IGI PUBLISHING **ITJ4167**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, **International Journal of Information Security and Privacy**, Volume 2, Issue 1
edited by **Hamid R. Nemati © 2008, IGI Global**

SEACON:
An Integrated Approach to the Analysis and Design of Secure Enterprise Architecture–Based Computer Networks

Surya B. Yadav, Texas Tech University, USA

ABSTRACT

The extent methods largely ignore the importance of integrating security requirements with business requirements and providing built-in steps for dealing with these requirements seamlessly. To address this problem, a new approach to secure network analysis and design is presented. The proposed method, called the SEACON method, provides an integrated approach to use existing principles of information systems analysis and design with the unique requirements of distributed secure network systems. We introduce several concepts including security adequacy level, process-location-security matrix, data-location-security matrix, and secure location model to provide built-in mechanisms to capture security needs and use them seamlessly throughout the steps of analyzing and designing secure networks. This method is illustrated and compared to other secure network design methods. The SEACON method is found to be a useful and effective method.

Keywords: *data-location-security; process-location-security; secure computer network; secure enterprise architecture-based network; secure enterprise network design; security adequacy level*

INTRODUCTION

Designing and implementing a secure computer network has become a necessity for companies big or small. Network security is no longer just a technical issue anymore (Sarbanes-Oxley Compliance Journal, 2005). It has also become an economic and legal issue for most companies. According to an IT security management survey, "Two-thirds of those who took part in the survey acknowledged that the wide range of government regulations, such as Sarbanes-Oxley, HIPAA, and GLBA, has affected their company's handling of IT security issues" (Sarbanes-Oxley Compliance Journal, 2005). According to CSI/FBI's Tenth Annual Computer Crime Security Survey, unauthorized access to information and theft of proprietary information showed significant increases in average loss per respondent (CSI/FBI, 2005). Hackers have also moved to new areas such as identity theft

(McMillan, 2005). As a consequence, the cost of information theft has jumped considerably. These surveys indicate that a better computer network design method is needed for designing a more secure computer network.

There has been increased activity in various aspects of security, network system security, and secure network design in the last several years. There are several good articles (Cisco Systems, 2001; Fisch & White, 2001; Ghosh, 2001; Oppenheimer, 2004; Southwick, 2003; Whitman & Mattord, 2005; Whitmore, 2001) that deal with secure network design. For example, Fisch and White (2001) discuss security models and various kinds of security measures in detail. Ghosh (2001) discusses principles of secure network design and an in-depth analysis of ATM networks and their security. Oppenheimer (2004) uses a top-down network design methodology to design an enterprise computer network. The emphasis is on the technical analysis and design of networks. Whitman and Mattord (2005) present a Security Systems Development Life Cycle (SecSDLC) methodology paralleling the basic system development life cycle (SDLC) methodology. There are sophisticated network simulation and performance tools such as OPNET (OPNET, 2005). Most of the existing work on secure network design, however, tends to lean more toward technical details. There is very little research that addresses the issue of security and business requirements of a computer network simultaneously. It is very important to understand an organization's business requirements to design an effective network (Oppenheimer, 2004). It is equally important to understand the organization's security requirements as well. To our knowledge, there is no published design method that integrates secure network requirements with business requirements to develop a secure network. In this article, we address the following research questions:

1. How can we identify security and business requirements of a network system seamlessly?
2. How can we identify all possible assets and resources, including business processes and data that need to be protected in a network system?
3. How can we incorporate and document security requirements into conceptual and logical network diagrams?

This article follows the DEACON method (Shaw & Yadav, 2001) and presents a new method that provides built-in mechanisms to carry secure network requirements along with business requirements seamlessly throughout the process of analyzing and designing secure network architecture. We have developed, as part of the method, several new concepts such as the security adequacy level, process-location-security matrix, data-location-security matrix, and secure location model to achieve a good interplay between network security requirements and business requirements.

CURRENT WORK ON DEVELOPING SECURE COMPUTER NETWORKS

Computer networking and its security is a vast area of research and study. The topics cover network security concepts, principles, frameworks, techniques, methods, laws, and practices. This article draws from research on several of the topics mentioned above; however, it is not practical for this article to review even a fraction of the literature covering those topics. Interested readers are kindly referred to Ghosh (2001), Kizza (2005), and Whitman and Mattord (2005) for a good review of topics related to secure computer networks. Here, we limit our literature discussion to research that deals with secure network design methods.

Paul Innella (Innella, 2001) presents a design method based upon the software process model. This is an interesting method but it is, in its current form, too general and too brief to be of any practical use.

Cisco Systems (2001) has developed a secure blueprint for enterprise networks (SAFE) to provide best practice information on designing