Abstract: Security testing and security risk analysis are key issues and central to strengthening the ability of companies to face the new security challenges posed by the future internet. We present a conceptual framework clarifying the notions of security testing, security risk analysis, and related concepts, as well as defining the relations among them. The conceptual framework is built upon established concepts from state-of-the-art standards. We focus on model-based approaches for security testing and security risk analysis and distinguish between model-based security testing (MST) and model-based security risk analysis (MSR). In particular, we present the two possible combinations of MST and MSR, which are risk-driven model-based security testing (RMST) and test-driven model-based security risk analysis (TMSR). The conceptual framework offers a basis for future research by providing a common understanding of the central notions within security testing and security risk analysis.

Key words: Security, Testing, Risk Analysis, Model, Risk-driven model-based security testing (RMST), Test-driven model-based security risk analysis (TMSR).

1. INTRODUCTION

As internet services, computerized systems and information infrastructure play a critical role in society, the need for security has become increasingly evident. While the future internet creates new business opportunities (e.g. online banking services), it also creates new security threats and vulnerabilities. The field of information security has grown and evolved significantly in recent years, including security testing and security risk analysis as important specialization areas.

Up to now, not much research has been conducted within risk based testing and test based risk analysis from a model driven perspective. The gap between the high-level abstraction of risk analysis and the low-level abstraction of security testing is a key challenge where there exists no clear methodology for the time being.

Our main objective is to develop guidelines and a supporting framework to help businesses find a balanced approach within the three-dimensional space of invested effort, security testing and risk analysis by transferring state-of-art security assessment techniques.

We aim to achieve a more efficient and effective approach for security testing and security risk analysis by facilitating their combination in a model driven setting, leading to RMST and TMSR.

In section 2, we introduce the concepts of security, security testing and security risk analysis, and thereafter the model based approach with definitions for MST and MSR are presented. In section 3, we describe the two new approaches of RMST and TMSR in detail. Section 4 presents the related work. Finally, in section 5, a brief conclusion is given.
2. BASIC CONCEPTS

We build the conceptual framework upon established concepts from state-of-the-art standards. However, we also make adjustments of established notions where seen necessary or appropriate, in order to achieve a consistent framework suitable for our particular goal.

We refer to security as the preservation of confidentiality, integrity and availability of information (adapted from [5]). Security testing is defined as the process of testing specialized towards security, where testing is the process of exercising the system to verify that it satisfies specified requirements and to detect errors (adapted from [6] [13]). Security risk analysis is defined as the process of risk analysis specialized towards security, where risk analysis is a collective term defining the process consisting of the following steps: establishing the context, risk identification, risk estimation, risk evaluation and risk treatment (adapted from [7] [8]).

We define MST as security testing that involves the construction and analysis of a system model, a test model and a test environment model to derive test cases. MSR is defined as security risk analysis in which every step of the process includes the construction and analysis of models.

3. THE COMBINATIONS

For combining MST and MSR, there are two main possibilities depending on which approach is taken as the starting point, i.e., whether the main purpose of the process is for security testing or security risk analysis.

As shown in the Figure 1, RMST is defined as model-based security testing that uses risk analysis within the security testing process. It is the combination of security testing and security risk analysis. The security risk analysis in step 2 and step 5 serve different purposes. The first usage i.e., security risk analysis before the test design & implementation (step 2) supports the security testing process by identifying the most important parts of the system to test, while the second usage i.e., security risk analysis after the test environment set-up & maintenance (step 5) supports the security testing process by identifying the most important security test cases that need to be prioritized in test execution.
The following describes each step of the RMST process:

Step 1: Test Planning. A test plan is created describing how to perform the RMST process. The test plan is established in terms of “what to test”, “how to test”, “what resources to use” and “when to test”. A system model is built based on the test plan.

Step 2: Risk Analysis. The security risk analysis process in this step is carried out in order to identify security risks of the system. The system model is used to develop a risk model based on identified security risks, and the important parts of the system to test are recognized.

Step 3: Test Design & Implementation. Test models, test cases and test procedures are developed according to the prioritized list of the most important parts of the system identified earlier.

Step 4: Test Environment Set-up & Maintenance. The required test environment is established and maintained.

Step 5: Risk Analysis. The security risk analysis process in this step is carried out in order to identify the most important security test cases that need to be prioritized in test execution.

Step 6: Test Execution. The test cases and the test procedures are executed in the prepared test environment based on the priority. Security test results are recorded.

Step 7: Test Incidents Reporting. As a result of test execution, the identified security issues that require further action are reported to the relevant stakeholders.

![Test-driven Model-based Security Risk Analysis (TMSR)](image)

As shown in Figure 2, TMSR is defined as model-based security risk analysis that uses testing within the security risk analysis process. It is the combination of security risk analysis and security testing in which security testing is carried out both before and after the security risk assessment process (the overall process of risk identification, risk estimation and risk evaluation) to serve different purposes. The first usage i.e., testing before the security risk assessment process (Step 2) supports the security risk analysis process by identifying potential risks, while the second usage i.e., testing after the security risk assessment process (Step 6) validates security risk models built earlier based on security testing results.

The following describes each step of the TMSR process:

Step 1: Establish Objective and Context. A basic idea about objectives, scale of analysis and corresponding context is established as an initial preparation for security risk analysis.
Step 2: Testing Process. Testing is used in this step to support the security risk analysis process by identifying potential risks. Test models are built to generate test cases. The test cases are executed, and the test results are used to indicate potential risks.

Step 3: Risk Identification. Risks are found, recognized and described in terms of the unwanted incidents, risk source and potential consequences to form an initial risk model (e.g. a risk model without likelihood and consequence values).

Step 4: Risk Estimation. The nature of identified risk is comprehended and the level of risk is determined by defining the likelihoods and consequences. A complete risk model is built.

Step 5: Risk Evaluation. The results of risk estimation is compared with risk criteria to determine whether the risk and its magnitude is acceptable or tolerable.

Step 6: Testing Process. Testing is used in this step to support the security risk analysis process by validating the risk models based on security testing results.

Step 7: Risk Validation and Treatment. The identified risk models are validated and risk modification is performed, involving e.g. risk mitigation, risk elimination or risk prevention.

4. RELATED WORK


Wong et al. [14] propose a static and a dynamic risk model using metrics collected based on the static structure of the source code or the dynamic test coverage of the code. Sauve [12] presents initial ideas concerning the application of risk to IT service management. And the focus is on the process of testing changes to a service where risk considerations are paramount with particular reference to the numerical representation of risk metrics and of risk appetite.

5. CONCLUSION

As a first step towards developing guidelines and a supporting framework to help businesses find a balanced approach within the three-dimensional space of invested effort, security testing and risk analysis, we have proposed a conceptual framework distinguishing between risk-driven model-based security testing and test-driven model-based security risk analysis. The results from an initial industrial case study in the use of TMSR is presented in [3]. We refer to the full report on the conceptual framework for more detailed argumentation and explanations [9].

ACKNOWLEDGEMENT

This work has been conducted within the DIAMONDS project, funded by the Research Council of Norway. The author acknowledges feedbacks from Ketil Stølen, Raghnild Kobro Runde, Gencer Erdogan and Fredrik Seehusen.
REFERENCES

[9] Li, Yan; Erdogan, Gencer; Runde, Ragnhild Kobro; Seehusen, Fredrik; Stølen, Ketil. The Conceptual Framework for the DIAMONDS Project; Technical report A22798. SINTEF ICT, 2012