DeSPoT: A Method for the Development and Specification of Policies for Trust Negotiation

Tormod Håvaldsrud, Birger Møller-Pedersen,
Bjørnar Solhaug and Ketil Stølen

Abstract Information systems are ever more connected to the Internet, which gives wide opportunities for interacting with other actors, systems and resources and for exploiting the open and vast marked. This pushes the limits for security mechanisms which in general are too rigorous to fully adapt to such a dynamic and heterogeneous environment. Trust mechanisms can supplement the security mechanisms in this situation to reduce the risk by means of trusted evidences. We propose DeSPoT, a method for the development and specification of policies for trust negotiation. DeSPoT is created to be easy to use for business level experts, yet demonstrated in an industrial study to be useful for those who develop and maintain the system conducting trust negotiation within acceptable risk. Adherence to a DeSPoT policy should ensure that the target fulfills the organizational level requirements to the trust behavior, and that the target is not exposed to unacceptable risk. The paper gives an example-driven presentation of the method.

Keywords Trust negotiation · Trust management · Risk management · Access control · Trust policy

T. Håvaldsrud (✉) · B. Solhaug · K. Stølen
SINTEF ICT, Oslo, Norway
e-mail: tormod.havaldsrud@sintef.no

B. Solhaug
e-mail: bjornar.solhaug@sintef.no

K. Stølen
e-mail: ketil.stolen@sintef.no

T. Håvaldsrud · B. Møller-Pedersen · K. Stølen
Department of Informatics, University of Oslo, Oslo, Norway
e-mail: birger@ifi.uio.no

James J. (Jong Hyuk) Park et al. (eds.), *Computer Science and Convergence*,
Lecture Notes in Electrical Engineering 114, DOI: 10.1007/978-94-007-2792-2_9,

1 Introduction

Systems at the Internet exploit the potential of the open market and the possibility of interacting with a vast number of other systems for the purpose of realizing opportunities. Trust mechanisms are introduced to mitigate the fact that security mechanisms usually are too rigorous to fully adapt to this dynamic and heterogeneous environment. When a system is exposed in an environment it is subject to risk, which we define as the combination of the likelihood of an incident and its consequence for an asset [1]. Security mechanisms are introduced to reduce the risk, but they are not able to eliminate it entirely. Moreover, increased security tends to be at the cost of interoperability. Security mechanisms should be used to achieve the necessary security level, i.e. keep risk below a certain critical level, and leave it to trust mechanisms to treat the residual risk by means of trust and perceived knowledge.

In practice we often need to make assumptions regarding uncertain information, and this forces us to take uncertainty into account when making decisions. Even though information is uncertain it provides important indications of the actual situation. The challenge is to make the uncertainty sufficiently visible so that we are aware of its extent and not just of its existence. In trust mechanisms uncertainty is the focal point of judgment, whereas security mechanisms hide uncertainty by the assumption that it is sufficiently small to be ignored in the clear defined situation.

To achieve trust, systems may conduct trust negotiation [2] utilizing trust mechanisms. The systematic use of trust mechanisms may be formulated in a trust policy. The developers need specialized methods to support the development and maintenance of the trust policy in the same way as they need specialized methods for the development and maintenance of security policies. A natural way to describe trust behavior is, as for security behavior, by means of rules. Many security systems do not explicitly define the rules, but rather embed them in the implementation of the system as actions triggered by events. For this reason it is natural to aim for a rule-based policy specification language.

The contribution of this paper is a *method for the Development and Specification of Policies for Trust negotiation* (DeSPoT). Correctly enforcing such a policy should ensure that the trust behavior realizes opportunities while keeping risks at an acceptable level. Focusing on the requirements to and the criteria for risk and trust at an organizational level, the method aims to support decision makers in understanding the potential implications of trust mechanisms without going into the low level details of trust negotiation protocols. This is achieved by systematically linking the high level organizational requirements and criteria to the developed trust policy, which in turn is linked to the low level trust behavior.

