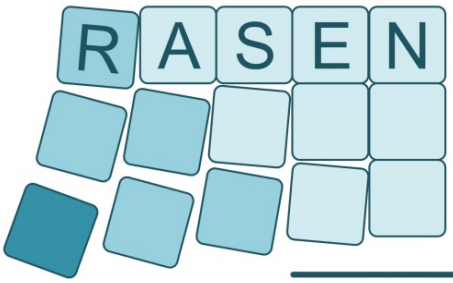

Compositional Risk Assessment and Security Testing of Networked Systems

Combining Security Risk Assessment and Security Testing

Jürgen Großmann[a], and Fredrik Seehusen[b]
[a]Fraunhofer FOKUS, [b]SINTEF ICT

Complex networked systems have become an integral part of our supply infrastructure. Mobile devices, home automation, smart grids and even vehicles are connected via the Internet and becoming accessible and thus vulnerable to hacker attacks. While the number of security incidents drastically increases, we are more than ever dependent on a secure and mature ICT infrastructure. One of the keys to maintain such a secure and dependable infrastructure are mature, systematic and capable proactive measures to reduce or prevent the risks of security incidents. This paper describes the systematic integration of security risk assessment and security testing to enable efficient and focused security assessments of networked systems.

Security risk assessment and security testing each contribute to an overall assessment of the security of a system. They are supported by existing standards such as ISO 31000[1] and ISO 29119[2] but are normally treated as distinct areas that are traditionally isolated from one another. While the industry demands integrative approaches that cope with security as a whole, currently no standard exists that sufficiently emphasizes the systematic integration of security risk assessment and security testing.

Motivating example:
An operator of an ICT-based organization or infrastructure is responsible for the infrastructure itself, its overall quality of service and its security. He has to decide how to set-up and maintain the infrastructure i.e. which systems and devices are to be integrated, how they are tested, and which rules and regulation need to be followed. However, he acts as a profit enterprise and thus needs to keep quality issues as efficient as possible. As a result, he has to identify, recognize and minimize operational risks in a process that keeps risk and quality control focused, concise, cost efficient and manageable.

The RASEN project develops methods that are dedicated to support companies and organizations in undertaking risk analysis for large scale and networked systems. These methods cover security risk assessments on different levels of abstraction and from different perspectives. Legal risk assessment especially addresses security threats in a legal context and under consideration of legal consequences. Security risk assessment specifically deals with the concise assessment of security threats, their estimated probabilities and their estimated consequences for a set of technical or business related assets. Finally, security testing can be used to actually examine the target under assessment for vulnerabilities and its actual quality.

The overall RASEN process of security risk assessment and security testing is derived from ISO 31000 and slightly extended to integrate security testing as one of the major tasks that need to be carefully aligned with typical risk assessment activities. It is defined independent from any application domain and independent from the level, target or depth of the assessment. It could be applied

[1] International Standards Organization. ISO 31000:2009(E), Risk management – Principles and guidelines, 2009
[2] International Standards Organization. ISO 29119 Software and system engineering - Software Testing-Part 1-4 , 2012

for legal risk as well as for any kind of technical assessment.

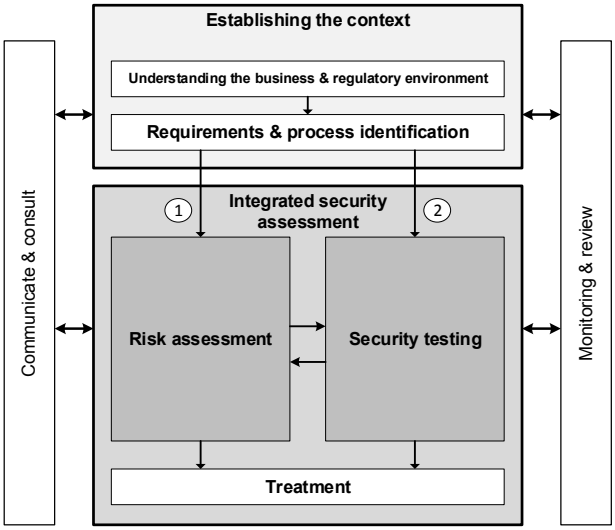

Figure 1 – Overall risk, compliance and quality assessment process

Figure 1 shows the main activities of a combined risk assessment and security testing process. It starts with a preparatory phase called *Establishing the context* and 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. The main part consists of typical security risk assessment activities that are defined in ISO 31000 and typical security testing activities that follow testing standards like ISO 29119.

