A revised taxonomy for intrusion-detection systems

Hervé DEBAR*,
Marc DACIER*,
Andreas WESPI+

Abstract

Intrusion-detection systems aim at detecting attacks against computer systems and networks, or in general against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, intrusion-detection systems have the task of monitoring the usage of such systems to detect apparition of insecure states. They detect attempts and active misuse, either by legitimate users of the information systems or by external parties, to abuse their privileges or exploit security vulnerabilities. In a previous paper [Computer networks 31, 805-822 (1999)], we introduced a taxonomy of intrusion-detection systems that highlights the various aspects of this area. This paper extends the taxonomy beyond real-time intrusion detection to include additional aspects of security monitoring, such as vulnerability assessment.

Contents

I. Introduction
II. Description of a generic intrusion-detection system
III. Taxonomy elements
IV. Knowledge-based versus behavior intrusion detection
V. Passive versus active intrusion detection
VI. Host-based versus network-based intrusion detection
VII. Detection paradigm
VIII. Continuous monitoring versus periodic analysis
IX. The reusability issue
X. Conclusion and future directions

References (73 ref.)

I. INTRODUCTION

Since the seminal work by Denning in 1987 [13], many intrusion-detection prototypes have been created. Sobirey maintains a partial list of 83 of them [66]. Intrusion-detection systems have emerged in the computer security area because of the difficulty of ensuring that an information system will be free of security flaws. Indeed, a taxonomy of security flaws by Landwehr et al. [43] shows that computer systems suffer from security vulnerabilities regardless of their purpose, manufacturer, or origin, and that it is technically difficult as well as economically costly (both in terms of building and maintaining such a system) to ensure that computer systems and networks are not susceptible to attacks.

This paper enhances a taxonomy of intrusion-detection systems, introduced in [12], at a time when commercial tools are increasingly becoming available. The taxonomy draws examples from both the research prototypes and commercial products to illustrate the most prominent features of intrusion-detection systems. The paper focuses on the TCP/IP/UNIX world, for which the largest number of prototypes and tools have been developed. However, a number of these products are now also available for Windows NT, which has been more widely deployed in the enterprise world and has recently been subject to increased scrutiny by the security and underground communities.

This paper does not attempt a complete survey of existing intrusion-detection tools, techniques, projects,
and products. Several surveys have indeed been published in the past [4, 17, 22, 34, 44, 46, 47, 49], but the growth of the intrusion-detection field has been such that many new projects have appeared in the meantime. Therefore, we shall present an updated image of the intrusion-detection field, organized around a proposed taxonomy for intrusion-detection systems, and illustrated with examples from past and current tools.

The paper is organized as follows. Section II describes the architecture of a generic intrusion-detection system. Section III presents the taxonomy we use to describe and classify intrusion-detection systems and examples of techniques and information sources. Sections IV to VIII detail the five elements of the taxonomy, drawing examples from past and current intrusion-detection projects, tools, and products. Section IX describes the reusability issue of intrusion-detection systems and their components.

II. DESCRIPTION OF A GENERIC INTRUSION-DETECTION SYSTEM

II.1. Terminology

The term system (a.k.a. target system) is used here to denote the information system being monitored by the intrusion-detection system. It can be a workstation, a network element, a server, a mainframe, a firewall, a web server, etc.

The term audit denotes information provided by a system concerning its inner workings and behavior. Examples of audits include, but are not limited to, C2 audit trail, accounting, and syslog in the Unix world, Syslog in the MVS world, the event log in Windows NT, and incident tickets in X25 networks. A description of some of these audits is given in Section VI.

The term component refers to a box inside an intrusion-detection system. There are many kinds of components, an overview of which is given in Section IV.

II.2. Description

An intrusion-detection system acquires information about its environment to perform a diagnosis on its security status. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches. A typical intrusion-detection system is shown in Figure 1.

An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system that is to be protected (Fig. 1). This detector can also launch probes to trigger the audit process, such as requesting version numbers for applications.

II.3. Efficiency of intrusion-detection systems

The following three measures have been proposed by Porras et al. [55] to evaluate the efficiency of an intrusion-detection system:

**Accuracy.** Accuracy deals with the proper detection of attacks and the absence of false alarms. Inaccuracy occurs when an intrusion-detection system flags as anomalous or intrusive a legitimate action in the environment.

**Performance.** The performance of an intrusion-detection system is the rate at which audit events are processed. If the performance of the intrusion-detection system is poor, then real-time detection is not possible.