ETSI EG 203 251 V1.1.1 (2016-01)

Methods for Testing & Specification;
Risk-based Security Assessment and Testing Methodologies

Reference

DEG/MTS-203251

Keywords

assurance, security, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document describes a set of methodologies that combine security risk assessment and security testing activities in a systematic manner. This includes both risk assessment aimed to improve security testing and test based activities used to improve the security risk assessment. The methodologies are built upon a collection of consistently aligned activities with associated rules, methods and best practices. The activities are described in such a way that they provide guidance for the relevant actors in security testing and security risk assessment processes (i.e. actors in the role of a security tester, security test manager, and/or risk assessor). The activities and their level of specification are based on standards like ISO 31000 [i.10], IEEE™ 829-2008 [i.6] and ISO 29119 [i.9] so that they apply for a larger number of security testing and risk assessment processes on hand.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Alberts, Christopher & C., J. and Dorofee, Audrey. A. J.: "OCTAVE Threat Profiles". Software Engineering Institute, Carnegie Mellon University, Criteria Version 2.0, Technical report CMU/SEI-2001. http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf-TR-016. ESC-TR-2001-016, 2001.

[i.2] Broy M. and Stølen K.: "Specification and Development of Interactive Systems: Focus on Streams, Interfaces and Refinement". Springer, 2001.

[i.3] ETSI TS 102 165-1 (2011): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.4] Herzog, P.: OSSTMM 2.1. Open-Source Security Testing Methodology Manual; Institute for Security and Open Methodologies, 2003.

[i.5] Howard, M. & Leblanc, D. E.: "Writing Secure Code"; Microsoft Press, 2002.

[i.6] IEEE™ Standard for Software and System Test Documentation (IEEE™ 829-2008), ISBN 978-0-7381-5747-4, 2008.

[i.7] ISO 27000:2009(E): "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary", 2009.

[i.8] ISO/IEC/IEEE™ 29119: "Software and system engineering -- Software Testing -- Part 1: Concepts and definitions", 2012.

[i.9] ISO 29119: "Software and system engineering -- Software Testing -- Part 2: Test process", 2012.

[i.10] ISO 31000:2009(E): "Risk management -- Principles and guidelines", 2009.

[i.11] ISTQB Glossary of testing terms version 3.0.1.

NOTE: Available at http://www.istqb.org/downloads/finish/20/206.html, as of date 29.09.2015.

[i.12] James J. Cebula, L. R. Y.: "A Taxonomy of Operational Cyber Security Risks", Carnegie Mellon, Software Engineering Institute, CERT Program, 2010.

[i.13] Jones, Jack A.: "An Introduction to Factor Analysis of Information Risk (FAIR)".

NOTE: Available at http://riskmanagementinsight.com/media/docs/FAIR_introduction.pdf, as of date 29.09.2015.

[i.14] Masse, T.; O'Neil, S. & Rollins, J.: "The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress", The Department of Homeland Security's Risk Assessment Methodology, 2007.

[i.15] OMG: UML testing profile version 1.1 (formal/2012-04-01).

NOTE: Available at http://www.omg.org/spec/UTP/1.1, as of date 29.09.2015.

[i.16] Souza, E.; Gusmao, C. & Venancio, John Wack, Miles Tracy, M. S.: "Guideline on Network Security Testing -- Recommendations of the National Institute of Standards and Technology"; NIST Special Publication 800-42, 2003.

[i.17] Saitta, P.: Larcom, B. & Eddington, M.: Trike v.1 Methodology Document; 2005.

[i.18] Testing Standards Working Party. BS 7925-1: "Vocabulary of terms in software testing", 1998.

