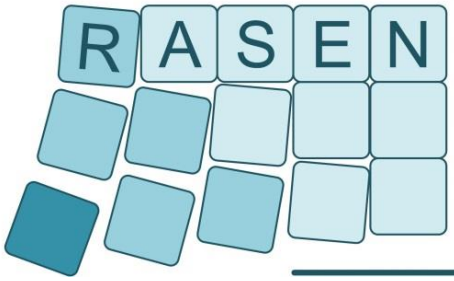

Compositional Risk Assessment and Security Testing of Networked Systems

An Industrial Perspective on Security Testing, Risk Assessment, and Legal Compliance

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

Existing security solutions promise to fulfill needs of modern industry with respect to security testing, risk assessment, and legal compliance to mitigate the overall risk exposure. The RASEN approach targets all of the above mentioned criteria by introducing a new methodology along with underlying toolset. In this white paper, the effectiveness and scope of RASEN is evaluated on three different scenarios, giving recommendations of its applicability, the integration of the provided tool-set, and an assessment to which degree the quality of software increased.

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 application of the RASEN approach on the RASEN pilots within their respective industry domains: Software AG (IT domain), InfoWorld (eHealth domain), and EVRY (Financial domain). Without loss of generality the RASEN framework can also be applied to companies outside RASEN to ensure legal and compliance assessment, risk assessment, enhance security testing and facilitate the support of related tools.

Enterprise Software Sector – Software AG

Software AG is among the top 10 fastest-growing technology companies in the world and ranked a "Leader" in eight analyst categories, including Service-Oriented Architecture (SOA), Business Process Management (BPM) and integration just to name a few. Software solutions produced and sold by Software AG are typically used by customers worldwide to build business critical applications that run at customer's sites. Their businesses rely on a very complex suite of interrelating products for their business-critical and highly sophisticated applications. Typically, such applications are distributed, logically and geographically, and encompass hundreds of installations, servers, and processing nodes.

Security Key-Requirements for Industries are Integration/Compatibility, Security, Correctness

As customers rely on this software, products should not expose vulnerabilities, but reflect the state of the art technology and obey security or technical risks. Failing to meet customer expectations would result in a loss of customer trust, customer exodus, financial losses, and in many cases in legal consequences and law suits. On the other hand, the impossibility to test and account for every potential security problem in advance is well-known within the field of security. Hence, the most critical and important security test cases must be identified. Any security problem in this software could lead to a considerable damage for the customer, be it its loss of business (e.g. when a successful DoS attack prevents business processes form being pursued), loss of data (due to unauthorized access) or malicious manipulation of business process sequences or activities.

Software AG takes the results from the RASEN project to evaluate and improve its software production process and relate security testing with risk assessment methodology. This is done on the one hand through a risk analysis of newly implemented features which continuously assures an exhaustive list of addressed risks and an estimate of how the risk level of the overall suite is affected by the implementation of a single feature. In addition, being able to select and mitigate risk products, risky features can be identified which contribute excessively to the overall resulting risk, allowing the risk managers to drill down the risk to the code and eventually decide whether to drop or replace the affected code fragments. From the perspective of software compositions, risk tracking is a desirable feature for all software vendors which enable developers to trace back vulnerabilities found in the code and relate them to features. The RASEN approach is thought to help development- and risk managers to prioritize developments on vulnerable components to mitigate defects and risk which maximize the impact on a single product but also on the solution portfolio.

eHealth domain – Info World

Info World is the largest company in Romania entirely focused on providing customized, modular eHealth solutions. The company's product stack includes end-to-end solutions that are focused on all facets of healthcare from the management of the healthcare unit and its specialists, management of financial assets and stock as well as patient-centric solutions. Info World currently has over 100 customers that include both public and privately-funded organizations ranging between private practices and multi-department units of care as well as university hospitals.

The company also strives to be at the forefront of enabling end-users to have better control over their health. The freely available Medipedia web portal, with over 40.000 registered users and over 150.00 weekly visits has proven its viability within its target market. Among other features, the Medipedia system allows registered users access to their electronic health record. As it includes sensitive personal data, access is provided on the basis of a signed agreement and data is secured via the user's account. Users can provide other users, such as family members or physicians registered within the platform access to some or all of their stored data, on the basis of a signed agreement. Moreover, granting a registered physician temporary access rights is also possible for the purposes of gaining a second opinion. In this way, physicians can access the patient's medical history in a centralized manner during the patient encounter, with no time or location constraints.

