

Chapter 4

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

Gencer Erdogan

SINTEF Digital, Norway

Ketil Stølen

SINTEF Digital, Norway

Phu H. Nguyen

SINTEF Digital, Norway

Jon Hofstad

PWC, Norway

Fredrik Seehusen

SINTEF Digital, 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

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.

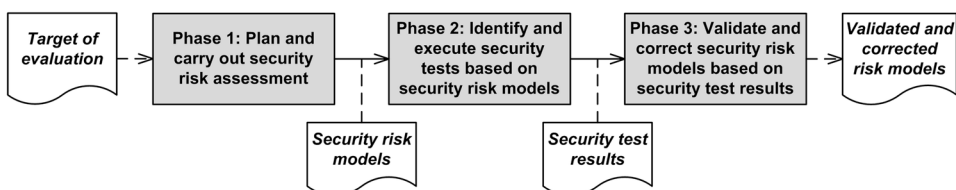
In order to mitigate this uncertainty, security risk analysis can be complemented by other ways of gathering information of relevance. One such approach is to combine security risk analysis with security testing, in which the testing is used to validate and correct the risk analysis results. This is 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.igi-global.com/chapter/an-evaluation-of-a-test-driven-security-risk-analysis-approach-based-on-two-industrial-case-studies/221713

Related Content

Security Testing Framework for Web Applications

Layla Mohammed Alrawais, Mamdouh Aleneziand Mohammad Akour (2022). *Research Anthology on Agile Software, Software Development, and Testing* (pp. 453-479).

www.irma-international.org/chapter/security-testing-framework-for-web-applications/294478

A Pliant-Based Software Tool for Courseware Development

Marcus Vinicius Santos Kucharski, Isaac Woungangand Moses Nyongwa (2009). *Software Applications: Concepts, Methodologies, Tools, and Applications* (pp. 1404-1424).

www.irma-international.org/chapter/pliant-based-software-tool-courseware/29453

Cyber Physical Internet

(2015). *Challenges, Opportunities, and Dimensions of Cyber-Physical Systems* (pp. 76-97).

www.irma-international.org/chapter/cyber-physical-internet/121251

Traffic Data Collection and Visualization Tool for Knowledge Discovery Using Google Maps

Iftekhar Hossainand Naushin Nower (2022). *International Journal of Software Innovation* (pp. 1-12).

www.irma-international.org/article/traffic-data-collection-and-visualization-tool-for-knowledge-discovery-using-google-maps/293270

A Conceptual Model for Describing the Integration of Decision Aspect into Big Data

Fatma Chiheb, Fatima Boumahdiand Hafida Bouarfa (2019). *International Journal of Information System Modeling and Design* (pp. 1-23).

www.irma-international.org/article/a-conceptual-model-for-describing-the-integration-of-decision-aspect-into-big-data/243437