

Combining Security Risk Assessment and Security Testing Based on Standards

Jürgen Großmann¹(✉) and Fredrik Seehusen²

¹ Fraunhofer FOKUS, Berlin, Germany

juergen.grossmann@fokus.fraunhofer.de

² SINTEF ICT, Oslo, Norway

fredrik.seehusen@sintef.no

Abstract. Managing cyber security has become increasingly important due to the growing interconnectivity of computerized systems and their use in society. A comprehensive assessment of cyber security can be challenging as it spans across different domains of knowledge and expertise. For instance, identifying cyber security vulnerabilities requires detailed technical expertise and knowledge, while the assessment of organizational impact and legal implications of cyber security incidents may require expertise and knowledge related to risk and compliance. Standards like ISO 31000 and ISO/IEC/IEEE 29119 detail the relevant aspects of risk management and testing and thus provide guidance in these areas. However, both standards are not exclusively dedicated to the subject of security and do not cover the explicit integration between security risk assessment and security testing. We think however, that they provide a good basis for that. In this paper we show how ISO 31000 and ISO/IEC/IEEE 29119 can be integrated to provide a comprehensive approach to cyber security that covers both security risk assessment and security testing.

1 Introduction

Security risk assessment and security testing both contribute to an overall assessment of the security of a system on different levels. Security risk assessment is the iterative process that analyses the potential threats to a system in order to calculate the likelihood of their occurrence and their consequence. It comprises the identification of assets, threats and vulnerabilities as well as the identification, specification and realisation of risk treatments. Security testing is dedicated to dynamically check the security properties of software. We generally distinguish functional security testing, robustness testing, performance testing and penetration testing. While security testing addresses technical security issues in particular, security risk assessment typically addresses higher level, non-technical issues as well. However, we believe that the systematic integration of activities that cover aspect from security testing, and security risk assessment provide added value to the overall goal in assessing the security of large scale, networked system. While the high level perspective of the security risk assessment can provide guidance (i.e. by helping focus on the relevant aspects) to the activities carried out during security testing, testing can provide factual feedback on the actual quality characteristics of a system and thus allow for improving the overall

assessment of the system. Integrating and interweaving the activities from both sides allows for a more precise, focused and dynamic assessment of systems, processes and other targets.

We refer to the use of security testing to improve the security risk assessment process as test-based security risk assessment, and the use of security risk assessment to improve the security testing as risk-based security testing. In this paper, we will address both kinds of integration.

Security risk assessment and testing are both covered by existing standards such as ISO 31000 [8] and ISO/IEC/IEEE 29119 (referred to as ISO 29119 in the following) [9]. However, both standards are not explicitly dedicated to the subject of security and currently no standard exists that sufficiently emphasizes the systematic integration of security risk assessment and security testing. ISO 29119 is not directly dedicated to security testing and, even if ISO 29119 already describes interaction between testing and risk assessment, both standards do not cover a concise integration between security risk assessment and security testing. While the industry demands integrative approaches that cope with security as a whole, both areas are normally treated as distinct areas that are isolated from one another. This paper describes the, from our experience, relevant points of integration between security risk assessment and security testing. The points of integration cover activities driven from security risk assessment as well as from security testing. They are documented along standardized process flows from ISO 31000 and ISO 29119 so that they are easy to integrate when these standards are in use.

This paper is structured as follows: Sect. 2 provides an overview on approaches to risk assessment and security testing, Sect. 3 describes our general idea of integration and the Sects. 4 and 5 document the actual points of integration by defining the notion of test-based risk assessment and risk-based security testing. Section 6 concludes the paper.

2 State of the Art

Security risk assessment and security testing are traditionally addressed as distinct domains with their own methods and processes. Arguably, the most well known processes within the two domains are ISO 31000 for risk assessment and ISO 29119 for testing. However, currently no standard exists that sufficiently emphasizes the systematic integration of security risk assessment and security testing. Neither are we aware of any work that attempts to integrate the ISO 31000 and the ISO processes.

Many specific approaches that combine testing and risk assessment have been proposed. See [1, 3] for a comprehensive survey of these approaches. As discussed by Erdogan et al. [3], most of these approaches that combine risk assessment and testing focus on specific aspects of the risk or testing process such as test case generation or risk estimation. This is in contrast to our approach that addresses the whole process.

The approaches that we are aware of that addresses the combination of risk assessment and testing at a more general level as we do, are [2, 4, 5, 6, 7, 12, 13]. However, our work differs from these approaches in that none of the approaches describe the relationship to well-established standards within the risk assessment and the testing domains.

