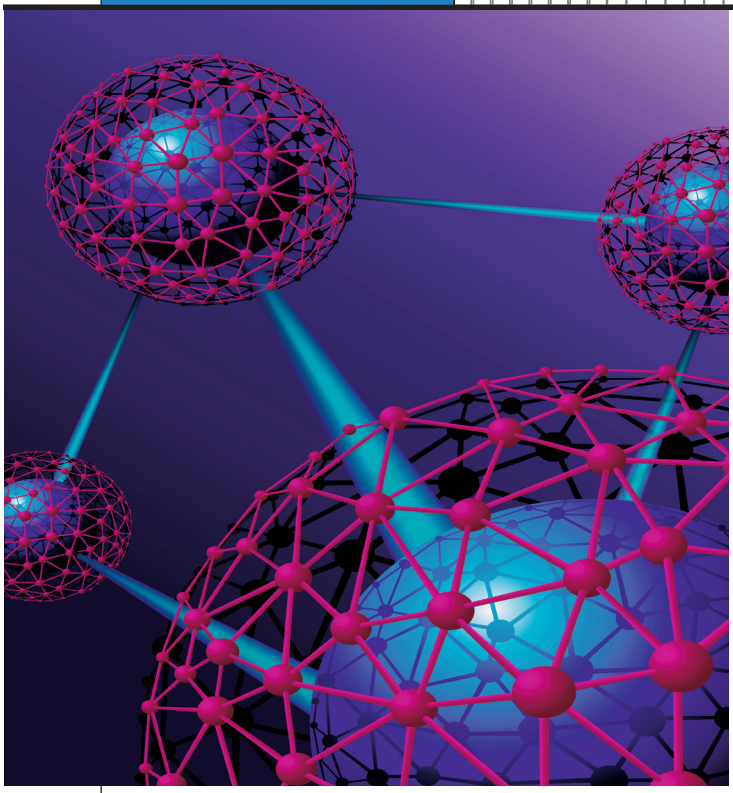

EVOLUTION IN RELATION TO RISK AND TRUST MANAGEMENT

Mass Soldal Lund and Bjørnar Solhaug, *SINTEF ICT*
Ketil Stølen, *SINTEF ICT and University of Oslo*

A methodology within risk and trust management in general, and risk and trust assessment in particular, isn't well equipped to address trust issues in evolution.

When improving an existing methodology to account for evolution, we must realize that methodological needs are strongly situation dependent. We therefore distinguish among three main assessment scenarios, each giving a particular perspective in relation to risk and trust assessment: *maintenance*, *before-after*, and *continuous-evolution*. For each perspective, we identify its main methodological challenges.

A risk picture typically focuses on a particular system configuration at a particular point in time and is thus valid only under the assumptions made when it was established. However, the system and its environment, as well as our knowledge, tend to evolve over time. State-of-the-art methodologies within risk management in general, and risk assessment in particular, aren't well-equipped to address evolution. A risk management standard such as ISO 31000[1,2] prescribes change detection and identification for emerging risks, but provides no guidelines. An important risk assessment methodology like OCTAVE[3] recommends reviewing risks and critical assets, but responds with silence when addressing how risk assessment results should be updated. Moreover, most academic studies have focused on either maintenance[4,5] or variants of reassessment.[6,7]

Matt Blaze[8] coined the term *trust management* in 1996, calling it a systematic approach to managing security policies, credentials, and trust relationships regarding authorization and delegation of security-critical decisions. Trust management has since been the subject of increased attention and today provides for a diversity of approaches. We view trust management as risk management with a special focus on understanding the impact that subjective trust relations within and between a target and its environment have on the target's factual risks. A methodology for trust management suffers from the same weaknesses we've identified for risk management and, further, brings in additional challenges due to trust's complexity and dynamic nature.

