FUNCTIONAL REQUIREMENTS FOR SECURE CODE: THE REFERENCE MONITOR AND USE CASE

Ken Trimmer, Idaho State University
Kevin R. Parker, Idaho State University
Corey Schou, Idaho State University

ABSTRACT

Information assurance, data security, and corresponding issues are traditionally presented in Systems Analysis and Design textbooks as non-functional requirements. Systems analysts can enforce secure design and code as one of the essential goals of systems analysis and design by using the Reference Monitor concept as a means of requirements and design specification. The application of the Reference Monitor during the early stages of systems requirements specification via the Use Case emphasizes that information assurance is a critical functional requirement.

INTRODUCTION

Failure to incorporate security into systems requirements is a concern dating back at least a quarter of a century (Schell, Downey & Popek, 1973, Pipkin, 2000). Compounding this oversight is the lack of attention paid to security in textbooks and the exclusion of security as a functional requirement (Haworth, 2002, Trimmer, Parker & Schou, 2007).

The lack of ubiquitous system security requirements yields the 'penetrate and patch' strategy for secure code maintenance. This strategy, in addition to being costly to enforce and a source of vulnerabilities, may compromise an organization's system resources and corresponding operations when considered from an Information Assurance (IA) perspective (Schou, Trimmer & Parker, 2005).

The pervasive use of data by those both internal and external to an organization has led to Information Systems (IS) becoming a component of the organization's communications infrastructure, much as the fax and the telephone were before the broad adoption of personal computers at all levels of organizations. Once the telephone became an integral component of organizations, certain functions became dependent upon it, such as the ability to quickly place or receive orders from someone not physically located at the organization. Fax machines extended this, as they enabled orders to vendors and from customers to contain considerable detail about multiple items that may have been more difficult to clearly communicate via verbal telephone communications.

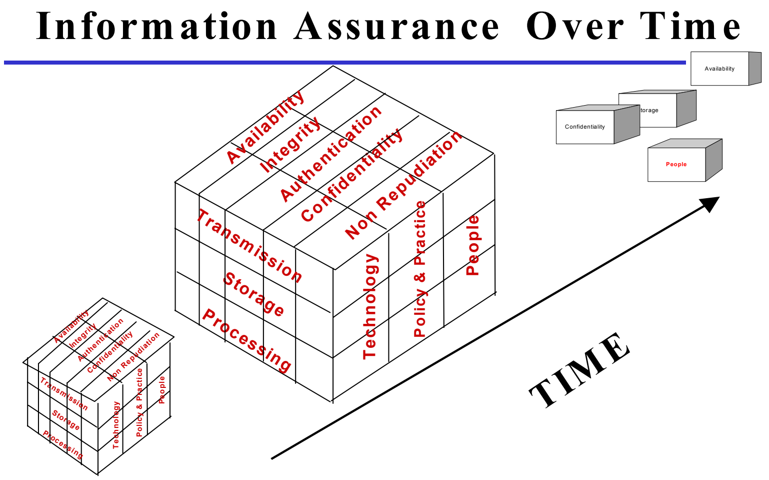
Electronic Data Interchange and e-commerce via the World Wide Web have escalated functional dependence upon IS. Furthermore, the emergence of ‘knowledge workers’ in organizations would be non-existent without IS. It is clear that the modern organization cannot exist in its evolved form without an IS. Further, the IS is unable to provide the necessary support for the dependent organizational functions unless the underlying principles of IA are considered and in place.

INFORMATION ASSURANCE

Information Assurance is an extension of computer security and information security processes. It encompasses the entire lifecycle of data and information from project inception to the retirement of the system and its contents. Because of the underlying design complexity of secure systems, security and information assurance are typically late binding design functions, if considered at all in the design phase (Schou, et al., 2005).

IA is both multidisciplinary and multidimensional. This was identified by McCumber in the representation of his model for computer security (McCumber, 1991). Spurred by the growth of the World Wide Web and e-commerce in the late 1990s, Maconachy, Schou, Ragsdale, and Welch (2001) developed the MSR model by extending McCumber’s robust information assurance model to include time as a fourth dimension, adding to Information States, Security Services, and Security Countermeasures.

Figure 1, Information Assurance as represented by Maconachy et al., 2001



Also in 2001, Maconachy et al. extended the basic information service dimensions of availability, integrity, and confidentiality with the additional dimensions of authentication and non-repudiation. The additions by Maconachy and his associates are displayed in Figure 1 (Maconachy et al., 2001). In 2008 the Joint Task Force on Computing Curricula adopted the MSR model as part of the information technology model curricula for information assurance and security (ACM, 2008, p. 73-74).

