An Approach for Independent Intrusion Detection Management Systems
A Standardized Intrusion Detection Parameterization Format

Björn-C. Bösch
Carl-von-Ossietzky-University Oldenburg
Faculty II - Department of Computing Science
System Software and Distributed Systems Group
Oldenburg, Germany

Abstract. Efficiency of Intrusion Detection Systems depends on their configuration and coverage of services. The coverage depends on used Intrusion Detection Systems with currently vendor-specific configurations. In case of usage of multiple systems the operations could become complex. This work provides an approach for a multi-vendor IDS implementation under one central administration and notification entity based on standardized communication between analyzer and manager.

1 Introduction

Intrusion Detection Systems (IDS) protect critical infrastructures and services against malicious actions. Detailed knowledge of application and communication are necessary to protect services adequate. IDS are scoped on a single application (special kind of Host based IDS), a single operating system (Host based IDS) or communication protocols (Network IDS). To detect intrusions in an IT composite, different IDS are required to protect and monitor computer systems at all levels, top to bottom.

Application-based IDS become more and more specialized and focusing to one single application. So, vendors provide own specialized IDS for their products. Current multi-vendor IDS architectures do not interact with each other. Additional IDS requires a full independent coexisting IDS solution. A full functional integration in an existing IDS is currently not possible. Based on the Intrusion Detection Message Exchange Format (IDMEF) [1] it is possible to integrate an additional general monitoring system as notification umbrella. This research is focused to separate the manager from the rest of an IDS, so that the manager is an independent entity to IDS analyzers and sensors.

The remaining paper is organized as follows: Section 2 describes the architectural solution approach and the methodology of parameterization. Subsequent the integrations in three different free open source IDS are briefly described. Section 3 concludes this work.
2 Approach

This section describes current IDS architectures and the architectural approach to separate the IDS manager. Subsequent the parameterization methodology was pointed out on a high level. This section is closed with a brief illustration of the IDPEF integrations.

2.1 Current IDS Architectures

The entities analyzer and sensor are vendor-specific entities. The manager is the only entity that could be shared with other IDS. The communication between a general manager and vendor-specific analyzers has to be standardized to manage a multi-vendor IDS architecture with one manager.

Today, IDMEF standardizes notifications to a monitoring application. As transport protocol the Intrusion Detection eXchange Protocol (IDXP) [2] is already created on top of the Blocks Extensible Exchange Protocol (BEEP) [3]. The BEEP framework provides confidentiality, integrity and authentication for the communication. IDXP provides a streamtype option and the value “alert” is already used by IDMEF. This work uses IDXP with the streamtype value “config” as communication framework.

The manager was separated from the rest of the IDS with a standardized communication between analyzer and manager. The communication between sensor and analyzer is continuously vendor-specific. The communication in the IETF IDS model [4] was modified. As visualized in fig. 1, the security policy will be applied to the manager and distributed to the analyzers and forwarded to the sensors instead of directly from the administrator to all IDS entities. Operators and administrators use the manager as single point of human interface to operate the entire IDS.

2.2 Parameterization Methodology

IDS have their individual structure, syntax and semantic for management and operations. Today, sharing of configuration files or references between IDS is not