RESEARCH PAPER | Engineering | Volume : 3 | Issue : 12 | Dec 2013 | ISSN - 2249-555X

An Integrated Information Security Framework for a Product Development Center

KEYWORDS: Compliance box, Intelligent decision, Network Address Translator

Chandrasekaran Subramaniam
Professor CSE SRM university Chennai

Vinod Duraivelu
Research scholar CSE Sathyabama university Chennai,

ABSTRACT *The objective of the paper is to propose an integrated information security framework for a product development centre. The various policies for the secured information flow within and outside the development center along with various types of attacks are discussed so as to enhance the overall security of the information system at the center. A layered architectural model for the information security of the center is considered to overcome the risks. The security policies and mechanisms are discussed not only in the access control level but also in achieving secured information communication level between the different entities. The earlier models did not address the secured information exchange in the trust and privacy perspectives with respect to time and context of exchanges. The limited access to the information can be prevented from being released outside the organization but cannot be protected from being propagated within the organization.*

INTRODUCTION

The systematic approaches to measure security are needed in order to obtain evidence of the security performance of an organization and it is best when built in the product development center. Information security is essential to organizations that depend on information systems. This fact becomes more obvious when an organization's information is exposed to the risk of cyber attacks and the resulting damages. Managers need to know the extent of the damage that a cyber attack can cause and the possibility of occurrence; so that they can determine what they need to do to prevent the attack by selecting appropriate safeguards or repairing damage [1]. The computer systems can accept only the simple actions that would be governed by security policies. However, computers are increasingly handling complex organizational tasks which may have complex preconditions and post conditions. As such, it is useful to be able to plan and schedule actions in advance in order to ensure that desired actions will be able to be carried out without violating the security policy [2]. Qualitative security properties, such as non interference, typically either prohibit any flow of information from a high security level, or they allow any information flow provided it processes through some release mechanism [3]. Information security models require that information of a given security level is prevented from leaking in to lower-security information. High-security applications must be demonstrably free of such leaks, but such demonstration may require substantial manual analysis [4]. Information leakage traditionally has been defined to occur when uncertainty about secret data is reduced. The experiment is being formalized as how an attacker, an agent that reasons about beliefs, revises his belief from interaction with a system, an agent that executes programs. The attacker should not learn about the high input to the program but it allows observing low input and outputting [5]. Models are developed that describes how attacker beliefs change due to the attackers' observation of the execution of a probabilistic (or deterministic) program. The security models have two goals preventing accidental or malicious destruction of information, and controlling the release and propagation of that information. The information flow control is vital for large or extensible systems where there are number of collaborating processes. The security between various nodes running in different platform has to be enhanced for the successful collaboration of the privacy policy. The privacy and non-repudiation policy are to be adapted in a dynamic run time environment to achieve the required level of information assurance. In any information security model, information security related activities are to be carried in a unified manner responding to information security incidents. Such a mathematical model of enhanced security for product development center can be arrived with suitable adaptation policy for information assurance and security.

SECURITY AGAINST OUTSIDE ATTACKS

The product development center security framework consists of security mechanisms outside the center to access the local network through a common firewall as shown in figure 1.The framework will prevent the entry of unauthorized users other than the individual clients who share a common firewall. The information request is given to the compliance box where the compliance processing of the requirements of each network is dealt. If the node request is checked for its entire compliance then a sequence of tasks are to be carried out. These tasks are performed in various layers of the proposed model. The layered model does the process of providing a secure information flow. If any error or threat is encountered by the monitor block in the layer model a report is sent to the evaluation block. The error or threat is then evaluated and the corresponding information is processed back to the compliance box. If there is no error or threat encountered in the layer model the monitor block directly sends the requirements to the research and development department for the product development center. It is then sent to the destined source through the compliance box. Now the decision about the node whether a valid or an invalid node will be recognized and intelligible decision will be taken by compliance box.