The legal compliance methodology facilitates structuring and acting upon legal information in view of new data protection regulations

The inherent complexity of systems such as Medipedia force parent companies to strike a continuous balance between fast development cycles requested by customers on one hand and usability and security aspects on the other. IW's participation to RASEN represent an investment in the development and adoption of new methodologies and tools that will mitigate the risks inherent to sweeping technological changes such as cloud computing and eHealth. As a direct impact of the project, IW expects to implement a well-defined, structured approach for legal risk identification and estimation as well as to deploy software tooling for automatic generation and execution of security test cases. These tools will allow the company to adapt to the newest legal requirements as well as reduce the time to market for newly developed features and products.

Financial Industry Domain – EVRY

The bank and finance sector is characterized by demanding customer expectations. Customers want innovative solutions with particular emphasis on self-service and automation. The high level of costs in the sector makes efficiency particularly important. By making greater use of automation and self-service solutions, banks can achieve lower costs, improved customer satisfaction and a greater degree of flexibility. EVRY invests continually in developing its solutions portfolio for the sector. Operational reliability and high security standards are crucial for services provided to the bank and finance industry. The systems EVRY offer in the financial sector handles both sensitive data like credit card numbers, personal information, and handles financial transactions. Security is of high

importance as vulnerabilities in these systems may lead to financial loss both for the customers and EVRY as well as loss of customer trust and reputation. Failing to meet the high expectation of security in the financial sector can also be in breach of compliance and financial law.

RASEN's security testing methodology describes the routines to ensure highest possible security level in the end product.

Due to the complexity of EVRY's IT systems, it is infeasible to test for every possible vulnerability and attack vector, so we need to identify the security test cases that cover the areas where the potential for security issues are highest and the issues would be most critical.

EVRY uses the RASEN results to improve the security testing methodology and test process. This is obtained by using the RASEN method and technique for risk-based test identification and techniques/tools for security test automation. The RASEN method hereby supports the identification and prioritization of test cases and scenarios to be able to use the test effort on the most important areas. In addition EVRY tries to use security test automation tool to lessen the effort needed for certain manual tests and conduct tests more efficiently.

Use Case Scenarios – Overview

The three companies serving as RASEN pilots are actively developing complex software and can be considered, at heart, as software development organizations. While working on different areas, the common denominator is represented by the sheer complexity of the deployed solutions, all companies provide complex network interconnected software systems which can easily be generalized and applied also to other industry domains.

Risk Management & Security Process in Business Industries

In order to deliver reliable and secure software to its customers worldwide, the production process of enterprise software at Software AG includes various stages of testing, starting from component testing, product testing, and testing of combinations of products. In addition the development process is compliant to the ISO 15408 ("Common Criteria for Information Technology Security Evaluation") Standard which defines a common criteria framework used to specify functional security and assurance requirements of IT products and computer systems. More over customers in particular from the United States require adherence to NIST publications like "Minimum Security Requirements for Federal Information and Information Systems" (FIPS PUB 200), "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST Special Publication 800-52), "Security Requirements for Cryptographic Modules" (FIPS PUB 140-2) and many more related to cryptography, security and secure hashing.

Benefits for Software AG from RASEN:

- **combat huge size of tests**
- **reduce complexity of security tests**
- **increasing the level of automation**
- **pinpointing attention to potentially problematic areas**

The pilot of Software AG is used to demonstrate RASENs ability to improve the software production process and relate security testing with risk assessment methodology. As of now it is considered as a great benefit of RASEN to enable the risk analysis of newly implemented features. Thus whenever a new feature is implemented, the requirement analysis contains a careful assessment of needs and conditions, taking into account existing possible conflicts with requirements from various stakeholders. In this sense risk analysis is continuously assuring an exhaustive list of addressed risks which eventually contribute to the risk level on the product level. To mitigate the overall risk to a justifiable level, risky features must be identified which contribute excessively to the overall resulting risk. Following this risk selection and mitigation approach will help to identify risky program code that can consequently be altered to mitigate the risk of the feature. The pilot further strives to demonstrate compositional risk tracking which enables developers to trace the security impact of a newly implemented feature based on the risk analysis

