

Chapter 53

Assessing the Usefulness of Testing for Validating and Correcting Security Risk Models Based on Two Industrial Case Studies

Gencer Erdogan

*SINTEF ICT, Norway & University of Oslo,
Norway*

Ketil Stølen

*SINTEF ICT, Norway & University of Oslo,
Norway*

Fredrik Seehusen

SINTEF ICT, Norway

Jon Hofstad

EVRY, Norway

Jan Øyvind Aagedal

Accurate Equity, Norway

ABSTRACT

The authors present the results of an evaluation in which the objective was to assess how useful testing is for validating and correcting security risk models. The evaluation is based on two industrial case studies. In the first case study the authors analyzed a multilingual financial Web application, while in the second case study they analyzed a mobile financial application. In both case studies, the testing yielded new information which was not found in the risk assessment phase. In particular, in the first case study, new vulnerabilities were found which 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: 10.4018/978-1-4666-9562-7.ch053

1. 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. We refer to this as test-driven security risk analysis.

We have developed an approach to test-driven security risk analysis, and as depicted in Figure 1, our 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.

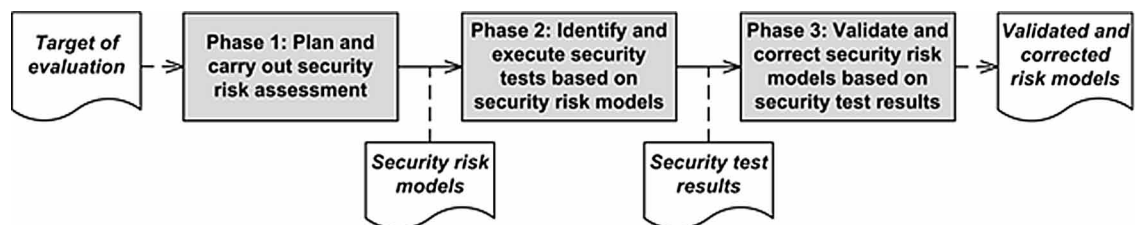
In this paper, we present an evaluation of our test-driven security risk analysis approach based

on two industrial case studies. The objective of the case studies was to assess how useful testing is for validating and correcting security risk models. The basis of our evaluation is to compare the risk models produced before and after testing. That is, we compare the difference in risk models produced in Phase 1 with the updated risk models produced in Phase 3.

The first case study was carried out between March 2011 and July 2011, while the second case study was carried out between June 2012 and January 2013. In the first case study we analyzed a multilingual financial Web application, and in the second case study we analyzed a mobile financial application. The systems analyzed in both case studies serve as the backbone for the system owner's business goals and are used by a large number of users every day. The system owners, which are also the customers that commissioned the case studies, required full confidentiality. The results that are presented in this paper are therefore limited to the experiences from applying the test-driven security risk analysis approach.

The reminder of the paper is structured as follows. Section 2 describes our test-driven security risk analysis approach. Section 3 describes our research method. Section 4 gives an overview of the two case studies. Section 5 describes the results obtained in the case studies which are the basis of our evaluation. Section 6 provides a discussion of the results with respect to our research questions and overall hypothesis. Section 7 discusses related work. Finally, Section 8 highlights our key findings and concludes the paper.

Figure 1. Overview of the test-driven security risk analysis approach



20 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/assessing-the-usefulness-of-testing-for-validating-and-correcting-security-risk-models-based-on-two-industrial-case-studies/142664

Related Content

Mandatory and Voluntary Adoption of RFID

Mohammad Alamgir Hossain and Mohammed Quaddus (2014). *Encyclopedia of Business Analytics and Optimization* (pp. 1457-1475).

www.irma-international.org/chapter/mandatory-and-voluntary-adoption-of-rfid/107340

Applications of Data Mining in Software Development Life Cycle: A Literature Survey and Classification

Naveen Dahiya, Vishal Bhatnagar, Manjeet Singhand Neeti Sangwan (2016). *Business Intelligence: Concepts, Methodologies, Tools, and Applications* (pp. 558-570).

www.irma-international.org/chapter/applications-of-data-mining-in-software-development-life-cycle/142638

A Business Intelligence Project-Oriented Course: A Breast Cancer Research Case

Dima Alberg (2019). *International Journal of Business Intelligence Research* (pp. 29-35).

www.irma-international.org/article/a-business-intelligence-project-oriented-course/232238

Computational Intelligence Applications in Business: A Cross-Section of the Field

Kevin E. Voges and Nigel K.L. Pope (2006). *Business Applications and Computational Intelligence* (pp. 1-18).

www.irma-international.org/chapter/computational-intelligence-applications-business/6016

A Systematic Approach for Business Data Analytics with a Real Case Study

Kaibo Liu and Jianjun Shi (2015). *International Journal of Business Analytics* (pp. 23-44).

www.irma-international.org/article/a-systematic-approach-for-business-data-analytics-with-a-real-case-study/132800