

Report

Evaluation of a Method for the Analysis and Development of Policies for Trust Negotiation

Author(s)

Tormod Våksvik Håvaldsrud
Bjørnar Solhaug
Ketil Stølen

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47 73593000
Telefax:+47 22067350

postmottak.ikt@sintef.no
www.sintef.no
Enterprise /VAT No.
NO 948 007 029 MVA

Report

Evaluation of a Method for the Analysis and Development of Policies for Trust Negotiation

KEYWORDS: ICT, field trial,
risk, trust, trust
negotiation

VERSION
1

DATE
2011-03-14

AUTHOR(S)
Tormod Vaksvik Håvaldsrud
Bjørnør Solhaug
Ketil Stølen

CLIENT(S)
Norwegian Research Council

CLIENTS REF.
180052/S10

PROJECT NO.
90B245

NUMBER OF PAGES/APPENDICES:
18/0

ABSTRACT

This report documents the evaluation of our method for the analysis and development of policies for trust negotiation. The method was evaluated in an industrial case study with evaluation criteria focusing on feasibility, effectiveness and usability.

PREPARED BY
Tormod Vaksvik Håvaldsrud

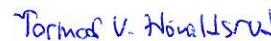


CHECKED BY
Mass Lund

APPROVED BY
Bjørn Skjellaug, Research Director

REPORT NO. SINTEF A18834
ISBN 978-82-14-04974-9

CLASSIFICATION
Unrestricted

SIGNATURE

Tormod V. Håvaldsrud

SIGNATURE

SIGNATURE


CLASSIFICATION THIS PAGE
Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2011-02-28	First full draft
0.2	2011-03-04	Quality check and minor revision
1.0	2011-03-14	Finalized

Evaluation of a Method for the Analysis and Development of Policies for Trust Negotiation

Tormod Håvaldsrud^{a,b}, Bjørnar Solhaug^a, Ketil Stølen^{a,b}

^a*SINTEF ICT*

^b*Department of Informatics, University of Oslo*

March 14, 2011

Abstract

This report documents an evaluation of a method for the analysis and development of policies for trust negotiation developed within the DIGIT project. The method was evaluated in an industrial case study with evaluation criteria focusing on feasibility, effectiveness and usability.

Contents

1	Introduction	7
1.1	Description of the Case and the Target of Analysis	7
1.2	Description of the Method that was Evaluated	7
2	Research Method	8
2.1	Sources of Evidence	9
2.2	Evaluation criteria	10
3	Facts and Evidence about the Case Study	10
3.1	Analysis Preparations	10
3.2	Analysis Meetings	11
4	Evaluation	14
5	Conclusion	16

1 Introduction

This report documents the results of an industrial case study evaluation of a method for the analysis and development of policies for trust negotiation [1]. The case study serves as the source of evidence and data for evaluating the feasibility of the method, as well as its effectiveness and usability with respect to its purpose.

In the remainder of this section we give a description of the case and the method under evaluation. In Section 2 we present the research method that we use for the evaluation, and we identify the evaluation criteria. In Section 3 we describe the facts about how the case study was conducted, as well as the evidence that was collected. In Section 4 we do the evaluation, before we conclude in Section 5.

1.1 Description of the Case and the Target of Analysis

Due to issues of confidentiality and trade secrets from the company commissioning the analysis that was conducted, we cannot report on actual details of the target of analysis in the case study or on the results of the analysis that we conducted. Instead we report on the empirical data regarding how the analysis was conducted, as well as the observations and experiences that we gathered regarding the evaluation of the method. In other words, we report on the evidence of relevance for the evaluation, focusing on the effectiveness and usability of the method in achieving its goal, namely to support the development and analysis of a trust policy that reflects the target owner's requirements to the trust-based behavior and the risk tolerance within the target system.