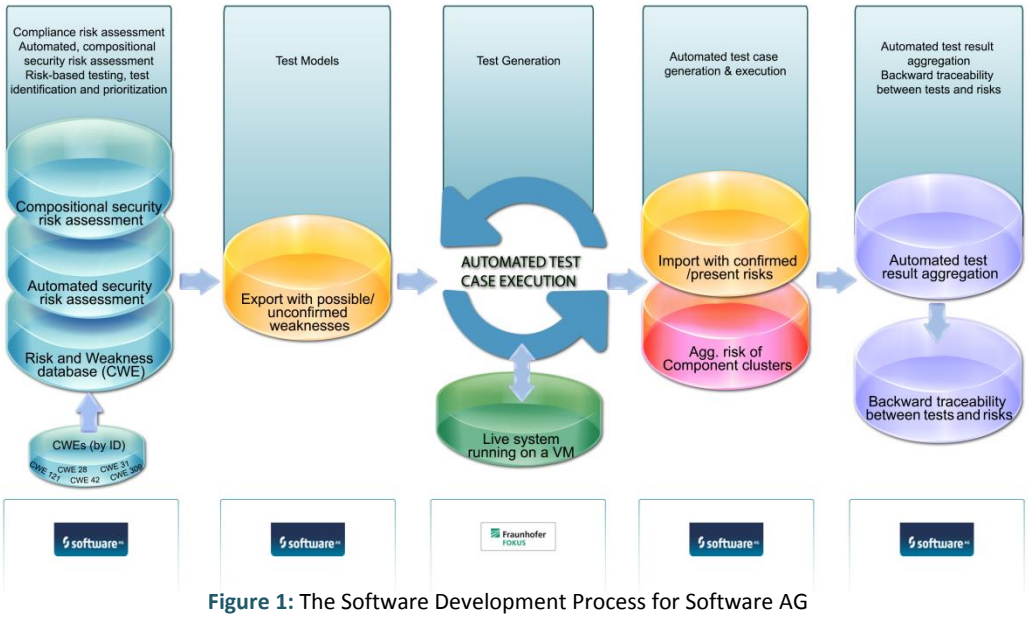

Figure 1: The Software Development Process for Software AG

and vice versa the risk analysis of the feature is automatically reflected in the risk analysis of the feature is automatically reflected in the risk analysis of the product. As the list of software products is extensive and the implementation of tools, processes, and measures across several hundred developers a challenge, results of the RASEN methodology should reveal a comparative product risk analysis in order to prioritize product prioritization and risk rating. A complete overview of the software development process including the RASEN methodology is depicted in Figure 1.

Test Automation for Medical Companies

The cornerstone of IW's use case is represented by the protection of our end-users' healthcare data. Current legal regulations are represented by the 95/46/EC Directive. However, the mid 2010's are a time of crossroads with regards to data privacy, as new data protection regulations are expected to come into effect in the form of the General Data Protection Regulation (GDPR) sometime after 2015. The GDPR is expected to provide an updated legal framework accounting for the effect of disruptive technologies such as rich Internet applications and cloud services. Coming into effect in a time frame where eHealth data breaches are becoming common, its adoption will require companies to recalibrate their efforts in order to ensure compliance with the upcoming regulations.

The latest draft of the GDPR article 31 specifies that all data breaches, regardless of caused prejudice must be reported to the supervisory authority within 24 hours, which changes the impact of data breaches independently of prejudice. This is compounded by increased administrative sanctions, which can now reach 2% of annual worldwide turnover. Furthermore, the draft also introduces the term "explicit consent", with data controllers such as Info World bearing the burden of proof for the data subject's consent.

As a highly visible, feature-rich system Medipedia provides a large attack surface. Any loss of data confidentiality or integrity can bear multiple financial and legal consequences imposed by the National Authority for Data Protection, partner medical clinics or compromised end-users. In addition, since medical decision are taken every day on the basis of the data stored in the system its corruption can have direct and undesirable medical consequence for its users. This outstanding combination between complex networked systems that handle highly-personal data such as Medipedia, the constantly changing and challenging security climate represented by an increasing number of threats to data security and privacy as well as the introduction of complex new legal requirements such as the GDPR means that companies which desire to remain at the forefront of their field must invest in new methodologies for ensuring the security and confidentiality of their most prized assets. The software development process with integrated RASEN artefacts is shown in Figure 2 below.

