Chapter 2
A Compliance-Driven Framework for Privacy and Security in Highly Regulated Socio-Technical Environments: An E-Government Case Study

Ayda Saidane
Independent Researcher, Canada

Saleh Al-Sharieh
University of Groningen, The Netherlands

ABSTRACT

Regulatory compliance is a top priority for organizations in highly regulated ecosystems. As most operations are automated, the compliance efforts focus on the information systems supporting the business processes of the organizations and, to a lesser extent, on the humans using, managing, and maintaining them. Yet, the human factor is an unpredictable and challenging component of a secure system development and should be considered throughout the development process as both a legitimate user and a threat. In this chapter, the authors propose COMPARCH as a compliance-driven system engineering framework for privacy and security in socio-technical systems. It consists of (1) a risk-based requirement management process, (2) a test-driven security and privacy modeling framework, and (3) a simulation-based validation approach. The satisfaction of the regulatory requirements is evaluated through the simulation traces analysis. The authors use as a running example an E-CITY system providing municipality services to local communities.

DOI: 10.4018/978-1-5225-5984-9.ch002

INTRODUCTION

Computer systems are too complex to be error-free. They are often dependent on off-the-shelf components, delegations to external service providers or non-documented legacy systems. These challenges make it difficult for organizations to both develop systems satisfying regulatory compliance and, the more so, diagnose failures and correct vulnerabilities. Meanwhile, hackers have become faster and faster in exploiting vulnerabilities and developing successful and widely spread attacks. Notably, there are no universal attacks; every attack targets specific vulnerabilities in specific software applications, hardware platforms or operation systems. Therefore, it is necessary to consider the threats and hazards that may violate the regulatory requirements of each computer system. Moreover, for security-critical and highly regulated ecosystems, it is crucial to ensure that the failure modes of the system-to-be fall always within fail-secure states.

Developing secure and compliant socio-technical systems is a complex and multi-dimensional issue that requires considering both the security functional aspects and the insider and outsider threat model for all the parties of the ecosystem. There are different proposals addressing individual steps of the development process, such as requirement engineering (e.g. secure Tropos, ACSP-RSL), security modeling (e.g. UMLsec, secureUML) or testing (e.g. Mouelhi et al. 2008, Bertolino et al. 2001). However, there are a few comprehensive end-to-end development frameworks that cover all the development process in a manner that addresses and enforces the security and compliance concerns at every step. In this chapter, the authors propose a comprehensive and complete development framework for highly regulated socio-technical systems. The authors address the regulatory compliance challenges using the Model Driven Engineering (MDE) methodology. The MDE development processes are automated using model transformations that are less error-prone than classical methodologies. In order to meet our own objectives of automated and documented validation activities, the authors enrich the MDE development process with compliance and security artifacts at every step.

As the quality of software systems depends on their architecture, the authors adopt this abstraction level for our framework. The early architecture model validation facilitates the detection and correction of design errors and reduces the costs of compliance management. In this research, the authors are interested in the privacy and security critical systems that require a reliable validation process. The authors propose a compliance management framework integrating 3 important views on the software ecosystem: 1) a risk-based requirements management process, 2) a modeling framework capable of integrating the security and privacy requirements, and 3) a simulation-based validation approach.

Electronic Intermediaries Managing and Orchestrating Organizational Networks Using E-Services

Marijn Janssen (2010). *Electronic Services: Concepts, Methodologies, Tools and Applications (pp. 1319-1333).*

www.irma-international.org/chapter/electronic-intermediaries-managing-orchestrating-organizational/44017