
Li, Yan
Contents

- Introduction
- Basic concepts
- The combinations of security testing and security risk analysis
- Conclusion
Introduction

• Motivation
  • Risk analysis and testing are conducted for different purpose
  • In the case of risk analysis, the aim is to fulfil the risk evaluation criteria
  • In the case of testing, the aim is to fulfil the test objectives
  • One may therefore argue that there are basically two main strategies for the combined use of risk analysis and testing
    – Risk-driven model-based security testing (RMST)
    – Test-driven model-based security risk analysis (TMSR)

• Approach
  – Conceptual framework based on state-of-the-art standards
  – Highlight model based approaches
  – Combine security testing and security risk analysis
Basic Concepts-Security Testing

- **Security:**
  The preservation of confidentiality, integrity and availability of information [ISO 27000].

- **Testing:**
  The process of exercising the system to verify that it satisfies specified requirements and to detect errors [ISO 29119].

- **Security testing:**
  The process of testing specialized towards security.
Basic Concepts-Security Risk Analysis

- **Risk analysis**: A collective term defining the process consisting of the following steps: establishing the context, risk identification, risk estimation, risk evaluation and risk treatment [ISO 31000, CORAS].

- **Security risk analysis**: The process of risk analysis specialized towards security.
MST & MSR & The Combinations

**Model-based Security Testing (MST)**
Security testing that involves the construction and analysis of a system model, a test model and a test environment model to derive test cases.

**Model-based Security Risk analysis (MSR)**
Security risk analysis in which every step of the process includes the construction and analysis of models.

**Risk-driven model-based security testing (RMST)**
Model-based security testing that uses risk analysis within the security testing process.

**Test-driven model-based risk analysis (TMSR)**
Model-based security risk analysis that uses testing within the security risk analysis process.
Model-based security testing that uses risk analysis within the security testing process.

Model-based security risk analysis that uses testing within the security risk analysis process.
Risk-driven Mode-based Security Testing (RMST)

Inputs: Test policy, Security test requirements
Output: Test plan, System model

Output: Test model, Test case, Test procedure

Output: Test environment model

Output: Test result

Output: Test result analysis

Risk-driven Model-based Security Testing (RMST)

Security Testing Process

- Step 1: Test Planning
- Step 3: Test Design & Implementation
- Step 4: Test Environment Set-up & Maintenance
- Step 6: Test Execution
- Step 7: Test Incident Reporting

Security Risk Analysis

- Step 2: Risk Analysis
- Step 5: Risk Analysis

Output: Risk model, Risk criteria, Prioritized security risks

Output: Risk model, Risk criteria, Prioritized risk

Technology for a better society
Test-driven Model-based Security Risk analysis (TMSR)

**Inputs:** Objective, Security requirements
**Output:** Assets, Risk criteria, System model

**Output:** Incomplete risk model

**Output:** Risk model

**Output:** Prioritized risk

**Output:** Treatment, Updated risk model
Related work

• We have conducted a systematic literature review, identifying 31 papers on approaches that combine risk analysis and testing.

• As a conclusion, we may say that the distinction between risk based testing (RT) and test based risk analysis (TR) is not clearly presented in most of these papers.

• Furthermore
  • Only 2 papers address security.
  • Only 9 papers address modeling explicitly.
Conclusion

• I have clearly distinguished between
  • Risk-based Model-driven Security Testing (RMST)
  • Test-based Model-driven Security Risk analysis (TMSR)

• Based on the systematic literature review, I have argued that this distinction is hardly present in existing approaches combining risk analysis and testing
  • Future work
    – Development of specialized methodologies for RMST and TMST
    – Our research will be driven by industrial case studies

• Full technical report http://heim.ifi.uio.no/~ketils/kst/Reports/2012.SINTEF-A22798.pdf
Thank you!