A Framework for Engineering Trustworthy Computer Systems

KASSEM SALEH AND AZIZ AL-KHAILI
Engineering Systems Management
American University of Sharjah
Box 26666 Sharjah
UNITED ARAB EMIRATES

Abstract: - A trustworthy computer system is a system that in addition to being secure and reliable, it provides privacy-sensitive services with the highest possible business integrity. In this paper, we describe a framework for the proper engineering of trustworthy computer systems. The proposed framework emphasizes the importance of services as the starting point for such engineering activities. Moreover, the framework covers security development and maintenance activities leading to trustworthy systems that provide trustworthy services.

Keywords:- framework, privacy, security, service, system, traceability, trustworthiness.

1 Introduction

Trustworthy computer systems provide the vehicle for delivering trustworthy services. Services are considered a main driver in modern western economies [1]. From a service provider side, service trustworthiness must be an ultimate goal to increase user's trust and to maintain high usability. As a generalization of Microsoft's view on trustworthy computing [2], we consider a service to be trustworthy if it is secure, reliable, sensitive to client's privacy concerns, and delivered with the highest possible business integrity. The concept of secure services and the engineering and management of security starting from services was not addressed in the current literature on services and security.

A service user expects to deal with her private information in a controlled manner. Also, a reliable service has to fulfill its functions whenever they are required. A service with high business integrity behaves in a responsible and responsive manner according to the provider's promises and client requirements. In addition to the increase in client's trust and loyalty, delivering trustworthy services leads to many advantages including: enhanced reputation, increased client's trust and base, and hence an increased profitability of the provided services. In this paper, we concentrate on the security aspect of system's trustworthiness and hence service trustworthiness.

The main objectives of a secure system are: accountability, security assurance and continuity. An accountable service in a system would ensure that security violations can be traced back to lead to the violators and support non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and recovery and legal actions. Service security assurance would provide a desirable level of confidence that the confidentiality, integrity and availability requirements of a system are met. Confidentiality ensures that only authorized users can have access to certain service. Integrity ensures that authorized users can only use services in an acceptable and controlled manner. Availability ensures that authorized users are guaranteed to have access to services at any time they desire or as promised. Continuity ensures that a life cycle approach to security engineering provides a level of confidence that accountability and security assurance are continuously maintained throughout the offering of the service.

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 managing the security of service-based systems. None of the published work addresses security engineering starting from services-sensitive consideration of the stakeholders needs. This results in weak and unusable security policies that cannot contribute to the trustworthiness of systems.

The main objective of this paper is to develop a framework for a life cycle approach for managing the provision, deployment and maintenance of secure services. The development phase starts from a services-oriented elicitation of security requirements. These policies will be implemented, deployed, enforced and monitored. Their continuous evaluation and assessment will ultimately lead to activities within the maintenance phase. Depending on the criticality of the assessment results, the appropriate step of the development process and its consequent steps will be performed in the maintenance phase. Furthermore, the proposed approach facilitates the traceability from service elements down 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 security life cycle can be easily tested and maintained in a continuous security assessment and review process.

The paper is organized as follows. After this introduction, Section 2 overviews the development and maintenance phases of the proposed framework. Then, each phase of the framework is analyzed, starting from the services objectives and identification in the development phase, to the review stage of the maintenance phase. Section 3 presents the security framework. Finally, Section 4 concludes the paper, and lists some areas requiring further investigations.

2 The Proposed Framework

We propose a generic security framework including a two-phase life cycle model, namely, the development and the maintenance phases. This framework supports and emphasizes the importance of services as the starting point to ensure system security and services trustworthiness. The framework can be easily implemented by any organization in any services-based industry, like education and finance. This framework is well-documented, traceable and modular. It allows for an easy forward and backward mapping between the various stages of the security framework for the purpose of easy maintenance, starting from service addition, deletion and update, and ending with controls, policies and procedures updates. Moreover, the framework keeps the security system live, effective, and updated faster than any other framework. The framework addresses security maintenance effectively and efficiently depending on the type and extent of the maintenance activity to undertake, as it will be explained later.

2.1 Development phase

This phase of the security framework leads to building security policies and procedures based on services in a well-documented and traceable manner. It starts by elaborating and identifying the service importance to the organization and ends up in having a full integrated set of security policies and procedures to effectively manage the system’s security. The six interdependent and sequential stages of this phase are described below.