The rest of the paper is organized as follows. We give an introduction to trust negotiation in Sect. 2. In Sect. 3 we provide an overview of our method. In Sect. 4 through Sect. 8, we present the five steps of our method in an example-driven manner. We conclude in Sect. 9 by characterizing our contribution and discussing

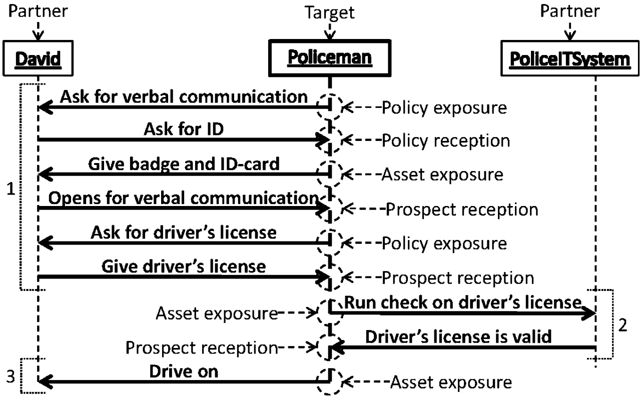

Fig. 1 Example of trust negotiation

related work. The reader is referred to the full technical report [3] on which this paper is based for further details about the DeSPoT method.

2 Introduction to Trust Negotiation

To introduce trust negotiation and our terminology we use an everyday example. Assume a policeman wants to check the validity of David's driver's license. The scenario is illustrated by the sequence diagram in Fig. 1. The diagram has three lifelines, David, the Policeman and PoliceITSystem. Everything is observed from policeman's perspective, so we tag him as the **target** of our analysis and David and the PoliceITSystem as **partners**. All events at the policeman's lifeline are tagged to show what kind of event it is with respect to trust negotiation from the policeman's perspective. In general, the chosen target of analysis is the system or organization for which the method aims to develop and analyze a policy to govern the trust negotiation. The partners are the trustees in potential interactions with the target.

When the policeman approaches David's car he notices that David is intimidated by his pose and checks that the doors of the car are locked. The policeman knocks on the closed window and makes it clear that he wants verbal contact. David indicates that he wants the policeman to identify himself. These two social messages are revealing parts of their respective trust policies; the policeman reveals some of his intentions and David requests some evidence from the policeman. As a reaction to David's request the policeman shows his ID card and his badge so that David can see for himself that the policeman really is a police officer and that it is his badge. The badge and the ID card are **assets** to the policeman, which he exposes to authenticate himself. An asset is something of value for the target and therefore needs protection against risk. David rolls down

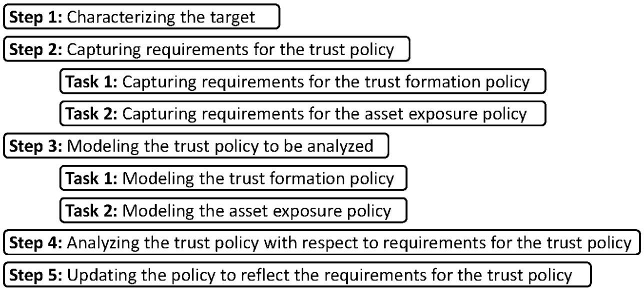
Step 1: Characterizing the target
Step 2: Capturing requirements for the trust policy
Task 1: Capturing requirements for the trust formation policy
Task 2: Capturing requirements for the asset exposure policy
Step 3: Modeling the trust policy to be analyzed
Task 1: Modeling the trust formation policy
Task 2: Modeling the asset exposure policy
Step 4: Analyzing the trust policy with respect to requirements for the trust policy
Step 5: Updating the policy to reflect the requirements for the trust policy

Fig. 2 The five step process

the window and hands over his driver's license on request from the policeman. David's driver's license is a **prospect** for the policeman; it can tell him whether David is allowed to drive or not. Generally, a prospect is something of value for the target that can be provided by a partner. To verify the validity of the driver's license, the policeman employs the PoliceITSystem and runs a validity check using the license number. For the policeman in this situation, the license number is an asset and the potential response from the PoliceITSystem is a prospect that may validate David's driver's license. After the interaction with the PoliceITsystem the policeman knows that David is allowed to drive a car.

