RASEN Compositional Risk Assessment and Security Testing of Networked Systems

Compositional Risk Assessment – Managing the Complexity of Large-Scale Systems

Atle Refsdal[a], Bjørnar Solhaug[a] and Ketil Stølen[a,b]
[a]SINTEF ICT, [b]Dep. of Informatics, Univ. of Oslo

Traditional methods for risk assessment are not well-equipped to tackle the complexity of large-scale, networked systems. The RASEN project proposes a novel divide-and-conquer strategy by means of compositional risk assessment.

In the information society of today the availability and protection of information and services are ever more important. A wide range of stakeholders, including enterprises, governments and citizens, depend on the reliable functioning of information systems and services on a daily basis. In fact, managing risk is of such importance that in many cases, laws and regulations impose explicit requirements on the performance, scope and frequency of risk analysis[1]. For example, this is the case for organizations that are responsible for parts of critical infrastructures, such as banking, transport, telecom, other critical ICT functions, power supply, and water supply. Non-compliance may have severe consequences for an organization, such as a costly fine or even loss of the license to operate. In a survey[2] conducted by Economist Intelligence Unit for KPMG in 2011, 55% of the respondents stated that the annual cost of GRC (Governance, Risk and Compliance) activities was between 1% and 5% of annual revenues.

For most organizations, risk management[3] is an indispensable part of the overall management process, the objective of which is to systematically and proactively identify the current risk picture and to ensure that the necessary controls are in place to maintain risks at an acceptable level. For this purpose, adequate and efficient methods and techniques for risk assessment are required. However, information systems and services become increasingly complex, heterogeneous, dynamic and interoperable. This is in particular the case for information and services that are provided over the Internet, with cloud services as a prominent example. Managing risks in such a setting is extremely challenging, and established methods and techniques are often inadequate. A main problem is that the overall risk picture becomes too complex to understand, and that the risks quickly and continuously change and evolve.

In the RASEN project we address this challenge by developing a novel approach to so-called compositional risk assessment. Following a divide-and-conquer strategy we aim for an approach to risk management where separate parts or aspects of a system or organization can be analyzed separately. Compositional techniques should then enable a systematic and sound composition of the individual risk models in order to derive the combined result. An important feature of our approach is that the risk model composition shall be conducted without having to reconsider or investigate the

[1] The following are a few examples from Norwegian laws and regulations: "Forskrift om IKT-systemer i banker mv" (§ 3), "Energiloven" (§ 9-3), and "Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen" (§ 2-4).

[2] The Convergence Evolution. Global survey into the integration of governance, risk and compliance. KPMG (2012)

[3] International Organization for Standardization. ISO 31000 Risk management – Principles and guidelines (2009)

internal details of the individual risk models. The latter is supported by our principle of risk model encapsulation, which involves hiding the internal details. Only the information that is required for a sound composition is visible via a well-defined risk model interface.

The RASEN project is conducted in close collaboration between research and industry. Targeting the specific industrial needs regarding how to manage security and risks of networked, large-scale and complex systems, our approach to compositional risk assessment has several advantages. First, for systems or organizations that are to be analyzed from scratch, a compositional approach allows the analysis to be split-up top-down in manageable chunks in such a way that the details of each individual analysis do not have to be reconsidered when the individual results are aggregated back into an overall risk model for the system or organization as a whole. Second, when there already are several risk analyses of different parts or aspects of some system or organization available, a compositional approach enables the overall risk picture to be derived bottom-up without re-analyzing what has already been analyzed. Third, if the target of one individual analysis, such as a component or a service, is reused in another context, also the risk analysis for the target in question should be reusable in the new context. Fourth, when a system changes due to replacement or introduction of new parts, we should be able to deduce the risk level by re-analyzing only the modified parts.

Motivating Examples

Irrespective of whether an organization has regulatory obligations with respect to risk management or not, in practice there will always be a need for risk management. Today almost all enterprises and organizations are exposed to many different kinds of risk, including security risk, operational risk, safety risk, and so on. The risk picture to which they are exposed will typically be highly complex and continuously changing. The ability to survive in a competitive market and a regulatory environment seems to be highly dependent on the ability of an enterprise or organization to deal with risk. In order to make good decisions, managers on all levels need at all times a thorough understanding of the current risk picture related to their domain of responsibility. However, obtaining such an understanding is extremely difficult and requires extensive effort and resources. The following two examples highlight this.

Example 1: A risk consultancy company has been contacted by a large bank. Before contacting the consultancy company, the bank has carried out a number of security risk analyses for different parts and aspects of their ICT systems and supporting organization, such as the central servers and physical access and damage to these, authentication mechanisms from stationary and local devices, outsourced services, availability of qualified personnel to deal with exceptional situations, and so on. The analyses have typically been initiated by managers in various units and levels of the bank organization, and each analysis has been documented in the form of written risk reports. However, this set of risk reports do not provide the overall view of the security risk picture for the whole organization that is needed by the senior management and expected by the regulatory authorities. The risk consultancy company has therefore been asked to produce a unified overall security risk report on the basis of the set of existing reports. However, they find this to be very difficult and time-consuming, as none of the standards, methods and tools available offer adequate support for such a task.

Example 2: An employee in a large company with several divisions and departments has been assigned the role of Risk Management Facilitator. One of her first tasks is to recommend a security risk management approach to be applied throughout the company. She has therefore initiated a small survey to identify the needs and preferences of the relevant actors in the organization. Based on the results, a number of requirements have been identified, including the following.