Integrating and interweaving the risk and security testing activities allow for a more precise, focused and dynamic assessment of systems. In principal there are two ways that security testing and security risk assessment can be combined. Either the testing process is integrated into risk assessment process or the risk assessment is integrated into the testing process.

1. A risk-based process to security testing will start like a typical testing process and uses risk assessment results to guide and focus the testing. Such a process involves 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.
2. A test-based process to security risk assessment starts like a typical risk assessment process and uses 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 to adjust risk values on basis of tangible measurements like test results. Security testing provides a concise feedback whether the properties of the target under assessment have been really met by the risk analysis.

The following two sections provide a detailed description of both of the processes.

Test-based risk assessment

The main purpose of integrating the testing process into the risk assessment process is to use testing to enhance some of the activities of the risk assessment process. This is achieved by ensuring that test results are used as explicit input to the risk assessment.

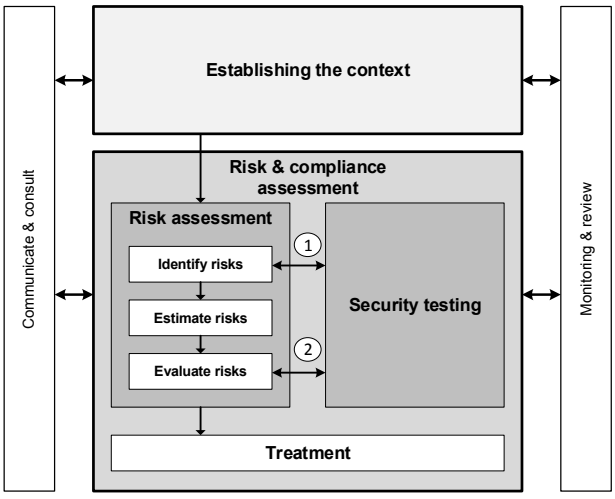

Figure 2 – Generic process for test-based risk assessment

Figure 2 shows how the unified RASEN process (shown in Figure 1) is refined into a process for test-based risk assessment. Here the risk assessment activity has been decomposed into the three activities identify risks, estimate risks and evaluate risks. 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 Figure 2, there are in par-

ticular two places where testing can in principle enhance the risk assessment process.

1. **Test-based risk identification:** In a risk assessment process, the risk identification activity is performed with respect to a target of analysis which is described and documented in the "establish context step". In a test-based risk assessment setting however, the risk identification is not only based on the documentation of the target of analysis, but also on relevant test results of target of analysis. Particularly relevant in this setting is testing using automated testing tools such as vulnerability scanners or network discovery tools.
2. **Test-based risk evaluation:** The risk assessment activity that can be enhanced by the testing process (denoted 2 in Figure 2) is risk evaluation. At this point in the process, risks have already been identified and estimated, and the main reason for doing testing here is to gain increased confidence in the correctness of the risk model. In particular, the likelihood estimates of the risk model might have a low confidence if they e.g. depend on vulnerabilities whose presence in the target of analysis is unknown. By doing testing in this setting, we may investigate whether such vulnerabilities really are present in the target of analysis, and then use the test results to update the confidence level of the risk model.

Risk-based security testing

Risk-based security testing methods help to optimize the overall security testing process. The result of the risk assessment, i.e. the identified vulnerabilities, threat scenarios and unwanted incidents, are used to guide the test identification and may complement requirements engineering results with systematic information concerning the threats and vulnerabilities of a system. A comprehensive risk assessment additionally introduces the notion of probabilities and consequences related to threat scenarios. These risk values can be 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. Furthermore, risk-based testing methods can help to optimize the risk assessment itself.