There are general technical recommendations on security testing techniques [7, 10, 11] that propose the use of risk analysis results to guide security testing. In a similar manner ISO 29119 addresses the use of risk assessment results to improve testing. However, these recommendations are very general in nature and describe in this sense no real method for risk-based testing.

3 Integrating Security Risk Assessment and Security Testing

The overall process of a combined security assessment described in this paper has been developed in the RASEN research project¹ and evaluated within 3 case studies. The process is derived from ISO-31000 and extended to highlight the integration with security testing. It is defined independent from any application domain and independent from the level, target or depth of the security assessment. It could be applied to any kind of technical security assessment and testing processes. The overall process covers two different workstreams that each consist of a combination of typical security risk assessment activities that are defined in ISO 31000 and typical security testing activities that follow testing standards like ISO 29119.

1. A test-based security risk assessment workstream starts like a typical risk assessment workstream and use testing results to guide and improve the risk assessment. Security testing is used to provide feedback on actually existing vulnerabilities that have not been covered during risk assessment or allows risk values to be adjusted on basis of tangible measurements like test results. Security testing should provide a concise feedback whether the properties of the target under assessment have been really met by the risk assessment.
2. The risk-based security testing workstream starts like a typical testing workstream and uses risk assessment results to guide and focus the testing. Such a workstream starts with identifying the areas of risk within the target's business processes and building and prioritizing the testing program around these risks. In this setting risks help focusing the testing resources on the areas that are most likely to cause concern or supporting the selection of test techniques dedicated to already identified threat scenarios.

According to Fig. 1, both workstreams start with a preparatory phase called *Establishing the Context* that includes preparatory activities like *Understanding the Business and Regulatory Environment* as well as the *Requirements & Process Identification*. During the first phase the high-level security objectives are identified and documented and the overall process planning is done. Moreover, the figure shows additional support activities like *Communication & Consult* and *Monitoring and Review* that are meant to set up the management perspective, thus to continuously control, react, and improve all relevant information and results of the process. From a process point of view, these activities are meant to provide the contextual and management related framework. The individual activities covered in these phases might differ in detail dependent on whether

¹ www.rasen-project.eu.

the risk assessment or testing activities are the guiding activities. The main phase, namely the *Security Assessment* phase covers the integration between the risk assessment workstream and a security testing workstream. This phase is detailed more closely in the following two sections.

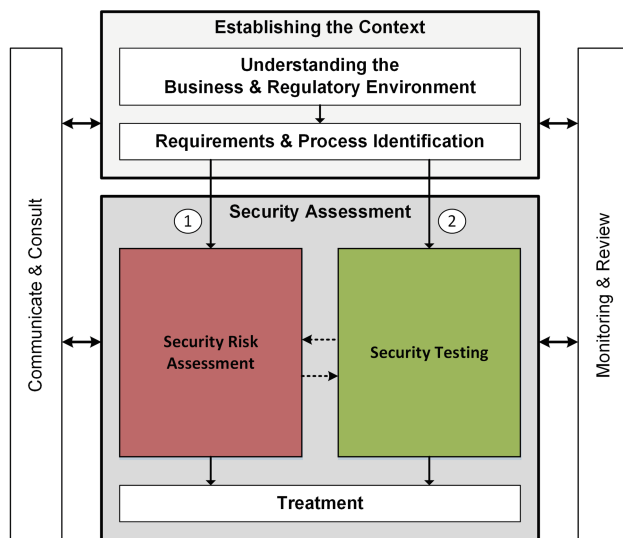


Fig. 1. The overall combined security assessment process

4 Test-Based Security Risk Assessment

Risk assessment is the overall process of risk identification, estimation, and evaluation. The typical outcome of a risk assessment is a set of treatments for unacceptable risks (if any) and a risk matrix that shows the risk values of identified risks. The information and knowledge on which a risk assessment is based has a big impact on the outcome of the risk assessment. The main reason for integrating testing into the risk assessment process is to use testing as a means of obtaining a better information basis on which to perform the risk assessment. Testing, as opposed to other forms of information gathering such as expert judgments and historical data, is particularly suited for obtaining low-level technical information which often is necessary for an accurate understanding of the target of evaluation.

From a testing perspective, the risk assessment can be used for representing test results in the context of risk assessment artefacts. This kind of high-level representation of test results can for instance be used to support management issues and control the overall test process during the test management.

In a test-based risk assessment, test results are used as explicit input to various activities of the risk assessment. Figure 2 shows how the overall security assessment process (shown in Fig. 1) is refined into a process for test-based risk assessment. Here the risk assessment activity has been decomposed into the three activities *Risk*

Identification, Risk Estimation, and Risk Evaluation. These three activities, together with the *Establishing the Context* and *Treatment* activities form the core of the ISO 31000 risk management process. As indicated in Fig. 2, there are in particular two places where testing can enhance the risk assessment process. The first, denoted 1 in the figure, is during risk identification, and the second is during risk estimation (denoted 2 in the figure). In the following, we describe in more detail how test results may be used as input to these activities.

