International Journal of Secure Software Engineering
Volume 8 • Issue 4 • October-December 2017

Risk Centric Activities in Secure Software Development in Public Organisations

Inger Anne Tøndel, Department of Computer Science, Norwegian University of Science and Technology (NTNU), Trondheim, Norway & SINTEF Digital, Trondheim, Norway

Martin Gilje Jaatun, SINTEF Digital, Trondheim, Norway

Daniela Soares Cruzes, SINTEF Digital, Trondheim, Norway

Nils Brede Moe, SINTEF Digital, Trondheim, Norway

ABSTRACT

When working with software security in a risk-centric way, development projects become equipped to make decisions on how much security to include and what type of security pays off. This article presents the results of a study made among 23 public organisations, mapping their risk-centric activities and practices, and challenges for implementing them. The authors found that their software security practices were not based on an assessment of software security risks, but rather driven by compliance. Additionally, their practices could in many cases be characterised as arbitrary, late and error driven, with limited follow up on any security issues throughout their software development projects. Based on the results of the study, the authors identified the need for improvements in three main areas: responsibilities and stakeholder cooperation; risk perception and competence; and, practical ways of doing risk analysis in agile projects.

KEYWORDS

Agile Development, Empirical Study, Public Organisations, Risk Analysis, Risk Centric Activities, Risk Communication, Risk Management, Software Security

1. INTRODUCTION

Today, nearly all sectors of society depend on software systems to operate efficiently. As the dependency on software has grown, so have the threats towards these systems and the potential consequences of incidents. Though network security measures (such as firewalls and anti-virus software) can improve the security of the software systems, these only address the symptoms of the real problem: software that is crippled with vulnerabilities (McGraw, 2006).

Building security into the software, through adopting software security activities and measures in the development process, is a direct and effective way of dealing with cyber threats towards software systems. This, however, adds to the development time and cost, and this addition needs to be justified. Working towards 100% secure systems is not feasible, thus it is necessary to identify which part of the software is more critical regarding security and which activities will be most efficient and effective in

DOI: 10.4018/IJSSE.2017100101

securing the software product. Taking a risk centric approach to software security means to identify what are the major risks of the particular software that is developed, and use this knowledge of risk to guide decisions regarding software security. This is commonly recommended by current secure Software Development Lifecycles (SDLs), frameworks and maturity models (Chandra, 2008; Howard & Lipner, 2006; McGraw, 2006; McGraw et al., 2016).

In many ways, security can be considered to be in conflict with the current trend of "continuous development" (Fitzgerald & Stol, 2017), reducing efficiency by delaying delivery of new features (at least in the shorter term, though costs may be saved through having to provide fewer fixes later). Agile software development uses an iterative approach to software construction, aimed at reducing development time, and prioritising value, while improving software quality and inherently reducing risk (Cockburn and Highsmith 2001). It is clear that people issues are the most critical in agile projects and that these must be addressed if agile is to be implemented successfully (Cockburn and Highsmith 2001). Even though agile methods claim to be risk driven (Beck, 2000; Eclipse, 2016), some authors have observed that risk management has been neglected in project management of agile projects (Hijazi et al., 2012; Ibbs & Kwak, 2000; Junior et al., 2012; Raz et al., 2002). It may be more difficult to establish a working process for software security activities in agile development compared to waterfall-based development, where you could more easily have mandatory or recommended security activities for the different software development phases (ben Othmane et al., 2014; Jaatun et al., 2015; Microsoft, 2009). Oyetoyan et al. (2017) provide a brief overview of secure SDLs and conclude that traditional approaches to software security do not necessarily work well with agile development processes. Additionally, security is largely a systemic property, and with agile development it can be more of a challenge to have a complete view of the final system (ben Othmane et al., 2014). At the same time, agile development may come with some opportunities regarding security, e.g. to adapt to new security threats and to have ongoing interaction with customers about security.

Risk centric software security is very much related to the way developers address security in the projects. Still, other roles in an organisation (e.g. procurers, legal experts and information security experts) can have major influences on a development project's approach to security and can have important parts to play when it comes to identifying and understanding risk, and in making risk-based decisions in the projects. About ten years ago, van Wyk and McGraw (2005) pointed out the important role of security experts in influencing and supporting the work on security in development projects. There has however not been much research on the interaction between security experts and development projects in agile development since then.

In this article, we address the following research question: How can current software organisations work with software security in a risk centric way? As implied by this research question, we study software security within development practices that are in major adoption today, meaning our context is agile development. However, whereas agile methods are centred on the activities of teams, we take a more holistic approach, including the perspectives of organisations and projects. To answer the research question, we make a mapping of the risk centric activities, practices and challenges for implementing them among 23 public organisations in Norway. This sector has been chosen for study for three reasons. First, this sector has experienced a strong security push from the authorities, causing them to prioritise security management in the organisations. As a consequence, the importance of having someone being responsible for security has been emphasised, something that makes this sector an interesting case to study when it comes to organisational influences on risk centric software security. Second, this sector's access to legal experts makes them aware of legal requirements on security, something that increases the likelihood that software security is given some attention in software development. Third, we had easy access to this sector through cooperation with the Norwegian Agency for Public Management and eGovernment (Difi). The organisations studied have adopted agile practices for software development for some time. In the organisations, we have talked mainly with information security people, as these are in general given broad responsibility for all issues regarding IT security,