2013 IEEE 20th International Conference on Web Services

RESTful Web Services for High Speed Intrusion Detection Systems

Mohsen Rouached
College of Computers and Information Technology
Information Technology Department
Taif University
Taif, Saudi Arabia
m.rouached@tu.edu.sa

Hassen Sallay
Deanship of Information Technology
Information Security Department
Al Imam Mohammad Ibn Saud Islamic University (IMSIU)
Riyadh, Saudi Arabia
hmsallay@imamu.edu.sa

***Abstract*—Since current heterogeneous Intrusion Detection Systems (IDSs) have not been designed to work in a cooperative manner, sharing security information among them poses a serious challenge especially in large-scale High Speed Networks (HSN) environment. The integration become more difficult when we should reduce computing and memory costs incurred by the high speed IDSs communication. Fortunately Web Services technology represents a good choice for IDSs integration thanks to its characteristics such as platform transparency and loose coupling. In this context, this paper presents a lightweight RESTful Communication model for coordinating different high speed distributed IDSs.**

***Keywords*-IDS; Web Services; REST/JSON; High Speed Network**

I. Introduction

Today intrusion detection is considered as one of the top priority tasks for network administrators and security professionals. Present networks provide essential services for businesses to perform optimally and are, thus, a target of attacks which aim to bring down the services provided by the network. This strengthens the need to develop powerful intrusion detection systems. Moreover, the attacks being sophisticated, unpredictable, frequent and from a wider range of sources are exceeding current IDS ability. The problem becomes more serious with the emergence of high-speed networks like Infiniband and Gigabit-Ethernet. One of the challenges is to keep up with the everincreasing Internet usage, and network link speeds as more and more data has to be scanned for intrusions. Research on intrusion detection in distributed systems is currently focusing on two main issues: scalability and heterogeneity. The IDSs in large distributed systems need to be scalable to accommodate the large amount of audit data in such systems. In addition, such IDSs must be able to deal with heterogeneous data from component systems of different types in order to collaborate with other types of IDSs.

In this paper, we propose to use RESTful Web services [1] for coordinating heterogeneous entities of a high speed distributed IDS. The rest of the paper is organized as follows. In section 2 details the overall architecture and the different components of the developed system. Section 3 presents some experimental results. Finally, section 4 concludes the paper and outlines future directions.

II. Architecture Overview

Recent standardization efforts related to the exchange of security information are being developed mainly by the Internet Engineering Task Force (IETF) through its IDWG working group. IDWG is finishing up the Intrusion Detection Message Exchange Format (IDMEF) [2] and Intrusion Detection Exchange Protocol (IDXP) [3] specifications. These efforts aim at the exchange of information among complete IDSs and IDS elements, and are XML based. We base our work on these specifications and adopt the taxonomy of the general model for intrusion detection [4] defined by IDWG. This model is illustrated in figure 1. A sensor is an element that collects data from one or

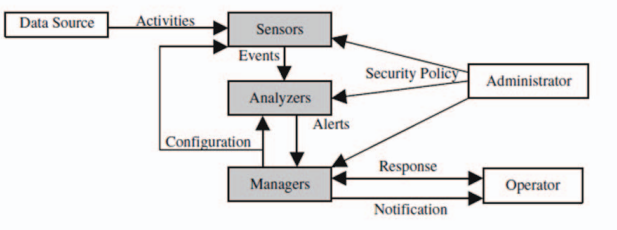

Figure 1. Basic elements of the IETF intrusion detection model

more data sources. The sensor is setup to forward events to the analyzer. An analyzer inspects data collected by a sensor looking for signs of unauthorized or undesired activity or for events that might be of interest to the security administrator. A sensor and an analyzer can be part of the same component. A manager manages the various elements of an IDS. Management functions typically include (but are not limited to) sensor configuration, analyzer configuration, event notification management, data consolidation, and reporting. IDS elements can be parts of a monolithic IDS or can be distributed on more than one location. In our work, we envision a new generation of IDSs defined by a set of services supporting security managers in improving the overall network security. Implemented algorithms and

978-0-7695-5025-1/13 $26.00 © 2013 IEEE
DOI 10.1109/ICWS.2013.92

methods may be very easily exchanged according to the characteristics of the monitored network and requirements with respect to the level of security that must be maintained. These services can be realized in two ways: 1) SOAP-based services and 2) RESTful services. For the service providers, RESTful services can improve system flexibility, scalability, and performance as compared to the SOAP-based Web services. It is equally attractive to end users as it consumes less resources (i.e., battery, processor speed, and memory). Thus, in our approach, communications between managers, sensors, and analyzers follow the REST architectural style and use JSON data format.

