SINTEF

SINTEF A22798- Unrestricted

Report

Conceptual Framework for the DIAMONDS Project

Author(s)
Gencer Erdogan, Yan Li, Ragnhild Kobro Runde, Fredrik Seehusen, Ketil Stølen

SINTEF ICT
Networked Systems and Services
2012-06-22

SINTEF

Report

Conceptual Framework for the DIAMONDS Project

KEYWORDS:
Security testing, security risk analysis, model, Test-driven model-based security risk analysis, Risk-driven model-based security testing

VERSION
Final

DATE
2012-06-22

AUTHOR(S)

Gencer Erdogan, Yan Li, Ragnhild Kobro Runde, Fredrik Seehusen, Ketil Stølen

CLIENT(S)
The DIAMONDS project supported by the Research Council of Norway

CLIENT'S REF.
201579/S10

PROJECT NO.
90B287

NUMBER OF PAGES/APPENDICES:
34/0

ABSTRACT

DIAMONDS is a research project addressing the combination of security testing and risk analysis. The 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. This report documents the conceptual framework for DIAMONDS by clarifying the notions of security testing, risk analysis, and related concepts, as well as defining the relations among them.

PREPARED BY	Yan Li	**SIGNATURE** Li, Yan
CHECKED BY	Bjørnar Solhaug	**SIGNATURE** Bjørnar Solhaug
APPROVED BY	Bjørn Skjellaug	**SIGNATURE**

SINTEF ICT
Networked Systems and Services
2012-06-22

Conceptual Framework for the DIAMONDS Project

Gencer Erdogan[1,2] Yan Li[1,2] Ragnhild Kobro Runde[1]
Fredrik Seehusen[2] Ketil Stølen[1,2]

[1] Department of Informatics, University of Oslo P.O. Box 1080
Blindern, N-0316 Oslo, Norway
ragnhilk@ifi.uio.no

[2] Department for Networked Systems and Services, SINTEF ICT
P.O. Box 124 Blindern, N-0314 Oslo, Norway
{gencer.erdogan,yan.li,fredrik.seehusen,ketil.stolen}@sintef.no

June 22, 2012

Contents

1 Introduction

DIAMONDS is a research project addressing the combination of security testing and risk analysis. The 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. This report documents the conceptual framework for DIAMONDS by clarifying the notions of security testing, risk analysis, and related concepts, as well as defining the relations among them.

The conceptual framework offers a basis for future research in the project by providing a common understanding of the central notions within security testing and security risk analysis. Our approach is to build the conceptual framework upon established concepts from state-of-the-art. However, we also make adjustments of established notions where seen necessary or appropriate, in order to achieve a consistent framework suitable for the particular target of the DIAMONDS project.

In DIAMONDS, we focus on model-based approaches to security testing and security risk analysis, where models are used as a main artifact both during the testing/analysis process and for documentation purposes. In particular we distinguish between model-based security testing (MST) and model-based security risk analysis (MSR). For combining MST and MSR, there are two main possibilities depending on which approach is taken as the starting point, i.e., the main purpose of the process. We will refer to these as risk-driven model-based security testing (RMST) and test-driven model-based security risk analysis (TMSR).

The remainder of this report is organized as follows: We start by introducing the overall risk management process in Section 2, before considering the basic notions of risk analysis, security, and testing in Sections 3, 4, and 5, respectively. In Sections 6 and 7 we build on the previous sections when presenting the definitions for security risk analysis and security testing, respectively. The basic concepts for models are presented in Section 8. In Sections 3-8 we use definitions from standards as much as possible, and additionally provide our interpretation of the relationships between the various concepts. The definitions of model-based security risk analysis (MSR) and model-based security testing (MST) are defined in Sections 9 and 10, respectively. Finally, we provide our proposal for test-driven model-based security risk analysis (TMSR) in Section 11, and for risk-driven model-based security testing (RMST) in Section 12.

2 Risk Management

It is necessary to introduce the overall risk management process before we look closer into risk analysis and other relevant concepts. ISO 31000 Risk management - Principles and guidelines [7] is our main building block in terms of defining and explaining the concept of risk management and the concepts related to risk management. The overall risk management process shown in Figure 1 is taken from [7, p.14].

There is however one deviation: Our definition of risk estimation is equivalent to what ISO 31000 refers to as risk analysis. Instead we use the term risk analysis in line with how the term is used in practice to denote the five step process in the middle of Figure 1 starting with establishing the context and ending with risk treatment.

