Proposal for tutorial at SECURWARE 2011

Title: Analysing risk in practice: The CORAS approach to model-driven risk analysis

Presenter:
Bjørnar Solhaug, PhD, Research scientist, SINTEF ICT, Norway
P.O. Box 124 Blindern, N-0314 Oslo, Norway
bjornar.solhaug@sintef.no

Length: 3 hours

Summary of contents:
The term "risk" is known from many fields. On an almost daily basis we face references to "contractual risk", "economic risk", "operational risk", "environmental risk", "health risk", "political risk", "legal risk", "security risk", and so forth. In order to identify and assess risks we may conduct risk analyses. The exact nature of an analysis, however, varies considerably depending on the nature of the risks we address. We may classify risk analysis approaches into two main categories: offensive (balancing potential gain against risk of loss) and defensive (protecting what is already there).

In order to defend something, it is important to know exactly what we are defending. This motivates asset-driven risk analysis, in other words risk analysis where the assets of the target (the tings of value) are identified as early as possible and where the rest of the analysis is driven by these assets. In order to analyse something, it is necessary to have a clear picture of what this something is. Understanding the structure and behaviour of the target of analysis is therefore important. However, understanding and modelling the target is only one aspect the modelling in a risk analysis; modelling what can go wrong is even more important. In fact, this is what risk analysis is all about. We then talk about risk modelling and model-driven risk analysis.

In this tutorial we present CORAS, which is an asset-driven, defensive approach to risk analysis. For risk analysis in practice, there is a need for well-defined methods, techniques and practical guidelines for how to do this. This is exactly what CORAS provides. The CORAS approach is a self-contained risk analysis methodology and the first to be truly model-driven in the sense that modelling is an integrated part in every part of the process. This means that target models and threat and risk models are applied in all phases of the risk analysis for visualization, communication and documentation of risk information, and are the main driver of the risk analysis process. The methodology is described in detail in the book *Model-Driven Risk Analysis: The CORAS Approach*, and has been validated through application in a large number of full-scale industrial analyses.

The CORAS approach consists of three main components: 1) The CORAS language, which is a language tailor-made for modelling risk in a precise and rigorous, yet intuitive and easily understandable manner. 2) The CORAS method, which provides detailed guidelines for how to conduct the various stages of a risk analysis in practice. 3) The CORAS tool, which is a modelling tool for editing models in the CORAS language.

In addition to presenting the basics of risk analysis and the CORAS approach, we also give a presentation of more advanced use of risk models expressed in the CORAS language.

Goals/objectives:

- Give the audience an introduction to the basics of risk analysis.
- Introduce the audience to model-driven risk analysis.
- Provide the audience with an overview of the CORAS method.
- Provide the audience with an understanding of risk modelling through basic and advanced use of the CORAS language.

Intended audience:

The intended audience is anyone with an interest in software engineering, security and risk management. The tutorial should be suitable both for persons new to risk analysis, as well as people familiar with risk analysis that are interested in the model-driven approach. No prior knowledge is required, but a general knowledge of software engineering and some interest in information security are recommended.

Outline of tutorial:

1st hour:

- Introduction to risk analysis
  - Central concepts
  - Relation to risk management
  - The ISO 31000 risk management standard
- Introduction to the CORAS approach
  - What is model-driven risk analysis?
  - The CORAS risk modelling language
  - The use of modelling in risk analysis in practice

2nd hour:

- Example-driven walk-though of the CORAS method
  - Establishing the context
  - Risk identification using threat diagrams
  - Risk estimation using threat diagrams
  - Risk evaluation using risk diagram
  - Risk treatment using treatment diagrams

3rd hour:

- Advanced use of risk models for change management
  - Changing and evolving target of analysis
  - Modelling and analysing changing and evolving risks

Biography of organizer/presenter:

Bjørnar Solhaug is employed as a research scientist at SINTEF ICT. He received his PhD in information science from the University of Bergen in 2009. His research interests include methods and languages for the modelling and analysis of systems with respect to security, risk and trust. He is one of the designers of the CORAS approach and has strong background in risk analysis.

References:

Gyrd Brændeland, Atle Refsdal, Ketil Stølen. Modular analysis and modelling of risk scenarios with dependencies. *Journal of Systems and Software*, 83: 1995-2013, Elsevier, 2010.

Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Evolution in relation to risk and trust management. *Computer*, 43(5):49-55, IEEE Computer Society, May 2010.

Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. *Model-driven risk analysis. The CORAS approach*. Springer, 2011.

Atle Refsdal, Ketil Stølen. Employing key indicators to provide a dynamic risk picture with a notion of confidence. Trust Management III. Third IFIP WG 11.11 International Conference (IFIPTM 2009), pages 215-233, Springer, 2009.