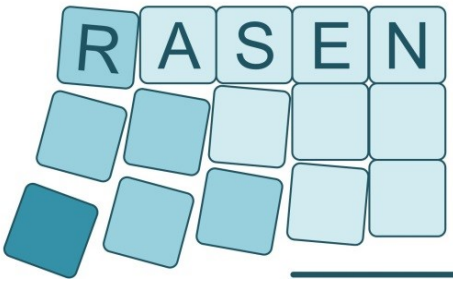

Compositional Risk Assessment and Security Testing of Networked Systems

The RACOMAT Tool

Risk Assessment COMbined with Automated Testing

Johannes Viehmann
Fraunhofer FOKUS

The RACOMAT tool allows users to combine component based security risk assessment with security testing. Testing can be integrated seamlessly into the incident simulations the tool uses for its compositional risk analysis. Taking benefit of libraries containing risk analysis artefacts like attack patterns and of libraries containing testing artefacts like security test patterns, the RACOMAT tool offers a high level of reusability. Using the assistance the tool offers, many steps of the analytical RACOMAT process form risk modelling to testing and updating the risk picture based on test results can be done automatically.

Security critical systems should be carefully analyzed with the help of well-known concepts like risk assessment (ISO31000[1]) and security testing (ISO 29119[2]). Especially for large scale systems, risk assessment and security testing might be difficult and expensive.

Reusing already created artefacts in combination with automation might help to minimize costs. It also might help to reduce the dependency on the expertise, skills and accuracy of the analysts. Hence, it might help to reduce human errors in the entire risk assessment and security testing process.

In fact, security testing itself can be seen as one possible way to make risk assessment more objective and more precise. There are other concepts and technologies which could be applied for the same purpose, including but not limited to formal verification, static analysis and simulation. While formal verification might be hard or infeasible for complex large scale systems and while testing might be expensive for such cases, simulations are probably most appropriate to deal with exactly those large systems and they could help to overcome scaling problems.

The RACOMAT process

If this observation is correct, then it makes eventually sense to use both simulation and testing technologies together in order to refine the risk assessment of systems which cannot be tested entirely. Combining simulation and security testing might lead to concepts for their integration into a new kind of risk assessment process. These basic ideas inspired the development of the RACOMAT process and of the RACOMAT tool.

The RACOMAT process integrates security testing tightly into incident simulations of a low level compositional security risk assessment. It basically unifies risk-based security testing (RBST, which tries to optimize the security testing process with the help of risk assessment) and test-based risk assessment (TBRA, which tries to improve the risk picture using test results).

This iterative process is designed to test exactly the most critical part with reasonable effort while other parts are simulated. The incident simulation itself is actually a kind of testing, too, but it is testing the risk model instead of testing the real system that is analyzed.

[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

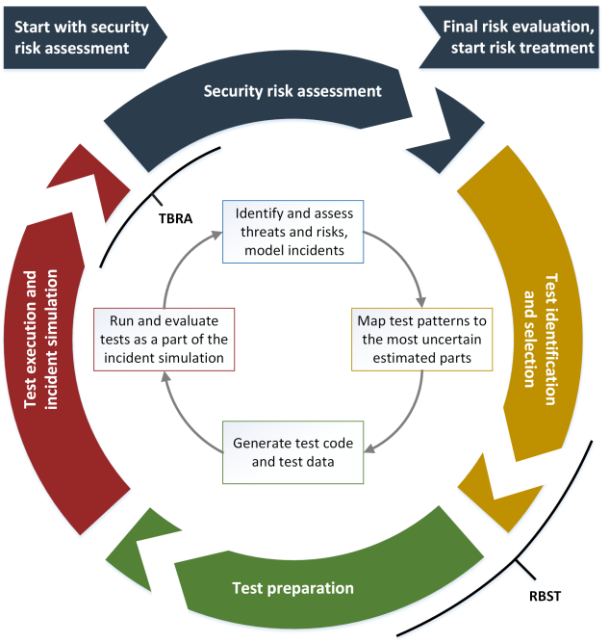

Figure 1 The RACOMAT process

The risk picture is improved with objective test and simulation results. Then the process continues with testing the next most critical part while the already tested parts are only simulated based on previous observations.