Generally speaking, the target of analysis was an ICT system that is critical for some of the core business activities of the company commissioning the analysis. The analysis focused on services provided by the company that involve the management of large projects in which several different users and user groups must be coordinated in order to fulfill the user needs and requirements.

1.2 Description of the Method that was Evaluated

Trust negotiation is an approach to build trust between two actors in order to enable an interaction that may involve risk. Basically, trust is built by the successive exchange of tokens, such as credentials, to prove or substantiate the trustworthiness of an actor. Once a sufficient level of trust is reached, the actors proceed with the interaction.

The interaction that is the goal of the trust negotiation usually involves the exposure to risk. The stakeholders therefore need policies that govern the trust negotiation and determine when to abort or proceed. These policies must in turn reflect the stakeholder's risk criteria and trust requirements.

The method for the analysis of trust negotiation and their policies reflects this setting by being based on three abstraction layers. The bottom layer is the most concrete, and is where the actual trust negotiation is conducted. The

middle layer describes the trust policy that characterizes the desired trust-based behavior. The topmost layer contains the requirements to the trust policy and relates the trust behavior to acceptable and unacceptable risk.

Orthogonal to this vertical dimension of abstraction layers is the horizontal dimension of input to and output from the trust formation that takes place. First, the target actor receives input from another actor in the form of prospects (for example credentials). Trust is then formed based on the properties of the prospects, and results in trust behavior as output. This trust behavior involves asset exposure, and thereby a certain level of risk.

The method makes extensive use of modeling for describing these various parts and the relationships between them. For this purpose, various kinds of table formats have been developed to support the documentation and analysis that is conducted by using the method. In particular, each kind of rule and requirement is modeled by means of specific tables.

The analysis is conducted by a well-defined process for applying the method. The process consists of the following five steps:

Step 1: Characterizing the target of analysis

Step 2: Capturing the requirements to the trust policy

Task 1: Capturing the requirements to the trust formation policy

Task 2: Capturing the requirements to the asset exposure policy

Step 3: Modeling the trust policy to be analyzed

Task 1: Modeling the trust formation policy

Task 2: Modeling the asset exposure policy

Step 4: Analyzing the trust policy with respect to its requirements

Step 5: Updating the policy to reflect its requirements

When applying the method in the case study, we decided to focus on the security domain. This was partly due to the target of analysis, and partly to test the method in a well-known domain where it can be compared with alternative and competing methods and approaches.

2 Research Method

As research method in conducting the evaluation we applied case study research with the use of so-called participant-observation as part of the data collection [2]. Following the framework in [2] for designing case studies, we have a single holistic case design: There is one case, one analysis to conduct, and one arena to collect the evidence.

2.1 Sources of Evidence

To achieve the best possible understanding of the case and its findings, it is important to have not only several sources of evidence, but also different kinds of sources. This case study provided the following main sources of evidence:

Documentation: Documentation of the target of analysis provided by the company commissioning the analysis. The documentation gives both direct information about the target system and about its context. It also gives information about how the company documents and share knowledge and information, both externally and internally.

Archival records: The annual report of the company, which provides a polished presentation of the company and reflects how it wishes to be seen by the rest of the world. In addition, it gives a concise overview of the business model and how the business is conducted.

Direct observations: To some extent we have direct observations documented by observers that were not directly involved in the analysis tasks. The notes made by the observers do not include direct citations or the like, but rather give indications of misunderstandings and important questions that arose during the analysis tasks and meetings.

Participant-observation: The analysis team consisted of an analysis leader and an analysis secretary, both of which were actively participating in all tasks and meetings. By their participant-observations through direct interaction, it has been possible to get an understanding of the informal processes undergone during the analysis. These observations served as a basis for expressing opinions about how the communication worked, how the analysis team's understanding of the target developed and evolved, and how the participants' common understanding and common way to express this understanding developed during the analysis.

