ISSN: 2230-9926

INTERNATIONAL JOURNAL OF DEVELOPMENT RESEARCH

Vol.6, Issue 09, September - 2014

IMPACT FACTOR / INDEXING JOURNAL

Available online at http://www.journalijdr.com

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 4, Issue, 9, pp. 1799-1801, September, 2014

Full Length Research Article

EMPIRICAL STUDY ON RISK ANALYSIS IN SECURITY TESTING

***Maragathavalli, P. and Dr. Kanmani, S.**

Department of Information Technology, Pondicherry Engineering College, Puducherry

ARTICLE INFO

Article History:
Received 12th June, 2014
Received in revised form
07th July, 2014
Accepted 21st August, 2014
Published online 30th September, 2014

Key words:
Risk analysis,
Risk-driven,
Test-driven,
Security testing,
Risk-based testing

ABSTRACT

Testing is the process of detecting errors present in a system with the given sample input. Risk is the vulnerability associated with the system and the type of testing which uncovers it is called security testing. Risk analysis is the process of determining the level of risk with the available information. Risk-based testing comprises of risk analysis, which is a part of model based testing and involves risk assessment. Risk analysis and security testing can be combined in two ways namely: Risk-driven Security Testing (RST) and Test-driven Security Risk (TSR) analysis. In RST, security testing is supported by risk analysis to make it more effective. The testing is focused on the most important parts of the system which is identified by the risk analysis results. In TSR, security testing develops or validates risk analysis. TSR focuses to strengthen the correctness of risk analysis models. The gap between high-level security risk analysis models and low-level security test cases can be easily addressed by both TSR and RST approaches.

INTRODUCTION

Testing is the process of analyzing the result of a system for particular test data. Testing result may identify the errors present in system functionalities. But the risk associated with the system can also make a system defective and the type of testing which helps to identify the defects and minimize them is known as security testing. Risk is the possibility of attack to a system and the process of determining the vulnerabilities present is called Risk analysis. In order to make a system less vulnerable to the risks, security testing and risk analysis is combined into two approaches namely: Risk-Driven Security

Testing (RST) and Test-Driven Security Risk Analysis (TSR). RST is a part of Risk-based testing which uses risk analysis results for test case identification and selection for optimizing the test process (Ina Schieferdecker *et al*., 2011). It bridges the hierarchy between risk analysis and security testing since the essential risk factors might be missed if risk analysis remains at a high level (Jan Stijohann and Jorge Cuellar, 2013). TSR focuses mainly on risk analysis where testing process is carried out to validate risk models. Figure 1 shows the design of RST. RST is defined as Model-Based Security Testing (MBST) that uses risk analysis within the security testing process (Yan, 212). MBST is a special form of Model- based testing (MBT) (Tim Miller and Paul Strooper, 2007) that focuses on the testing of security properties of a system (Jurgen Grobmann *et al*., 2013).

The first two steps deals with the identification of test objectives and model. It is followed by Risk assessment which identifies the risk associated with the system. The result from the risk assessment is used for test case generation and prioritization. It is again subjected to risk assessment and the significant test cases are executed. Figure 2 shows the design of TSR. In TSR, risk analysis is supported by security testing in order to develop or validate risk models. The first step is to find the target system for risk analysis. It is followed by test case generation and execution for the development of risk models by identifying potential risks which is subjected to risk assessment. The testing process is again repeated to validate risk models which are then subjected to risk treatment.

Literature Survey

Table 1 describes about the survey on risk analysis in security testing and its role in various Risk-Based Testing approaches.

****Corresponding author: Maragathavalli, P.***
Assistant Professor, Department of Information Technology, Pondicherry Engineering College, Puducherry

Table 1. Study on Risk-based Security Testing

S. no.	Title	Year	Techniques	Description of the Technique	Metrics	Systems/ Models used
1	Risk-driven Security Testing versus Test-driven Security Risk Analysis	Feb 15, 2012	Risk-driven security testing and Test-driven security risk analysis	In RST security testing is supported by security risk assessment in order to make security testing more effective. The aim is to focus the security testing process to carry out security tests on the most important parts of the system under test, and to execute only the most important security test cases. In TSR security risk analysis is supported by security testing in order to develop and/or validate risk models. The aim is to strengthen the correctness of the security risk analysis models.	Confidentiality , Integrity, Availability and Accountability.	Industrial Case Study.
2	Baseline for Compositional Test-Based Security Risk Assessment	Jan 31, 2013	Table based risk assessment technique	This approach mainly focuses on verifying risk mitigations and providing a clear traceability between risk-related requirements and the test cases. The table consists of a description of the risk related requirement, the risk, the risk level, the risk mitigation and identifiers for the test cases that have the objective to verify the risk mitigation.	Risk identification, Risk Analysis, Risk Evaluation and Risk Treatment	Common Vulnerability Scoring system
3	Baseline for Compositional Risk-Based Security Testing	Jan 31, 2013	Risk-based vulnerability testing	The objectives of this paper are: • To use techniques addressing both risk-based test identification and test prioritization to drive the overall testing generation process. For this purpose, CORAS capabilities are extended to allow the guidance of security test generation techniques on the basis of risk assessment results. • To drive model-based testing generation using risk assessment results in order to generate vulnerability test purposes and test cases. This novel approach is called risk-based vulnerability testing (RBVT). • To drive behavioural fuzzing testing approaches using models annotated by security information coming from risk assessment results. This novel approach is called risk-based fuzzing. • To define a dedicated methodology for security testing metrics and to elaborate a dashboard for presenting the security testing results based on risk assessment.	Severity, Testability, Uncertainty, reusability	Scalable network system
4	Risk-based Statistical Testing: A Refinement based Approach to the Reliability Analysis of Safety-Critical Systems	May 2009	Model-based statistical testing, Markov chain test models	In this paper, a method is presented that allows to automatically generate test cases for risk-based testing of safety critical systems and it utilizes Model-based Statistical Testing which uses Markov chain test models to describe the stimulation and usage profile of the system under test (SUT). Our goal is the generation of test cases that trigger a certain critical situation. These test cases are called critical test Cases.	Safety Integrity Level (SIL)	Critical systems like fire alarm, railway control system
5	Effort-dependent technologies for multi-domain risk-based security testing	Sept 27, 2010	Light weight risk and security testing	The system model is used to generate traces or test cases for implementation, according to a test case specification. It is a selection criterion on the set of the traces of the model. The risk analysis, which is conducted on the basis of the system model, is used to define the appropriate test case specifications.	Proof-of-Performance, Proof-of-Concept, Proof-of-Existence	Security Audit of Supplier services, Maintaining security in virtual organization.