[i.19] Wing, J. M.: "A specifier's introduction to formal methods". IEEE™ Computer 23(9), 8, 10-22, 24, 1990.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

asset: anything that has value to stakeholders, its business operation and their continuity

consequence: outcome of an event affecting objectives [i.10]

event: occurrence or change of a particular set of circumstances [i.10]

likelihood: chance of something happening [i.10]

objective: something the stakeholder is aiming towards or a strategic position it is working to attain

risk: combination of the consequences of an event and the associated likelihood of occurrence (adapted from ISO 31000 [i.10])

risk level: magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood [i.10]

risk source: element which alone or in combination has the intrinsic potential to give rise to risk [i.10]

security requirement: specification of the required security for the system (adopted from [i.18])

security risk: risk caused by a threat exploiting a vulnerability and thereby violating a security requirement

security risk assessment: process of identifying, estimating and evaluating security risks

stakeholder: person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity [i.10]

test case: set of preconditions, inputs (including actions, where applicable), and expected results, developed to determine whether or not the covered part of the *test item* has been implemented correctly

test completion criteria: set of generic and specific conditions, agreed upon with the stakeholders, for permitting a testing process or a testing sub process to be completed

test condition: testable aspect of the test item (i.e. a component or system), such as a function, transaction, feature, quality attribute, or structural element identified as a basis for testing

test coverage item: attribute or combination of attributes to be exercised by a *test case* that is derived from one or more test conditions by using a test design technique

test incident: event occurring during testing that requires investigation (adopted from ISTQB [i.11])

test incident report: detailed description for any unexpected incident or test that failed

test item: work product (e.g. system, software item, requirements document, design specification, user guide) that is an object of testing

test log: recording which tests cases were run, who ran them, in what order, and whether each test passed or failed

test plan: detailed description of test objectives to be achieved and the means and schedule for achieving them, organized to coordinate testing activities for some test item or set of test items

test procedure: sequence of *test cases* in execution order, and any associated actions that may be required to set up the initial preconditions and any wrap up activities post execution

test result: indication of whether or not a specific test case has passed or failed, i.e. if the actual result corresponds to the expected result or if deviations were observed [i.8]

test (design) technique: compilation of activities, concepts, processes, and patterns used to identify *test conditions* for a *test item*, derive corresponding test coverage items, and subsequently derive or select test cases

threat: potential cause of an unwanted incident [i.7]

vulnerability: weakness of an asset or control that can be exploited by a threat [i.7]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CVSS	Common Vulnerability Scoring System
FAIR	Factor Analysis of Information Risk
ISO	International Organization for Standardization
ISTQB	International Software Testing Qualifications Board
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
SQL	Structured Query Language
SRA	Security Risk Analyst
SRAT	Security Risk Assessment Tool
ST	Security Tester
STET	Security Test Execution Tool
STMT	Security Test Management Tool
STST	Security Test Specification Tool
SUT	System Under Test
TM	security Test Manager
TVRA	Threat Vulnerability and Risk Analysis
UML	Unified Model Language
UTP	UML Testing Profile

4 Overview

The present document describes methodologies and their underlying activities that are dedicated to support companies and organizations in undertaking security assessments for large scale, networked systems. The methodologies cover security assessments on different level of abstraction and from different perspectives. Security risk assessment by itself can be applied with different goals in mind. 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, compliance assessment and security testing can be used to actually examine the target under assessment, i.e. an organization or system, for compliance issues or vulnerabilities.

Security testing is considered to discover flaws, vulnerabilities and other technical issues to security by applying test procedures to the actual system under test. In contrast, security risk assessment is meant to analyse potential threats to a system, often on a higher, non-technical level, by especially addressing legal or business related issues. The present document describes the systematic integration of security testing and security risk assessment. Integrating and interweaving the activities from both work streams, thus a systematic integration and completion of risk assessment activities with security testing results or the systematic guidance of security testing by means of risk assessment results, allows for a more precise, focused and dynamic assessment of the security of systems and associated processes.

In the following clauses the integration between security risk assessment and security testing is described in more detail. In clause 5 the overall integration approach is introduced. Clauses 6 and 7 precisely specify the aspects of integration. Clauses 5, 6 and 7 focus on a description on process level that is generic and that is applicable to all system lifecycle phases as well as to all kinds of security testing. Clause 8 shows that application of the integration in the different phases of a system lifecycle. All integration related activities are documented in a similar manner using the template shown in table 1.

Table 1: Template for documenting process activities

Name	The name of the activity
Actors	The actors that are referred to in the activity
Tools	The tools that are involved in the activity
Precondition	The condition that needs to be fulfilled before the activity could be initiated successfully.
Result	Describes the desired results of the activity.
Scenario	The scenario that describes the individual actions taken by the actors
Data exchanged/ processed	The data that are exchanged during the integration use case: **In:** *The data that go into the activity. Terms from the conceptual model are used to describe the data.* **Out:** *The data that are the outcome of the activity. Terms from the conceptual model are used to describe the data.*

The possible actors and tools that can be referred to are described as follows:

Actors:

- **Security Risk Analyst (SRA):** The person responsible for doing the security risk assessment.
- **Security Test Manager (TM):** The person responsible for doing the security test management.
- **Security Tester (ST):** The person responsible for doing the security testing.

