Chapter 98

Towards a Security Competence of Software Developers:
A Literature Review

Nana Assyne

https://orcid.org/0000-0003-0469-6642

University of Jyväskylä, Finland

ABSTRACT

Software growth has been explosive as people depend heavily on software on daily basis. Software development is a human-intensive effort, and developers' competence in software security is essential for secure software development. In addition, ubiquitous computing provides an added complexity to software security. Studies have treated security competences of software developers as a subsidiary of security engineers' competence instead of software engineers' competence, limiting the full knowledge of the security competences of software developers. This presents a crucial challenge for developers, educators, and users to maintain developers' competences in security. As a first step in pushing for the developers' security competence studies, this chapter utilises a literature review to identify the security competences of software developers. Thirteen security competences of software developers were identified and mapped to the common body of knowledge for information security professional framework. Lastly, the implications for, with, and without the competences are analysed and presented.

INTRODUCTION

The current explosive growth being observed in the software industry requires high-level corresponding software security. This is because "software vulnerabilities or flaws are often key entrance door for attackers" (Sametinger, 2013). They include buffer overflows, SQL injection, cross-site scripting, stack overflow, inconsistent error handling, and so on (McGraw, 2004). Previously, software security used to be an afterthought, but recently it is being addressed actively from the planning stage of software development. Additionally, in today's software development process, software testing includes security testing instead of only functional testing (Mano, Duhadway, & Striegel, 2006), thus making the security

competences of the developers more eminent in software development. Coupled with the fact that research work on software developers' competence is not lacking (Lenberg, Feldt, & Wallgren, 2015), the security competences of software developers should be well recorded in literature. But on the contrary, that is not the case. However, when they are recorded, they are recorded as a subsidiary of security engineers' competence instead of software engineers' competence, thus making it counterproductive to develop and maintain the security competences of software developers to the benefit of the possessors (developers), those who train the possessors of the competences (educators), and users of the competences (industry).

McGraw (2004) defines software security as "the idea of engineering software so that it continues to function correctly under malicious attack". And, Hazeyama & Shimizu (2012), goes further with the definition by stating that "software security deals with security during the whole software development process". On the other hand, software engineering competence is defined by the Institute of Electrical and Electronics Engineers (IEEE) as knowledge, skills, and attitudes of software developers to fulfil a given task in a software development project (IEEE, 2014). Thus, the author of this chapter defines security competence of software developers as those specific security competences required by a developer to deal with security during the whole software development process. An example is an SQL injection skills and security pattern skills.

As mentioned above, one cannot afford to leave software security as an afterthought; developers must strive to improve software security issues from the planning stage to the maintenance stage. The works of Cheng et al. (2008), Hilburn and Mead (2013), and Riehle and Nürnberg (2015) are studies that investigated methods to handle software security using the lifecycle of software development. It is also well established that vulnerabilities and flaws are the doors attackers exploit. Works such as Kaur and Kaur (2016), McGraw (2004), Park et al. (2010), and Wegerer and Tjoa (2016) confirm this assertion in literature. In addition, assailants of software systems are persons or entities, who are active and keep on improving their skills in attacking software systems to satisfy their desire (Cheng et al., 2008). However, the security competences of the developers of the software are not well established in literature.

Whilst introducing security engineering environment studies for software developers, Cheng et al. (2008) point out that there is urgent need to create an environment that integrates various tools and provides comprehensive facilities to the designers, developers, users, and maintainers of a software system (Cheng et al., 2008). The development and maintenance of such an environment requires knowledge of security competences of the developers to prepare and develop them to withstand the intrinsic difficulty of assailants of a software system (Cheng et al., 2008). This implies that security know-how of the developer is very crucial. Hazeyama and Shimizu (2012) and Hilburn and Mead (2013) reiterate the need for awareness to be channelled towards developers' skills regarding security. However, previous studies provide less concise and coordinated information on security competences of developers.

Summarily, these competences are scattered in several different studies. Thus, the following questions arise: *what are the security competences of software developers? How can they be improved?* As part of broader research on software developers' competences, we set our research question as *what are the security competences of a software developer that are available in literature?* The remainder of this work includes: Section 2 presents previous studies and background. Section 3 looks at the methodology used in this study. Section 4 looks at the results. Section 5 and 6 presents the discussion and conclusion.

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/towards-a-security-competence-of-software-developers/294558

Related Content

Malware Analysis and Its Mitigation Tools
D. R. Janardhana, A. P. Manu, K. Shivannaand K. C. Suhas (2023). *Malware Analysis and Intrusion Detection in Cyber-Physical Systems (pp. 263-284).*
www.irma-international.org/chapter/malware-analysis-and-its-mitigation-tools/331308

Opinions of the Software and Supply Chain Assurance Forum on Education, Training, and Certifications
Beatrix Boyens (2018). *International Journal of Systems and Software Security and Protection (pp. 1-13).*
www.irma-international.org/article/opinions-of-the-software-and-supply-chain-assurance-forum-on-education-training-and-certifications/221919

A Proficient Approach for Load Balancing in Cloud Computing-Join Minimum Loaded Queue: Join Minimum Loaded Queue
Minakshi Sharma, Rajneesh Kumarand Anurag Jain (2020). *International Journal of Information System Modeling and Design (pp. 12-36).*
www.irma-international.org/article/a-proficient-approach-for-load-balancing-in-cloud-computing-join-minimum-loaded-queue/250311

Method Using Command Abstraction Library for Iterative Testing Security of Web Applications
Seiji Munetohand Nobukazu Yoshioka (2018). *Application Development and Design: Concepts, Methodologies, Tools, and Applications (pp. 192-215).*
www.irma-international.org/chapter/method-using-command-abstraction-library-for-iterative-testing-security-of-web-applications/188208

Mobile Applications Programming Platforms and Development Tools
Damianos Gavalasand Daphne Economou (2012). *Handbook of Research on Mobile Software Engineering: Design, Implementation, and Emergent Applications (pp. 250-264).*
www.irma-international.org/chapter/mobile-applications-programming-platforms-development/66471