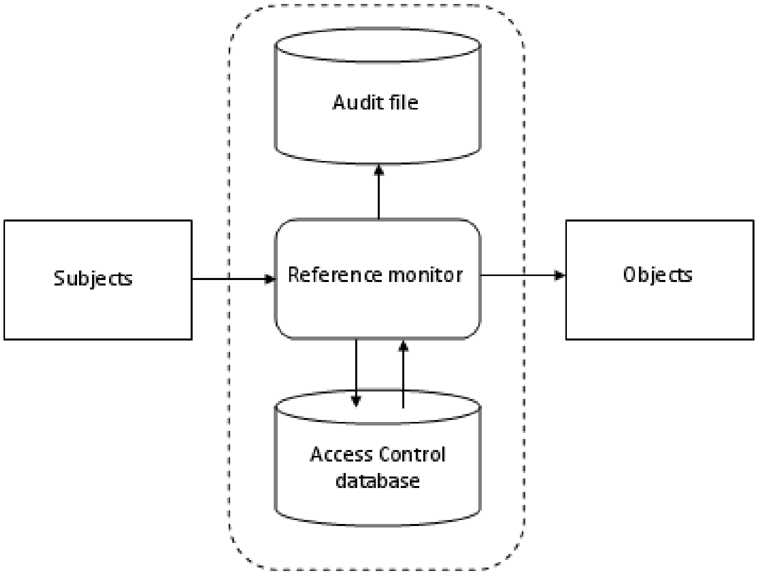
REFERENCE MONITOR

Irvine (1999, p. 3) in referencing Anderson (1972) defines the Reference Monitor (RM) as having the following requirements:

- ♦ *The access mediation mechanism is always invoked.*
- ♦ *The access mediation mechanism is tamperproof.*
- ♦ *It "must be small enough to be subject to analysis and tests, the completeness of which can be assured".*

Irvine continues her discussion of the RM, addressing the need to consider it in systems requirements as it is a broad tool that enables the systems analyst to identify abstract requirements. Trimmer et al. (2007) provide a similar argument, making a distinction between a Requirements RM and a Design RM, to be addressed as broad systems requirements and incorporated into the initial design. The incorporation of both RMs is to be performed regardless of the specific development methodology employed.

Figure 2, Concept of Reference Monitor, after Cho et al. (2008)



Furthermore, satisfying RM requirements is a basic security component of both mandatory and verified protection for software that satisfies US Department of Defense requirements for secure system controls. The RM is a component of the Trusted Computer System Evaluation Criteria (Department of Defense, 1985).

Correspondence between the service dimensions of authentication and non-repudiation in the model shown in Figure 1 and the RM are represented by Cho, Moon, and Baik (2008). This concept is displayed in Figure 2. The dotted line has been added to show the integral nature of the RM – it is implicit that it is self contained. In this representation, the subject authenticates through the RM, which uses its integral Access Control Database. Provided the subject has rights given their authentication, s/he is granted access to the objects. This access is recorded in the integral Audit File to support non-repudiation.

USE CASE

The Use Case, a component of the Unified Modeling Language (UML) (Satzinger, Jackson & Burd, 2005), represents a user as existing outside a system, making requests to the system. Traditionally, this corresponded to individuals within an organization who required specific system support to carry out their organizational functions. The advent of the Internet in business commerce further complicated the process, as supply chain enablement permits both suppliers and customers to remotely interact with the system. The Use Case serves as a requirements gathering tool not only for the UML methodology, but also for more traditional analysis and design modeling tools such as Data Flow Diagrams and Entity Relationship Diagrams (Whitten, Bentley & Dittman, 2004).

The representation of the RM by Cho et al. (2008) in Figure 2 is illustrative of applying the RM concepts as an underlying condition for the Use Case. Cho et al. (2008) use the RM as the focal point for an end user's home gateway model. They provide a user scenario as an example of user access and maintenance of a temperature control service. This scenario also presents the events in another type of UML Diagram, the Sequence Diagram.

The following discussion addresses the use of the RM, using the representation in Figure 1. This discussion focuses on the general accessing of information by an employee (A) and an online consumer (B). In both scenarios the user gains access to the information through a web portal.