Tools:

- **Security Risk Assessment Tool (SRAT):** The tool that supports the security risk assessment.
- **Security Test Management Tool (STMT):** The tool that supports the security test management.
- **Security Test Specification Tool (STST):** The tool that supports the security test specification.
- **Security Test Execution Tool (STET):** The tool that supports the execution of test procedures and test cases.

The methodologies and activities have been developed and evaluated in the RASEN research project (www.rasenproject.eu).

5 Integration outline

5.1 Security risk assessment

Security risk assessment is an iterative process that analyses the potential threats to a system in order analyse their impact and to estimate the likelihood of their occurrence. The risk assessment comprises the identification of assets, threats and vulnerabilities as well as the identification, specification and realization of risk treatments (i.e. security controls and other countermeasures). Risk itself is a metric that relates the frequency and/or likelihood of unwanted incidents to their impact.

From a process point of view risk assessment is considered as the overall process of risk identification, risk estimation and risk evaluation.

- Risk identification is a set of activities dedicated to 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 stakeholders' needs. It typically comprises a threat analysis as well as a vulnerability analysis.
- Risk estimation is the process of determining the level of risk. This involves developing an understanding of the nature of a risk, its sources and its consequences.
- 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 and on the most appropriate risk treatment strategies and methods.

Currently there is a larger number of security risk assessment methods like ETSI TVRA [i.3], CVSS [i.14], STRIDE/DREAD [i.5], OCTAVE [i.1], FAIR [i.13] and Trike [i.17], which provide dedicated guidance on how to identify the sources of risks, their causes and their potential consequences within different contexts and with different strategies. Their main purpose is to provide systematic guidance and the definition of a consistent and unambiguous vocabulary for risk identification and handling. Security risk assessment can be qualitative or quantitative as well as informal (check-list based) or formal (model-based). Qualitative risk assessment is based on qualitative risk and quantitative risk assessment is based on some quantities, numbers, or measurements. In model-based security risk assessment, the security risk assessment is conducted with a language for the documentation of assessment results and a clearly defined process for conducting the assessment. In this regard the Carnegie Mellon University's Computer Emergency Response Team provides a taxonomy on operational cyber security risks [i.12]. The taxonomy identifies sources of operational cyber security risks and separates them into four classes. It distinguishes between risks caused by actions of people, by systems and technology failures, by failed internal processes, or by external events. Each class is broken down into further subclasses, which are described by individual elements (e.g. "actions of people" is subdivided into "Inadvertent Actions", "Deliberate Actions" and "Inaction"). The Factor Analysis of Information Risk (FAIR) [i.13] provides an information security risk taxonomy, which is comprised of two main branches according to the FAIR's overall risk definition "Risk = Loss Event Occurrence and Probable Loss Magnitude". The OCTAVE method defines the main tasks during risk assessment with threats identification, security measures identifications, definition of business impacts, and the definition of security measures' costs and their standardized values. A step by step approach eases the estimations on the individual risk factors. It starts with the definition of asset-based threat profiles. In this phase the members of an organization identify important information assets, the threats to those assets and the security requirements of the assets. A second phase targets the identification of infrastructure vulnerabilities. Especially the information technology infrastructure is examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action. The last phase is dedicated to the development of a security strategy. The information generated by the organizational and information infrastructure evaluations are carefully analysed to identify risks to the organization and to the organization's mission as well as to identify countermeasures.

5.2 Security testing

The term security testing or software security testing designates activities that check the security properties of software. While a number of approaches have long been around targeting specific attacks on systems (e.g. vulnerability scanners), more systematic security testing of systems with respect to specified policies or security properties are a relatively new approach that has started to be addressed since around the year 2000. In general the software security testing activities can be divided into functional security testing, robustness testing, performance testing and penetration testing. While functional security testing, robustness testing and performance testing are used to check the functionality, availability, and efficiency of the specified and carefully planned security functionalities and systems (e.g. firewalls, authentication and authorization subsystems, access control), penetration testing or security vulnerability testing directly addresses the identification and discovery of system vulnerabilities undiscovered until a given point in time and caused by security design flaws. These kind of tests analyse systems for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. Penetration test objectives are to determine feasibility of an attack and the impact of a successful exploit.