2.1.1 Service identification

Our methodology of building a security framework is based on looking at the organization or system from the service point of view. Identifying services is a critical step in developing a services-oriented security framework in any services-oriented business sector. The ideas about desirable internal an external service features must be considered when designing business services.

In addition to identifying the service features, senior management can elaborate the business objectives of each service and determine the importance and contribution of each service to the organization. This decision depends mainly on the organization’s strategic business objectives and how the service features can meet them, in addition to the human factors, and the criticality of the service. In the following we will elaborate on the importance of the service elements:

- Service features: These features can be reported by the service manager and submitted to senior management. This process should be performed as frequent as the service importance increases or in case of change or update to the service features. In addition, the mode of operation related to the geographic location of service offering should be identified for each service.

- Service importance to the organization: This is related to how important is the service to the organization, and how a change in this service will affect the overall mission and objectives. Also, it includes the relation of the service to the business objectives and economic returns to the organization. In other words, it specifies the service profitability compared to other services provided by the same organization.

- Service users: There are many types 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 into consideration the feedback of each type of users, to simply understand the service importance from the user's view.

- Service criticality: It specifies how critical is the service to the organization and its customers.

Identifying the importance of each service will help senior managers decide on the classification and prioritization of provided services.

2.1.2 Asset identification

To identify the asset and its importance, we should identify the asset features, importance, criticality, and their users. In the following we will elaborate the asset importance elements: Asset elements: An organization comprises two 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 operational assets. Both types of assets are equally important 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 features: An asset has the same features of a service, but while in this paper we concentrate on the service, we will not explain these features.

- Asset importance: Following this methodology, we will consider the assets value according to its contribution to the profitability and importance to the organization main services supporting the overall mission. For example, if there are two machines in a factory, one is expensive and produces inexpensive products, and the second machine is less expensive and produces expensive products. Logically, we would consider the second machine to be more important than the first one. Recently, all the current methodologies and international standards start building their security system from the assets value regardless of their contribution to the main services they support. Considering the impact on services goes in tandem with the current efforts developing the idea of the services industry.

- Asset criticality: It specifies how critical this asset is to the services offered. Influencing factors include: current market value, dependence on it, maintenance cost, backup requirement, skill level to operate it, and its uniqueness.

Identifying the asset importance will help the service managers to decide the overall importance for each service. The load distribution among each property of the asset like its importance and criticality should be assigned by the senior management.

2.1.3 Risk identification

Security risk identification is a systematic attempt to specify known risks or predict new risks leading to threats and vulnerabilities. Also, the identification includes studying the effect and sensitivity of each risk. All the risks surrounding system assets should be identified and analyzed by the direct managers or risk management team in the organization.

After identifying each risk, we can categorize them according to their exposure or sensitivity levels: 1) critical risk: Critical assets loss or compromise would cause extensive system loss and service interruption that would prevent the system from carrying out its mission, 2) essential risk: Essential assets loss or compromise would cause severe or wide-spread system loss and service interruption that would reduce the capability of the system to execute essential services, 3) routine risk: Routine assets loss or compromise would cause minor system loss and interruption that would not significantly degrade the system from performing essential services, and 4) minor risk: that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the assets.

For each risk we should calculate the risk impact which is a product of how frequent it happens (risk probability) by how much damage it will cause (risk damage). Consequently, identified risks can be prioritized and classified. The accuracy of risk identification and quantification increases with the experience of the risk management team.

2.1.4 Security requirements specifications

Requirements are needed to impose high-level criteria and conditions to meet the identified security risks. Security requirements must be complete, unambiguous, consistent and correct. These requirements must cover all identified risks and should be stated in a clear and concise ways. Formal specifications languages like UMLsec and GRL [16] been developed to allow for such clear requirements. Classification or categorization of the types of requirements helps in the elicitation of the possible requirements. As discussed in Section 2, [15] provided a useful classification of security requirements.

2.1.5 Security controls specifications

Based on the security requirements, appropriate security controls must be identified by security professional in the security team. Controls can be addressing the various security concerns ranging from detective and preventive physical security to detective and preventive logical security including computer, network and software security. The specification and choice of these controls require current knowledge in the available security products and their features. A security control possesses many features including, its cost, its predicted risk leverage, the types of requirements it covers, and whether expertise is needed and/or is available. Also, the prescribed control could be a composite control itself made of two or more controls. After identifying all the possible controls, the selection of the specific controls will be based on the allocated budget for security and the risk leverage for each alternative control.