RISK MANAGEMENT

The recently published risk management standard ISO 31000[1,2] defines risk management as coordinated activities

0018-9162/10/$26.00 © 2010 IEEE Published by the IEEE Computer Society

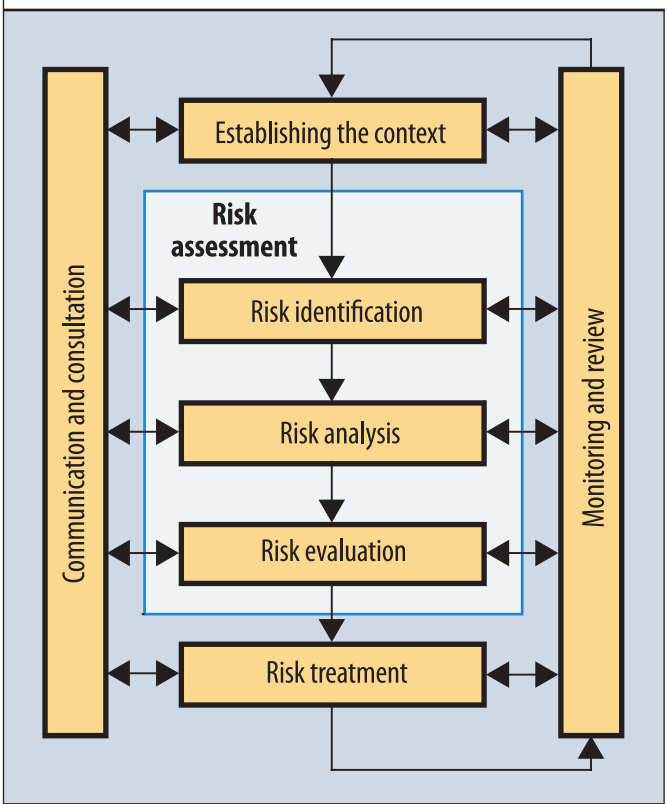

Figure 1. Risk management process. ISO 31000 defines risk management as coordinated activities to direct and control an organization's risk, defined as a combination of an event's consequences and their associated likelihood.

to direct and control an organization's risk, defined as a combination of an event's consequences and its associated likelihood. The risk management process is defined as the systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk. Figure 1, from *ISO 31000, Risk Management: Principles and Guidelines*,[1] shows the risk management process's seven subprocesses.

Seven subprocesses define risk management as a series of coordinated activities, as follows:

- *Establishing the context* defines the external and internal parameters to be accounted for when managing risk, and sets the scope and risk criteria for the risk management policy.
- *Risk identification* finds, recognizes, and describes risks.
- *Risk analysis* comprehends the nature of risk and determines its level.
- *Risk evaluation* compares the results of risk analysis with risk criteria to determine whether the risk and its magnitude are acceptable or tolerable.
- *Risk treatment* is the process of modifying risk.
- *Communication and consultation* are the continual and iterative processes an organization conducts to provide, share, or obtain information and to engage in dialogue with stakeholders about risk management.
- *Monitoring* involves continually checking, supervising, and critically observing risk status to identify changes from the performance level required or expected, whereas *review* focuses on the activity undertaken to determine the suitability, adequacy, and effectiveness of the subject matter necessary to achieve established objectives.

The *monitor and review* subprocess supposedly detects "changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities."[1] Hence, ISO 31000 covers evolution, but we must still address evolution in the more technical risk management activities, particularly the three subprocesses that Figure 1 refers to as *risk assessment*.

EVOLUTION IN RELATION TO RISK ASSESSMENT

A risk assessment as traditionally performed focuses on a particular target configuration at a particular point in time, and is thus valid only under the assumptions made when conducting the assessment. Because systems and environments change, we need more powerful risk assessment methodologies that can address changing and evolving targets.

How we should handle change and evolution in relation to risk assessment depends greatly on the context and kind of changes we face:

- Do the changes result from maintenance or from bigger, planned changes?
- Do the changes comprise a transition from one stable target state to another, or do they reflect the continuous evolution of a target designed to change over time?
- Do the changes occur in the target or in the target's environment?

The answers to such questions, as well as the risk assessment's practical setting, decide the methodological needs.