Physical artifact: A concrete source of evidence of the case is the minutes from each of the meetings. These were distributed to all participants after every meeting, and give insight into the status of the process and steps at any given time. In addition to the minutes, we have the presentations (slides) from the meetings, the results documented during and after each meeting, as well as the final analysis result.

In this evaluation we aim at maintaining a chain of evidences by tracing the evidences from the research question through the documentation to the case report. By this we mean that every claim in the evaluation must be backed by evidences, and every evidence should be taken into account in the evaluation.

A challenge with respect to this in this particular case study is to do this in a convincing way without disclosing confidential information.

2.2 Evaluation criteria

We identified the following criteria for evaluating the effectiveness and usability of the method for the development and analysis of policies for trust negotiation:

EC1 (Modeling): The method should provide the means to formulate the trust policy reflecting the behavior of the target.

EC2 (Comprehensibility): The method should be able to capture the opinion and perception of the commissioning party regarding trust behavior and risk.

EC3 (Communication): The method should be able to communicate the trust policy and the requirements for the trust policy to the participants.

3 Facts and Evidence about the Case Study

In this section we describe the facts about how the case study was conducted and the evidence that was collected. Due to confidentiality issues, we leave out all information that may identify the target of analysis or the company, i.e. the target owner. Consequently, we also leave out some specific details and information of relevance to the case study. However, this information is fortunately less relevant for the evaluation of the method, which is the purpose of this report. Nevertheless, having the case study as the sole source of evidence, we realize that it is obviously more challenging for third parties to verify our conclusions.

With respect to the reported man-hour consumption, notice that there were some persons from our research institute attending the meetings having no active role in the analysis. For the sake of the evaluation of the method, it has been important to single out the time used by the ones having active roles only when calculating the man-hours. As for the participation from the company, the man-hours of every participant is counted.

3.1 Analysis Preparations

Before the actual analysis started, the analysis team was provided with comprehensive and quite unstructured information about the target of analysis. As part of the preparations, the analysis team browsed this information, extracting and structuring the important and relevant parts.

The documents were of various forms and types, including an annual report, several slide presentations describing core business models, services and applications, service level agreements, diagrams and textual documents describing

architecture and database structures, and so forth. In combination, this provided broad information about the database structure and the logical structure of the digital infrastructure, but no information about the security technology utilized.

Further analysis preparations included several preliminary meetings with the analysis team and representatives from the company. The company presented their business segment, products, production systems, and their main support tool. The analysis team moreover received documentation of the core system.

Subsequently, the analysis team presented their understanding of the organization and the target system to ensure a correct and common understanding.

There were three concrete goals for the preliminary meetings. First, discover weaknesses that should be analyzed in more details, i.e. identify the focus of the analysis. Second, achieve relevant knowledge about the target system and its work processes. Third, ensure a correct and common understanding among the analysis team and the customer representatives about the intended target of analysis.

Observations: The focus area was successfully identified and described. Moreover, to the judgment of the analysis team, a correct and common understanding of the identified target system and the analysis challenges were established.

We found that most of the input textual documentation was satisfactory, but a lot of the graphical illustrations had small and large errors which led to some misunderstandings. The documentation that was provided was extensive with respect to the database architecture and structural information, but very limited with respect to what ended up as the main target of analysis: the main target was mentioned in half a page of text and in two graphical illustrations out of 320 pages and 150 slides.

3.2 Analysis Meetings

Five meetings gathering the analysis team and representatives from the customer were organized for conducting the analysis. The analysis meetings were held as workshops guided by the analysis leader. In this subsection we report the facts and observations about and the evidence gathered from these meetings.

Table 1 gives an overview of the meetings, showing the time between meetings, the duration of the meetings, the number of participants from the customer (PC), as well as the consumed man-hours. In the following we describe further details of each meeting, including the goals and results. Notice that both the analysis leader and the analysis secretary participated at all meetings, apart from meeting M3 where the analysis secretary was absent.

Meeting 1

Participating roles: Decision-makers, system users, business experts, system experts and system developers.