- The approach should allow managers at all levels to obtain a simple overall risk picture for their complete area of responsibility. This should be an aggregated and abstracted view of all analyses at lower levels, preferably containing no more than seven risks.
- The approach should be flexible w.r.t. specific risk analysis techniques to be used and the level of detail, as the needs and prefer-

ences vary quite a lot between departments.

- The approach should not impose strict restrictions of the assets to be addressed, as what is considered to be the important assets vary a lot between business areas, organizational units and management levels.

The Risk Management Facilitator searches available standards, methods and tools in order to find an approach on which to base her recommendation, but is unable to find any candidates that satisfy the needs and requirements of the company.

Lack of Proper Support

Surprisingly, the plethora of risk management approaches on offer today provides very little help for one of the major challenges of risk management, namely the following:

> *How do we ensure that the risk management approach provides each organizational unit and management level with a risk picture suitable for their particular needs while ensuring consistency between risk pictures at all times and avoiding loss of essential information?*

While a Managing Director may be concerned with big issues such as the overall information risk picture to which the organization is exposed and the potential impact of a security breach on the company reputation, a low-level technical manager may be concerned about whether opening certain ports in a firewall would imply unacceptable risk. Presenting all the risks that have been identified throughout the organization to the Managing Director at the same level of detail that is useful at the lower management levels would drown her in information that from her perspective would be next to useless. What she needs is an *aggregated and abstracted view* that summarizes the important risks for the whole organization in a comprehensible manner.

Current approaches offer little or no support for this. Composition, aggregation and abstraction are typically either not addressed at all, or based on one or more of the following techniques: 1) simply counting of the number of risks within a predefined category, 2) adding up the likelihood, consequence and/or risk level assessments for all the risks within a category, or 3) selecting only a subset of the risks identified in a detailed analyses to be escalated to a higher level, typically based on estimated risk level. Such approaches are not satisfactory, as they build on assumptions that are hardly ever fulfilled in a practical setting. Counting the number of risks only makes sense if they are all described at the same level of detail and have approximately the same risk level. Adding up likelihood, consequence and risk assessments requires that there is no overlap or dependencies between risks, while escalating only a few selected risks means that groups of risks that may have a cumulative effect and should be considered in combination are not taken into account and that essential information may get lost. The lack of adequate support to address these issues may lead to

- costly analysis processes,
- analysis results that are not well suited as decision support for the intended user or provide only a fragmented risk picture,
- a lack of understanding of the actual risks of relevance, therefore leading to
- poor decisions.

Compositional techniques should enable a systematic and sound composition of individual risk models in order to derive the combined result for the larger system.

The RASEN Approach – A Notion of Risk Model Encapsulation

The full risk picture for an organization will be large and complex, and therefore very hard to grasp for any human decision maker. To deal with this problem the RASEN project puts forward a new approach based on divide-and-conquer. The overall hypothesis is the following:

> *Providing adequate risk support to organizations requires a notion of risk model encapsulation that allows composition/decomposition and abstraction/specialization of risk models.*

By risk model we mean any representation of any risk information that is captured and documented as part of the risk management, regardless of the media or format of the documentation. Typically, a

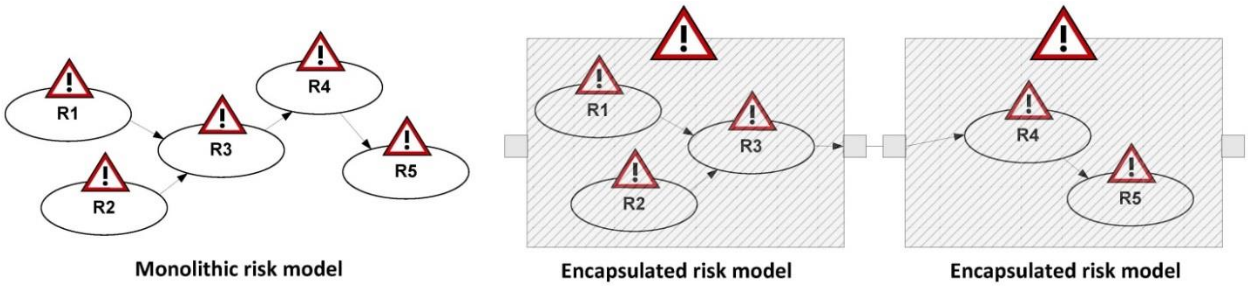

Figure 1. Encapsulation of risk models. A monolithic risk model for the system as a whole is depicted to the left, whereas compositional risk modeling is depicted to the right. The contents of the shaded boxes represent details that are hidden when composing the respective models to derive the combined result.

risk model may contain information about threats, vulnerabilities, unwanted incidents, likelihood estimates, consequence estimates and so on, as well as the relations between them.

By encapsulation we mean that only the elements of the risk model that are essential for the composition of risk models are externally observable. Figure 1 illustrates this concept.

The left-hand part of the figure represents an approach where encapsulation is not used. A single monolithic risk model is presented with all details visible. Such approaches do not scale, and make it extremely hard to obtain an overall comprehensible risk picture as risk models grow. The right-hand part of the figure illustrates an approach where encapsulation has been exploited. Here, the monolithic model has been divided into two encapsulated risk models (represented by large shaded boxes with a warning sign on top). Each encapsulated model can be viewed and reasoned about on its own, without worrying about its inner details. The two models have been composed via their externally observable elements (represented by the small boxes at the border of the encapsulated models). Note that although we have used a transparent grey color in the illustration to show that there is a relation between the detailed model on the left-hand side and the hidden contents of the components, it is common to use the term black box for approaches based on the hiding of details.

The RASEN Project

The main 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.

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.