Maintenance perspective

We can describe the scenario corresponding to the maintenance perspective in the following example: risk assessors conducted an assessment three years ago and are now requested by the same client to reassess and update the risk picture to reflect changes to the target or environment, thereby restoring the assessment's validity.

The changes we address from the maintenance perspective are those that accumulate more or less unnoticed over time. Such changes can be bug fixes and security patches, an increase in network traffic, or an increase in the number of attacks. In this case, the risk picture remains more or less the same, but risk values might have changed such that previously acceptable risks could now be unacceptable, or vice versa. The objective then becomes maintaining the previous risk assessment's documentation by conducting an update.

Figure 2 shows the principle by which risk assessors conduct such a reassessment from the maintenance perspective. Assuming that we have descriptions of the old target and the updated target available, including environment descriptions, we start by identifying the changes that have occurred. We then use the relevant changes as input to the risk reassessment when deriving the current risk picture.

From a methodological viewpoint, the main challenge involves reusing the old risk assessment and avoiding a restart from scratch. This demands identifying the updates made to the target, updating the target description accordingly, and identifying which risks—and hence which parts of the risk picture—the updates affect. Finally, we update the risk picture without making changes to the unaffected parts.

Before-after perspective

The motivating scenario for the before-after perspective is risk assessors that are asked to predict the effect that implementing changes in the target has on the risk picture.

The changes we address from the before-after perspective are planned and anticipated, but could still be radical. Such changes can, for example, involve rolling out a new system or making major organizational changes such as implementing a merger agreement between two companies. We thus must understand the current risk picture, the risks that might arise from the very process of change, and the future risk picture.

Figure 3 shows the principle by which we conduct a risk assessment from the before-after perspective. Assuming we have descriptions of the current target and the change process to bring it from the current to the future state, we can devise a coherent risk picture for the future target and the change process.

From a methodological viewpoint, the main challenges involve obtaining and presenting a risk picture that unambiguously describes the current and future risks and the impact of the change process itself. This requires an approach for presenting a target description that unambiguously characterizes the target both "as is" and "to be," specifying the process of change in sufficient detail, identifying current and future risks without doing double work, identifying risks due to the change process.

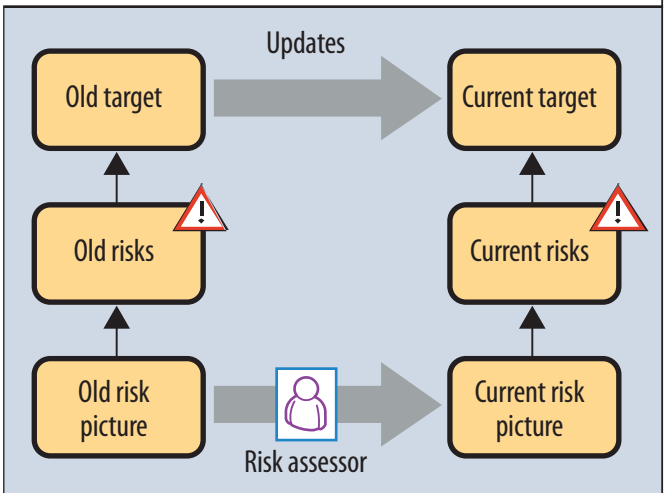

Figure 2. Maintenance perspective. Assuming we have descriptions of the old target and updated target available, including environment descriptions, we start by identifying the changes that have occurred in between, and then use the relevant changes as input to the risk assessment when deriving the current risk picture.