2.1.6 Security policies and procedures

This is the final stage of the development phase, requirements and controls are clustered in various security policy types such as email, website, password, data, information... For example, an email security policy would include a high level statement about the commitment of the organization to meet the related requirements, which are ultimately related to specific services. Procedures on putting the related controls into effect are then listed.

Figure 1 shows the elements of the development stages of the proposed security framework.

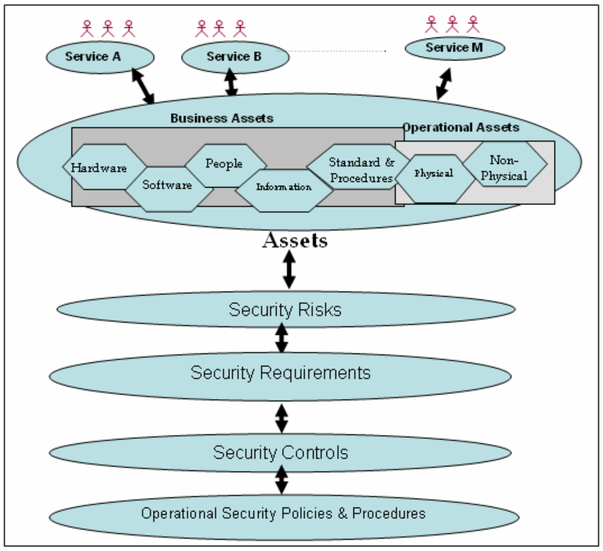

Fig 1. Elements of the development stages of the security framework.

2.2 Maintenance phase

After the development stages of our services-oriented framework, security policies and procedures are now well-defined and relate to the provided services. The policies and procedures are ready to be operational. The policy maintenance phase is entered and consists mainly of three main continuous stages, namely: implement and educate stage, enforce and monitor stage, and finally, the evaluate and revise stage. The third stage relates directly to the development phase and may include one or more of its stages depending on the required maintenance activity. In the following, we describe each of the maintenance stages.

2.2.1 Implement and educate

This is the first stage of the maintenance phase after creating the security policies and the operational procedures. This stage consists of two related activities. The first one is implementing the result of the development phase by putting the operational procedures into practice. This activity is very critical to the whole security and any delay would compromise the system's security and jeopardize the security of the services provided. The second activity is educating all the relevant human resources on the policies and procedures. Awareness programs should be developed and implemented, including, giving classes and seminars, training courses, workshops, brochures, posters, memos, periodic exams, video clips, and other awareness items. In fact, any creative way to educate and make people take the security responsibility seriously should be sought.

2.2.2 Enforce and monitor

Policies and procedures should be enforced by managers at all necessary levels. Commitment by management provides a high importance and visibility to support the success of the implemented security measures. In fact, some policies may include statements from the management and statements on rewards or penalties in cases of policy abuses. The monitoring of the various elements of the procedures provides an assurance of the seriousness of the policies and their related procedures. Monitoring of some procedures could be done continuously, periodically, or randomly. Also, monitoring can be either automated or performed by humans, and can be either physical or logical. The effectiveness of monitoring plays an important role in the success of the security system.

2.2.3 Evaluate and revise

In this stage, vulnerability assessments and security penetration tests are conducted to check how current and appropriate are the currently implemented procedures. The obtained results together with the assessment of the monitoring results of the previous stage, a plan of action will be identified. This plan may include an intervention requiring the execution of one or more of the stages of the development phase. The revision may include many actions to apply on the policies and their procedures like adjusting, correcting, improving, and changing the current security procedures to be better and more effective. According to the required improvement, this process can interact with the development phase and reignite the development processes according to the specific need for modification or improvement.

3 Security framework

After introducing the development and maintenance phases of our security framework, we explain the relation between maintenance and the stages of the development phase. The revision stage of the maintenance phase will require a transfer of flow to the needed stage of the development process. The more extensive is the required revision, the earlier is the entry point in the development phase. From the entry stage, all subsequent development stages will be exercised until the updated policies and procedures are implemented as they enter the maintenance stages. Figure 2 shows the relation between the stages of the development and maintenance phases. The extent of the required revision will depend upon the results of the continuous analysis of the collected audits and monitoring information, an immediate or scheduled corrective maintenance should take place. In this generic framework, while we are in the third step of the maintenance phase, we can simply continue to the required step from the development phase according to the situation and the required reaction. This corrective security maintenance may be triggered by the need to add, remove or update services, assets, risks, security requirements, or policies and procedures. Therefore, the maintenance process may involve one or more of the security development stages according to the maintenance needed.

