Evaluation of the Challenges of Developing Secure Software Using the Agile Approach

Hela Oueslati, Technical University Darmstadt, Darmstadt, Germany
Mohammad Masudur Rahman, Technical University Darmstadt, Darmstadt, Germany
Lotfi ben Othmane, Fraunhofer SIT, Darmstadt, Germany
Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Adila Firdaus Arbain, Universiti Teknologi Malaysia, Malaysia

ABSTRACT

A set of challenges of developing secure software using the agile development approach and methods are reported in the literature. This paper reports about a systematic literature review to identify these challenges and evaluate the causes of each of these challenges, with respect to the agile values, the agile principles, and the security assurance practices. The authors identified in this study 20 challenges, which are reported in 28 publications. They found that 14 of these challenges are valid and 6 are neither caused by agile values and principles, nor by the security assurance practices. The authors also found that 2 of the valid challenges are related to the software development life-cycle, 4 are related to incremental development, 4 are related to security assurance, 2 are related to awareness and collaboration, and 2 are related to security management. These results justify the need for research to make developing secure software smooth.

KEYWORDS

Agile Development Approach, Challenges, Security Assurance Practices, Secure Software

1. INTRODUCTION

Companies commonly use the agile development methods, such as Scrum (Schwaber and Beedle, 2001), and Extreme Programming (XP) (Martin, 2003) to develop their evolving software. These methods are associated with better developers’ productivity, product quality, and customers’ satisfaction than the waterfall methods (Dyba and Dingsoyr, 2008). They embrace requirement changes, prefer frequent deliveries, and their practices do not include security engineering activities. These characteristics, and others, make developing secure software using these methods challenging (McGraw, 2002). For instance, it is difficult to implement verification gates in the processes that implement these methods because the cost of these gates is very high, if they were to be repeated several times during the development of the project (Ben Othmane et al., 2014).

Many papers discuss the challenges of developing secure software using the agile development methods. For instance, Beznosov and Kruchten evaluated the mismatches between security assurance methods/techniques and agile practices (Beznosov and P. Kruchten, 2004), Ferdous et al. (Adila, et al., 2014) reviewed the challenges of developing secure software using the Feature Driven Development (FDD) method and assessed the feasibility of integrating security activities into FDD. Companies
and researchers proposed some solutions to these challenges. They focus, in general, on enhancing the agile development methods, such as Scrum, XP, FDD and the Dynamic Systems Development Method (DSDM) by introducing security activities and security expert roles in the development process (Sullivan, 2010), (Ben Othmane et al., 2014), (Imran, et al., 2014), (Imran and Izzaty, 2013), (Adila, et al., 2013) and (Sani, et al., 2013). The other challenges are, in general, not addressed.

This paper addresses the following questions:

- What are the challenges of developing secure software using the agile methods that have been proposed in the literature?
- And are these challenges valid?

There are currently no comprehensive systematic literature reviews that address these questions properly. A systematic literature review is a mean to identify, analyze, and interpret the available evidence (from publications) relevant to a research question by using a sound approach (Kitchenham and S. Charters, 2007), (Wohlin, 2012). The answers to both these questions should contribute to identifying the research challenges that the community shall address so organizations can use the agile methods to develop secure software.

The paper reports about a study that examines the validity of the challenges of developing secure software using the agile development methods. It summarizes the challenges reported in 28 publications and evaluates their validity with respect to a set of agile development criteria and developing secure software criteria. It is organized as follows. First we provide a short background about the agile approach and development of secure software in Section 2. Then, we describe in Section 3 the research method that we used to identify and validate the challenges. Next, we present in Section 4 the challenges that we identified from the publications that we selected and analyze the validity of the identified challenges in Section 5. We discuss the limitations and impacts of the study afterwards in Section 6 and conclude the paper in Section 7.

This paper extends our earlier paper presented at the The First International Workshop on Agile Secure Software Development (Oueslati et al. 2015).

2. BACKGROUND

This section provides an overview of the Agile Software Development (ASD) approach and of developing secure software.

2.1. Overview of the Agile Development Approach

Seventeen software developers met on February 2001 in the Wasatch Mountains of Utah, USA to try to find a common ground about their perception of software development (Beedle et al. 2015). They agreed on four values that the software methods they created share in a manifesto and named the approach they created agile software development. Then, they developed twelve supporting principles for the manifesto. Figure 1 shows the manifesto and Table 1 lists the principles.

We note that there is a disagreement among researchers on whether the concept “working software” includes only the software functionalities or it includes by default also the quality requirements, such as security requirements. In this evaluation, we use “working software,” without considering quality requirements, unless requested by the customers.

The values and principles of the agile approach are implemented by several methods including: Scrum, XP, Agile Modeling (AM) (Ambler, 2009), and FDD (Palmer and Felsing, 2002). Thus, the methods enable producing potentially shippable working software at regular intervals (Ambler, 2009) named iterations (a.k.a. cycles), provide customers high value features (customers-valued product functionalities) in short time, and accommodate several classes of software, such as Web applications.
Related Content

Enhancing ERP System with RFID: Logistic Process Integration and Exception Handling
*International Journal of Systems and Service-Oriented Engineering* (pp. 63-79).
[www.igi-global.com/article/enhancing-erp-system-rfid/58513?camid=4v1a](www.igi-global.com/article/enhancing-erp-system-rfid/58513?camid=4v1a)
Towards Next Generation Provenance Systems for E-Science
Fakhri Alam Khan, Sardar Hussain, Ivan Janciak and Peter Brezany (2013).
*Frameworks for Developing Efficient Information Systems: Models, Theory, and Practice* (pp. 51-75).
[www.igi-global.com/chapter/towards-next-generation-provenance-systems/76618?camid=4v1a](www.igi-global.com/chapter/towards-next-generation-provenance-systems/76618?camid=4v1a)

Understanding the State of Quality of Software
[www.igi-global.com/chapter/understanding-the-state-of-quality-of-software/189684?camid=4v1a](www.igi-global.com/chapter/understanding-the-state-of-quality-of-software/189684?camid=4v1a)

Execution Management for Mobile Service-Oriented Environments
[www.igi-global.com/chapter/execution-management-mobile-service-oriented/66793?camid=4v1a](www.igi-global.com/chapter/execution-management-mobile-service-oriented/66793?camid=4v1a)