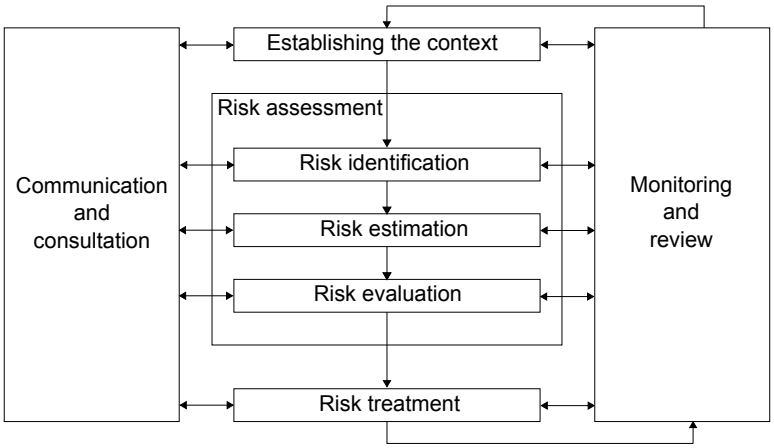

Figure 1: *The overall risk management process (adapted from [7, p.14]).*

As stated in ISO 31000 [7, p.1], all activities of an organization may involve risk. Organizations usually manage risk by identifying it, estimating it and then evaluating it to see whether the risk should be modified by risk treatment in order to satisfy the risk evaluation criteria. Through this process, communication and consultation are carried out with stakeholders to monitor and review the risk, and controls that are modifying the risk are implemented to ensure that no further risk treatment is required. Risk management can be applied to an entire organization, at its many areas and levels, at any time, and to specific functions, projects and activities. Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization.

- **Risk Management**

  Risk management refers to the coordinated activities to direct and control an organization with regard to risk [7, p.2].

- **Risk Management Process**

  Risk management process is the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk [7, p.3].

- **Communication and Consultation**

  Communication and consultation refers to the continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialog with stakeholders regarding the management of risk [7, p.3].

- **Establishing the Context**

  Establishing the context refers to the process of defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the remaining process (adapted from [7, p.3]).

- **Risk Assessment**

  Risk assessment is the overall process of risk identification, risk estimation and risk evaluation(adapted from [7, p.4]).

- **Risk Identification**

  Risk identification is the process of finding, recognizing and describing risks. This involves identifying sources of risk, areas of impacts, events (including changes in circumstances), their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs [7, p.4].

- **Risk Estimation**

  Risk estimation is the process of comprehending the nature of risk and determining the level of risk. This involves developing an understanding of the risk. Risk estimation provides the basis for risk evaluation and decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods (adapted from [7, p.5]).

- **Risk Evaluation**

  Risk evaluation is the process of comparing the results of risk estimation with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment (adapted from [7, p.6]).

- **Risk Treatment**

  Risk treatment is the process of modifying risk which can involve risk mitigation, risk elimination or risk prevention.(adapted from [7, p.6]).

- **Risk Analysis**

  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, p.14]).

- **Monitoring**

  Monitoring is the continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected [7, p.7].

- **Review**

  Review is the activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives [7, p.7].

3 Risk Analysis

The conceptual model and notions defined here are based on the ISO 31000 standard [7]. Figure 2 shows the conceptual model for risk analysis adopted by the DIAMONDS project.

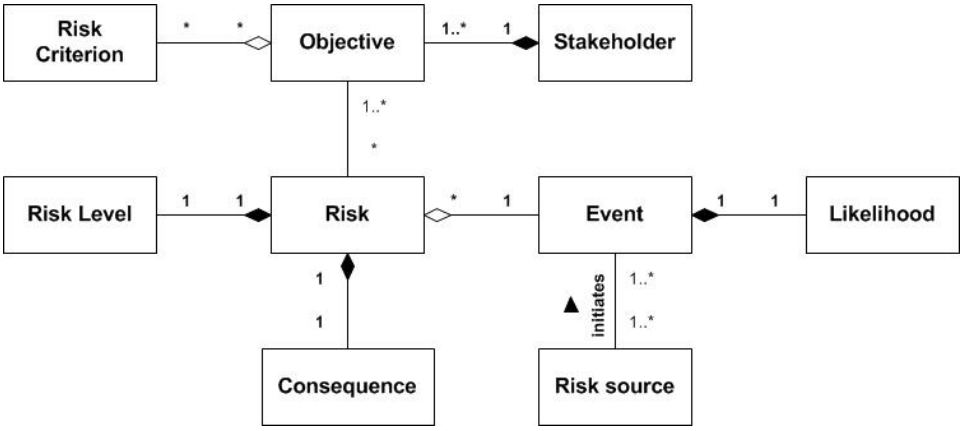

Figure 2: *Conceptual model for risk analysis.*

- **Risk**

  Risk is the combination of the consequences of an event with respect to an objective and the associated likelihood of occurrence (adapted from [7, p.1]).

- **Objective**

  An objective[1] is something the stakeholder is aiming towards or a strategic position it is working to attain (adapted from [12]).

- **Risk Source**

  Risk source is an element which alone or in combination has the intrinsic potential to give rise to risk [7, p.4].

- **Stakeholder**

  Stakeholder is a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity [7, p.4].

- **Event**

  Event is the occurrence or change of a particular set of circumstances [7, p.4].

[1]Note that although the notion of objective is used in ISO 31000, it is not defined in the standard.

- **Likelihood**

  Likelihood is the chance of something happening [7, p.5].

- **Consequence**

  Consequence is the outcome of an event affecting objectives [7, p.5].

- **Risk Criterion**

  A risk criterion is the term of reference against which the significance of a risk is evaluated [7, p.5].

- **Risk Level**

  Risk level is the magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood [7, p.6].

4 Security

The terms information security, computer security and information assurance are frequently used interchangeably. These fields are often interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them [1].