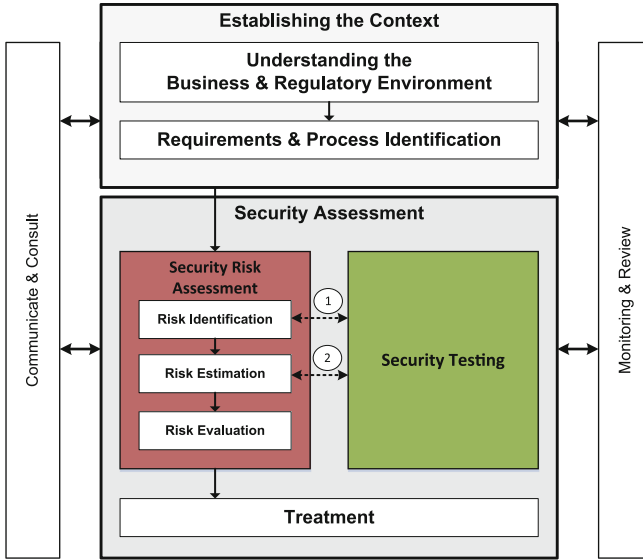


Fig. 2. Generic workstream for test-based risk assessment

4.1 Test-Based Risk Identification

Risk identification is the process of finding, recognizing and describing risks. This involves identifying sources of risk (e.g. threats and vulnerabilities), areas of impacts (e.g. the assets), events (including changes in circumstances), their causes and their potential consequences. The *Establishing the Context* activity is assumed to be performed before the risk identification. A typical starting point for the risk identification step is: a description of the target of evaluation, a definition of likelihood and consequence scales, risk evaluation criteria (often expressed in the form of risk matrices), and asset definitions.

The typical artefacts that are identified during the risk identification activity are threats, threat scenarios, vulnerabilities, and unwanted incidents that may constitute risks. In Fig. 3, we show how the risk identification can be structured w.r.t. to the identification of these artefacts. As indicated in the figure, there are in particular two activities that can be integrated with testing:

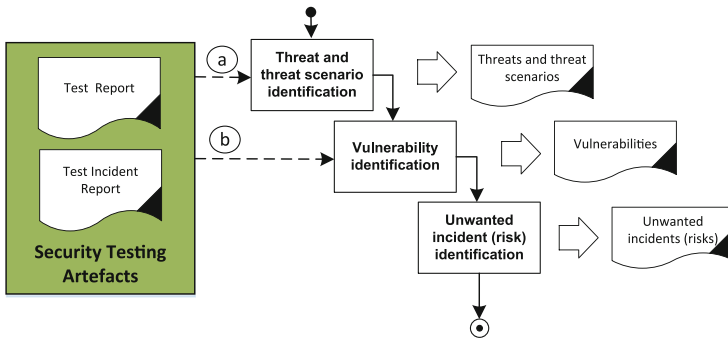


Fig. 3. Test-based risk identification

(a) Test-based threat and threat scenario identification

(b) Test-based vulnerability identification

In the following, we describe these activities in more detail.

4.1.1 Risk Identification: Test-Based Threat and Threat Scenario Identification (a)

The purpose of this activity is to identify threats and threat scenarios. A threat is a potential cause of an unwanted incident. A threat may be human or non-human, malicious or non-malicious. A hacker is an example of a typical malicious human threat. A threat scenario is a series of events that is initiated by a threat and that may lead to an unwanted incident. A cyber security attack such as SQL injection is a typical example of a threat scenario.

Testing can be used in order to obtain information that can support the identification of threats and threat scenarios. Particularly relevant in this setting are testing and analysis techniques that yield information about the interfaces/entry points, the attack-surface, and potential attacks against the target of evaluation. The tools that can be used for this purpose are typical security testing tools like network discovery tools, web-crawlers, and fuzz testing tools as well as analysis tools like static code analysis tools.

4.1.2 Risk Identification: Test-Based Vulnerability Identification (b)

A vulnerability is a weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset. Test-based vulnerability identification refers to the use of testing to obtain information that supports the vulnerability identification activity. Testing techniques that yield information about the presence of actual vulnerabilities in the target of evaluation or *potential* vulnerabilities that *may* be present in the target of evaluation are relevant in this activity. The kinds of testing tools that can be used for this purpose are penetrating testing tools, model-based security testing tools, static and dynamic code analysis tools, and vulnerability scanners.