3 Overview of the Method

The overview of the five steps of the DeSPoT process is given in Fig. 2. The process provides guidance in correctly capturing the target's trust policy requirements and the trust policy. The next five sections exemplify each step in turn.

4 Step 1: Characterizing the Target

The characterization of the target is conducted in close cooperation with the commissioning party, who is usually the target owner. Our example target is a power grid system where we focus on the balancing of the production and the consumption of electrical power. This task is quite complex and for the purpose of this paper we simplify the system so that we are able to focus on the important features of DeSPoT. The balancing of the production and consumption is conducted in real time, but it also needs planning from day to day. It is this day to day planning on which we focus.

The selected target is the Power Production Organizer (PPO) which is a central software system collecting and spreading key information about power production and consumption. Several systems communicate with the PPO; some are providing necessary information, some are providing business crucial information and others are just providing supplementary information. A power flow sensor measures the flow of power through a line. It informs the PPO how much power is transported through the power line during the last 24 h. A power station provides the PPO with information on produced power during the last 24 h, as well as the expected production capacity. Sometimes the capacity is lower because of maintenance, while in other situations the power stations may have higher capacity than usual, for example due to heavy rain. In addition to this, the power station needs to know how much power it is expected to feed into the grid the next 24 h to adjust its production. When the PPO has collected all the information, the PPO finds the best suited production profile for the next 24 h. It then assigns production quotas for the next 24 h to all the power stations.

Now we continue by defining the scales for prospect value, asset value and trust level from the perspective of the target. These scales may be both quantitative and qualitative, depending on the desired granularity of the analysis or what is otherwise suitable for the target in question.

The prospect value scale is used to measure the value of objects and information given to the target by partners. The value should reflect the direct value, the sensitivity and how easy it is to fake. For example, a credential that is very easy to fake should be given a relatively low value, whereas an unforgable message about the delivery of a crate with high quality goods can be given a high value. The prospect value scale chosen for the PPO is of five values from 1 to 5. Each of these values must be defined in terms of a precise interval or a qualitative description.

Next we define the scale used to measure the value of assets. As already indicated, an asset is something the target already possesses and that should be protected from harmful incidents. An asset may for instance be sensitive information. Breach of confidentiality, integrity or availability, for example, could be exploited to damage the reputation or revenue of the target. In this situation the potential total loss should correspond to the assigned asset value. The asset value scale chosen for the PPO is of four values from 1 to 4, each of which must be precisely defined.

The last scale needed to be defined is the trust level scale. We use this scale to measure the target's trust in a partner's capability and intention to protect the target's assets. The trust level scale chosen for PPO is *No*, *Low*, *Medium* and *High*, each representing an interval of subjective probabilities between 0 and 1.

5 Step 2: Capturing Requirements for the Trust Policy

The **trust formation policy requirements** specify how the target is allowed to use incoming prospects as evidence to form trust. In general, the trust formation policy requirements restrict how the target is allowed to perceive the world with respect

Table 1 The trust formation policy requirements

Prospect value	Maximal trust level
1	Low
2	Medium
3	Medium
4	High
5	High

to trust. The trust formation policy requirements for the PPO are defined in Table 1 and regulate how prospects are allowed to influence the trust level. The interpretation of the second row, for example, is that a prospect with prospect value 2 can at most support a trust level *Medium*.

The **asset exposure policy requirements** specify the trust level the target must have in order to expose assets with a specific value. The trust level is an indirect measure of the likelihood of something going wrong, and the level of this risk can be deduced from the trust level and asset value. The asset exposure policy requirements hence specify the acceptable risk level in this setting.

