Chapter 4 An Evaluation of a Test– Driven Security Risk Analysis Approach Based on Two Industrial Case Studies

Gencer Erdogan SINTEF Digital, Norway

Phu H. Nguyen SINTEF Digital, Norway

Fredrik Seehusen SINTEF Digital, Norway Ketil Stølen SINTEF Digital, Norway

> Jon Hofstad PWC, Norway

Jan Øyvind Aagedal Equatex, Norway

ABSTRACT

Risk-driven testing and test-driven risk assessment are two strongly related approaches, though the latter is less explored. This chapter presents an evaluation of a test-driven security risk assessment approach to assess how useful testing is for validating and correcting security risk models. Based on the guidelines for case study research, two industrial case studies were analyzed: a multilingual financial web application and a mobile financial application. In both case studies, the testing yielded new information, which was not found in the risk assessment phase. In the first case study, new vulnerabilities were found that resulted in an update of the likelihood values of threat scenarios and risks in the risk model. New vulnerabilities were also identified and added to the risk model in the second case study. These updates led to more accurate risk models, which indicate that the testing was indeed useful for validating and correcting the risk models.

DOI: 10.4018/978-1-5225-6313-6.ch004

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Security risk analysis is carried out in order to identify and assess security specific risks. Traditional risk analyses often rely on expert judgment for the identification of risks, their causes, as well as risk estimation in terms of likelihood and consequence. The outcome of these kinds of risk analyses is therefore dependent on the background, experience, and knowledge of the participants, which in turn reflects uncertainty regarding the validity of the results.

In order to mitigate this uncertainty, security risk analysis can be complemented by other ways of gathering information of relevance. One such approach is to combine security risk analysis with security testing, in which the testing is used to validate and correct the risk analysis results. This is referred to as test-driven security risk analysis.

The authors have developed an approach to test-driven security risk analysis, and as depicted in Figure 1, the approach is divided into three phases. Phase 1 expects a description of the target of evaluation. Then, based on this description, the security risk assessment is planned and carried out. The output of Phase 1 is security risk models, which is used as input to Phase 2. In Phase 2, security tests are identified based on the risk models and executed. The output of Phase 2 is security test results, which is used as input to the third and final phase. In the third phase, the risk models are validated and corrected with respect to the security test results.

Although strongly related, it is important to note that test-driven risk analysis is different from the more common combination of risk analysis and testing, which is referred to as risk-driven (or risk-based) testing. The purpose of risk-driven testing is to makes use of risk assessment within the testing process to support risk-driven test planning, risk-driven test design and implementation, and risk-driven test reporting. Großmann and Seehusen (2015) provide a detailed explanation of these two approaches by combining the well-known and widely used standards ISO 31000 (ISO, 2009) and ISO/IEC/IEEE 29119 (ISO, 2013a), with a focus on security.

Figure 1. Overview of the test-driven security risk analysis approach Source: Authors' work



33 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.igiglobal.com/chapter/an-evaluation-of-a-test-driven-securityrisk-analysis-approach-based-on-two-industrial-casestudies/221713

Related Content

Enhancing the Browser-Side Context-Aware Sanitization of Suspicious HTML5 Code for Halting the DOM-Based XSS Vulnerabilities in Cloud

B. B. Gupta, Shashank Guptaand Pooja Chaudhary (2018). *Application Development and Design: Concepts, Methodologies, Tools, and Applications (pp. 216-247).* www.irma-international.org/chapter/enhancing-the-browser-side-context-aware-sanitization-of-suspicious-html5-code-for-halting-the-dom-based-xss-vulnerabilities-in-cloud/188209

Designing an Efficient and Scalable Relational Database Schema: Principles of Design for Data Modeling

Rajesh Kanna Rajendranand T. Mohana Priya (2023). *The Software Principles of Design for Data Modeling (pp. 168-176).*

www.irma-international.org/chapter/designing-an-efficient-and-scalable-relational-database-schema/330495

Approximate Algorithm for Solving the General Problem of Scheduling Theory With High Accuracy

Vardan Mkrttchianand Safwan Al Salaimeh (2019). *International Journal of Software Innovation (pp. 71-85).*

www.irma-international.org/article/approximate-algorithm-for-solving-the-general-problem-of-scheduling-theory-with-high-accuracy/236207

Designing Mobile Aspect-Oriented Software Architectures with Ambients

Nour Aliand Isidro Ramos (2012). *Handbook of Research on Mobile Software Engineering: Design, Implementation, and Emergent Applications (pp. 526-543).* www.irma-international.org/chapter/designing-mobile-aspect-oriented-software/66485

A Case Study of Dynamic Analysis to Locate Unexpected Side Effects Inside of Frameworks

Izuru Kume, Masahide Nakamura, Naoya Nittaand Etsuya Shibayama (2015). International Journal of Software Innovation (pp. 26-40).

www.irma-international.org/article/a-case-study-of-dynamic-analysis-to-locate-unexpected-sideeffects-inside-of-frameworks/126614