4.2 Test-Based Risk Estimation

Risk estimation is the process of estimating likelihood and consequences values for risks and their causes (i.e. threat scenarios). Accurate risk estimation is essential for a successful outcome of a risk assessment. However, risk estimation is one of the hardest activities of a risk assessment since the information basis for the estimation is often imprecise and insufficient, and we are often forced to rely on expert judgment. This might result in a high degree of uncertainty related to the correctness of the estimates.

As shown in Fig. 4, the risk estimation activity can be decomposed into the three sub-activities: Likelihood Estimation, Consequence Estimation, and Estimate Validation. The last sub-activity refers to checking and/or gaining confidence in the correctness of the risk estimates. As indicated in Fig. 4, there are in particular two activities that can be integrated with testing:

- (a) Test-based likelihood estimation
- (b) Test-based estimate validation

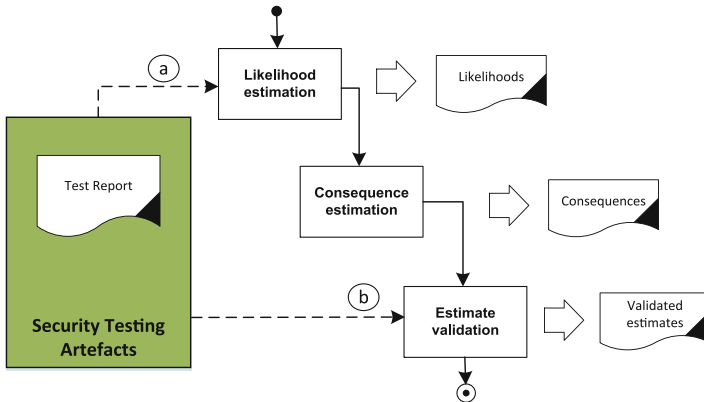


Fig. 4. Test-based risk estimation.

4.2.1 Risk Estimation: Test-Based Likelihood Estimation (a)

Likelihood estimation is the activity of estimating likelihoods for risks and their causes. In a security setting, this involves estimating the likelihood that: security attacks will be initiated; attacks will be successful if initiated; successful attacks will lead to identified risks. Likelihoods should be document using the likelihood scales defined in the *Establishing the Context* step of the risk assessment.

Testing is particularly relevant for obtaining information that can support the estimation of the likelihood that an attack will be successful if initiated. This is because security testing is most often used for identifying vulnerabilities, and the presence of these has a direct impact on this likelihood. Thus the testing techniques used for test-based likelihood estimation are similar to those used for test-based vulnerability identification (as described in Sect. 4.1.2). The main difference between these activities is that in the former, information about the vulnerabilities is only used as a means of supporting likelihood estimation.

4.2.2 Risk Estimation: Test-Based Estimate Validation (b)

Validation is the activity of checking or gaining confidence in the correctness of the estimated risk values. In a test-based setting, we recommend that uncertainty related to the correctness of an estimate be explicitly expressed. For instance, instead of using single likelihood values such as frequency or probability, we can use intervals of likelihoods to express the belief that the correct likelihood lies somewhere within the interval without knowing precisely where. Uncertainty can then be measured in terms of the breadth of the interval - the broader the intervals, the more uncertainty there is.

As for the likelihood estimation activity, testing is particularly useful for obtaining information that supports the estimation of likelihood of successful attacks. The main difference between test-based likelihood estimation and test-based likelihood validation, is that in the former activity, testing is used to obtain the likelihood in the first place, whereas in the second activity, the purpose is to validate or gain confidence in the correctness of a likelihood value which has already been estimated. If uncertainty is expressed explicitly, the test results may be used to lower this uncertainty value. For instance if likelihood intervals are used, the test results may result in a narrowing of the intervals. Recalculating the likelihood values of risks as a result of the updated uncertainty is a good way of showing how the test results have impacted the risks.

5 Risk-Based Security Testing

The risk-based security testing workstream is structured like a typical security testing process. It starts with a planning phase, a test design & implementation phase and ends with test execution, analysis and summary. The result of the risk assessment, i.e. the identified vulnerabilities, threat scenarios and unwanted incidents, are used to guide the test planning, test identification and may complement requirements engineering results with systematic information concerning the threats and vulnerabilities of a system.

Additional factors like probabilities and consequences can be additionally used to weight threat scenarios and thus help identifying which threat scenarios are more relevant and thus identifying the ones that need to be treated and tested more carefully. From a process point of view, the interaction between risk assessment and testing could be best described following the phases of a typical testing process. Figure 5 illustrates the three phases of a testing process that are affected and supported by risk-based security testing.

