A Structured Approach to Selecting Data Collection Mechanisms for Intrusion Detection

Ulf E. Larson
Chalmers University of Technology, Sweden & Omegapoint, Sweden

Erland Jonsson
Chalmers University of Technology, Sweden

Stefan Lindskog
Norwegian University of Science and Technology, Sweden & Norway and Karlstad University, Sweden

ABSTRACT

This chapter aims at providing a clear and concise picture of data collection for intrusion detection. It provides a detailed explanation of generic data collection mechanism components and the interaction with the environment, from initial triggering to output of log data records. Taxonomies of mechanism characteristics and deployment considerations are provided and discussed. Furthermore, guidelines and hints for mechanism selection and deployment are provided. The guidelines are aimed to assist intrusion detection system developers, designers, and operators in selecting mechanisms for resource efficient data collection.

DOI: 10.4018/978-1-60960-836-1.ch001
A Structured Approach to Selecting Data Collection Mechanisms

INTRODUCTION

Collection and analysis of audit data is a critical component for intrusion detection. Previous research efforts (Almgren et al., 2007; Axelsson et al., 1998; Kuperman, 2004; Lundin Barse & Jonsson, 2004; Price, 1997; Zamboni, 2001) have concluded that by carefully selecting and configuring data collection mechanisms, it is possible to obtain better and more accurate analysis results. However, data is required to be correct and to be delivered in a timely fashion. The data should also be sparse to reduce the amount of resources used to collect and store it. Since production of audit data directly depends on the deployed data collection mechanisms, adequate mechanism knowledge is thus a critical asset for intrusion detection system (IDS) developers, designers, and operators.

This chapter consists of a theoretical part which introduces the basic concepts of data collection, and a practical part where guidelines and hints for mechanism selection are discussed. The theoretical part discusses the basics of data collection from several perspectives. The components and operation of a generic IDS is described, followed by an in-depth discussion of the components and operation of a generic data collection mechanism. Then, two taxonomies are presented, discussing mechanism characteristics and deployment considerations, respectively. Thereafter, the practical part discusses operational considerations and outlines a deployment strategy. Finally, future challenges are discussed, followed by some concluding remarks and an appendix providing a classification of 50 studied data collection mechanisms and techniques.

Both the appendix and the guidelines can be used when selecting mechanisms. They can also assist when a specific type of data collection is desired. For example, it is easy to find out what mechanisms collect samples for execution profiling, and what mechanisms that can be reconfigured without the need for restart. This is a valuable source of information which removes the need to browse multiple manual pages and white papers to find the desired mechanism. Furthermore, by using the selection guidelines, we can obtain a more resource efficient data collection and obtain a more accurate data analysis.

RELATED WORK

Anderson (Anderson, 1980) proposed to use data collection and analysis as a means of monitoring computer systems for detection of different types of intruders. Denning (Denning, 1986) proposed An Intrusion-Detection Model and pointed out specific log information that is useful for intrusion detection. Price (Price, 1997) then derived the audit data needs of a number of misuse detection systems and investigated how
Related Content

Security Protection for Critical Infrastructure
www.igi-global.com/chapter/security-protection-critical-infrastructure/13532?camid=4v1a

Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era
www.igi-global.com/chapter/privacy-design-origins-meaning-prospects/61500?camid=4v1a

Data Security for Storage Area Networks
www.igi-global.com/chapter/data-security-storage-area-networks/20672?camid=4v1a
Comprehensive Risk Abatement Methodology as a Lean Operations Strategy
www.igi-global.com/article/comprehensive-risk-abatement-methodology-as-a-lean-operations-strategy/127540?camid=4v1a