Service-Oriented Approach to Visualize IT Security Performance Metrics

Clemens Martin, Mustapha Refai
1 University of Ontario Institute of Technology, Canada
clemens.martin@uoit.ca
2 University of Ontario Institute of Technology, Canada
mustapha.refai@mycampus.uoit.ca

Abstract. In this paper we propose a metrics visualization system design. Visualization is a key component in our Policy-Based Metrics Framework for Information Security Performance Measurement. To achieve openness and interoperability we have based our approach on a Service Oriented Architecture. The tight integration of a visualization component into our framework allows improved control of the metrics collection process, gives continuous access to security performance information, shows deviations between current data and set targets and displays developing trends. Thus management is enabled to more thoroughly understand their business' security posture and is supported in their IT security related decision making processes.

1 Introduction

Measuring security performance is slowly becoming a more and more accepted tool to management, because "if you cannot measure performance, you cannot control it and if you cannot control it, you cannot improve it" as [1] expresses it.

We observe that businesses deploy more and more security measures throughout their organization by installing security products, establishing security teams and following security programs; however, little work has been done with regard to measure the effectiveness of these measures. Moreover, the automation of the performance measurement processes resulting in solid metrics becomes a necessary tool that management will depend on to understand their business' security posture at any given time. Although metrics programs have been accepted as a valid approach to measure overall IT security performance, the lack of a comprehensive approach supporting the development and automating the collection of security metrics and providing a clear view of the overall IT security posture is indisputable [2].

We present a visualization approach as a key component in our Policy-Based Metrics Framework for Information Security Performance Measurement. To achieve openness and interoperability we have based our approach on a Service Oriented

Please use the following format when citing this chapter:

Martin, C. and Refai, M., 2007, in IFIP International Federation for Information Processing, Volume 238, Trust Management, eds. Etalle, S., Marsh, S., (Boston: Springer), pp. 403–406.

Architecture. Our approach is embedded in our framework that is based on the seventeen security control areas as proposed by the U.S. National Institute of Standards and Technology (NIST) in [3, 4] to measure security performance because these controls are widely accepted as the minimum requirements for metrics programs.

This paper is organized as follows: Section 2 contains a brief discussion of our approach for a Policy Based Security Metrics Framework. We detail the Service Oriented Architecture Approach to Metrics Visualization in Section 3. We discuss the results of our work and present our conclusions in the final section.

2 Framework for a Policy-Based Metrics Approach

We base our approach on the seventeen security controls areas as proposed by NIST in [3, 4] to measure security performance because these controls are widely accepted as the minimum requirements for metrics programs. We propose to expand these controls by one additional control a Policy Performance Control. This control is intended to monitor and measure organization security policies vis-à-vis their completeness and effectiveness to the business' IT security goals. The framework is a starting point for our policy-based metrics approach. Establishing an organization's security policy entails capturing mission and objectives of the organization. We introduce a set of modules and components that interact in providing a comprehensive overview of an organization's security posture.

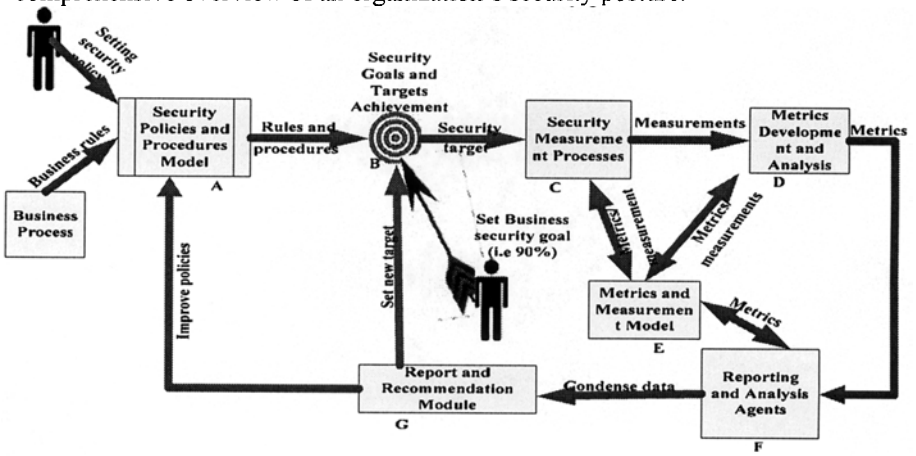

Fig. 1. Security performance framework

Improving the security performance of an organization has to be based on a good understanding of the current security situation with respect to all of the security controls. This level of security can be considered as the baseline toward achieving the next desired security goal set by the organization (Fig. 1).

The framework is composed of the following components: Security Policies and Procedures Model, Security Goals and Targets Achievement, Security Measurement Processes, Metrics Development and Analysis, Metrics and Measurement Model, Reporting and Analysis Agents, and Report and Recommendation Module.