No.	Week	Dur.	PC	MHC	MHA	MHP	MHT
M1	W1	1.5	6	9.0	3.0	8.0	20.0
M2	W10	1.5	5	7.5	3.0	6.0	16.5
M3	W11	1.5	2	3.0	1.5	2.0	6.5
M4	W14	1.5	5	7.5	3.0	5.0	15.5
M5	W18	1.0	4	4.0	2.0	5.0	11.0
Total man-hours:				31.0	12.5	26.0	69.5

Legend: *No.* is meeting number; *Week* is the week number counting from first meeting; *Dur.* is the meeting's duration; *PC* is the number of participants from the company; *MHC* is the man-hours used by the company; *MHA* is the man-hours used by the analysis team; *MHP* is the man-hours used by analysis team in meeting preparations; *MHT* is the total man-hours used. Note that only the analysis leader represented the analysis team at meeting M3.

Table 1: Overview of meetings with duration and man-hours

Goals: Delimit the target of analysis according to Step 1 of the process; define scales for measuring credential quality, access level and asset value.

Results: The target of analysis was delimited and the scale for access level defined.

Other details:

- The analysts' use of graphical and precise notations for describing the target proved useful for increasing the understanding of the target, identifying misconceptions and agreeing on the delimitation of the target. The choice of notation was inspired by an informal graphical notation that was already known by the participants.
- The definition of the scales was supported by explained tables. As a technique for aiding the participants and provoking discussions, the tables were partially filled in advance with suggested values from the analysts. Of five tables, only one was successfully filled in during the meeting. This was more likely a problem of contents rather than comprehensibility, as some of the relevant data could not be disclosed to the analysis team due to issues of confidentiality.

Meeting 2

Participating roles: Decision-makers, system users, business experts and system experts.

Goals: Complete Step 1 of the method by defining the remaining two scales; conduct Step 2 by defining requirements for the security policy; start looking at the security policy as preparation for Step 3.

Results: Step 1 and Step 2 was completed; initial modeling of the security policy.

Other details:

- The meeting was conducted 9 weeks after the previous meeting due to holiday season in between.
- The analysis leader was additionally attending a meeting internal to the commissioning company for clarifying further issues concerning the target of analysis. The role of the analysis leader at this meeting was mainly as observer.
- For the remaining parts of Step 1, the analysis team made suggestions that were corrected and modified. The same approach was used for the tables in Step 2 defining the requirements for the security policy. The interaction with the participants and their corrections and modifications indicated that the tasks and the tables were well understood.
- The specification of the security policy was made in two new kinds of tables.

Meeting 3

Participating roles: System users, business experts and system experts.

Goals: Complete the modeling of the security policy.

Results: Finalizing Step 3 by an updated and more comprehensive specification of the security policy for the target of analysis.

Other details:

- The meeting was conducted 3 days after the previous meeting due to the importance of continuation of the cognitive processes; it was a between-workshops meeting to more closely discuss the security behavior of the system.
- The analysis leader presented models and tables updated and adjusted according to his understanding from the previous meeting. The meeting was used to further detail the models and to fine tune them to reflect the behavior of the system.

Meeting 4

Participating roles: Decision-makers, system users, business experts, system experts and system developers.

Goals: Summarize the modeling of the security policy and present the analysis results with respect to non-conformities between the policy requirements

and the security policy; discuss the findings, their properties and impact, capturing how the participants perceived these findings. Approve Step 2 and Step 3 in the light of these findings of Step 4.

Results: The participants confirmed that the security policy was reflecting their understanding of the system; broad feedback on the participants' opinions about the non-conformity.

Other details:

- The analysis team presented the results in tables only, with no illustrations other than some textual explanations.
- Seven tables were presented in total.

Meeting 5

Participating roles: System users, business experts, system experts and system developers.

