Chapter VIII

An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications

Mikko T. Siponen
University of Oulu, Finland

Recently, several Information Systems Security (ISS) development approaches that support modeling have been presented. This chapter analyzes and compares the recent approaches for the development of secure ISs. The comparison and analysis will be carried out from the viewpoints of a conceptual meta-model for IS; research methods used; the organizational roles of IS security; the objectives of the research; selected philosophical foundations (underlying epistemology, philosophy of science) and applicability. This contribution of the chapter can be divided into descriptive (assumptions that researchers should be aware of) and prescriptive implications (the direction of future research).

INTRODUCTION

Until recently, ISS design relied on conventional ISS methods such as checklists. More recently, computer science and IS research communities have awakened to extend their considerations to the security issues of IS. As a result, several more advanced but less well-known approaches to develop secure ISs and respective modeling have been suggested. These recent approaches can be classified as paradigms, or schools of ISS development, namely Information/Data Base modeling approaches (Pernul, 1992; 1998; Elmer et al.
1995), responsibility approaches (Dobson, 1990; Strens & Dobson, 1993; Backhouse & Dhillon, 1996; Dhillon, 1997; McDermott & Fox, 1999), and the security-modified IS development approaches (Baskerville, 1988; Hitchings, 1995; Booysen & Eloff, 1995; James, 1996). This chapter analyzes these approaches. A systematic in-depth analysis of the recent IS security methods would be worthwhile for several reasons. It is common that humans reflect (even follow) different beliefs and grains of knowledge instilled upon them through upbringing, education or acquired by personal experiences (Hare, 1952). This is also true with the IS development (Hirschheim, & Klein, 1989) and, consequently, there are different views on how to develop IS (e.g. Hirschheim et al., 1995). Therefore, it is advisable that researchers are aware of the different underlying philosophical assumptions of different methods (Hirschheim et al., 1995; Dhillon, 1997). Furthermore, due to disjointed and isolated views of IS development methodologies, a comparative study is as valuable as the addition of a new method (Hirschheim et al., 1995). The situation concerning IS security methods is at least diverse. Hence, an in-depth analysis concerning the different approaches to develop secure ISs is justified. This chapter analyzes these approaches holistically. The information provided by the analysis - to observe the differences, possible strengths and weaknesses of the different approaches - should also be important for practitioners. Finally, such analysis is hopefully welcomed for education purposes. Since the traditional IS development methods do not trouble themselves with security concerns (Baskerville, 1993), the information about how to develop secure ISs should be equally important for IS developers as for the security community.

The composition of the chapter is following. In the second section, an overview of the approaches for secure IS development, the framework for analysis and the related works are presented. In the third section, the recent approaches are reviewed. The fourth section is discussion. In the fifth section, the key findings (descriptive implications) and prescriptive implications are summarized.

**THE FRAMEWORK FOR ANALYSIS, RELATED WORK AND AN OVERVIEW OF THE APPROACHES**

Figure 1 presents an overview of the approaches for secure IS development. The generation divisions were originally presented by Baskerville (1988) and are separated by lines. The arrow shows influences or inspirations (since the influence from works of earlier authors is very weak). Broken arrows mean that the approach is influenced by the deficiencies of a certain approach. The tradition (Computer science, Data Modeling, IS, and Practitioners/Consultant community; IS community) from which the works have sprung is described using italics. For example, security semantics (e.g. based on ER and DFD notation) is developed in the Data Modeling community. The practitioner community dominates the principles, checklists and most standards for secure systems development. The “research” problems often arise from their practical experiences (hence, the label practitioners). Formal development is particularly favored by the computer science community. The (security) data modeling has been done by database/data modeling scholars. Many recent approaches for developing secure IS systems are suggested by the IS community (for that reason, we shall call them security-modified IS development approaches).

First and second generations methods are aimed at finding out what can be done, with the help of available technical solutions. Third generation approaches include modeling,
Related Content

Business Continuity Planning: A Strategic Dilemma?
[www.irma-international.org/chapter/business-continuity-planning/43816/](www.irma-international.org/chapter/business-continuity-planning/43816/)

Exploring Secure Computing for the Internet of Things, Internet of Everything, Web of Things, and Hyperconnectivity
Maurice Dawson (2017). *Security Solutions for Hyperconnectivity and the Internet of Things* (pp. 1-12).

Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence
[www.irma-international.org/chapter/data-protection-law/50420/](www.irma-international.org/chapter/data-protection-law/50420/)

Security Engineering for Ambient Intelligence: A Manifesto
[www.irma-international.org/chapter/security-engineering-ambient-intelligence/23320/](www.irma-international.org/chapter/security-engineering-ambient-intelligence/23320/)

E-Voting Risk Assessment: A Threat Tree for Direct Recording Electronic Systems
[www.irma-international.org/article/voting-risk-assessment/58980/](www.irma-international.org/article/voting-risk-assessment/58980/)