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is mainly concerned with the confidentiality, integrity and availability of data regardless of the form the data may take, such as electronic, print, or other forms. Computer security mainly focuses on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Information assurance focuses on the reasons for assurance that information is protected, and is thus reasoning about information security [1].

In the DIAMONDS project we use the term security in the meaning of information security, where the definition of information security has been taken from ISO/IEC 27000 Information Security Management System [6], as shown in Figure 3.

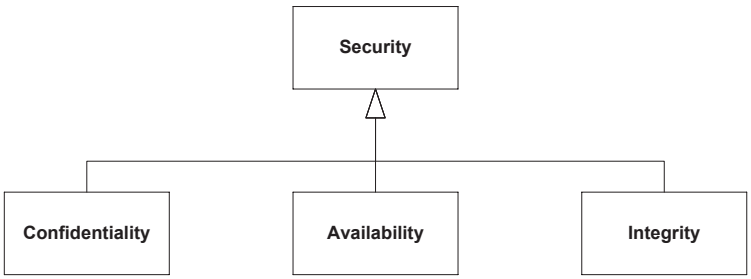

Figure 3: *Conceptual model for Security.*

- **Security**

  Security refers to the preservation of confidentiality, integrity and availability of information (adapted from [6, p.3]).

- **Confidentiality**

  Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [6, p.2].

- **Availability**

  Availability is the property of information being accessible and usable upon demand by an authorized entity [6, p.2].

- **Integrity**

  Integrity is the property of protecting the accuracy and completeness of information (adapted from [6, p.4]).

5 Testing

In this section, we particularly focus our conceptual clarification on software testing related to the DIAMONDS project. Our primary source for the notion of software testing and related notions is the upcoming international standard ISO/IEC 29119 Software Testing [8] defined by Software and Systems Engineering Standards Committee of the IEEE Computer Society.

However, ISO/IEC 29119 is still under development, and we only have access to a draft version of Part 2 (ISO/IEC 29119 Draft Part 2-Testing Process) at the time of writing. For related notions not found in Part 2, we use IEEE 829 [5] and BS 7925-1/-2 [11], which are expected to be incorporated into ISO/IEC 29119.

As stated in ISO/IEC TR 19759 [3], testing concepts, strategies, techniques, and measures need to be integrated into a defined and controlled process which is run by people. The testing process provide support for testing activities as well as guidance for testing teams. It provides justified assurance that the test objectives will be met cost-effectively. We introduce the overall testing process (see Figure 4) defined in ISO/IEC 29119 [8] before we define the specific testing process used in the DIAMONDS project.

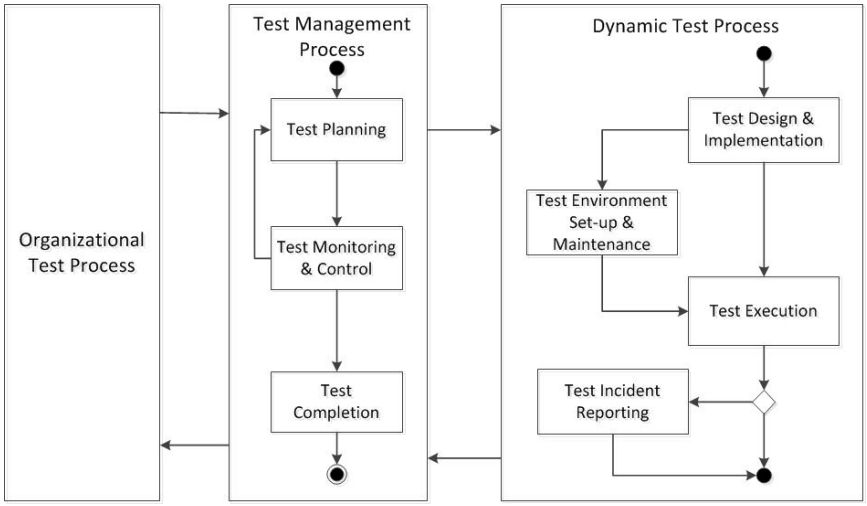

Figure 4: *Overall test process [8, p.7-p.22].*

The testing activities that are performed during the life cycle of a software system may be grouped into a three layers test process [8, p.2], as shown in Figure 4.
The aim of the organizational test process layer is to define a process for

the creation and maintenance of organizational test specifications, such as organizational test policies, strategies, processes, procedures and other assets [8, p.2].

The aim of the test management process layer is to define processes that cover the management of testing for a whole test project or any test phase or test type within a test project (e.g. project test management, system test management, performance test management) [8, p.2].

The aim of the dynamic test process layer is to define generic processes for performing dynamic testing. Dynamic testing may be performed at a particular phase of testing (e.g. unit, integration, system, and acceptance) or for a particular type of testing (e.g. performance testing, security testing, and functional testing) within a test project [8, p.2].

What we refer to at the testing process in the DIAMONDS project is basically what Figure 4 refers to as the dynamic test process. However, as indicated by Figure 5 we also add a test planning step capturing the test planning of the test management process of relevance for one run of the dynamic test process.