1. Risk-based security test planning deals with the integration of security risk assessment in the test planning process.
2. Risk-based security test design, implementation deals with the integration of security risk assessment in the test design and implementation process.
3. Risk-based test execution, analysis and summary deals with a risk-based test execution as well as with the systematic analysis and summary of test results.

5.1 Risk-Based Security Test Planning

According to ISO 29119, test planning is the activity of developing the test plan. It aims for determining the test objective, the test scope, and the risks associated to the

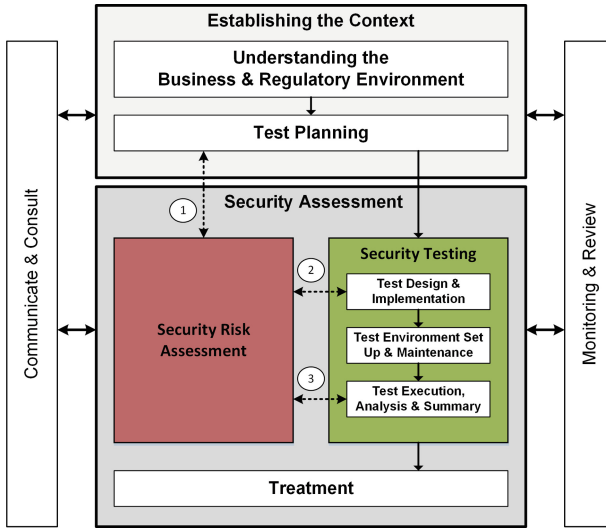


Fig. 5. Process model for risk-based security testing

overall testing process. The main outcome of test planning is a test strategy and a plan that depicts the staffing, the required resources, as well as a schedule for the individual testing activities. While functional testing is more or less guided directly by the system specification (i.e. features, requirements, architecture), security testing often is not. Security is a non-functional property and thus requires dedicated information that addresses the (security) context of the system. Security risk assessment can be used to roughly identify high-risk areas or features of the system under test (SUT) and thus determine and optimize the respective test effort. Moreover, a first assessment of the identified vulnerabilities and threat scenarios may help to select test strategies and techniques that are dedicated to deal with the most critical security risks. Figure 6 shows the integration of security risk assessment results in the overall test planning process. We have identified three integration activities that all serve different purposes:

- (a) Integrate risk analysis
- (b) Risk-based test strategy design
- (c) Risk-based security resource planning and test scheduling

Before starting any of these activities, contextual information i.e. legal or regulatory requirements, organizational test and security policies, organizational or higher-level test strategies, and technical limitations as well as resource limitations and the security risk assessment results (threat, vulnerability and risk estimations) that capture the technical, business, regulatory, and legal requirements should be available.

5.1.1 Security Test Planning: Integrate Risk Analysis (a)

Typically, project risk analysis is a substantial part of the test planning process. The risk analysis is done to get an estimate on the specific project risks, considering the availability of test resources, considering specific product risks and other project related

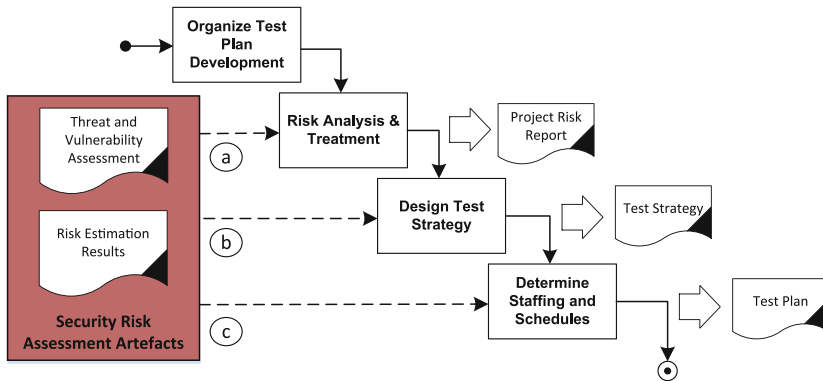


Fig. 6. Process model for risk-based security test planning

issues. The security risk assessment typically addresses the security risk of the product (i.e. the test item). As such, this kind of risk assessment can serve the project risk assessment with valuable estimates on the major product risks. The test manager should review the relevant security risks to identify those, which have a special role for security testing and should try to identify additional product and project related risks like missing resources, technical issues related to the test infrastructure etc. Finally, the test manager should develop an overall risk picture for the test project and communicate the risk picture to the Stakeholders.