Goals: Get feedback on the results of Step 4. Present and get feedback on the preliminary results of the analysis, including proposed changes to the security policy of Step 5.

Results: The preliminary results were presented, and the participants gave the impression that they were pleased with the results, which they also found interesting.

Other details:

- The meeting was conducted four weeks after the previous meeting due to difficulties in finding a date suitable for all participants.
- The analysts presented the main results from the whole analysis process, from textual and graphical descriptions of the target to tables specifying the security policy.
- A risk matrix-inspired illustration was used for presenting the policy requirements and for pinpointing the findings in an intuitive way.
- The analysis work in preparation to this meeting was more time consuming than for the others, due to the need to come up with suggestions based on the analysis results.

4 Evaluation

In this section we evaluate the method with respect to the criteria of Section 2 and the facts and evidences of Section 3.

EC1 (Modeling): The modeling approach of the evaluated method is a table-based approach with formats customized for the tasks, purposes, analysis needs and documentation needs of the method. The experience from the case study is that the tables were adequate and usable for formulating distilled and pinpointed knowledge and information. The tables have a clear focus and delimitation, and present the trust policy and the trust behavior, as well as the relations between them, in a way that the participants seemed to understand well.

EC2 (Comprehensibility): Due to some limitations for the analysis team in being granted access to information about the target of analysis, the analysis process relied heavily on direct communication with the participants during the meetings. This communication was facilitated by extensive use of informal graphical illustrations.

In our experience, the use of diagrams and graphical illustrations in the case study were advantageous and fruitful in situations where the goal was to achieve a common understanding, and to explore and discuss important aspects.

We want to stress that the knowledge of more formal modeling techniques and diagrams from the side of the analysis team was essential in the drawing of the graphical illustrations. The analysis team had to be explicit about the semantics of the diagrams, although the semantics was not formalized in the context of the case study. In other words, for their usefulness and for fulfilling their purpose, the illustrations had to have a clear meaning with little ambiguity.

The discussion nevertheless often drifted away from the focus when the participants followed chains of thoughts into details, digressions, opinions on internal procedures, and so forth. This could indicate that the diagrams distract the discussion. In reality, however, when the discussion was guided back on track, the diagrams proved to be an excellent means for keeping adequate and relevant discussions about central topics; our impression was that the graphical diagrams helped keeping the focus of the discussions on what was depicted at any time.

The participants seemed sufficiently familiar with the notation for the illustrations to serve as a reminder of the focus of the discussion, and for the diagrams to support the participants in communicating their opinions and perceptions.

EC3 (Communication): When a new table for describing a trust policy or its requirements was introduced, the analysis team explained its semantics. Furthermore, whenever the table was used again later, the analysis team attached a short textual description to remind the participants about the semantics. Due to this, the participants in our experience seldom misunderstood the information conveyed by the tables.

5 Conclusion

This case study substantiates the feasibility and usability of the method. Even though the analysis team had little concrete documentation of the target, they were able to conduct the analysis and make new findings.

One finding was with respect to breach of the policy requirements, and one finding was related to lack of sufficient control and knowledge of the involved risk. A third finding was related to a beneficial treatment to reduce the risk of the operational application.

The variety of the findings and the usefulness of the knowledge obtained during the analysis are good indications of the adequacy and usefulness of the analysis method. The evaluation of the method with respect to the identified criteria gives further favorable indications. In our experience, the method provides useful means for policy modeling and for communicating the meaning of the policy, and it moreover facilitates a process where the theory of the method can be applied and presented in a comprehensive manner to people with no prior knowledge about the method and its techniques.

References

- [1] Tormod Håvaldsrud, Birger Møller Pedersen, and Ketil Stølen. A method for the development and analysis of policies for trust negotiation. To appear.
- [2] Robert K. Yin. *Case Study Research – Design and Method*, volume 5 of *Applied Social Research Method Series*. Sage Publications, third edition, 2003.



Technology for a better society
www.sintef.no