The asset exposure policy requirements for the PPO are defined in Table 2, where each row forms an asset exposure rule requirement. The interpretation of row three, for example, is that when the target has trust level *Medium* it is allowed to expose assets with value 3 or lower, while the last row allows the target to expose all assets (because 4 is the highest asset value) to partners in which its trust is *High*.

6 Step 3: Modeling the Trust Policy

The trust formation policy specifies how the target should form trust based on prospects and their properties. The first task is to specify the prospects and their values, as illustrated in Table 3. The third row means that a prospect matching the prospect description *Consumer authentication* has the prospect value 3.

A **trust formation rule** defines what may form evidence and how this evidence should influence the target's trust level with respect to a partner. The evidence consists of a prospect, a prospect property and an evidence type. The prospect is received from a partner and can be anything that may give insight into this partner's properties, such as intention or capabilities to take care of the target's assets. The **prospect property** may be as simple as the confirmed existence of the prospect itself, but also complex properties such as authenticity and validity of a chained signed electronic certificate. There are two different sorts of evidence, namely supporting and exposing. The **supporting** evidence may build trust, whereas **exposing** evidence on the other hand may reduce trust. The exposing prospect rules are overruling the supporting, such that the trust is governed by the worst exposing evidence and otherwise by the best supporting evidence.

Table 2 Asset exposure policy requirements

Trust level	Maximal asset value
No	1
Low	2
Medium	3
High	4

Table 3 Prospect values

Prospect description	Prospect value
Partner's access policy	1
Full postal address	2
Consumer authentication	3
Power certificate signature	4
Master certificate signature	5
Certificate validation	5

Table 4 Trust formation rules

Prospect description	Property	Evidence type	Trust level
Power certificate signature	Invalid	Exposing	No
Full postal address	Existing	Supporting	Low
Consumer authentication	Valid	Supporting	Medium
Power certificate signature	Valid & Correct	Supporting	High
Master certificate signature	Correct	Supporting	High
Certificate validation	Trusted	Supporting	High

The first row in Table 4 should be understood as follows: If a partner provides an invalid power certificate signature, it is perceived as an exposing evidence and results in a trust level no higher than *No*. Sometimes a prospect property must be verified by another prospect. This is typically the case in chains of certificates. In order to take into account and keep track of such relations, we document these in a designated table as exemplified in Table 5. The first row should be understood as follows. A *Certificate validation* prospect with the property *Trusted & CertValid* verifies the *Valid* property of a *Power certificate signature* prospect. Moreover, the *Trusted* property of the former can in turn be verified by the *Correct* property of *Master certificate signature* in the third row.

The **policy reception rules** specify how to handle requests from the partner. These are referred to as such, because in trust negotiation the partners expose their policy when requesting assets from the target. The policy reception rules for the PPO are documented in Table 6. The first row should be understood as follows. If the partner requests that the target system provides a *Power certificate signature* the target may raise the trust level up to *Low* based on this evidence.

Table 5 Prospect property verification

Prospect description	Required property	Prospect description	Verified property
Certificate validation	Trusted & CertValid	Power certificate signature	Valid
Certificate validation	Trusted & CertInvalid	Power certificate signature	Invalid
Master certificate signature	Correct	Certificate validation	Trusted

Table 6 Policy reception rules

Requested asset	Evidence type	Trust level
Power certificate signature	Supporting	Low
Report power flow	Supporting	Low
Get assigned power quota	Supporting	Low
Report power consumption	Supporting	Low

Table 7 Defining asset values

Asset description	Asset value
Get total power consumption	1
Target's access policy	2
Report consumer consumption	3
Report power production	3
Get assigned power quota	3
Report power production capacity	4
Report power flow	4

The assets identified for PPO are listed in Table 7 together with their respective values. The asset *Get total power consumption*, for example, is assigned the asset value *1*. This is a service provided by the target system and exposes an asset.

