Chapter 12

Challenges in Agile Security Engineering: A Case Study

Kalle Rindell
University of Turku, Finland

Sami Hyrynsalmi
Tampere University of Technology, Finland

Ville Leppänen
University of Turku, Finland

ABSTRACT

This chapter describes a case of a large ICT service provider building a secure identity management system for a government customer. Security concerns are a guiding factor in the design of software-intensive products and services. They also affect the processes of their development. In regulated environments, development of products requires special security for the development processes, product release, maintenance and hosting, and also require security-oriented management and governance. Integrating the security engineering processes into an agile development model is argued to have the effect of mitigating the agile methods’ intended benefits. The project case was an effort of multi-team, multi-site, security engineering, and development work, executed using the Scrum framework and regulated by governmental security standards and guidelines. In this case research, the experiences in combining security engineering with agile development are reported, challenges discussed, and certain security enhancements to Scrum are proposed.

DOI: 10.4018/978-1-5225-6313-6.ch012
1. INTRODUCTION

Security regulations are an important driver in various aspects of software development and information systems and services. Even in the cases when formal security standards or guidelines are not strictly required the drive for security still guides the selection of design patterns and technological components, as well as the design and development work. Increasing diversity in development methods, technology, and the environments where the systems are used, have prompted organizations to follow various security standards, as well as created the need to establish new ones to guarantee adequate security assurance. In 2001, the government of Finland begun to issue a set of security regulations, called VAHTI instructions\(^1\). Compliance with the instructions is now mandatory for all government agencies and the regulation is also applied to any information system and data connected to a VAHTI-classified system.

While the importance and use of security regulations has increased, the use of lightweight software development processes and methods, i.e., *agile development*, has become the *de facto* standard in the industry (VersionOne, 2016). While there exists a series of suggested methods how to conduct security engineering activities in an agile project (see e.g. Baca & Carlsson, 2011; Beznosov & Kruchten, 2004; Fitzgerald, Stol & Sullivan, 2013; Ge, Paige, Polack & Brooke, 2007; Pietikäinen & Röning, 2014; Rindell, Hyrynsalmi & Leppänen, 2015:1), the empiric evidence is still largely anecdotal and the cases reported specific to an industry or a single company. The study reported in this paper is exploratory, and thus the research, by its nature, explorative. This study reports the experiences in agile development in a security-regulated environment. The research objective (RO) is:

**RO:** Identify advantages, best practices and the possible disadvantages of using agile software development methodologies in security engineering.

The results contribute to the on-going discussion by being a result of a deep analysis of combining security engineering with an agile method in an industry setting. Furthermore, the result of this study pave the way for further work deepening our understanding on the benefits and drawbacks of using agile software development methodologies in security sensitive development work.

In the case examined, a Scrum project was conducted with the objective of building an IDM system for information systems compliant with the security regulations. This included building a secure compliant server platform to host the IDM; the same platform would be utilized also to host the client’s other information systems. Also software development projects’ infrastructure would be hosted on the same platform, although with certain (unrelated) dispensations from the client’s security regulations.
Assisting Learners to Dynamically Adjust Learning Processes Through Software Agents


[www.igi-global.com/chapter/assisting-learners-dynamically-adjust-learning/29449?camid=4v1a](www.igi-global.com/chapter/assisting-learners-dynamically-adjust-learning/29449?camid=4v1a)