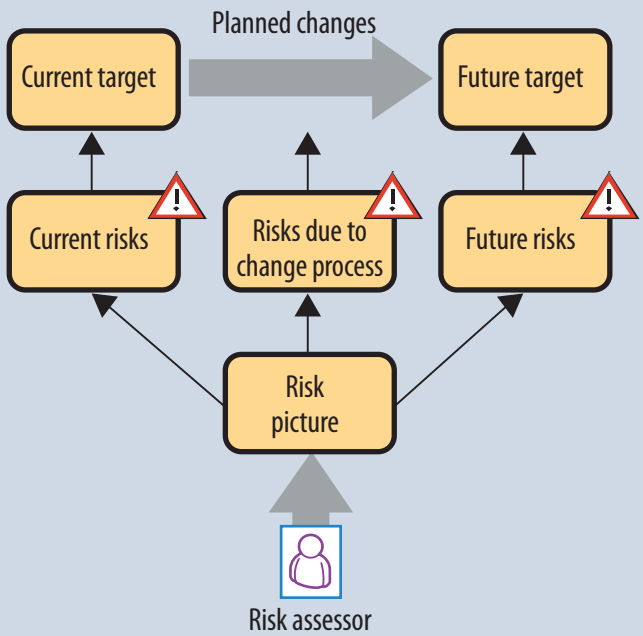

Figure 3. The before-after perspective. Assuming that descriptions of the current target and the change process bring the target from the current to the future state, we can devise a coherent risk picture for the future target and the change process.

Continuous-evolution perspective

The continuous-evolution perspective applies in the scenario that risk assessors are requested to predict future evolution of risk. It mandates that risk assessors conduct an assessment that establishes a dynamic risk picture reflecting the target's expected evolution. The changes we

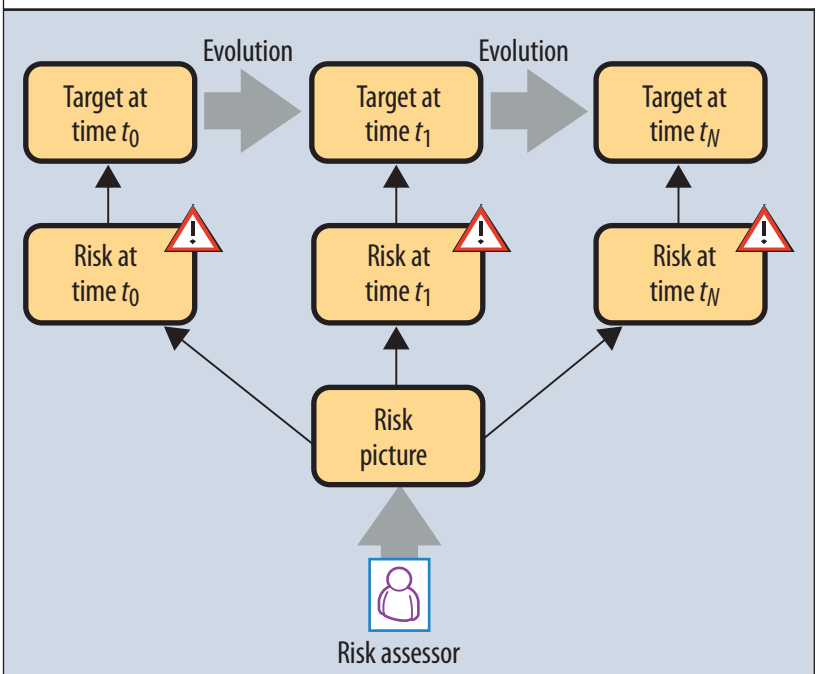

Figure 4. Continuous-evolution perspective. Given a description of the target as a function of time that we can derive at any point, we use this information to inform the risk assessment. Knowing how the target and its environment will evolve, we can create a risk picture as a function of time that describes how risks evolve.

address from the continuous-evolution perspective are predictable and gradual evolutions, described as functions of time. These predictions can be based on well-founded forecasts or planned developments. Examples include the slow increase in the number of components working in parallel, or gradually including more sites in a system. Examples of well-founded forecasts can include the expected steady increase of end users, adversary attacks, and annual turnover.

Figure 4 shows the principle by which we conduct a risk assessment from the continuous-evolution perspective. Assuming that we have a description of the target as a function of time, such that we can derive the target at any point, we use this as input to the risk assessment. Knowing how the target and its environment evolve, we seek to craft a risk picture as a function of time that shows how risks evolve.

From a methodological viewpoint, the main challenges are how to identify evolving risks and present them in a dynamic risk picture. Obtaining this information requires that we generalize the target description such that it characterizes the evolution of the target and its environment, identify and generalize the risks affected by evolution, characterize the evolution of risks in the dynamic risk picture, and relate the evolution of risks to the target's evolution as captured by the target description.