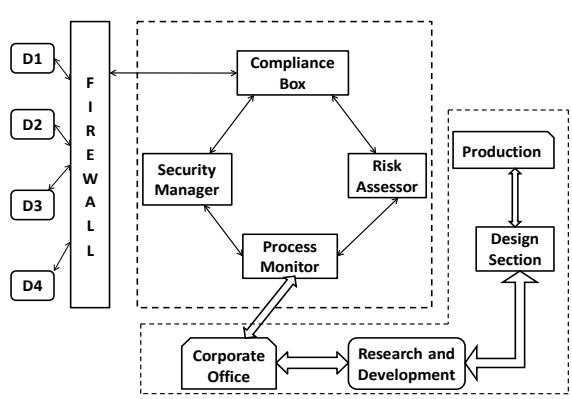

Figure1. Security framework of a product development center

Each information will be checked thoroughly by compliance

Volume : 3 | Issue : 12 | Dec 2013 | ISSN - 2249-555X

box. It checks whether the information is valid for the destination. In order to enhance the output an intelligent decision is taken to avail the source meant for a node.

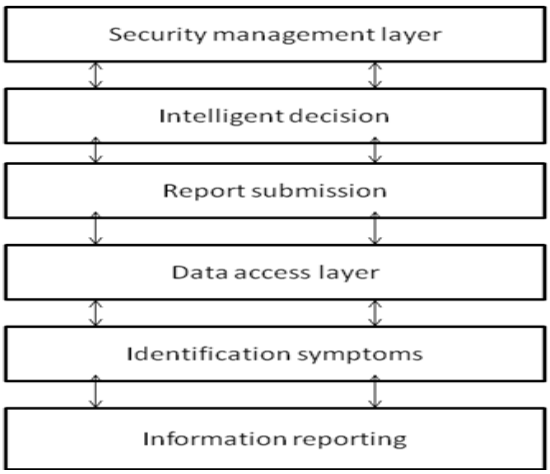

Figure 2. Layered architecture of security management

Secure accessibility of a data request inside the product development center in different stages is shown in figure 2.In the Information Reporting Layer (IRL), the IP (Internet Protocol) address of the entered node and its domain are read. For example, if the Domain Address (DA) is 2.2.2.2 and IP address is 192.168.0.1, then the above addresses about the node will be reported as an input to the Identification Symptoms layer (ISL). In this layer, the validity of the IP and the domain addresses are checked. The Responded Addresses (RA) is the address which is responded from the product development center server, say 12.1.1.1. In the Data Access Layer (DAL) data that are accessed by the entered node and respond address is matched with the entered IP. In the Report Submission Layer (RSL) the report about the nature, purpose and the actions played by the visiting node, IP and its domain and responded addresses is sent to the Intelligent Decision Layer (IDL), so that accessibility mode for a node is activated. The IDL verifies the authenticated IP, compares it with the Medium Access Control (MAC) and checks for the correct and incorrect match thus making a protection against hardware usability. In the Security Management Layer (SML), the entered node is not allowed to modify the accessed data. The authenticated IP is given as an input to the security management layer and it provides secure access to the database as shown in figure 3.

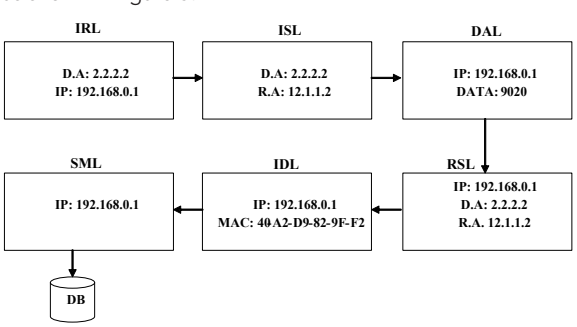

Figure 3. Information Flow between layers

CASE STUDY: Secure information flow within an organization

The secure information flow within an organization like a product development center can be modeled with two different stages. The various securities related policies and their implementations are to be integrated to achieve performance oriented security results. The synchronization and collaboration of the activities can bring the expected safety and security results only when there is a multiplexing of the methods. The first stage is being the pre deployment stage and the next one is the post deployment stage. In the pre deployment stage, the information as a bundle of data or messages and the various processes and controls with which the information is to be processed. The Network Address Translator (NAT) routers allow data to pass from the internal secure Local Area Network (LAN) to the external insecure internet Wide Area Network (WAN) but will automatically block the data as a sort of one-way valve [6]. In the post deployment stage the information flow is determined by the underlying networks services and end users trust levels. A pipe-valve-tank model is proposed to incorporate the security requirements in controlled information flow as shown in figure 4.The Non-integrated Information Security approach (NIS) may be considered as the sum of the products of the various policy levels and the organizations functional capability. This may be represented as a set of equations for both pre and post deployment of information outside the organization.