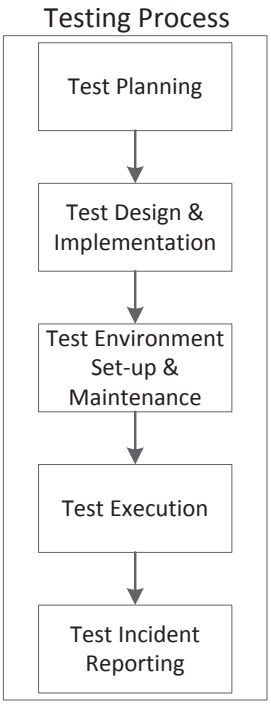

Figure 5: *The testing process used in DIAMONDS, adapted from [8].*

- **Testing**

  Testing is the process of exercising the system to verify that it satisfies specified requirements and to detect errors (adapted from [11]).

- **Test Planning**

  The test planning is the process of developing the test plan. Depending on where in the project this process is implemented this may be a project test plan or a test plan for a specific phase, such as a system test plan, or a test plan for a specific type of testing, such as a performance test plan (adapted from [8, p.8]).

- **Test Design and Implementation**

  The test design and implementation is the process of deriving the test cases and test procedures (adapted from [8, p.23]).

- **Test Environment Set-up and Maintenance**

  The test environment set-up and maintenance process is the process of establishing and maintaining the environment in which tests are executed (adapted from [8, p.27]).

- **Test Execution**

  The test execution is the process of running the test procedure resulting from the test design and implementation process on the test environment established by the test environment set-up and maintenance process. The test execution process may need to be performed a number of times as all the available test procedures may not be executed in a single iteration (adapted from [8, p.28]).

- **Test Incident Reporting**

  The test incident reporting is the process of managing the test incidents. This process will be entered as a result of the identification of test failures, instances where something unusual or unexpected occurred during test execution, or when a retest passes (adapted from [8, p.30]).

The conceptual model for testing used in DIAMONDS is defined in Figure 6.

- **Test Policy**

  The test policy is a document that describes the purpose, goals, and overall scope of the testing within the organization (adapted from [8, p.4]).

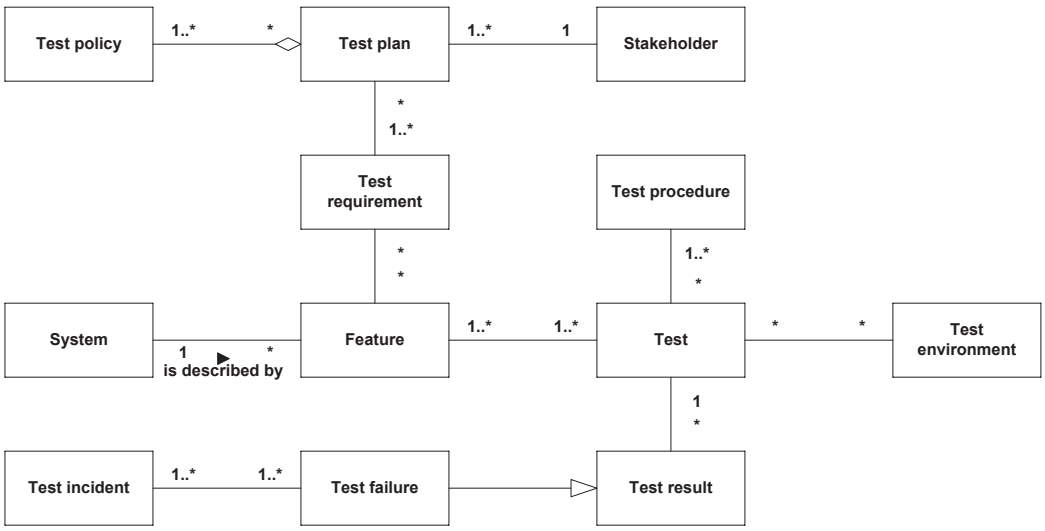

Figure 6: *Conceptual model for Testing.*

- **Test Plan**

  Test plan is a document describing the objective, scope, approach, resources, and schedule of intended test activities(adapted from [5, p.11]).

- **Test Requirement**

  Test requirement is a capability that must be met or possessed by the system (requirements may be functional or non-functional) - (adapted from [11]).

- **System**

  A system is an interacting combination of elements that aims to accomplish a defined objective. These include hardware, software, firmware, people, information, techniques, facilities, services, and other support elements [3, p.2-3].

- **Feature**

  Feature is a distinguishing characteristic of a system (includes both functional and nonfunctional attributes such as performance and reusability)(adapted from [5, p.9]).

- **Test**

  Test[2] is a set of inputs, execution preconditions, and expected outcomes developed for a particular objective, such as to exercise a partic-

[2]Note that the term test as defined here is sometimes referred to as test case in other resources.

ular program path or to verify compliance with a specific requirement (adapted from [11]).

- **Test Procedure**

  Documentation that specifies a sequence of actions for the execution of a test [5, p.11].

- **Test Environment**

  Test environment is the description of the hardware and software environment in which the tests will be run, and any other software with which the software under test interacts (adapted from [11]).

- **Test Incident**

  Test incident is an unplanned event occurring during testing that has a bearing on the success of the test. Most commonly raised when a test result fails to meet expectations [11].

- **Test Failure**

  Test failure is the deviation of the software from its expected delivery or service (adapted from [11]).

- **Test Result**

  A test result is an actual outcome or a predicted outcome of a test (adapted from [11]).