TRUST MANAGEMENT VS. RISK MANAGEMENT

Researchers agree that trustworthiness is a more general issue than risk-related factors such as dependability, security, and safety. For example, although the underlying system could be completely dependable in the traditional sense, it might not be trustworthy unless a suitable legal framework exists on which the trustor can rely should problems arise. Trust is nevertheless inherently related to risk, and an important part of managing trust is understanding the risks involved in trust-based interaction.

Following the example of Diego Gambetta[9] and Audun Jøsang and colleagues,[10] we define trust as the subjective probability by which the trustor expects that another entity—the trustee—performs a given action on which the actor's welfare depends. By this definition, trust is a belief the trustor holds about the trustee with respect to a particular action as a probability ranging from 0 (complete distrust) to 1 (complete trust). The trustor's welfare refers to its assets. If the trustee performs as expected, it might have a positive effect on the trustor's welfare; otherwise, it might have a negative effect.

The positive and negative outcomes correspond to opportunity and risk, respectively.[11,12] Issues of trust arise when deception or betrayal are possible, creating an inevitable relation between trust and risk. Likewise, trust always relates to opportunity, which is risk's counterpart. In a trust-based transaction, the trustor might be willing to accept the risk considering the opportunities involved.

We can calculate the risk level as a function R from the consequence (loss) l of a harmful event and the probability p of its occurrence. We define the dual notion of opportunity as the combination of the gain and likelihood of a beneficial event, and give the level of opportunity as a function O from the gain g of the beneficial event and the probability p of its occurrence.

Assume that the trustor has trust level p in the trustee performing an action with gain g for the trustor and that deception has loss l. The trustor must then weigh the opportunity $O(g, p)$ and risk $R(l, 1 - p)$ against each other when deciding whether to engage in the trust-based interaction. For example, assume a situation in which the trustor considers lending \$80 to the trustee, with the promise of being repaid the amount with 50 percent interest, a gain of \$40. The trust level is 0.9. Using multiplication as the risk and opportunity functions, the opportunity level is $0.9 \times 40 = 36$, and the risk level is $0.1 \times 80 = 8$. Because the

opportunity outweighs the risk, the trustor should accept the transaction.

Trust is just a belief held by the trustor, so the estimated trust level might be wrong and so too might the subjectively estimated levels of risk and opportunity. Trust is important precisely for decisions that must or should be made, even when confronting a lack of evidence about the trustee's future behavior. To precisely assess and evaluate trust-based decisions, however, the trustor's belief and the basis for it must be considered.

We say that trust is well-founded if the trustor's assessment equals the trustee's trustworthiness—that is, the objective and factual probability by which the trustee performs a given action on which the trustor's welfare depends. Only in the case of well-founded trust can the trustor correctly estimate the involved risks and opportunities. If trust is ill-founded, there's a chance of misplacing it. If the trust level is higher than the trustworthiness, the transaction might be at greater risk than the trustor believes. On the other hand, if the trust level is lower, distrust is misplaced, and the actual risk is lower than believed. To continue the example, assume the trustor's trustworthiness with respect to the transaction in question is only 0.65. The factual opportunity level is then $0.65 \times 40 = 26$, and the factual risk level is $0.35 \times 80 = 28$, making the risk higher than the opportunity.

Three focal points of trust management

In today's information society, traditionally face-to-face or human-to-human interactions are increasingly conducted remotely over the Internet. Moreover, computerized agents communicate and negotiate based on policies resembling those of humans. Because trust often is a precondition for such interactions to take place, trust must be managed. The adequate or appropriate approach, however, depends on the particular viewpoint and setting. Specifically, we must distinguish among three different focal points that might require less systematic management—namely, trust management from the focal point of the trustor, the trustee, and risk management.