The RACOMAT tool

Initial assessment and analysis

In spite of relying upon a specific risk assessment method, the RACOMAT tool can use different kinds of risk assessment methods, including fault tree analysis (FTA), event tree analysis (ETA) and the CORAS method, as proposed within the RASEN project. In general, the RACOMAT tool supports component based risk analysis and compositionality. The RACOMAT tool uses intuitive risk graphs to represent and to visualize the risk picture.

For enabling automation of risk based testing, the risk assessment must be made on a low level. The RACOMAT tool allows risk analysts to model close relations to parts and components of the systems that are analyzed. Therefore, the RACOMAT tool introduces the concept of threat interfaces representing entire components and threat ports representing parts of the input / output interface.

In order to reduce the manual effort of low level system analysis, the RACOMAT tool integrates techniques for analyzing components automatically. Given (X)HTML pages, source code, compiled programs or listening to common network protocols, it tries to identify the public interfaces of any components and especially the functions as well as ports that could be used for interaction with other components or users. Thereby, an initial system model can be generated without requiring a lot of manual actions.

Since low level risk assessment for large scale systems could be very difficult and expensive, reusability of existing artefacts is a vital part of the RACOMAT tool. The RACOMAT tool assists the risk analysts by suggesting lists of common weaknesses or vulnerabilities, attack patterns, unwanted incidents and treatments. The assistants take advantage of existing risk related libraries like MITRE CAPEC and CWE or BSI IT-Grundschutz. The elements of such catalogues already contain vital information for example about typical likelihoods or potential consequences.

For identified threat interfaces and threat ports, the RACOMAT tool displays only subsets of the large existing risk catalogues that might be relevant especially for the analyzed parts of the system. The component based approach in combination with preselected subsets of libraries of existing risk analysis artefacts like attack patterns can make the analyst's life way simpler. For some common types of components, the RACOMAT method suggests using entire predefined threat interfaces that do not require any further work.

Using the RACOMAT tool, the task of the analysts is not to find the relevant risk artefacts. It is rather to exclude the non-relevant artefacts. This assisted "negative", excluding risk assessment technique is somehow similar to check lists, limiting the chance that relevant aspects are simply overlooked.

Dependencies and incident Simulations

In the RACOMAT tool risk artefacts are added with simple drag and drop. Thereby, they can be immediately linked with the elements of the automatically generated system models.

For most common artefacts, the RACOMAT tool already suggests other typically related artefacts. For instance, a vulnerability might typically be used by attackers to do a certain kind of an attack. The related attack pattern again typically can be used to produce several incidents. The RACOMAT tool does not only present the related elements, but it

also models the correct dependency relations automatically if the related artefacts are added to the risk graph.

With the RACOMAT tool, it is especially possible to model dependencies between events (faults, incidents) precisely. The RACOMAT tool offers directed weighted relations and gates that can be used to express how base incidents might trigger dependent incidents.

The initial risk assessment has to be performed until it results in a risk graph with dependencies between the events and likelihood notations at least for the occurrence of independent incidents. Such a risk graph can already be used to calculate dependent likelihoods.

One possible method for calculating even dynamically changing likelihoods for incidents of complex systems is to use Monte Carlo simulations. The idea is basically to test the risk model for the occurrence of incidents using random distributed values and evaluating the modeled dependencies and the likelihood estimates for base incidents. Such simulations using simplified models are applicable to analyze even complex dynamically changing systems for which calculating precise likelihood values would be too difficult.