The asset exposure policy specifies how the target may expose assets based on the trust level. The *asset exposure rule* for PPO is modeled in Table 8. The first column specifies the minimum trust level for exposing the associated asset. Hence, the asset *Power certificate signature* can be exposed when the trust level is *Low* or higher. Or, given the trust level *Medium*, all the assets of the first five rows can be exposed.

PPO also needs to expose parts of its own trust policy. These exposures may be sensitive and for that reason we explicitly model how the target is allowed to expose policies through **policy exposure rules**. These are presented in Table 9. The first row should be understood as follows: The target must have at least trust level *No* in the particular partner to be allowed to request the partner for the asset *Power certificate signature*.

Table 8 Asset exposure rules

Needed trust	Requested asset
Low	Power certificate signature
Low	Report consumer consumption
Low	Get total power consumption
Medium	Report power production
Medium	Get assigned power quota
High	Report power flow
High	Report power production capacity

Table 9 Policy exposure rules

Needed trust	Asset description token
No	Power certificate signature
No	Consumer authentication
No	Postal address

7 Step 4: Analyzing the Current Trust Policy with Respect to its Requirements

At this point we have both the trust policy and its requirements. In this step we look for possible gaps between them. Every trust formation rule forms trust based on a prospect with a specific value. It can therefore be easily checked against the corresponding trust formation rule requirement which specifies the highest acceptable trust to be formed for a prospect of this value. Consider, for example, the fourth trust formation rule in Table 4. The prospect description is *Power certificate signature*. According to Table 3 this prospect has value 5. Further on, evidence formed by the rule supports trust level *High*. To sum up, the rule supports trust level *High* based on a prospect of value 5. To check whether this trust formation rule adheres to the trust formation requirements we look into Table 1. This table states that evidences based on prospects with prospect value 4 and 5 can support trust level *High*. This means that the fourth prospect rule in Table 4 meets the trust formation requirements.

The second asset exposure rule in Table 8 assigns access to the service *Report consumer consumption* and requires at least trust level *Low*. The service *Report consumer consumption* has the asset value 3 as shown in Table 7. This rule is then exposing an asset with asset value 3 based on a trust level *Low*. According to the PPO’s asset exposure policy requirement shown in Table 2, it is not allowed to give access to assets of value above 2 when the trust level is at *Low*. Hence, this is an example of an asset exposure rule that does not adhere to the asset exposure policy requirements. This is the only breach of adherence in the case of our example.

8 Step 5: Updating the Trust Policy to Reflect its Requirements

The trust policy formulated above allows the consumers to report their power consumption just by giving their postal address, which is not hard to fake. If the asset exposure rule had required trust level *Medium* instead of *Low* the customer would be required to log on with their *Customer authentication* which is quite normal for this kind of service. In that case, adherence with respect to the asset exposure policy requirement would be ensured. This change is implemented by inserting *Medium* instead of *Low* in the second row of Table 8.

9 Conclusion

We have presented DeSPoT, a method for the development and specification of policies for trust negotiation. The trust policy is linked to risk assessment through the requirements for the trust policy. The trust policy must adhere to the trust policy requirements to delimit the trust behavior within acceptable risk. The method supports negative (exposing) as well as positive (supporting) evidences, sensitive assets (credentials), separation between the trust formation and the asset exposure, static adherence check of the policy with respect to the trust policy requirements, and prospects that verify the properties of other prospects which are the general mechanism behind delegation of trust (recommendation). The method is built around a five step process. Our rule-based approach enables the development of a trust policy the enforcement of which ensures trust negotiations within the limits of acceptable risk. The method is independent from specific trust negotiation protocols, and does not assume such protocols to be predefined.

Our focus has been to create an easy-to-understand language for trust policies with few details, nevertheless containing the most important trust mechanisms. The language is made to be understandable for people knowing the target (e.g. a company) at the business level, while being useful and understandable for those that develop and maintain the business application. In this way we are able to assemble a trust policy that contains both the risk and asset knowledge from the business level and the technical knowledge about different security technologies in one trust policy. Such a combination may reveal inconsistencies in the perception of the trust domain internally in the company.

