Chapter 5
Security Over the Information Systems Development Cycle

C. Blanco  
University of Cantabria, Spain

D. G. Rosado  
University of Castilla-La Mancha, Spain

C. Gutiérrez  
Correos Telecom, Spain

A. Rodríguez  
University of Bio-Bio, Chile

D. Mellado  
Spanish Tax Agency, Madrid, Spain

E. Fernández-Medina  
University of Castilla-La Mancha, Spain

J. Trujillo  
University of Alicante, Spain

M. Piattini  
University of Castilla-La Mancha, Spain

ABSTRACT

Information security is currently considered to be a crucial aspect of systems development. However, it has traditionally been considered during the final stages of development, once the main components of the system have been developed and therefore provides solutions which are inappropriate for security integration. Software engineering has traditionally been separated from security engineering, and security issues have not usually been included in software engineering processes, activities, techniques, models, and so on. Furthermore, security engineering has not been aligned with information systems, and has focused rather on the definition of protocols, cryptographic algorithms, access control policies, etc. However, the scientific community is beginning to realize the importance of aligning software
Security Over the Information Systems Development Cycle

1. INTRODUCTION

Software Engineering is defined as the area of engineering which applies a systematic, disciplined and quantifiable approach in order to develop software systems (IEEE, 1990). Software Engineering has thus improved the development process through methodologies, techniques, models and tools which provide systems that are close to the client’s needs and have a predictable cost and time. However, the complexity of the software systems to be developed has increased dramatically, thus making their development more difficult.

System requirements, which are the kernel of the development process, specify the functions that the system or system components should perform. Requirements in the development process therefore need to be identified as soon as possible in order to be able to develop analysis models which represent these requirements, design models which integrate the requirements in the high level solution, and finally, carry out an implementation which respects these needs through an integrated and robust solution.

If requirements are not identified and integrated during the first stages of the development process, the needs they represent will not be appropriately integrated into the system and the development will be less robust, more expensive and its maintenance will be more complex. It is therefore crucial to analyze, elicit, specify and model information system requirements from the early stages of development. These functional requirements represent the functionality of the system and describe what the software will do, but too many manners in which to provide this functionality exist.

Nonfunctional requirements are, moreover, important since they describe how the software will carry out its purpose, and they involve several issues such as security constraints, performance requirements or quality attributes. These nonfunctional requirements should therefore also be identified during the first stages of the software development process for the reasons previously mentioned. Furthermore, security is considered to be an important aspect in the development of quality software (Devanbu and Stubblebine, 2000, Ferrari and Thuraisingham, 2000, Ghosh et al., 2002), so by improving the security, we also improve the quality of the software. Indeed, the ISO 9126 standard includes security as a characteristic of software quality which contains the following properties: availability, confidentiality, integrity, non-repudiation, accountability, authenticity and compliance.

However, although security is an important type of requirement, Software Engineering and Security Engineering have traditionally been independent of each other (Giorgini et al., 2007). On the one hand, software engineering is focused on the systematic development of information systems, and does not consider security as an important issue. It recognizes the importance of security as a nonfunctional requirement, but software engineering techniques and methods do not incorporate security. On the other hand, security engineering is focused on the definition of formal and theoretical methods (such as protocols, cryptographic algorithms, access control policies or information flow control), which are...