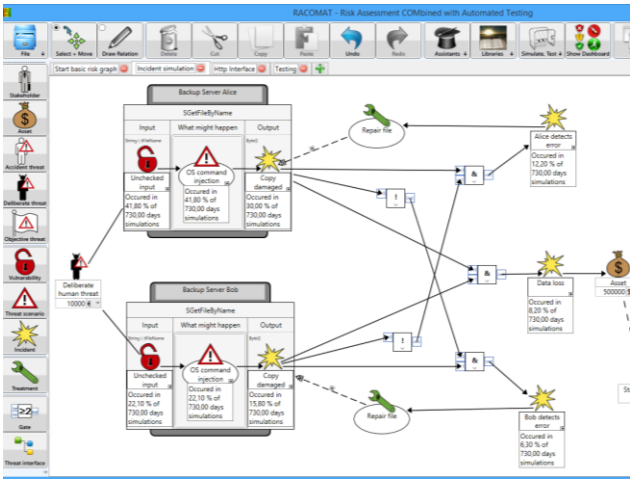

Figure 2 Incident simulation in the RACOMAT tool

The RACOMAT tool supports Monte Carlo simulations in order to calculate likelihoods for dependent incidents. Even simulations in risk graphs with cycles are supported, e.g. to model self-repairing features. However, for cyclic graphs, a delayed incident propagation has to be determined manually for at least one relation per cycle.

A high level of automation, composition with reusable components and incident simulations make the RACOMAT tool applicable for complex large scale systems.

Testing

Results of any calculation for dependent likelihood values will only be as good as the model and the estimates the calculation is based upon.

The idea to improve the risk picture and to reduce the dependency on the initial modelling and estimations is to replace some parts of the simulation with testing the real system components. That is, instead of simulating whether some event occurred based upon random values and likelihood functions, the RACOMAT tool tries to actually trigger the real incident.

The RACOMAT tool can identify the not yet tested element that has the greatest impact on the overall risk picture or which has the most uncertain likelihood estimate based on the analysts judgement. This element (typically an attack pattern) should probably be tested in the first place.

Automated or at least semi-automated testing is done with the help of test patterns. The RACOMAT tool provides an extendable catalogue of security test patterns for most common attack patterns.

Existing security test patterns are automatically associated with risk analysis artefacts as well as system model components (e.g. input and output ports). If no appropriate test patterns exist in the library, the RACOMAT tool allows its users to create new reusable test patterns within the tool. Given an appropriate test pattern, test generation, execution and result aggregation are at least semi-automated. But for example for overflow tests, even complete automation is achievable.

Eventually, it might be necessary to generate some base incidents during for running the tests. Therefore, the RACOMAT tool uses the concept of incident stubs. These stubs are small programs that create the required incidents juts for testing purpose so that they can trigger the real system under test.

As test results, the RACOMAT tool yields which incidents have occurred. Hence, it is possible to directly transfer the occurrence states of those incidents that are already modeled in the risk graph back into the incident simulation. Note that there might also occur incidents that have not yet been modeled in the risk graph. Such unexpected test results can be introduced into the risk graph by drag and drop.