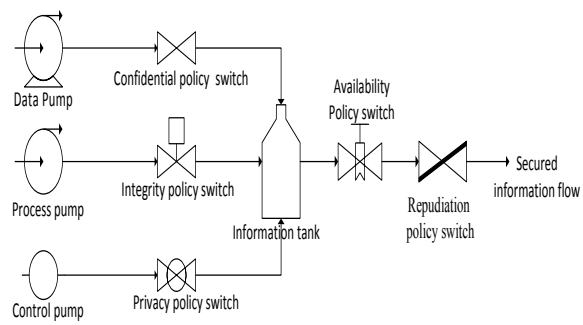

Figure 4. Non - Integrated information security

The integrated approach of information security describes about the security of information flow which can be achieved through five policies namely confidentiality, integrity, privacy, availability and non-repudiation. The data is being pumped through the data source where the security of the data is controlled by a confidential policy as a switch or a valve. The prioritization of the data is to be done in this section into low, medium and high levels. The processes maybe considered as if they are passed into the integrity policy switch which checks for the consistency of the data. The Privacy policies are more like finely tuned control valves that direct the flow of information where customer's along with company executives want it to flow for the best outcome[7]. In addition to that the control flow works on the change of control over the processes which maintains the privacy of the information that is being transmitted. The closed information tank contains the entire storage of the data as well as its association in specific contexts. The net outflow of the proposed model is a secure flow of information. The availability policy switch helps in the checking for the availability of data always or when it is on demand.

CONCLUSIONS

A security framework for a product development center integrating the various policies for an effective security management is proposed. The outside attacks on the network and inside threats are also considered. A multiplexing mechanism is used through which the priority, criticality and urgency of the various information are achieved. The effective implementation and the trusted collaborations within the security management and the risk assessor modules will enhance not only the availability but also privacy of various entities. The model may be updated through the incorporation of current and future standards of information exchange by the compliance box module. The pre and post deployment of information within the organization can be made secured through the model cryptographic with the pulse in the intranet and internet.

Volume : 3 | Issue : 12 | Dec 2013 | ISSN - 2249-555X

REFERENCE

[1] Fariborz Farahmand, Shamkant B. Navathe. Gunter P. Sharp and Philip H. Enslow,"Managing Vulnerabilities of Information Systems to Security Incidents", ACM International Conference Proceeding Series; Vol. 50 Proceedings of the 5th international conference on Electronic commerce, ACM, New York, NY, USA, pp. 348 - 354. | [2] Keith Irwin, Ting Yu, and William H. Winsborough, "Avoiding Information Leakage in Security-Policy-Aware Planning", Conference on Computer and Communications Security Proceedings of the 7th ACM workshop on Privacy in the electronic society, ACM, New York, NY, USA, pp. 85-94. | [3] Andrew C. Myers and Barbara Liskov, "A Decentralized Model for Information Flow Control", ACM Symposium on Operating Systems Principles | Proceedings of the sixteenth ACM symposium on Operating systems principles, ACM, New York, NY, USA, pp. 129-142. | [4] Michael R. Clarkson, Andrew C. Myers and Fred B. Schneider, "Quantifying Information Flow with Beliefs", Journal of Computer Security, Volume 17, Issue 5 (October 2009) 18th IEEE Computer Security Foundations Symposium (CSF 18), IOS Press Amsterdam, The Netherlands, pp. 655-701. | [5] Roderick Chapman and Adrian Hilton", Enforcing Security and Safety Models with an Information", Annual International Conference on Ada Proceedings of the 2004 annual ACM SIGAda international conference on Ada: The engineering of correct and reliable software for real-time & distributed systems using Ada and related technologies, ACM, New York, NY, USA, pp. 39-46. | [6] NAT Router Security Solutions, http://www.grc.com/nat/nat.htm,from Gibson Research Corporation. | [7] Allan Holmes, "The Profits in Privacy", CIO Magazine, March 2006, pp. 1-42.