5.1.2 Security Test Planning: Risk-Based Security Test Strategy Design (b)

A test strategy defines the test phases, the types of testing, the test techniques and the test completion criteria. A special challenge in security testing is the identification of dedicated and effective security testing techniques. This process could be optimized when the identification and selection of security testing techniques is based on the potential threats and vulnerabilities, which have been identified during a preceding security risk assessment. The test manager should assign vulnerabilities and threat scenarios to test items (interfaces, operations, components) and/or test conditions and try to identify the potential vulnerabilities that have the highest impact on the overall security risks when they are detected. Additionally, the test manager should assign test completion criteria to each test item and/or each test condition and prioritize test item and/or for each test condition by considering the required test efforts to match the completion criteria and the impact testing may have on the overall security risks (i.e. when vulnerabilities are detected or test suites pass without detecting anything).

5.1.3 Security Test Planning: Risk-Based Security Resource Planning and Test Scheduling (c)

The second major activity during test planning is the identification and allocation of resources as well as the related schedule of all relevant security testing activities. Since the main task of security testing is finding vulnerabilities, resource planning and test schedules should be aligned with the major security risks so that resources and the

order of testing allows for a focused testing of the test items or test condition where the detection of vulnerabilities shows the largest impact. The test manager should check for required security testing competences and should acquire new competences if certain security testing tasks require these competences. The test manager should allocate resources considering the required test efforts for that test items or test conditions where testing may have the largest impact in terms of treating or minimizing the identified security risks. He should plan the test schedules so that test items or test conditions where testing might have the largest impact in terms of treating or minimizing the identified security risks are tested first.

5.2 Risk-Based Security Test Design and Implementation

The test design and implementation process is mainly dedicated to derive the test cases and test procedures that are later on applied to the system under test. Security-risk assessment in general provides two different kinds of information that are useful within this process. On the one hand information on expected threats and potential vulnerabilities can be used to systematically determine and identify test conditions (testable aspects of a system) and test purposes. On the other hand side the security risk assessment provides quantitative estimations on the risks, i.e. the product of frequencies or probabilities and estimated consequences. This information can be used to select and prioritize either the test conditions or the actual tests when they are assembled to test sets. Risks as well as their probabilities and consequence values to set priorities for the test selection, test case generation as well as for the order of test execution expressed by risk-optimized test procedures.

Considering security testing, especially the derivation of test conditions and test coverage items are critical. A recourse to security risks, potential threat scenarios and potential vulnerabilities provide a good guidance which of the features and test conditions require testing, which coverage items should be covered in which depth and how individual test cases and test procedures should look like. Figure 7 shows the typical course of test design activities and the respective integration points with security risk assessment. Below, the associated and (through risk assessment) enhanced activities are listed.

- (a) Risk-based identification and prioritization of features sets
- (b) Risk-based derivation of test conditions and test coverage items
- (c) Threat scenario based derivation of test cases
- (d) Risk-based assembly of test procedures

5.2.1 Security Test Design: Risk-Based Identification and Prioritization of Features Sets (a)

A first step during the test design phase is the identification and categorization of the security features that will be tested. Since security features describe functional security measures this approach especially allows for testing the correctness of the feature implementation. Security risk assessment can be used to determine the most critical security features so that these features are tested more intensively and in more detail.

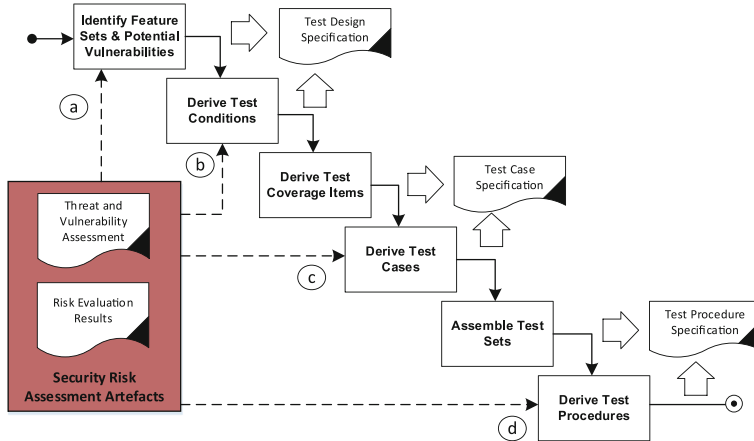


Fig. 7. Process model for risk-based security test design

The security tester should identify testable security features that need to be covered by security testing and prioritize them using the risk levels that are associated with the threat scenario/vulnerabilities.

5.2.2 Security Test Design: Risk-Based Derivation of Test Conditions and Test Coverage Items (b)

After a set of testable security features have been identified the security tester should derive the test conditions and test coverage items. This could be done on basis of the identified features (see phase a) but need to especially consider that security is a non-functional property and that a correct implementation of all security features may not ensure a secure system. Thus, additional test conditions and coverage items are required that especially address the detection of currently unknown vulnerabilities (vulnerability and robustness testing). Security risk assessment should be used to provide a systematic guidance for the derivation of especially these test conditions and test coverage items. Test coverage items and the respective test depth should be chosen according to the impact testing may have on the overall associated security risks.