5.3 Combining the security testing and security risk assessment workstreams

The overall process of a combined security assessment is derived from ISO 31000 [i.10] and slightly extended to highlight the identification and evaluation of compliance and quality issues as one of the major tasks that need to be carefully aligned with typical risk assessment activities. It is defined independent of any application domain and independent from the level, target or depth of the security assessment. It can be applied to legal risk and compliance assessment as well as for any kind of technical security assessment and testing processes.

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*" 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 fixed. The latter phase is meant to analyse and document the technical context of the target under assessment. 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 information for the combined security assessment and are considered to be common for security risk assessment workstream as .well as for the test-based risk assessment workstream.

The main part, namely the "*Security Assessment*", covers the integration between the risk assessment workstream and a security testing workstream. It consists of a combination of typical security risk assessment activities that are defined in ISO 31000 [i.10] and typical security testing activities that follow testing standards like ISO 29119 [i.9].

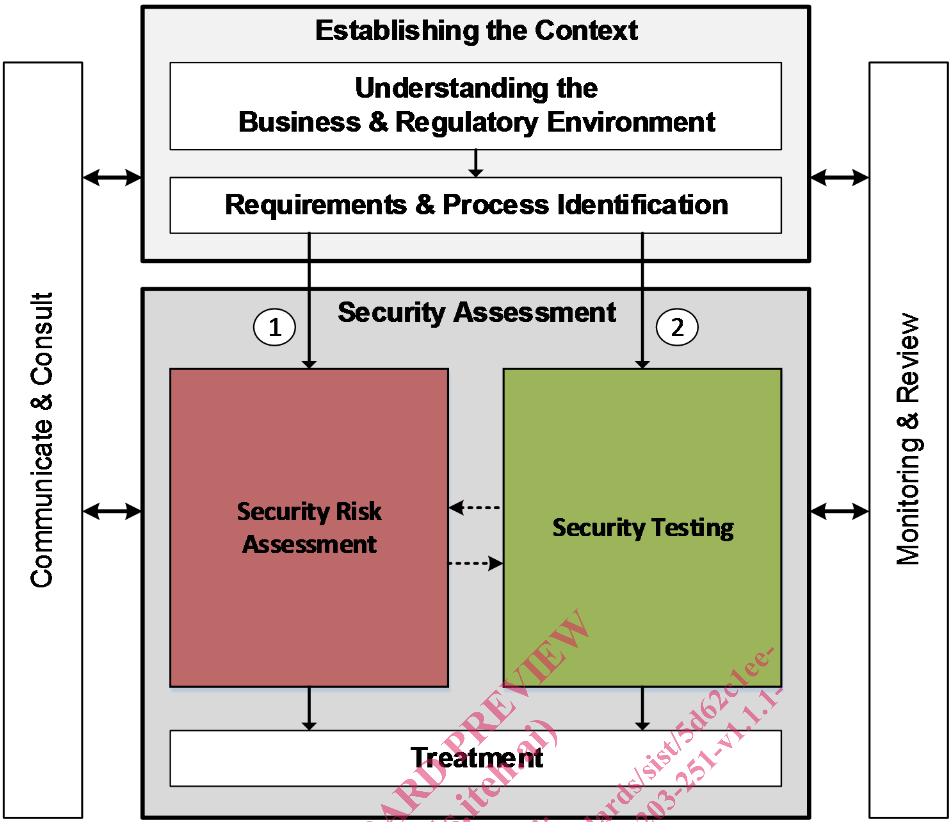

Figure 1: Main activities of a combined risk assessment and security testing process

The present document distinguishes two main perspectives, each represented by a set of activities that are combined to form a workstream carried out during system development or operation.

1) A test-based security risk assessment workstream should start like a typical risk assessment workstream and should 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 to adjust risk values 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 analysis.

2) The risk-based security testing workstream should start like a typical testing workstream and uses risk assessment results to guide and focus the testing. Such a workstream should start 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.