IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITB12700

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

A Services-Oriented Approach to Developing Security Policies for Trustworthy Systems

Kassem Saleh, Abdulaziz Alkhaili, & Ibrahim Alkattan
American University of Sharjah, School of Engineering, Engineering Systems Management, Box 26666, Sharjah, UAE, ksaleh@aus.edu

ABSTRACT

Security nowadays is considered to be the cornerstone for delivering services using a trustworthy system. In addition to security, trustworthiness is based on the privacy, reliability and business integrity of the system [1]. If system security requirements are not met, privacy, reliability and business integrity would inevitably suffer, and consequently the overall system trustworthiness is affected. The use of a well-structured process for developing requirements and policies as part of a security engineering life-cycle is essential. In this paper, we present a services-oriented risk-driven approach for the development of trustworthy systems. Our approach starts with the identification of services, then classifying assets and identifying risks on assets, leading to the elicitation of security requirements and policies supporting these requirements.

INTRODUCTION

Security management has become an integral part of engineering systems management. Providing a secure system is a challenging and complex task to manage. The importance of security is more evident as the value of system assets to protect increases. Providing a secure, trustworthy and dependable system operation to customers and stakeholders is becoming a business management objective. Technology alone cannot guarantee the security in systems. The human element plays an important role in the success of security controls. Management needs to be proactive in safeguarding system security by developing security policies and procedures, enforcing them and continuously monitoring and modifying them.

Organizations and businesses often face the challenge of integrating security into their systems development life cycle. While there is a general agreement on the need for such integration, opinions and approaches vary on the most effective means for such integration. Once a secure system has been designed and implemented, a usable and effective security policy must be developed. A security policy is a high-level statement of purpose and intent. It should specify the business' goals on security and indicate who is responsible for managing security and should show the business commitment to security [2,3,4]. In more technical terms, a security policy includes a set of security rules enforced by the different appropriate security controls. Finally, security policies must be communicated to and accepted by all stakeholders including employees, managers and customers.

A services-oriented approach to security policy development emphasizes the importance of services provided by the system to secure before considering the assets. Service resiliency and dependability requirements, and their prioritization are identified first. A non-service-oriented risk-driven approach to security policies implies that the policy development depends on the risk exposure (level, frequency and cost) the business is willing to take. It is obvious that the more valuable the business assets are, the more important is system security, and consequently the more strict, clear and elaborate should the security policy be, with most probably more expensive security controls to implement.

Statistics show that many medium and large organizations do not have a security policy to ensure the proper operations and security for their assets and resources hence affecting the security of their provided services. In a Global Information Security survey conducted by Ernst & Young [5] found that only 51% of businesses (54% in financial services) worldwide have implemented an information security policy Moreover, most existing security policies were developed in a non-systematic, adhoc manner and as a reaction to the pressing need to develop one.

In this research, a multi-layered services-oriented and risk-driven approach is developed for eliciting security engineering requirements starting from the service functions offered to the service stakeholders. Once developed, these requirements form the basis for writing security policies.

Although there are many standards and research developed on the various aspects of system security including, risk management, security requirements and security administration, it is noticed that there is a lack of systematic and comprehensive strategies and frameworks for developing security policies. None of the published work addresses security policy development starting from a services-oriented consideration of the stakeholders needs. This results in weak and unusable security policies that cannot contribute to the trustworthiness of systems and their provided services. Also, no considerations are made to the post-policy writing in terms of maintenance and traceability.

SERVICES-ORIENTED APPROACH

In the proposed services-oriented approach to security policy development, there are five interdependent layers as shown in Figure 1. The first layer consists of understanding the business services provided to the stakeholders. The second layer consists of the assets supporting these services, including business-related assets (physical and non physical), and operation-related assets. In addition to their explicit value, assets should be evaluated based on their projected contributions to the provision of services. The third layer identifies the security risks and their assessments. An analysis of each of the services and their supporting assets will be conducted by studying all the possible threats these services may be subjected to. Risk impacts, risk control strategies and risk leverages are identified among other risk features. In addition to technical risks, political, economic, social, and environmental risks will be elicited. By applying risk assessment and analysis procedures, one can recognize what are the system requirements (general and specific) and how important is to secure the system elements to reduce the risk in question. Risk analysis helps determining risk exposures, and allows organizations to integrate financial objectives with security objectives. As a result, a successful security policy which is flexible and services-oriented can be developed. The fourth layer consists of the security requirements that must be satisfied to address the identified risks. From the interrelationships between the stakeholders services and security risk analysis, one can define the security requirements needed to deliver trustworthy services. A categorization of security requirements proposed in [6] helps in eliciting requirements in a systematic way. These requirements categories include identification, authentication, authori-

zation, immunity, integrity, intrusion detection, non-repudiation, privacy, auditability, survivability, physical protection, and system maintenance requirements. Furthermore, these security requirements can be elicited against the system elements including hardware, software, information, people, and standards and documentation [7]. The fifth layer consists of the elements of a suitable and traceable services-oriented security policy. Each element of this comprehensive policy can be easily mapped or traced back to the services, assets, risks and requirements it covers, hence allowing easy updates to the policy as a result of updates to the services provided or to the assets supporting existing services.

In the following, we elaborate on the first two stages of our approach, namely, service identification and asset identification.