3 Metrics Visualization

The power of visualization is the ability to combine and condense complex information for the stakeholder in an easily understandable way. The visual components we are proposing attempt to simplify the complexity of the results of IT security measurement processes, and provide snapshots of the organization's security posture at any given point in time. We present the underlying data in a set of situation-adjusted graphical representations alongside recommendations to address identified security problems. Reports and recommendations are derived from the NIST guides and recommendations [3-6].

We have designed our metrics framework to work on a distributed system that includes all running systems within the organization's network that need to be monitored and analyzed for security performance measurement purposes.

The overall system is composed of three major components: Control Manager, Agents, and the Reporting and User Interface. The Control Manager is the central component within the metrics framework. Its role is to manage and control communication with different services, such as communicating with agents on different systems, or with another instance of the Control Manager on a different server. It is responsible for the persistence of the relevant metrics data, the question and role-based survey pools, the infrastructure and organizational models, as well as configuration settings for distributed Agents and roles. The Control Manager interacts with the Agents to distribute measurement, data collection, and condensation tasks and retrieve results from them.

The Control Manager consists of the Access Control Manager, Central Processing Services, Reporting, and User Interface Support Services. It plays an important role in providing an interface between the services, Agents, and systems. The design of all system components has been chosen to be service-oriented to achieve interoperability and scalability. Thus, we can separate the services that produce and expose functionality from the consumers that use the services, enabling the extensibility and adaptability of the framework.

Agents on the other hand are services that perform data analysis on logs, reports, or events generated by the system in the network. Once Agents are satisfied with analysis and metrics extraction, they communicate their findings back to the central services. The design has the form of pyramid view where the base represents the system that holds the data to be analyzed and extract metrics from. The middle layer represents information that is extracted from the data layer. The top layer represents the information that can be presented through the user interface components as reports, recommendations, and security posture diagrams.

Agents can be deployed on organization machines/devices to monitor the security performance of the security application running on those devices - Intrusion Detection/Prevention, vulnerability scanner, firewall, etc. They can be configured and instructed by the Control Manager, and then report their findings back to it. A flexible Agent system can accommodate a wide variety of devices and their performance capabilities. One of the main advantages of this design is the ability and flexibility of Agents' deployment across the network. Furthermore, it offers an excellent way of automating the data collection from the systems in question without the need for human interference. In a similar fashion, the Reporting and User Interface subsystem is constructed in an Agent-based approach. Thus, it can easily be

deployed on display devices on the network and communicate with the Control Manager for its visualization tasks. The diagram represents the level of achievement with respect to the 17 NIST controls, as well as our newly introduced policy performance control. We also present an overall security posture of the organization as a weighted mean of the individual control achievement levels.

4 Conclusion and Future Work

We attempt to provide an answer to the question about the current state of organizational security – its security posture – by collecting and condensing data to visual representations of past and current situations and bring them in context with future goals. Our design approach is a step toward achieving this goal. Its advantage is the automation of data collection whenever possible to avoid human error and improve the trustworthiness of the end result. It is based on a service-oriented architecture approach that provides flexibility and scalability. Furthermore, it is designed with security in mind and we have implemented and tested the services that support the notion of XML digital signature and encryption, as well as XACML access control process service. We are currently implementing the remaining modules of the framework in order to demonstrate an integrated IT security performance measurement methodology across a complete organization.

Acknowledgment

This work is currently being funded by the Bell University Labs and the Faculty of Business & Information Technology at the University of Ontario Institute of Technology.

References

1. T. Bahil and D. Frank. (2006, May 19, 2006). What is systems engineering? A consensus of senior systems engineers. [Online]. *2006(June 2)*, pp. 13. Available: http://www.sie.arizona.edu/sysengr/whatis/whatis.html

2. F. Robrt. (2004, April 09, 2004). Collecting effective security metrics. [Online]. *2006(May 20)*, pp. 5. Available: http://www.csoonline.com/analyst/report2412.html

3. NIST 800-53. (2006, July 2006). Security metrics guide for information technology system. [Online]. *2006(May 15)*, pp. 159. Available: http://csrc.nist.gov/publications/drafts/800-53-rev1-clean-sz.pdf

4. NIST SP 800-80. (2006, May 2006). Guide for developing performance metrics for information security. [Online]. *2006(June 1)*, Available: http://csrc.nist.gov/publications/drafts/draft-sp800-80-ipd.pdf

5. NIST 800-26. (2005, August 2005). Security metrics guide for information technology system. [Online]. *2006(May 15)*, pp. 106. Available: http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf

6. NIST 800-55. (2003, July 2003). Security metrics guide for information technology system. [Online]. *2006(May 15)*, pp. 99. Available: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf