Available online at www.sciencedirect.com
SCIENCE DIRECT®
Information Systems 30 (2005) 609–629
www.elsevier.com/locate/infosys

When security meets software engineering: a case of modelling secure information systems ☆

Haralambos Mouratidis[a,*], Paolo Giorgini[b], Gordon Manson[a]

[a]Department of Computer Science, University of Sheffield, UK
[b]Department of Information and Communication Technology, University of Trento, Italy

Received 27 February 2004; accepted 7 June 2004

Abstract

Although security is a crucial issue for information systems, traditionally, it is considered after the definition of the system. This approach often leads to problems, which most of the times translate into security vulnerabilities. From the viewpoint of the traditional security paradigm, it should be possible to eliminate such problems through better integration of security and software engineering. This paper firstly argues for the need to develop a methodology that considers security as an integral part of the whole system development process, and secondly it contributes to the current state of the art by proposing an approach that considers security concerns as an integral part of the entire system development process and by relating this approach with existing work. The different stages of the approach are described with the aid of a real-life case study; a health and social care information system.

Keywords: Information system design; Requirements analysis; Security engineering

1. Introduction

As information systems (IS) become more and more critical in every aspect of the human society, from the health sector to military, so does the demand to secure these systems. This is mainly because private information is stored in computer systems and without security, organisations (and individuals) are not willing to share information or even use the technology.

Consider, for example, a health and social care information system containing health data of

☆This is an extended and revised version of the "Integrating Security and Systems Engineering: towards the Modeling of Secure Information Systems" paper presented at the 15th International Conference on Advanced Information Systems Engineering (CaiSE 2003) and published in *Advanced Information Systems Engineering*, J. Eder and M. Missikiff (Eds.), Springer LNCS 2681, 2003.

*Corresponding author. School of Computing and Technology, University of East London, Barking Campus, Longbridge Road, Dagenham RM8 2AS, UK. Tel.: +44-20-8223-3315; fax: +44-20-8223-2963

E-mail addresses: haris@uel.ac.uk (H. Mouratidis), paolo.giorgini@dit.unit.it (P. Giorgini), g.manson@dcs.shef.ac.uk (G. Manson).

0306-4379/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.is.2004.06.002

different individuals. Security in such a system, as in any health and social care information system, is very important since security breaches might result in medical history to be revealed, and revealing a medical history could have serious consequences for particular individuals.

Software Engineers consider security as a non-functional requirement, but unlike other non-functional requirements, such as reliability and performance, security has not been fully integrated within the development lifecycle and it is still mainly considered after the design of the system. However, security introduces not only quality characteristics but also constraints under which the system must operate. Ignoring such constraints during the development process could lead to serious problems [1], since security mechanisms would have to be fitted into a pre-existing design, therefore leading to design challenges that usually translate into software vulnerabilities [2].

We believe that security should be considered during the whole development process and it should be defined together with the requirements specification. By considering security only in certain stages of the development process, more likely, security needs will conflict with functional requirements of the system. Taking security into account along with the functional requirements throughout the development stages helps to limit the cases of conflict, by identifying them very early in the system development, and find ways to overcome them. On the other hand, adding security as an afterthought not only increases the chances of such a conflict to exist, but it requires huge amount of money and valuable time to overcome it, once they have been identified (usually a major rebuild of the system is needed).

However, current methodologies for IS development do not meet the needs for resolving the security related IS problems [3], and fail to provide evidence of integrating successfully security concerns throughout the whole range of the development process.

There are at least two reasons for the lack of support for security engineering [4]:

1. Security requirements are generally difficult to analyse and model. A major problem in analysing non-functional requirements is that there is a need to separate functional and non-functional requirements yet, at the same time, individual non-functional requirements may relate to one or more functional requirements. If the non-functional requirements are stated separately from the functional requirements, it is sometimes difficult to see the correspondence between them. If stated with the functional requirements, it may be difficult to separate functional and non-functional considerations.
2. Developers lack expertise for secure software development. Many developers, who are not security specialists, must develop systems that require security features. Without an appropriate methodology to guide those developers on the development processes, it is likely that they will fail to produce effective solutions [5].

In this paper we present an approach that integrates security and systems engineering, using the same concepts and notations, throughout the entire system development process. This work falls within the context of the Tropos methodology [6,7] in which security requirements are considered as an integral part of the whole development process.

The paper is structured as follows. Section 2 provides an introduction to the Tropos methodology describing briefly the methodology stages and its concepts. Section 3 describes the security extensions to the Tropos methodology to enable it to model security issues, whereas Section 4 describes a health and social care information system that is used as a case study throughout the paper. Section 5 illustrates how our approach integrates security and systems engineering within the Tropos development process and Section 6 relates our work to the literature by providing an overview of related work. Finally, Section 7 provides directions for future work and it concludes the paper.

2. Tropos methodology

Tropos is a development methodology tailored to describe both the organisational environment of a system and the system itself. Tropos is