6 Security Risk Analysis

Lund et al. [9] classify risk analysis approaches into two main categories:

- Offensive approaches: Risk analysis concerned with balancing potential gain against risk of investment loss. This kind of risk analysis is more relevant within finance and political strategy making.
- Defensive approaches: Risk analysis concerned with protecting what is already there.

In the context of security, the defensive approach is the one that is relevant. The conceptual model for security risk analysis is shown in Figure 7. For the definitions of risk, objective, risk source and event see Section 3.

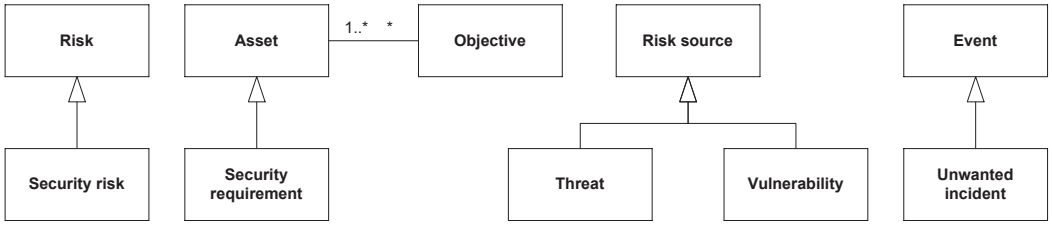

Figure 7: *Conceptual model for security risk analysis.*

- **Security Risk Analysis**

  Security risk analysis is the process of risk analysis specialized towards security.

- **Asset**

  Asset is anything that has value to the stakeholders (adopted from [6]).

- **Security Requirement**

  Security requirement is a specification of the required security for the system (adopted from [11]).

- **Security Risk**

  Security risk is a risk caused by a threat exploiting a vulnerability and thereby violating a security requirement.

- **Unwanted Incident**

  Unwanted incident is an event representing a security risk.

- **Threat**

  Threat is potential cause of an unwanted incident [6].

- **Vulnerability**

  Vulnerability is weakness of an asset or control that can be exploited by a threat [6].

7 Security Testing

Based on the notions of security and testing we define security testing as follows:

- **Security Testing**

  Security testing is the process of testing specialized towards security.

To be more specific, we can understand security testing as the testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise [4]. The basic security concepts that need to be covered by security testing are confidentiality, availability, and integrity. The conceptual model for security testing is shown in Figure 8. For the definition of test requirement see Section 5.

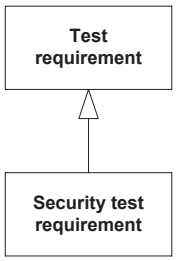

Figure 8: *Conceptual model for security testing.*

- **Security Test Requirement**

  A security test requirement is a test requirement specialized towards security.

8 Model

This section clarifies the notion of model (see Figure 9). The concepts described here are based on TOGAF (The Open Group Architecture Framework) [10], System Analysis and Design [13] and SWEBOK (Software Engineering Body of Knowledge) [3].

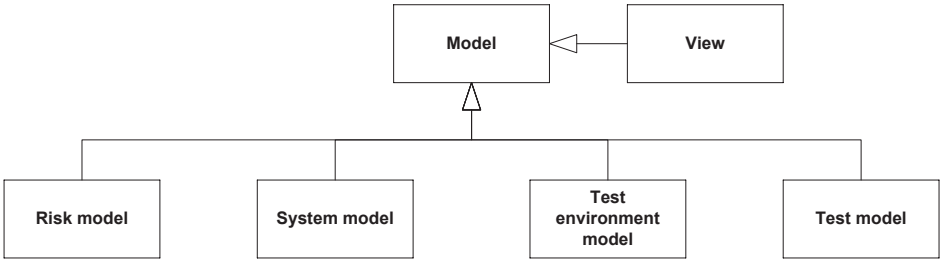

Figure 9: *Conceptual model for model.*

- **Model**

  Model is a representation of a subject of interest. A model provides a smaller scale, simplified, and/or abstract representation of the subject matter (adapted from [10]).

- **View**

  A view represents a related set of concerns.

- **System Model**

  A system model represents a system.

- **Risk Model**

  A risk model represents risks.

- **Test Model**

  A test model represents tests.

- **Test Environment Model**

  A test environment model represents the test environment.

9 Model-based Security Risk Analysis

Based on the notions of model and security risk analysis we define the term model-based security risk analysis as follows:

- **Model-Based Security Risk Analysis**

  Model-based security risk analysis (MSR) is security risk analysis in which each step of the process includes the construction and analysis of models.

10 Model-based Security Testing

Model-based testing is a software testing approach that relies on models of a system under test and its environment to derive test cases. Usually, the testing model is derived in whole or in part from a model that describes functional or non-functional aspects (e.g. performance, security, ergonomics) of the system under development [2].

- **Model-based Security Testing**

  Model-based security testing (MST) is security testing that involves the construction and analysis of a system model, a test model and a test environment model to derive tests.

11 Test-driven Model-based Security Risk Analysis

Test-driven model-based security risk analysis is defined as 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 to serve different purposes. The first usage (i.e., testing *before* the security risk assessment process, as shown in Step 2 in Figure 10) supports the security risk analysis process by identifying potential risks, while the second usage (i.e., testing *after* the security risk assessment process, as shown in Step 6 in Figure 10) validates security risk models based on security testing results.