In what follows, we mainly focus on the exchange protocols and communications between the sensors, the alert aggregator, and the rule manager. The load balancing process and the event calculus analyser are beyond the scope of this paper and was described a previous work.Our communication model is depicted in figure 2. In a REST

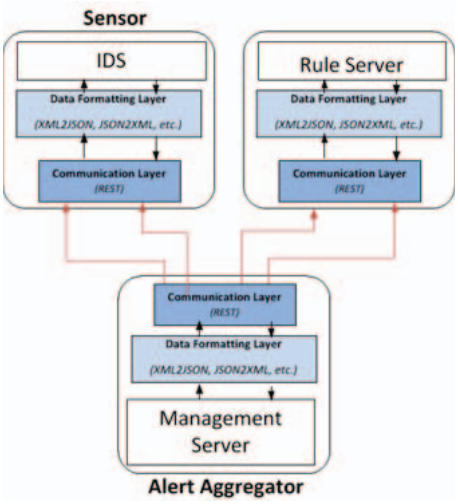

Figure 2. Communications between sensors, alert aggregator, and rule server

architecture a resource is an abstraction controlled by the server and identified by a Universal Resource Identifier (URI). Using REST architecture, sensors are considered as abstract resources identified by URIs, represented with arbitrary formats and manipulated with the same methods as HTTP. As shown in figure 2, we propose to directly implement a RESTful Application Programming Interface (API) on each entity (sensor, rule server, alert aggregator) in order to grant an easy communication between them. Concerning the data exchange format, we use the JavaScript Object Notation (JSON). JSON is more compact than XML as it provides an implicit data structure format. The key features of the RESTful Web services model are:

1) JSON data exchange format to ensure communication between sensors and the alerts aggregator using IDMEF format [1] . JSON objects are roughly inspired from the IDMEF format using a XML2JSON parser that takes as input the XML message format and provides as out the corresponding JSON code.
2) JSON data exchange format fo communication between the alerts aggregator and the rule server using the Common Intrusion Detection Signatures Standard (CIDSS)[2]. Mapping from XML CIDSS format to JSON corresponding objects is done automatically using the same XML2JSON parser.
3) The interaction between the Data Formatting Layer in figure 2 can be implemented as a GLUE-Layer linked with each modified IDS or as a separated process with IPC (Inter-Process-Communication) capabilities.

Details about the transformation of the different elements of IDMEF and CIDSS messages can be found at http://svn.amansystem.com/svn/SnortHSN2010/trunk/xml2jsonConverter/..

III. Conclusion

The purpose of this paper is to present an RESTful communication model for high speed IDSs to overcome limits of available solutions to IDSs problems in terms of scalability and heterogeneity. The main features of this model are the adoption of the REST technology and the JSON data format. The proposed model was validated and tested. To improve the efficiency of our proposed architecture, we plan to enhance the IDS entities behaviors with semantics, so that high levels of automation can be reached throughout the whole configuration and management tasks process.

Acknowledgments.

This paper is a partial result of a research project granted by King Abdul Aziz City for Sciences and Technology (KACST), Riyadh, Kingdom of Saudi Arabia, under grant number INF 36-8-08.

References

[1] P. Cesare and W. Erik. Restful web services: principles, patterns, emerging technologies. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 1359–1360, New York, NY, USA, 2010. ACM.

[2] H. Debar, D. Curry, and B. Feinstein. The intrusion detection message exchange format. internet draft draft-ietf-idwg-idmef-xml-16, ietf, 2006.

[3] B. Feinstein, G. Matthews, and J. White. The intrusion detection exchange protocol(idxp). internet draft draft-ietf-idwg-beep-idxp-07, ietf, 2002.

[4] M. Wood and M. Erlinger. Intrusion detection message exchange requirements.internet draft draft-ietf-idwg-requirements-10, ietf, 2002.

[1] http://www.ietf.org/rfc/rfc4765.txt
[2] http://tools.ietf.org/html/draft-wierzbicki-cidss-04