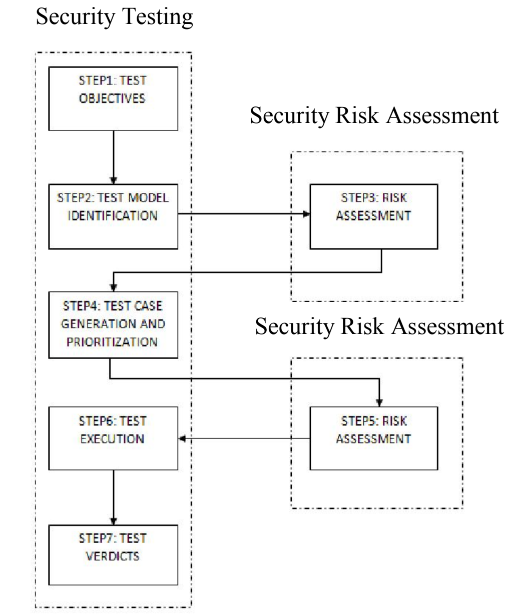

Figure 1. Risk-Driven Security Testing (RST)

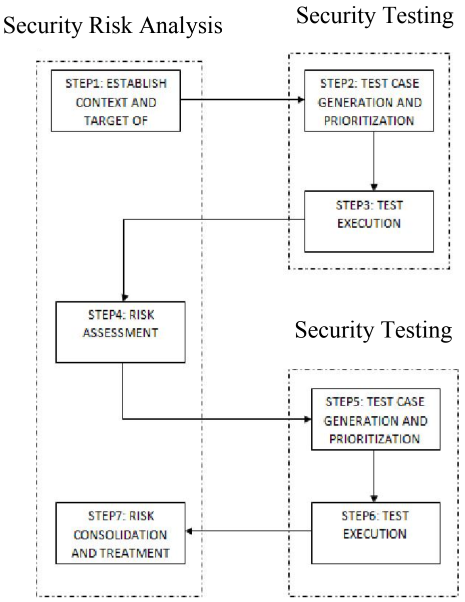
Security Risk Analysis
Security Testing
STEP1: ESTABLISH CONTEXT AND TARGET OF
STEP2: TEST CASE GENERATION AND PRIORITIZATION
STEP3: TEST EXECUTION
STEP4: RISK ASSESSMENT
Security Testing
STEP5: TEST CASE GENERATION AND PRIORITIZATION
STEP6: TEST EXECUTION
STEP7: RISK CONSOLIDATION AND TREATMENT

Figure 2. Test-Driven Security Risk Analysis (TSR)

Conclusion

Risk analysis and security testing led to two approaches namely Test-driven security risk analysis and Risk-driven security testing where risk analysis is used to improve testing results and vice versa. It also addresses the problem of gap between high-level security risk analysis models and low-level security test cases. From the above survey a clear idea about RST and TSR and their areas of application are obtained. In future, a quantitative analysis on risks present in system can be made with parameters namely risk possibility, risk threshold, risk impact, severity and complexity and the technical and non-technical threats can also be considered to improve testing results effectively.

REFERENCES

Ina Schieferdecker, Jurgen Grobmann, Axel Rennoch Fraunhofer: “Model Based Security Testing Selected Considerations”*, Berlin*, 2011, PP. 1-19.

Jan Stijohann and Jorge Cuellar: “Towards a Systematic Identification of Security Tests Based on Security Risk Analysis” , *Siemens AG, Germany*, 2013, PP. 1-6.

Jurgen Grobmann, Toblas Mahler, Fredrik Seehusen, Bjonar Solhaug: “Baseline Methodologies for Legal, Compositional and Continuous Risk Assessment and Security Testing”, *RASEN Baseline,* 2013, PP. 1-41.

Tim Miller and Paul Strooper: “A case study in model-based testing of specifications and implementations”*, Software testing, Verification and reliability Published online in Wiley Inter Science,* 2007, PP. 1-40.

Yan Li: “Conceptual Framework for Security Testing, Security Risk Analysis and their Combinations”, *System Testing and Validation,* 2012, PP. 1-5.

****

INTERNATIONAL JOURNAL OF

DEVELOPMENT RESEARCH