- **Test-driven Model-based Security Risk Analysis (TMSR)**

  Test-driven model-based security risk analysis (TMSR) is model-based security risk analysis that use testing within the risk analysis process.

Figure 10 illustrates the process of TMSR defined as a specialization of the risk analysis process illustrated in Figure 1, with establish objective introduced in Step 1 and risk validation introduced in Step 7. The testing process in Step 2 and Step 6 is the testing process defined in Section 5 specialized towards security.

The following describes the steps in the TMSR process including the inputs and outputs for each step.

Step 1: Establish Objective and Context
The first step is the initial preparation for risk analysis in which a basic idea about objectives, scale of analysis and corresponding context are established. This can be performed by an introductory meeting with the customer on the behalf of which the analysis is conducted. The representatives of the customer can present their overall objectives of the analysis, security requirements and the system they wish to have analyzed in structured meetings, to ensure a common initial understanding of the analysis. After defining the overall objectives, the rest of the analysis is planned by defining assets that need to be defended, risk criteria and system model.

- **Input**: Objective, security requirement
- **Output**: Assets that need to be defended, risk criteria, system model

Step 2: Testing Process
The purpose of the testing process used in this step is to support the security risk analysis process for identifying potential risks. Based on the identified

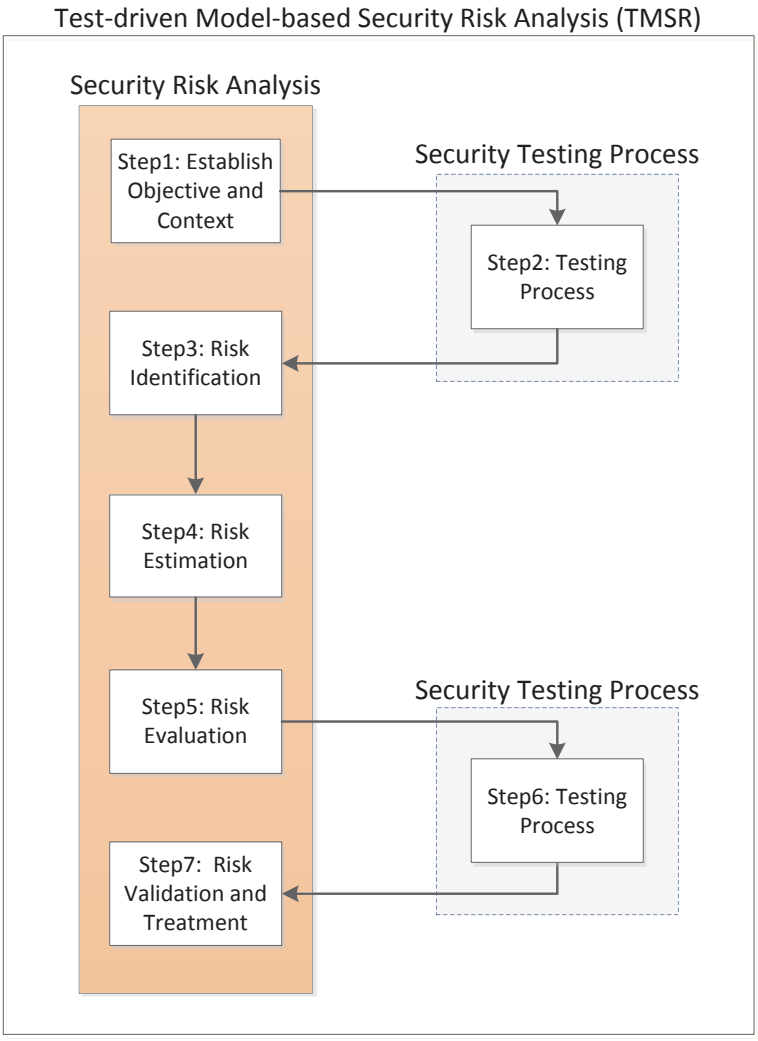

Figure 10: *Test-driven Model-based Security Risk Analysis process*

assets, risk criteria and system models, the relevant items of the system are selected and considered as test objectives defined in test plan. Test models are then built according to the test objectives and security requirements, and are in further used to generate tests. After tests have been executed, the test result is reported and directed as an input to Step 3 for risk identification.

- **Input**: Assets that need to be defended, risk criteria, system model
- **Output**: Test result

Step 3: Risk Identification
Risk identification is the process of finding, recognizing and describing risks in terms of the events (including changes in circumstances), their risk source

and potential consequences to form an incomplete risk model(e.g. a risk model without likelihood and consequence values). It involves a systematic identification of threats, unwanted incidents, and vulnerabilities with respect to the identified assets and according to the security test results from Step 2. Taxonomy-based questionnaires or risk checklists may be used by project members in a structured brainstorm meeting. And particular focus will be put upon security risks that are related to software functionality and requirements.