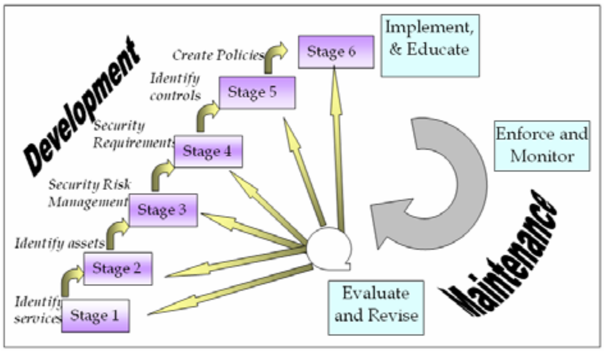

Fig. 2. The development and maintenance stages of the security framework.

The proposed framework for developing and maintaining system security allows a very structured approach to dealing with security. The stages of the framework are very well defined and their proper execution leads to an efficient and effective handling of the overall system security. A services-oriented security framework enables organizations to understand their current security postures and surrounded risks, establish a baseline relevant to our own policies and philosophies, and continuously monitor all application environments for anomalies. The automated implementation of the framework can be done using various forms and databases providing forward and backward links between services, assets, risks, requirements, controls and policies. This will allow an easy traceability and browsing across the different elements of the framework.

4 Conclusions and Future Work

The main contribution of this research was the introduction of a comprehensive services-oriented framework for security engineering and management including both development and maintenance phases aiming at enhancing system and service trustworthiness, and consequently enhancing user's trust in the provided services. This framework allows for a direct impact on the business objectives through the emphasis on services security. In addition, the proposed framework 1) links in a generic way the maintenance stages with the appropriate development stages allowing an efficient and effective maintenance of the security policies and procedures, 2) emphasizes the importance of layered framework traceability allowing easy modification of, and expansion to any layer of the framework, and 3) provides an approach leading to the efficient allocation of security budget to various risk controls aiming at maximizing the services trustworthiness by selecting the controls with the highest possible risk leverages. Possible future work includes 1) the application of the framework to real-life systems and services, 2) the use of the framework as a reference model to audit the appropriateness of existing policies, and 3) the embedding of the framework in an automated tool.

References:

[1] Tien, J., Berg, D., March 2006. A case for service systems engineering, Journal of Systems Science and Systems Engineering, 12(1).

[2] Mundie, C., deVries, P., Haynes, P., Corwine, M., 2002. Trustworthy computing, Microsoft White Paper, 10 pages.

[3] Mattord, H., Whitman, M., 2004. Management of Information Security, Thomson Course Technology.

[4] Pfleeger, C., Pfleeger, S.L., 2003. Security in Computing, third Edition: Prentice Hall.

[5] Ernst & Young, 2004. Global Information Security Survey.

[6] Johnston, J., Eloff, J., Labuschagne, L., 2003. Security and human computer interfaces, Computers & Security, 22(8), 675-684.

[7] Whitman, W., Mattord, H., 2004. Principles of Information Security, Thomson Course Technology.

[8] Barman, S., 2001. Writing Information Security Policies, New Riders.

[9] ISO/IEC 17799, 2000. International Organization for Standardization (ISO), Code of Practice for Information Security Management, Switzerland.

[10] Wai, L.W., 2001. Security life cycle, SANS Document.

[11] Lowery, L. C., 2002. Developing effective security policies, Dell power solutions.

[12] Flinn, D., 2003. Managing security policy change, Pedestal Software, Systems Engineering.

[13] Bayne, J., 2002. "An overview of threat and risk assessment", SANS Document.

[14] Small, B., 2003. Engineering secure systems using threat modeling, Software Productivity Consortium NFP.

[15] Firesmith, D., 2003. Engineering security requirements, Journal of Object Technology 2(1), 53-68.

[16] El-Shahry, G., 2005. A Systematic Approach to the Management of System Security Reengineering Process, Master Thesis, American University of Sharjah, UAE.