5.2.3 Security Test Design: Threat Scenario Based Derivation of Test Cases (c)

In this step, the security tester should derive test cases on basis of test conditions and test coverage items. The security tester determines the pre-conditions for the individual tests by selecting adequate input values, the actions to exercise the selected test coverage items, and determines the expected results. Since security risk assessment has been used to identify the test conditions and the test coverage items it is already considered through the activities before. However, threat scenarios and potential vulnerabilities that have been identified during risk assessment might still help by identifying the preconditions, input values, actions and expected results in case it has not been done before. The test designer should identify the preconditions for the tests, the

test data, the test actions and the expected results by examining the test conditions, test coverage items, threat scenarios and potential vulnerabilities.

5.2.4 Security Test Design: Risk-Based Assembly of Test Procedures (d)

In this step, the test cases should be assembled to test sets and test procedures. While test sets group test cases with common constraints on test environment or test items, test procedures defines the order of test execution and thus have to respect the pre- and post conditions. Security risk assessment should be used to prioritize the order test cases and thus the order of testing with respect to the associated risks. The test designer should assemble test sets and test procedures in such a way, that the most relevant tests are executed first. The most relevant test cases are the test cases that address the most critical risks.

5.3 Risk-Based Test Execution, Analysis and Summary

The decision of how extensive testing should be is always a question of the remaining test budget, the remaining time and the probability to discover even more critical errors, vulnerabilities or design flaws. Risk-based test execution allows the prioritization of already existing test cases, test sets or test procedure during regression testing. Risk-based security test analysis and summary aims for improving the evaluation of the test progress by introducing the notion of risk coverage and remaining risks on basis of the intermediate test results as well as on basis of the errors, vulnerabilities or flaws that have been found during testing. In summary we have identified the following three activities that are supported through results from security risk assessment (Fig. 8).

- (a) Risk-based test execution prioritization
- (b) Risk-based test analysis
- (c) Risk-based test summary

5.3.1 Test Execution, Analysis and Summary: Risked-Based Test Execution Prioritization (a)

The execution of test cases can be done several times for the same test cases and test procedures. Normally the execution order for test cases and test procedures is determined at test design by the assembly of test procedures. However, there are a number of regression test scenarios where reprioritization becomes necessary. In this case a risk-based approach for test executions prioritization may help to cover the most relevant remaining security risks. The security tester should prioritize test cases and test procedures in such a way that the most relevant tests are executed first. The most relevant test cases are the test cases that address the most critical risks.

5.3.2 Test Execution, Analysis and Summary: Risked-Based Test Analysis (b)

The test analysis process is used for the evaluation of the test results and the reporting of test incidents. This process will be entered after the test execution and it mainly covers the analysis and evaluation of test failures and issues where something unusual

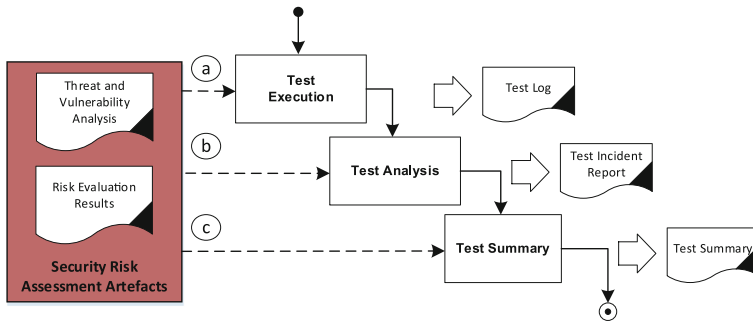


Fig. 8. Process model for risk-based test execution, analysis and summary

or unexpected occurred during test execution. Its main purpose is to categorize the issues that occurred during testing and put them into context so that the test manager can rate them. The security tester should classify newly identified incidents by means of their relation to artefacts from the security risk assessment (e.g., risks, threat scenarios, vulnerabilities) and prioritize the newly identified incidents by means of associated artefacts from the security risk assessment. Issues related to critical risks should be rated higher than the ones that are associated with minor risks. New and/or updated incidents are communicated to the relevant stakeholders.

5.3.3 Test Execution, Analysis and Summary: Risked-Based Test Summary (c)

Finally, the overall test results, i.e. the test verdicts, the issues and their categorization are summarized such that the stakeholder can understand the outcome of the tests. The security tester should analyse the test logs and separate security risks that have been tested successfully (all tests are passed) and those that have not been tested successfully (issues have been found). He should (re-) characterize the security risks by interpreting the test results and make use of dedicate test metrics to determine the quality of test procedures and thus the significance and validity of the test results.

