution or file access (An Introduction, 1995) (Noel et al., 2002). The recording of events is performed chronologically and takes the form of a file which includes the date and the time of the occurring event, the identifier of the user who initiates the event, the application employed to execute the event as well as the result of the event progress (success or failure). Audit trial is a chronological sequence of event records. It represents the full history of any user activity, system process or application process (An Introduction, 1995) (Mé, 1997). Audit trials analysis enables reconstructing the complete activity, determining its duration, the user who accomplished it, the involved system resources and the results of its achievement (success or failure).