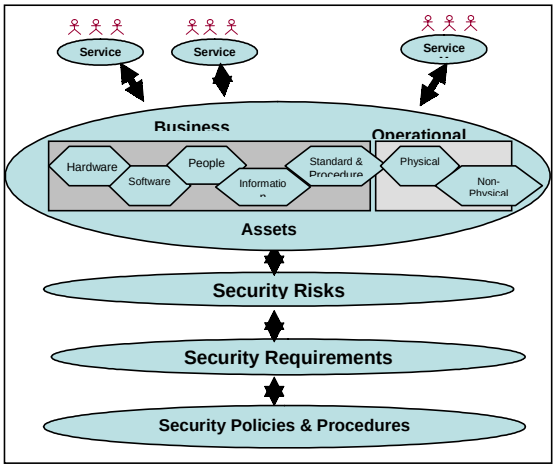
Service Identification

This methodology of building a secure framework is basically look to system from the services point of view, so identifying services is a critical step in developing a service-oriented security framework to any service-oriented sector.

In addition to identifying the service features, senior management can elaborate the business objectives of each service and determine the service importance to the organization. This decision mainly depend on the organization main objectives and how the service features can met them, human factors, and criticality of the service. In the following we will elaborate on the service features.

- Service importance to the organization: It means, how this service is important to the organization, and how is the change in this service will affect the overall mission and objectives. Also, it includes the business objective and economic return to the organization. So, it specifies the service profitability comparing to other service.
- Service users: There are many categories of service users like upper managers, medium managers, direct managers, technical operation users, naive users, and customers. To figure out the service importance from the user point of view, we should take in our consideration the feedback of each kind of users, to simply understand the service importance from the user view.
- Service criticality: It specifies how this service is critical to the organization and customers, when it falls in one of the following cases:
- The service has high economic return comparing to others to the organization..
- It contributes effectively to other services (other service depend critically on it).
- It depends mainly on critical assets (this is will be explained later in asset criticality).
- The business environment is aggressive, many competitors offering the same service.
- It is for critical users (if this service is only for certain customers, or the customers are very sensitive, or the customer society level is high).
- It is a unique service or it's only offered by the organization.
- Any service feature internal/external can be critical depending on the service function and its contribution to the organization main objectives.

Figure 1. *Layers of the traceable services-oriented approach*



Asset Identification

This is the second stage of the development phase in building our services-oriented security framework. To identify the asset and its importance, we should identify the asset elements, asset features, asset importance, asset criticality, and asset users. In the following we will elaborate on the important features of assets.

- Types of assets: The first type includes operating-related assets which can be (1) physical, like raw material in a factory, storage devices, hardware, like internal network equipments, computing equipments and human resources in the factory, or (2) non physical, like operating programs and software. (All the assets relating directly to the operational system). The second type includes the business related assets of the system which comprise (1) hardware, like external network equipments, computing equipments (2) software, like applications, , customers inter-relationship software, and antivirus programs, data stored in an information-based business (3) people, like, administrators, users, auditors, suppliers, customers service people and developers, (4) information/knowledge, including databases on objects needed for the system's business functions, and finally, (5) standards, procedures and documentation on the business functions (all the assets relating directly to the business activities system). Therefore securing a system involves securing its business-related and operating assets. However, the operating elements are more essential from a security point of view since any attack on the confidentiality, integrity or availability of one or more of these elements can breach the system's security, and hence the trustworthiness of the whole system.
- Asset importance: we will consider an asset value according to its contribution to the organization main services which they support the overall mission. All the current methodologies and international standards start building their security policies from the assets value regardless of their contributions to the main services.
- Asset criticality: It specifies how this asset is critical to the services offered.

SUMMARY AND CONCLUSIONS

Only about half of organizations worldwide have developed a security policy [4]. There is an urgent need to develop security policies that are usable and effective and address the real stakeholders' needs, i.e., the delivery of services they trust. This paper proposes an approach for the systematic development of security policies starting from a services-oriented risk-driven elicitation of security requirements. Consequently, policies developed using the developed approach will be addressing the real needs of the system stakeholders.

Furthermore, the proposed approach facilitates the traceability from service elements to policy elements and vice-versa. The developed policy can be easily extended to accommodate additional policy elements reflecting additional service requirements, and operational or security constraints. Also, the developed policies can be easily tested and maintained in a continuous security assessment and review process.

ACKNOWLEDGEMENT

The authors would like to acknowledge support of this work by a travel grant from research administration at the American University of Sharjah.

REFERENCES

[1] C. Mundie, P. deVries, P. Haynes, and M. Corwine, "Trustworthy computing", Microsoft White Paper, October 2002, 10 pages.

[2] D. Goodhue and D. Straub, "Security concerns of system users: a study of perceptions of the adequacy of security", *Information and Management*, Vol. 20, Issue 1, pp. 13-27, 1991.

[3] C. Pfleeger and S. Pfleeger, Security in Computing, Third Edition: Prentice Hall, 2003.

[4] S. Barman, S, Writing Information Security Policies, First Edition: New Riders, 2001

[5] Information Security Breaches Survey 2004 by PriceWaterhouseCooper.

[6] D. Firesmith, "Engineering Security Requirements", *Journal of Object Technology*, Vol. 2, No. 1, Jan-Feb 2003.

[7] M. Whitman and H. Mattford, Management of Information Security, 2004, Thomson Course Technology.