6 Conclusion and Future Work

The integration of risk assessment and security testing offers a number of advantages that are intuitive and easy to grasp. In fact, a non-systematic integration of these two workstream has already been applied in practical settings. Integrating risk assessment artefacts in the security testing process allow for a concise selection of test techniques, the adequate choice of the required expertise and it supports the targeted prioritization of testing tasks and test cases. Additionally, the interpretation of the test results in the context of a security risk analysis can provide a meaningful feedback to the management level. In addition, security testing can be used to complement the assumptions made during risk assessment with a factual basis obtained by the tests.

The method for security assessment described in this paper provides a comprehensive approach to cyber security assessment and management. It might address low-level technical issues as well as high-level non-technical issues. The method integrates two areas that are traditionally addressed in isolation: security risk assessment and security testing. Each of the two areas is represented by an individual workstream, so that they could be processed independent from each other and at different points in time. The overall process of each of the workstreams is based on recognized standards, namely ISO 31000 and ISO 29119 and thus allow for an easy integration in industrial settings. In the past, we have been able to repeatedly elaborate useful integration scenarios based on the proposed integration scheme. The workstreams and their points of integration were successfully evaluated within several case studies representing relevant industrial domains like banking, e-Health and software development. In the near future, we will provide systematic guidance on how to apply our method to dedicated fields of application. We will provide tailored instantiation of our method to serve the special requirements coming from areas like cyber security, information security and critical infrastructure protection. Moreover we will show how our approach can be integrated in the different phases and with the different activities of a typical system life cycle.

Acknowledgements. This work has been conducted as a part of EU project RASEN (316853) funded by the European Commission within the 7th Framework Program.

References

1. Alam, M., Khan, A.I.: Risk-based testing techniques: a perspective study. *Int. J. Comput. Appl.* **65**, 33–41 (2013)
2. Anland, S.: Risk-based testing: Risk analysis fundamentals and metrics for software testing including a financial application case study. *J. Syst. Softw.* **53**(3), 287–295 (2000)
3. Erdogan, G., Li, Y., Runde, R., Seehusen, F., Stølen, K.: Approaches for the combined use of risk analysis and testing: A systematic literature review. *Int. J. Softw. Tools Technol. Transfer* **16**, 627–642 (2014)
4. Felderer, M., Haisjackl, C., Breu, R., Motz, J.: Integrating manual and automatic risk assessment for risk-based testing. In: Biffl, S., Winkler, D., Bergsman, J. (eds.) *SWQD 2012. LNBIP*, vol. 94, pp. 159–180. Springer, Heidelberg (2012)
5. Felderer, M., Ramler, R.: Experiences and challenges of introducing risk-based testing in an industrial project. In: Winkler, D., Biffl, S., Bergsman, J. (eds.) *SWQD 2013. LNBIP*, vol. 133, pp. 10–29. Springer, Heidelberg (2013)
6. Felderer, M., Schieferdecker, I.: A taxonomy of risk-based testing. *Int. J. Softw. Tools Technol. Transfer* **16**(5), 559–568 (2014)
7. Herzog, P.: *OSSTMM 2.1. Open-Source Security Testing Methodology Manual*; Institute for Security and Open Methodologies (2003)
8. International Standards Organization. *ISO 31000:2009(E), Risk management – Principles and guidelines* (2009)
9. International Standards Organization. *ISO/IEC/IEEE 29119 Software and system engineering - Software Testing-Part 1-4* (2012)

10. Michael, C.C., Radosevich, W.: Risk-Based and Functional Security Testing. Cigital, Inc. (2005)
11. Murthy, K.K., Thakkar, K.R., Laxminarayan, S.: Leveraging risk based testing in enterprise systems security validation. In: Proceedings of the First Int Emerging Network Intelligence Conference, pp. 111–116 (2009)
12. Redmill, F.: Exploring risk-based testing and its implications: research articles. *Softw. Test. Verif. Reliab.* **14**(1), 3–15 (2004)
13. Redmill, F.: Theory and practice of risk-based testing: Research Articles. *Softw. Test. Verif. Reliab.* **15**(1), 3–20 (2005)

Risk Assessment and Risk-Driven Testing

Third International Workshop, RISK 2015, Berlin,

Germany, June 15, 2015. Revised Selected Papers

Seehusen, F.; Felderer, M.; Großmann, J.; Wendland,
M.-F. (Eds.)

2015, IX, 121 p. 39 illus. in color., Softcover

ISBN: 978-3-319-26415-8