RASEN
Compositional Risk Assessment and Security Testing of Networked Systems

Industry challenges addressed by the RASEN project

Frank Werner[a], Albert Zenkoff[a], Arthur Molnar[b], Erlend Eilertsen[c]
[a]Software AG, [b]Info World, [c]EVRY

Current existing and conventional tools fail to support industrial needs adequately. Although requirements are very diverse there is a common set of industry generic requirements applicable to a large number of industrial software developing companies. The RASEN project is addressing those, striving to deliver a new methodology and a supporting software environment.

In the RASEN project – an European research project – risk assessment, legal compliance, and testing within the area of cyber security are addressed. In the present work, we describe the challenges addressed and the expected benefits of RASEN from the point of view of three companies acting as use case providers within their respective industry domains: Software AG (IT domain), InfoWorld (eHealth domain), and Evry (Financial domain).

Enterprise Software Sector – Software AG

Software AG has a vast solution portfolio which helps companies to optimize and modernize existing technologies to achieve business results faster. Different software solutions belong to Software AG's key competences like Adabas, the first high-performance transactional database, ARIS -- the first business process analysis platform, the first B2B server, SOA-based integration platform, webMethods; and pioneering big data technology with Terracotta's BigMemory. Today, there are no existing means within software industry to efficiently relate security testing with risk assessment. Due to price pressure from customers and the demand to deliver high quality software, Software AG is constantly exploring ways to improve the software production process by reducing prohibitively expensive testing through conventional methods to an acceptable level by

- combating the huge size of tests
- reducing the complexity of security tests
- increasing the level of automation
- pinpointing attention to potentially problematic areas instead of "carpet bombing"

Risk assessment for large scale networked systems is one of the most pressing requirements in enterprise software development.

In the current software development process of Software AG, existing and newly developed code is analyzed and risks are defined in terms of the sources. A definition of the risks in the source code and how to search for it can be accomplished but risks cannot be aggregated upwards into an all-encompassing overview. At the same time from the top level perspective, risks are analyzed from the highest level of every product and various parameters are estimated. Unfortunately it is impossible to break the product model down into smaller components to reach the lower levels of a product.

Figure 1. Industry Domains covered by the RASEN approach

Software AG is facing two disjoint models which describe the risk analysis at a very abstract level of the product while the other delivers an estimate for security through code quality and correspondence to certain security rules. However there is a gap in between that does not allow any correspondence or correlation between the two, causing loss of transparency, introducing security risk, and making risk based testing impossible.

RASEN aims to solve the above challenges by bridging the gap between the high level risk assessment and the low level code analysis and testing, creating a correspondence and input the results of the low level assessments into the risk analysis. A composition of the analysis into the higher levels further allows a verification of the risk analysis results at the higher level and decomposition to feed the results of the residual risk analysis into lower levels to influence the testing and analysis at the low level.

With the RASEN approach Software AG strives to solve the following challenges

1. Risk Analysis of newly implemented features
2. Risk selection and mitigation
3. Compositional risk tracking
4. Product prioritization and risk rating

From the perspective of Software AG, the RASEN solution is expected to support:

- Risk analysis of newly implemented features, delivering an estimate on how the risk level of the overall suite is affected by the implementation of a single new feature
- Risk selection and mitigation: As risk awareness is highly dependent on the deployment and varies in different environments. Products may not be suitable for an environment for which they were initially not designed as they exhibit an unacceptable risk. By identifying which features have to receive the mitigation attention, a desired level of residual risk is obtained and the overall risk of the product can be mitigated (e.g., by simply dropping this risky feature) in a way that enables the deployments in even more critical environments
- Compositional risk tracking, to enable tracking of risks in both directions meaning the security impact of the feature is analyzed based on the risk analysis and the risk analysis of the feature is automatically reflected in the risk analysis of the product.
- Product prioritization and risk rating, to deliver a comparative product risk analysis in order to prioritize the mitigation of different defects and risks in software products

eHealth domain – Info World

Info World (IW) is a supplier of IT solutions dedicated exclusively to the healthcare field. The company provides customized modular integrated solutions for both clinical and economic management of healthcare facilities. Info World also offers training, service and maintenance for products in its portfolio and is currently active in Europe, America, Africa and Asia.

Info World products are implemented in a modular fashion so they can be combined into customized configurations. In addition, Info World provides deployment, training and support services to assist customers in using the delivered products in order to ensure optimal patient care. The present section details Info World's domain of activity highlighting general technical and legal issues and briefly details the actors that represent the company solutions' end users.

One of the defining characteristics of eHealth software relates to the specific privacy and safety requirements that permeate all aspects of plan-

ning, analysis, development, deployment and maintenance. This includes both actions required to ensure that eHealth software works reliably and correctly, together with ensuring the security and privacy of highly-sensitive customer data in front of accidental of malicious data leaks. As the developer of several eHealth suits that include deployments in 100+ units of care and a nation-wide eHealth portal where our customers entrust us with their electronic healthcare data, Info World is well-aware of these requirements and dispenses great effort in ensuring that provided solutions work reliably and provide an adequate level of privacy.

" Info World would greatly benefit from the need to automate the security testing process. "

However, currently Info World's development and security testing processes lack a rigorous structure and are undertaken in a mostly manual fashion guided by the expertise and experience of our analysis, development and testing staff. In brief, this leads to difficulties with planning testing effort, lengthens time-to-fix, time-to-new-feature for existing solutions together with adding development and testing effort for those solutions under development.