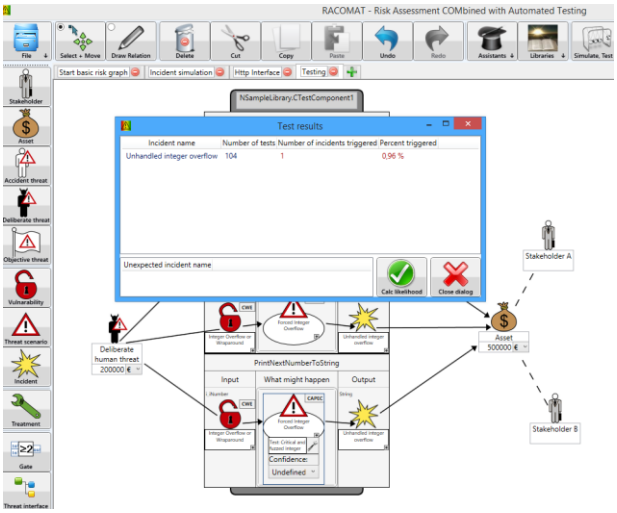

Figure 3 Testing in the RACOMAT tool

All test and simulation results can be used to update the risk graph with interpolated likelihood values or with more complex likelihood functions which approximate the observed behavior. The RACOMAT tool provides a catalogue of common security testing metrics for that interpolation. These metrics include simple coverage metrics, but also advanced metrics that take economic aspects into account, for example. Nevertheless, users may also create their own metrics. The test- and simulation-based likelihood values or likelihood functions can then be used within future simulation runs to imitate the already tested components accurately.

Integrating security tests into incident simulations, the RACOMAT tool offers an innovative compelling concept to update risk models based on test results.

The iterative RACOMAT process continues eventually by analyzing the next most uncertain asserted component with testing the corresponding real component in the next updated incident simulation.

Finishing the RACOMAT process

If all components have been tested or if the testing budget is used up, then the latest risk picture becomes the final test-based risk assessment result. Further risk management might continue with additional evaluation of the results and with risk treatment. The RACOMAT tool supports these steps with Dashboard overviews of the final risk picture and capabilities for managing the risk treatment process.

Interaction with Other Tools

The RACOMAT tool can be used as a stand-alone tool. It covers the entire process of combined test-based risk assessment (TBRA) and risk-based security testing (RBST). Nevertheless, it is also possible to use other eventually more specialized tools for some steps in that process. In particular, the RACOMAT tool can be used in conjunction with the other tools developed and used within the RASEN project. Since the RACOMAT tool supports the entire process, it makes sense to use the RACOMAT tool as the central platform for the data exchange and for any other interaction between the tools. Figure 2 illustrates how such a risk assessment and security testing process using the RACOMAT tool as central platform and different tools for some sub tasks could work.

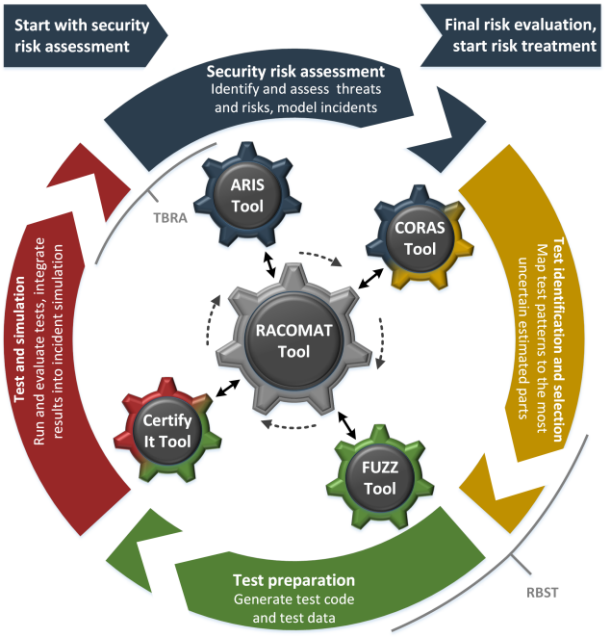

Figure 4 The RACOMAT process with various tools

Conclusion and ongoing work

The RASEN project envisions the overall integration of test-based risk assessment and risk-based security testing. The RACOMAT tool itself integrates the entire RBST and TBRA process. The tool is applied within the project case studies. Besides being a stand-alone tool, it can also be used as a central integration platform in combination with other tools.

With its unique concept of treating security tests as a part of an incident simulation that is based upon a risk model like a fault tree, the RACOMAT tool provides especially a natural understanding of how the test results should be interpreted in order to update the risk picture.

In the future, it will be possible to share security test patterns, security testing metrics, threat interfaces and other artefacts with other users.

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. The RACOMAT tool is one of the major innovations of the project.

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