Chapter 5.30
Information Security Risk Analysis:
A Pedagogic Model Based on a Teaching Hospital

Sanjay Goel
University at Albany, SUNY, and NYS Center for Information Forensics and Assurance, USA

Damira Pon
University at Albany, SUNY, and NYS Center for Information Forensics and Assurance, USA

ABSTRACT

There is a strong need for information security education, which stems from the pervasiveness of information technology in business and society. Both government departments and private industries depend on information systems, as information systems are widespread across all business functions. Disruption of critical operational information systems can have serious financial impacts. According to a CSI/FBI report (2004), losses from security breaches have risen rapidly in recent years and exceeded $200 million in 2003. The information security field is very diverse and combines disciplines such as computer science, business, information science, engineering, education, psychology, criminal justice, public administration, law, and accounting. The broad interdisciplinary nature of information security requires several specialists to collaboratively teach the curriculum and integrate different perspectives and teaching styles into a cohesive delivery. This chapter presents a pedagogical model based on a "teaching hospital" concept that addresses the issues introduced above. By using a specific information-risk-analysis case, the chapter highlights the basic concept of the teaching hospital and its application in teaching and learning contexts.

LEARNING OBJECTIVES

After completing this chapter, you will be able to:

- Discuss the issues associated with information assurance education.
- Describe the basic concept of teaching hospital approach in information security risk analysis.
- Understand the case development methodology used to support the teaching hospital.
- Suggest possible improvements to the cases described in the chapter.

INTRODUCTION

Information assurance (IA) is a complex field, especially due to the dynamically changing security environment and constant evolution of practices and procedures. It is difficult to provide training in such an area since material developed becomes obsolete very quickly. To develop a better understanding of IA, concepts should be assimilated from several disciplines (i.e., computer and information science, law, business, etc.) and blended into the context of real problems. In this chapter, a teaching hospital model that has been developed for IA training in the context of information security risk analysis is described. The teaching hospital approach involves incorporating real cases to supplement existing curriculum, which keeps teaching material relevant over time through infusion of current research problems in the curriculum and creates a rich learning environment that is both stimulating and dynamic. The New York State Center for Information Forensics and Assurance (CIFA) at the University at Albany has developed a teaching hospital for IA education (Goel & Pon, 2005). Within this teaching hospital, a research program that solves current industry problems is combined with a teaching program responsible for dissemination of curriculum. Problems from public and private sector organizations are introduced in the research lab, which are solved and abstracted into living cases that are then used to supplement the training material. Bridges and Hallinger (1999) have shown case-based learning to be a powerful pedagogical tool for dissemination of instruction. The teaching hospital model provides a constant stream of cases that keeps the curriculum current. Though effective, such an approach is still labor-intensive and contingent upon smooth functioning of research and educational case development programs. The field of security is so vast that a considerable time will elapse before most of the information security domain is covered through cases. Over time, it is envisaged that a library of cases will emerge, requiring less effort in new case development.

The general philosophy behind use of cases in curriculum and in context of the teaching hospital proposed is detailed in the chapter. The rest of the chapter is organized as follows: We first introduce the case-based learning techniques and the concept of a teaching hospital. We then present a case on risk analysis that demonstrates the use of the teaching hospital in information assurance curriculum. Finally, we conclude the chapter, followed by a brief summary

TEACHING HOSPITALS AND CASE-BASED TEACHING

Teaching hospitals have been used extensively for medical training since the 20th century (Barzansky, Jonas, & Etzel, 1998). They enabled control on medical student production and medical education quality monitoring. Training is provided to medical students and doctors-in-training through direct clinical experience of treating actual patients under the supervision and guidance of attending physicians in medical wards. Medical teaching hospitals are important because their students need hands-on experience; otherwise, it

Related Content

Privacy-Preserving Techniques for Online Social Networks Data

Yousra Belfaik, Abdelhadi Zineddine, Yassine Sadqiand Said Safi (2024). *Risk Assessment and Countermeasures for Cybersecurity (pp. 62-78).*

www.irma-international.org/chapter/privacy-preserving-techniques-for-online-social-networks-data/346080

A Rule-Based and Game-Theoretic Approach to Online Credit Card Fraud Detection

Vishal Vatsa, Shamik Suraland A. K. Majumdar (2007). *International Journal of Information Security and Privacy (pp. 26-46).*

www.irma-international.org/article/rule-based-game-theoretic-approach/2465

Artificial Intelligence Tools for Handling Legal Evidence

Ephraim Nissan (2007). *Encyclopedia of Information Ethics and Security (pp. 42-48).*

www.irma-international.org/chapter/artificial-intelligence-tools-handling-legal/13450

Secure Transmission of Analog Information using Chaos

A.S. Dmitriev, E.V. Efremova, L.V. Kuzmin, A.N. Miliou, A.I. Panasand S.O. Starkov (2011). *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption (pp. 337-360).*

www.irma-international.org/chapter/secure-transmission-analog-information-using/43304

An Ensemble Approach for Feature Selection and Classification in Intrusion Detection Using Extra-Tree Algorithm

Ankit Rajeshkumar Kharwarand Devendra V. Thakor (2022). *International Journal of Information Security and Privacy (pp. 1-21).*

www.irma-international.org/article/an-ensemble-approach-for-feature-selection-and-classification-in-intrusion-detection-using-extra-tree-algorithm/285019