- **Input**: Assets that need to be defended, system model, test result
- **Output**: Incomplete risk model

Step 4: Risk Estimation
Risk estimation is the process of comprehending the nature of risk and determining the level of risk. This involves developing an understanding of the risk by defining the likelihoods and consequences of the risks identified in Step 3. These values in combination indicate the risk level for each of the identified risks and that further form the basis of complete risk models which we refer to risk model. It provides the basis for risk evaluation and decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. The risk estimation can be conducted as a brainstorming session involving personnel with various backgrounds.

- **Input**: Assets that need to be defended, risk criteria, system model, incomplete risk model
- **Output**: Risk model

Step 5: Risk Evaluation
Risk evaluation is the process of comparing the results of risk estimation with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable, considering assets that need to be defended. It assists in the decision about which risks need treatment and the priority for treatment implementation according to risk criteria.

- **Input**: Assets that need to be defended, risk criteria, risk model
- **Output**: Risk prioritized with respect to risk criteria

Step 6: Testing Process
The testing process used here is to support the security risk analysis process for validating the risk models. Based on the prioritized risks, risk model and system model, relevant system components are analyzed and considered as test objectives in test plan. Test models are then built according to test objectives and security requirements. Furthermore, tests are created and executed based on the security test models. The test result is reported and directed as an input to Step 7.

- **Input**: Assets that need to be defended, system model, risk model, risk prioritized with respect to risk criteria
- **Output**: Test result

Step 7: Risk Validation and Treatment
Risk validation and treatment is the process of validating risk models made earlier and modifying risk which can involve risk mitigation, risk elimination or risk prevention. Security testing results from Step 6 are used to validate the risk models. The unacceptable risks are further evaluated with possible treatments to reduce likelihoods and negative consequences, according to risk criteria. Subsequently, the risk model will then be updated as well.

- **Input**:Assets that need to be defended, risk criteria, risk model, test result
- **Output**: Treatment, updated risk model,

12 Risk-driven Model-based Security Testing

Risk-driven model-based security testing is defined as the combination of security testing and security risk analysis in which security risk analysis is carried out both before and after the test design & implementation step to serve different purpose. The first usage (i.e., security risk analysis *before* the test design & implementation step, as shown in Step 2 in Figure 11) supports the security testing process by identifying the most important parts of the system, while the second usage (i.e., security risk analysis *after* the test design & implementation step, as shown in Step 5 in Figure 11) supports the security testing process by identifying the most important security tests that needs to be executed.

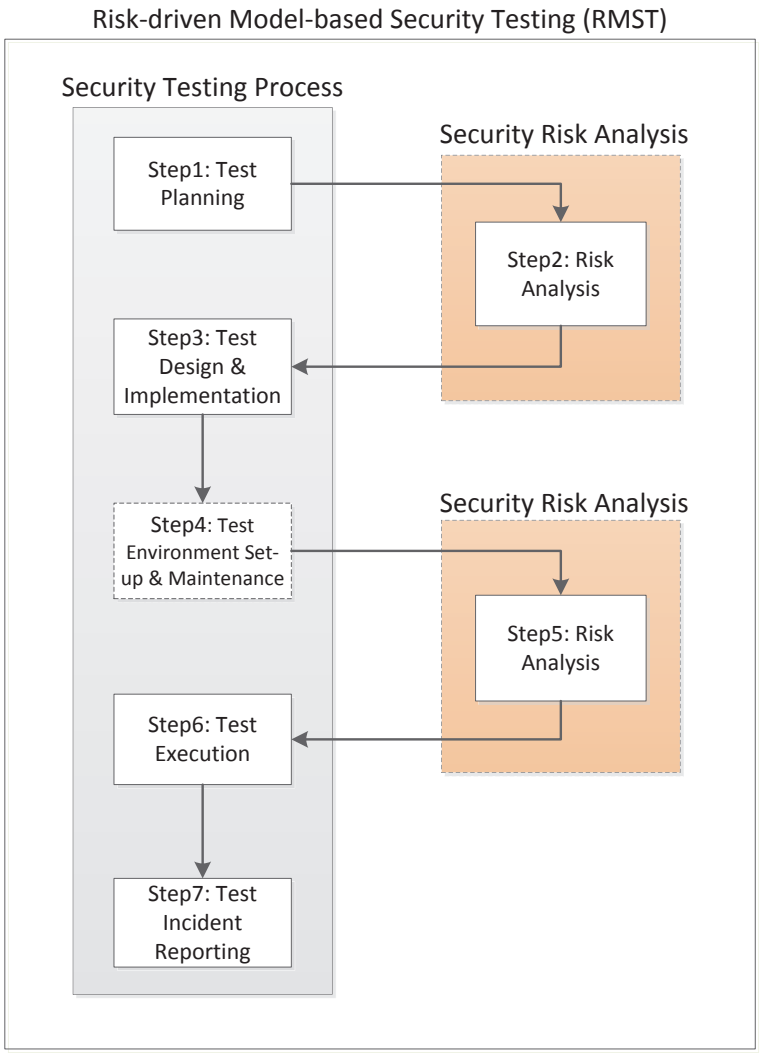

Figure 11: *Risk-driven Model-based Security Testing process.*

- **Risk-driven Model-based Security Testing**

  Risk-driven model-based security testing (RMST) is model-based security testing that use risk analysis within the security testing process.

The security risk analysis process in Step 2 and Step 5 in Figure 11 is equivalent to the security risk analysis process given in Figure 10.
The following describes the steps in the RMST process including the input and output for each step.