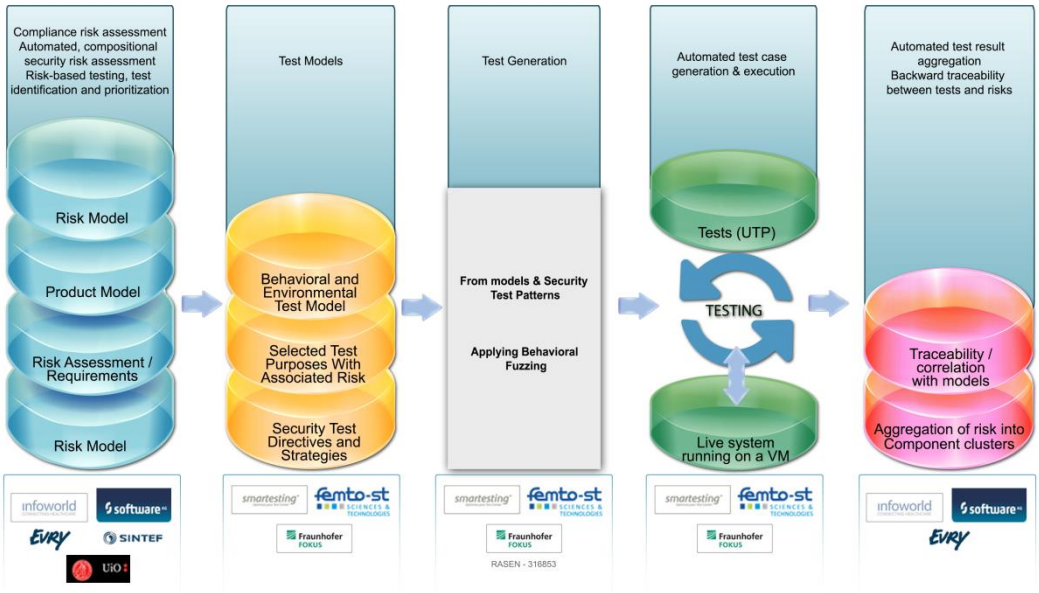

Figure 2: The Software Development Process for Info World and EVRY

Advantages for Finance Industries

EVRY's use case is used to show how RASEN can improve the security test methodology and process by using RASEN's method and technique for risk-based test identification and prioritization. EVRY's financial suite that consist of various financial system, ranging from net banks for private customers (which we have used in EVRY's use case) to management systems for banks, need to have a high level of security since these systems handles huge transfers of funds and handles sensitive and business critical data. The results from RASEN should show that by introducing formal risk assessment and prioritization methods should do lead to more effective and less time consuming security testing. An overview of the resulting process including the RASEN toolbox is shown above (Figure 2).

Assessing a company's security, risk and legal compliance level

Improving the state of security processes within a company is not possible unless first having a clear picture of the current status. This is made difficult however by the sheer diversity of organizational processes, structures and information flows. An important step within the RASEN project was to create a general assessment scheme that worked for the business, financial as well as medical sectors and which can also be applied to business active in other domains.

The result of this is the Compliance and Risk Security Assessment Profiling, or CRSTIP scheme. A CRSTIP assessment consists of establishing the proficiency of an organizational process within four key areas: *legal and compliance assessment*, *risk assessment*, *security testing* and *tool support*. To keep things simple, organizations can be ranked within each key area on a four-level scale, going from basic to advanced security and compliance processes. More information regarding the CRSTIP scheme, together with an online questionnaire that facilitates generating a report for your organization is available on our website[1]. Adopting the tool-backed RASEN methodology can help organizations within many industry fields to improve the quality of their security processes, maintain an updated risk picture and eliminate guesswork from legal as well as compliance issues.

Measuring the Impact from RASEN on the Industrial Pilots

By applying the RASEN methodology **Software AG** as an increased use of developer-capacities through the prioritization as most vulnerable components and code fragments are revealed through the automated testing. As such the software development cycle substantially improved with respect to facilitating management decisions on investments to achieve the maximum risk mitigation while raising the awareness of confirmed risks software areas that represent vulnerabilities. Though the product management is able to evaluate and mitigate risks on software products both, on product and on company level.

[1] The CRSTIP online questionnaire - http://www.rasenproject.eu/crstip/

As it is infeasible to test for every vulnerability, an automation of risk assessment and security testing is obtained. When considering the benchmark of the CRSTIP Evaluation, SAG already has a mature and exhaustive software development where the overall software quality of software could be further improved through the application automated security testing as proposed by RASEN. Beyond those achievements, there are still theoretically unsolved questions regarding the meaning of risk when considering the composition of components which need to be further investigated.

For **Info World**, the adoption of the RASEN tool-backed methodology is expected to bring several benefits. First of all, by employing a well-defined, structured approach to legal and compliance assessment facilitates communication of new requirements across organizational levels and allows maintaining exact records regarding legal requirements, risks as well as necessary steps that need to be taken. As the upcoming GDPR brings several important changes for eHealth companies, this is one of the key aspects of RASEN adoption for the company. Second of all, automation of the security testing process facilitates faster implementation of required features and a quicker time to market of new products. Even more so, updating the product risk picture from security test results allows maintaining an updated per-product risk picture that facilitates taking any required measures, thus lessening the company's exposure to actions from National Authorities for Protection of Personal Data or the loss of reputation that is to be suffered from the public at large.

In the **EVRY** case RASEN is expecting to deliver a more effective use of the testing time available by introducing risk-based test identification. This goes along with an increased level of confidence that correct test cases with highest impact on overall security level is selected. As future work EVRY plans to generalize the input from RASEN to be used in the general methodology to be used in all security testing, and not only in the system used for the test case.

Conclusion

Through the application of the RASEN methodology and tools all RASEN pilots managed to increase their efficiency in their development process while increasing the quality of their developed software in the areas of security testing, risk assessment, legal compliance assessment, and tool support and automation. As the use case providers represent through their diversity a large group of the software vendors on the market, the results can be generalized.

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