Info World's expectations from RASEN target the creation of a structured security risk-assessment methodology able to bridge the high-low level gap between risk-assessment and security testing. As an eHealth solution provider, Info World stands much to gain from deploying RASEN:

- Deploy a structured security risk-assessment process across all company products, reducing manual effort and shortening the time required for detecting and fixing bugs as well as for the development of new features.
- Automate the security testing process, which provides added confidence in the security characteristics of our products in front of accidental leaks or malicious attack.

In addition to adding structure and automation to key company processes, RASEN is expected to bring forth several advantages that are out of reach using today's technology:

- Structured prioritization of security risks and their mitigation. Having a formally defined risk-picture that is backed by risk-based security testing will allow us to better understand risks at both technical and organizational levels and to develop a clear strategy for their mitigation.
- Prioritization of security testing. The same risk model will be employed to guide security testing. While Info World currently employs security testing, it is driven by the experience of our technical teams and does not have a structured baseline that bridges the company's organizational levels.
- Clear assessment of legal compliance. The following years will witness a significant change in the EU's privacy policy as existing regulations will be replaced by the unified General Data Protection Regulation, expected to come into effect sometime around 2016. The RASEN tool-backed methodology that includes a legal compliance process will provide us the necessary tools to identify, develop and test any changes that will be required in our software.

Financial Industry Domain – Evry

In banking and finance, customers rightfully expect a lot. Banks have to offer a complete, up-to-date range of services. In this market we face global competitors as well as new fast moving players. EVRY provides all IT solutions necessary to facilitate a successful bank or finance operation. The customer chooses from a wide range of components, which EVRY in turn customize to meet requirements.

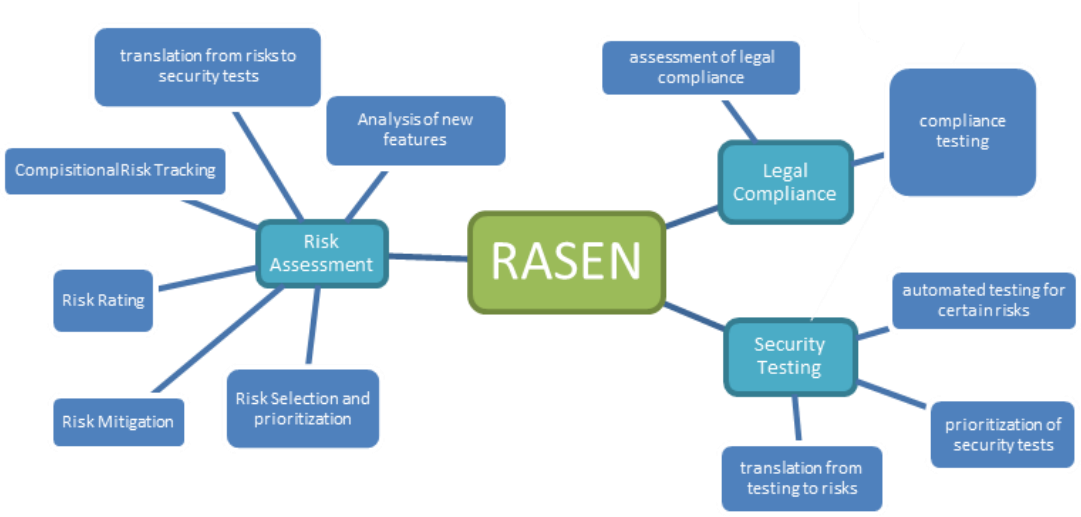

Figure 2. The RASEN approach and areas tackled by it.

In the eBanking sector security and privacy of customer and user data is a major concern. There are security demands both from IT laws and from customers we need to fulfill. Additionally EVRY strive to have a high level of security throughout the IT system.

In the current security testing process EVRY has no structured way to prioritize the test effort for security testing, often resulting in all areas of a system being tested. This is time consuming and leads to either longer test time or less effective testing in a given time frame. Additionally EVRY lacks a way to give feedback to the development team how to avoid high risk vulnerabilities and in which part of the system they most likely will be introduced.

" EVRY often ends up security testing everything instead of a prioritized set of areas"

By introducing a structured risk assessment and risk based security testing through the RASEN project EVRY will gain improvements:

- Risk based security testing will be introduced to our security test methodology and will be used for security testing throughout the organization.
- The introduction of risk based security testing will able us to identify which high risk vulnerabilities is likely to be introduced. This can be used as feedback to the development team to help them avoid this.
- More automated security testing with the help of various test tools will lead to less use of time consuming fully manual testing.

Top 7 Pressing Requirements in Industries

A high demand for a methodology and associated toolset that supports:

1. Formalizing and automating security risk assessment
2. Formalizing and automating product-level security risk assessment in the context of gaining new functionalities
3. Ascertaining the legal compliance of developed software components against a set of well-defined legal norms
4. Ascertaining the legal compliance of customized product deployments based on developed software components
5. Automated generation and execution of security tests based on security risk assessment results
6. Aggregation and composition of component security testing results into the risk picture
7. Aggregation of external security evaluation results into the risk picture

- Since the financial industry is regulated by laws EVRY has to comply to, EVRY can benefit from the tools that assesses legal compliance in our systems.

Impact of RASEN on other Industries

The RASEN Project contributes a flexible methodology and supporting tooling chain to combine compositional risk assessment and security testing of networked systems, such as shown within Figure 2. The testimonials of the RASEN use case providers clearly show that the RASEN approach is applicable but not limited to the areas of business software development, the eHealth solutions, and the banking sector.

The methodology which has been developed within the project is not limited to the sectors covered by present use case providers. As known issues are present also in other industry sectors, the proposed solution is rather a general means of relating security testing with risk assessment in order to deliver high quality software solutions at a lower price. The approach is generally-applicable and can be deployed within organizations facing the same problems faced by the industrial partners of the consortium.

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
- rasen-web@list.modelbased.net

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