A. *An employee of an agricultural firm is out of town, and needs to process an expense transaction and check on the status of a prior request. The employee gains access to the Internet via a secure WiFi at their hotel, and proceeds to the corporate website. After selecting 'Secure Login', the employee enters their user identification and password. This is passed to the RM, which provides access to the employee's web page, which provides access to only those corporate information resources to which the employee has rights. The employee selects Expense Transactions, and the RM is again engaged,* *providing the employee read/write access to New Transactions and read - only access to Transaction Status and Transaction Reports for Expense items.*

B. *A consumer Googles a product made by the same agricultural firm and finds that they can place a direct order of $1000 or more without going through a distributor. The consumer selects the product and places it in a Shopping Cart. At this point, the consumer has only read access to an online catalog. When the consumer is done selecting products and quantities and makes the 'Purchase' request, they are led to a site that asks if they are a registered user or if they would like to proceed as a guest. If they are a registered user, they will be asked for a user name or email address and password. The RM will then be invoked and the consumer will be authorized to proceed to the transaction and gain access to a set of choices similar to those seen by the Employee in scenario A, with corresponding read/write and read-only privileges. The Guest will be taken to a screen that will allow them to write one and only one transaction.*

In both cases, the RM validates the user authentication and records a corresponding transaction unseen by the user. Access to the system is necessary for either user to perform their corresponding functions. Furthermore, as discussed by Cho, et al. (2008), the RM also checks for user services, thereby calling into play an additional component of Figure 1, Availability. Another characteristic addressed in Figure 1 is Integrity, as the user has write access to only new transactions. The final of the original three dimensions in the McCumber Cube, Confidentiality, is also addressed by the RM in that only those employees, groups of employees, and customers performing functions are granted rights to certain data elements and applications.

The corresponding Use Cases must contain an "Includes" of the RM by each specific process requested by the user. By considering the RM during requirements modeling, the underlying data elements and processes will enable the user to complete the specific tasks associated with their function either internal or external to an organization. Although it can be argued that in times of system outage a user could resort to manual systems to perform their function, such actions could lead to a compromise of system integrity and corresponding user functions and should be discouraged. The role of the RM and IA is even more necessary for the completion of the knowledge management functions in the modern organization.

CONCLUSION

Systems designers must begin to incorporate secure code concepts throughout the analysis and design process. By requiring that the concept of the Reference Monitor be considered as a functional requirement in Use Case Diagrams, the designer will incorporate authentication and non-repudiation throughout the systems development life cycle, regardless of the methodology chosen. By including the RM, the designer will be forced to consider the related information characteristics of availability, integrity, and confidentiality under the umbrella of Information Assurance – critical functional requirements for the modern organization.

REFERENCES

ACM. (2008). ACM Computing Curricula Draft, Information Technology Volume. Retrieved December 21, 2008, from http://campus.acm.org/public/comments/it-curriculum-draft-may-2008.pdf

Anderson, J. P. (1972). Computer Security Technology Planning Study. *Technical Report ESD-TR-73-51*, Air Force Electronic Systems Division, Hanscom AFB, Bedford, MA.

Cho, E., C. Moon & D. Baik (2008). Home Gateway Operating Model using Reference Monitor for Enhanced User Comfort and Privacy. *IEEE Transactions on Consumer Electronics, 54*(2), 494-500.

Department of Defense (1985). Trusted Computer System Evaluation Criteria. DoD 5200.28-STD.

Haworth, D. (2002). Security Scenarios in Analysis and Design, The SANS Institute.

Irvine, C. E. (1999). The Reference Monitor Concept as a Unifying Principle in Computer Security Education. *Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education*, 27-37.

Maconachy, W. V., C.D. Schou, D. Ragsdale & D. Welch (2001). A Model for Information Assurance: An Integrated Approach. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 306-310.

McCumber, J. (1991). Information Systems Security: A Comprehensive Model. *Proceedings 14th National Computer Security Conference*. 328-337.

Pipkin, D. (2000). *Information Security: Protecting the Global Enterpris*e. Upper Saddle River, N.J.: Prentice Hall PTR.

Satzinger, J.W., R.B. Jackson & S.D. Burd (2005). *Object-Oriented Analysis & Design with the Unified Process.* Boston, MA: Thomson/Course Technology.

Schell, R.R., P.J. Downey & G.J. Popek (1973). Preliminary Notes on the Design of Secure Military Computer Systems, MCI-73-1, The MITRE Corporation, Bedford, MA 01730. Retrieved December 21, 2008, from http://seclab.cs.ucdavis.edu/projects/history/CD/index.html#sche73

Schou, C., K. Trimmer & K.R. Parker (2005). Forcing Early Binding of Security Using a Design Reference Monitor Concept in Systems Analysis and Design Courses. *Proceedings of the International Conference on Informatics Education and Research*, 321-331.

Trimmer, K., K.R. Parker & C. Schou (2007). Forcing Early Implementation of Information Assurance Precepts throughout the Design Phase. *Journal of Informatics Education Research, 9*(1), 95-120.

Whitten, J.L., L.D. Bentley & K.C. Dittman (2004). *Systems Analysis and Design Methods (Sixth Edition)*. Boston, MA: McGraw-Hill/Irwin.