From the trustor's focal point, there's a need to assess the trustworthiness of other entities to make trust-based decisions. From the trustee's focal point, there's a need to increase and correctly represent the trustee's trustworthiness as well as its systems and services.[10] The third focal point, trust management in the setting of risk management, is an important concern and involves understanding the impact of trust on the target's factual risk picture. The target then includes actors that base some of their decisions on trust, wherein the trust relations might be both within the target and between the target and its environment. These actors could be human, but they might also be organizations, businesses, or computerized entities behaving on behalf of other actors.

When conducting trust management from the focal point of risk management, we seek to direct and control an organization with regard to the risk and opportunity that stems from trust relations. To appropriately address and assess trust in this setting, we must generalize the risk management process depicted in Figure 1 by making the corresponding trust assessment steps accompany the identified risk assessment steps:

- *Identification of trust* relations focuses on existing and potential trust relations that might serve as a basis for trust-based decisions of actors within the target.
- *Trust analysis* estimates the trustee's trustworthiness in each such relation and estimates the potential for gain and loss for each potential trust-based decision. The trust analysis also includes an evaluation of the extent to which trust is well-founded.

Common for any trust management in the risk management setting is the dynamic and evolving nature of trust.

- *Trust evaluation* determines the risk and opportunity levels associated with the trust relations and thereby identifies favorable and unfavorable trust-based decisions.

The final risk management step should also be generalized to include strategies that ensure the actor makes only beneficial trust-based decisions in which opportunity outweighs risk. Such a strategy can, for example, be specified and enforced as a trust policy. A strategy to ensure well-founded trust should also be identified in case the trust analysis reveals significant discrepancy between trust and trustworthiness.

EVOLUTION IN RELATION TO TRUST MANAGEMENT

We can classify evolution in relation to trust management into the same three perspectives as evolution in relation to risk management. It is, however, more challenging because we must consider that trust relations are highly dynamic and can evolve as any other feature of the target; moreover, we must contemplate that the change itself can impact trust relations.

Common for any trust management in the risk management setting is the dynamic and evolving nature of trust. For a given trust relation, the trust level, and thus the trust-based decision, might change over time, even for the same trustor, trustee, and action, because the trustworthiness evidence might change—for example, if the trustee acts

deceitfully or makes a severe mistake, or if the trustee's reputation changes.

Maintenance perspective

The basis for a trust assessment from the maintenance perspective lies in the previously conducted assessment, which might need updating to reflect changes that can, for instance, provide improved mechanisms for authentication and nonrepudiation that should relax requirements on the trustees' trustworthiness. Or it could be an increase in threats such as viruses and infected websites that should result in a stricter trust policy. From the maintenance perspective, the trust-based decision points are basically the same after the changes, but the previous assessments to evaluate trust and identify appropriate trust policies might no longer be valid. Changes in the level of potential gain and loss associated with a trust relation can also be affected.

Starting from the old target description and the old risk picture, the methodological challenges of the maintenance perspective involve facilitating a systematic reassessment of trust relations: for each change in the target or its environment, we must check whether any trust relation is affected and, if so, determine the effect on the target's factual risk level.

Before-after perspective

In the before-after perspective, the changes are planned or anticipated, so we can predict their effect on trust relations. Because the changes could be substantial, we might not only need to reassess existing trust relations but also consider that new relations can arise and old ones disappear. Such a change can, for example, be caused by an enterprise entering a joint venture with another, which could involve the exchange of sensitive information such as trade secrets and intellectual properties. The future decisions of whether to reveal certain information might then need to be based on trust relations.

The methodological challenges of the before-after perspective involve identifying the trust relations that persist through the changes and will therefore still remain, how to identify the trust relations that changed and therefore must be reassessed, how to identify and reassess the new trust relations from scratch, and how to identify the trust relations that must be removed. The challenges further involve assessing the impact of the change process itself on trust relations.

Continuous-evolution perspective

The continuous-evolution perspective addresses predictable changes, which can also involve alterations to trust relations and levels, as well as potential loss and gain. A continuous evolution could, for example, be the steady and predictable increase of viruses and infected websites yielding a corresponding decrease in the trustworthiness of websites generally. The evolution toward more sophisticated methods for cybercriminals to exploit sensitive information provides further proof that the consequences of trust breaches could become more severe over time. The methodological challenges of this perspective involve being able to capture evolution with respect to notions such as trust, subjective risk, and subjective opportunity for the actors within the target and, moreover, relating these to the evolution of the target's factual risk picture.