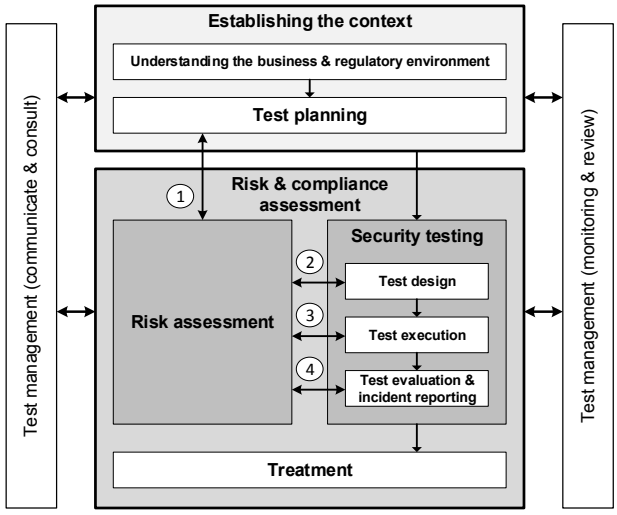

Figure 3 – Generic process for risk-based security testing

Figure 3 shows the instantiation of the overall risk and compliance assessment process to serve risk-based security testing. It consists of the classical phases of a testing process like it is specified in ISO 29119 and adds up to four additional activities, namely risk-based security test planning & management, risk-based security test design, risk-based security test selection, and security risk control. The activities are described in detail below.

1. **Risk-based security test planning:** Risk assessment is used to roughly identify high-risk areas or features of the system under test (SUT) and thus determine and optimize the respective test effort that is needed to verify the related security functionality or to address the related vulnerabilities. Moreover, a first assessment of the identified vulnerabilities and threat scenarios my help to select test strategies and techniques that are dedicated to deal with the most critical risks.
2. **Risk-based security test design and implementation**: During the test design and implementation phase, test cases are derived, implemented and assembled to test procedures. Security-risk assessment results contain qualitative information on expected threats and vulnerabilities for a certain kind of application. This kind of information can be used to systematically determine what and how to test. It can be used to identify test condition (testable aspects of a system) as well as test purposes or high-level test scenario that are dedicated to simulate potential threats and potential vul-

nerabilities that are not covered by e.g. the security functional requirements.

3. **Risk-based security test selection & execution**: In risk-based testing coverage can be described in terms of the identified risks, their probabilities and consequences. Risk-based security test selection criteria can be used to control the selection or the selected generation of test cases. The criteria are designed by taking the risks as well as their probabilities and consequence values to set priorities for the test selections, test case generation as well as for the order of test execution.
4. **Risk-based security test monitoring and control:** The decision on 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 security test monitoring and control aims for improving the monitoring and control activities 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 so far.

While security test planning as well as security test monitoring and control belong to the test management process, security test design and implementation as well as security test selection and execution belong to the dynamic test process that is controlled by the test management process.

Conclusion

The RASEN project envisions the overall integration of test-based risk assessment and risk-based security testing. Such an approach allows for addressing risks on different levels such as legal risks, business risks and technical risks in an integrated manner. Within this respect, the legal risk assessment defines the contextual background for technical risks and the related vulnerabilities. Technical risks and the vulnerabilities that have been discovered by understood and analyzed with respect to their impact on legal or business issues. The other way round, legal or business related risk assessment can be used to a priori focus the technical risk-assessment as well as the security testing on the areas, which are most likely to cause legal or business concern. The combination of security risk analysis and security testing allows for an improved and measurement-based approach to risk analysis and a focused approach to security testing. Based on this kind of integration organizations and companies will be able to concisely and effectively assess security risks for different levels of concerns, e.g. legal concerns, business concerns or technical concerns.

The RASEN Project

The overall objective of the RASEN project is to strengthen European organizations' ability to conduct security assessments of large scale networked systems through the combination of security risk assessment and security testing, taking into account the context in which the system is used, such as liability, legal and organizational issues as well as technical issues.

Consortium

The RASEN project is coordinated by SINTEF ICT and consists of the following partners:

- **EVRY**, Norway (www.evry.no)
- **Fraunhofer FOKUS**, Germany (www.fokus.fraunhofer.de)
- **Department of Private Law**, University of Oslo, Norway (www.jus.uio.no/ifp)
- **Info World**, Romania (www.infoworld.ro)
- **SINTEF ICT**, Norway (www.sintef.no)
- **Smartesting**, France (www.smartesting.com)
- **Software AG**, Germany (www.softwareag.com)

Contact

Visit the RASEN website or contact us by email.

- www.rasenproject.eu
- contact@rasenproject.eu

The project can also be followed on LinkedIn and Twitter.

- @RASENProject
- #RASENProject

www.linkedin.com/groups?home=&gid=7429037

Acknowledgments

The RASEN project (2012-2015) is funded by the European Commission via the Seventh Framework Programme, grant agreement no. 316853.

SEVENTH FRAMEWORK PROGRAMME

RASEN