Step 1: Test Planning
The purpose of the test planning step is to create a test plan for one run of 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" (see Section 5 for the definition of test plan). The test plan is developed together with the stakeholder and with respect to the stakeholder's test policy, the system model and the features. Based on the test policy, the system model and the features, security test requirements are defined and documented as part of the test plan.

- **Input**: Test policy, system model, feature
- **Output**: Test plan, security test requirement

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, the features and the security test requirements from Step 1 are used as an input to this step. Based on these inputs, risk models are developed in order to identify security risks, and risk criteria are defined in order to estimate, evaluate and prioritize the identified security risks.

- **Input**: System model, feature, security test requirement
- **Output**: Risk model, risk criteria, prioritized security risks with respect to risk criteria

Step 3: Test Design and Implementation
The purpose of this step is to derive test models, tests and test procedures. **First**, the most important parts of the system are identified and prioritized with respect to the prioritized security risks and their underlying risk models obtained in Step 2. **Second**, the test plan is updated according to the prioritized list of the most important parts of the system. **Third**, the test models, tests and test procedures are developed according to the prioritized list of the most important parts of the system. The test models are derived in terms of interaction models with respect to the information gathered from the system model, risk model, features and security test requirements.

Tests are derived from the test models. Test procedures are derived by ordering tests according to dependencies described by pre-conditions and post-conditions within the tests and other security test requirements. A pre-condition is an environmental and state condition which must be fulfilled before a test can be executed with a particular input value (adapted from [11]). A post-condition is the predicted outcome of a test under the specified pre-condition.

- **Input**: Risk model, risk criteria, prioritized security risks with respect to risk criteria, test plan, system model, feature, security test requirement
- **Output**: Test model, test, test procedure

Step 4: Test Environment Set-up and Maintenance
The purpose of this step is to establish and maintain the required test environment. The test environment is set up with respect to the test plan, system model, test model, tests and test procedures. Additionally, maintenance of the test environment may involve changes based on the results of previous tests. Where change and configuration management processes exist, changes to the test environments may be managed using these processes.

- **Input**: Test plan, system model, test model, test, test procedure
- **Output**: Test environment model

Step 5: Risk Analysis
The security risk analysis process in this step is carried out in order to identify security risks explored by the tests. The system model, test model and security test requirements are used as an input to this step. Based on these inputs, risk models are developed in order to identify security risks, and risk criteria are defined in order to estimate, evaluate and prioritize the identified security risks.

- **Input**: System model, test model, security test requirement
- **Output**: Risk model, risk criteria, prioritized security risks with respect to risk criteria

Step 6: Test Execution
The purpose of this step is to execute the tests and the test procedures in the test environment. **First**, the most important tests are identified and prioritized with respect to the prioritized security risks and their underlying risk models obtained in Step 5. **Second**, the test plan is updated according to the prioritized list of the most important tests. **Third**, the tests and the test procedures are executed according to the prioritized list of the most

important tests. The test execution may be iterative according to the complexity, scope, and attribute of the system under test. The test model and test environment model may be used as supporting material while executing the tests.

- **Input**: Risk model, risk criteria, prioritized security risks with respect to risk criteria, test plan, test, test procedure, test model, test environment model
- **Output**: Test result

Step 7: Test Incident Reporting
The purpose of this step is to report security issues requiring further action identified as a result of test execution to the relevant stakeholders. Security test results are documented, analyzed and validated according to system security test requirements. If test execution is carried out iteratively, the test incidents reporting may also be carried out iteratively.

- **Input**: Test result
- **Output**: Test result analysis

References

[1] Information security. http://en.wikipedia.org/wiki/Information_security, last date accessed 17.09.2011.

[2] Model based testing. http://en.wikipedia.org/wiki/Model-based_testing, last date accessed 17.09.2011.

[3] P. Bourque and R. Dupuis. Guide to the software engineering body of knowledge 2004 version. Technical report 19759, IEEE Computer Society, 2004.

[4] The Committee on National Security Systems. *National Information Assurance (IA) Glossary, CNSS Instruction No. 4009*, 2010.

[5] IEEE Computer Society. *IEEE 829 - Standard for Software and System Test Documentation*, 2008.

[6] International Standards Organization. *ISO 27000:2009(E), Information technology - Security techniques - Information security management systems - Overview and vocabulary*, 2009.

[7] International Standards Organization. *ISO 31000:2009(E), Risk management – Principles and guidelines*, 2009.

[8] International Standards Organization. *ISO 29119 Software and system engineering - Software Testing-Part 2 : Test process (draft)*, 2012.

[9] M.S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis: The CORAS Approach*. Springer, 2011.

[10] The Open Group. *The Open Group Architecture Framework Version 9.1*, 2011.

[11] Testing Standards Working Party. *BS 7925-1 Vocabulary of terms in software testing*. 1998.

[12] F. John Reh. Glossary of business management terms and abbreviations. http://management.about.com/cs/generalmanagement/g/objective.htm, last date accessed 19.04.2012.

[13] S. Chao William. *System Analysis and Design: SBC Software Architecture in Practice*. Lambert Academic Publishing, 2009.

Technology for a better society

www.sintef.no