Improving risk assessment to take evolution into consideration raises new, strongly situation-dependent, methodological needs. Three particular situations lead to three distinct assessment scenarios—maintenance, before-after, and continuous-evolution—each requiring distinctive procedures.

The notion of trust management has yet to be as well-established as risk management. Still, the same scenarios apply when evolution is taken into account in trust management, but with additional challenges originating from trust's highly dynamic nature.

Acknowledgments

The work on which this article reports was partly funded by the EU IST Framework 7 projects SecureChange and MASTER, as well as the DIGIT-project (180052/S10) funded by the Research Council of Norway.

References

1. *ISO 31000, Risk Management: Principles and Guidelines*, Int'l Organization for Standardization, 2009.
2. *ISO Guide 73, Risk Management: Vocabulary*, Int'l Organization for Standardization, 2009.
3. C.J. Alberts and A.J. Dorofee, *OCTAVE Method Implementation Guide Version 2.0*, Software Eng. Inst., Carnegie Mellon Univ., June 2001.
4. S.A. Sherer, "Using Risk Analysis to Manage Software Maintenance," *J. Software Maintenance*, vol. 9, no. 6, 1997, pp. 345-364.
5. M.S. Lund, F. den Braber, and K. Stølen, "Maintaining Results from Security Assessments," *Proc. 7th European Conf. Software Maintenance and Reengineering* (CSMR 03), IEEE CS Press, 2003, pp. 341-350.
6. S. Goel and V. Chen, "Can Business Process Reengineering Lead to Security Vulnerabilities: Analyzing the Reengineered Process," *Int'l J. Production Economics*, vol. 115, no. 1, 2008, pp. 104-112.
7. E. Lee, Y. Park, and J.G. Shin, "Large Engineering Project Risk Management Using a Bayesian Belief Network," *Expert Systems with Applications*, vol. 36, no. 3, 2009, pp. 5880-5887.
8. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proc. IEEE Conf. Security and Privacy* (SP 96), IEEE CS Press, 1996, pp. 164-173.

9. D. Gambetta, "Can We Trust Trust?" *Trust: Making and Breaking Cooperative Relations*, Dept. Sociology, Univ. of Oxford, 2000, pp. 213-237.
10. A. Jøsang, C. Keser, and T. Dimitrakos, "Can We Manage Trust?" *iTrust 2005*, LNCS 3477, Springer, 2005, pp. 93-107.
11. B. Solhaug, D. Elgesem, and K. Stølen, "Why Trust Is Not Proportional to Risk," *Proc. 2nd Int'l Conf. Availability, Reliability, and Security* (ARES 07), IEEE CS Press, 2007, pp. 11-18.
12. A. Refsdal, B. Solhaug, and K. Stølen, "A UML-Based Method for the Development of Policies to Support Trust Management," *Proc. 2nd Joint iTrust and PST Conf. Privacy, Trust Management and Security* (IFIPTM 08), vol. 263, Springer, 2008, pp. 33-49.

Mass Soldal Lund *is a research scientist at SINTEF ICT. His research focuses on formal and semiformal specification techniques and languages, risk analysis and threat modeling, and model-based testing. Lund received a PhD in informatics from the University of Oslo. Contact him at mass.s.lund@sintef.no.*

Bjørnar Solhaug *is a research scientist at SINTEF ICT. His research focuses on methods and languages for the modeling and analysis of systems with respect to security, risk, and trust. Solhaug received a PhD in information science from the University of Bergen. Contact him at bjornar.solhaug@sintef.no.*

Ketil Stølen *is a chief scientist at SINTEF ICT and a professor at the University of Oslo. His research focuses on model-based system development, security, risk assessment, trust management, and formal methods. Stølen received a PhD in computer science from the University of Manchester. Contact him at ketil.stolen@sintef.no.*