The approach to system authentication presented in [4] implements trust negotiation as described in [5] to build trust. Approaches like Trust-X [5], [6], [7], TrustBuilder [8], [9] and Protune [10], [11], [12] are examples of policy based access control systems for automated trust negotiation. While these approaches make use of mechanisms for building trust, the involved trust level is only implicit and not extracted as an explicit element of value in itself. Yao et al. presents in

[13] a value and privacy scoring for credentials and find an optimal exposure with minimal privacy and sufficient value to achieve access.

The automated trust negotiation proposed in [14] emphasizes that negative evidences cannot be supported because an agent only controls what it sends and not what it receives and therefore opens for Denial of Service (DoS) attacks. For this reason there is very few that support negative evidence. We believe, however, that negative trust evidence is important in trust management. Revocation of certificates, banning of accounts and blocking of credit cards are examples of activities based on new information resulting in lower trust. Hence, not all digital trust functions are non-decreasing. In our approach every use of evidence is based on the trust in the partner providing it. To conduct a DoS attack through negative evidence, one must exploit misplaced trust and be able to pose as a trusted communication partner. If this posing is possible, then the trust in the evidence is overrated. In a trust policy as well as in a security policy the risk may be underrated as this is a possibility in all risk analysis. The vital thing is to be aware of this fact, and try to avoid it.

Acknowledgments The research on which this paper reports has partly been funded by the Research Council of Norway through the DIGIT (180052/S10) project, and partly by the European Commission through the NESSoS network of excellence.

References

1. International Organization for Standardization (2009) ISO 31000 Risk management—principles and guidelines
2. Winslett M (2003) An introduction to trust negotiation. In: iTrust 2003, LNCS vol 2692. Springer pp 275–283
3. Håvaldsrud T, Møller-Pedersen B, Solhaug B, Stølen K (2011) DeSPoT: A method for the development and specification of policies for trust management. Technical report A20174, SINTEF
4. Seigneur J-M, Farrell S, Jensen CD, Gray E, Yong Chen Y (2004) End-to-end trust starts with recognition. In: Secur Pervasive Comput LNCS 2802:130–142
5. Bertino E, Ferrari E, Squicciarini A (2004) Trust negotiations: concepts, systems, and languages. Comput Sci Eng 6:27–34
6. Bertino E, Ferrari E, Squicciarini A (2004) Trust-X: a peer-to-peer framework for trust establishment. IEEE Trans Knowl Data Eng 16(7):827–842
7. Squicciarini A, Bertino E, Ferrari E, Paci F, Thuraisingham B (2007) PP-trust-X: A system for privacy preserving trust negotiations. ACM Trans. Inf Syst Secur 10
8. Lee A, Winslett M, Perano K (2009) TrustBuilder2: A reconfigurable framework for trust negotiation. In: Trust management III, IFIP, Advances in information and communication technology, vol 300. Springer, pp 176–195
9. Winslett M, Yu T, Seamons KE, Hess A, Jacobson J, Jarvis R, Smith B, Yu L (2002) Negotiating trust in the web. Internet Comput IEEE 6(6):30–37
10. Bonatti P, De Coi JL, Olmedilla D, Sauro L (2010) A rule-based trust negotiation system. IEEE Trans Knowl Data Eng 22:1507–1520
11. Bonatti P, Olmedilla D (2005) Driving and monitoring provisional trust negotiation with metapolicies. In: Proceedings of the sixth IEEE international workshop on policies for distributed systems and networks (POLICY'05), IEEE Computer Society, pp 14–23

12. De Coi JL, Olmedilla D, Zerr S, Bonatti P, Sauro L (2008) A trust management package for policy-driven protection and personalization of web content. In: Proceedings of the 2008 IEEE workshop on policies for distributed systems and networks (POLICY'08), IEEE Computer Society, Washington, DC, pp 228–230
13. Yao D, Frikken KB, Atallah MJ, Tamassia R (2008) Private information: To reveal or not to reveal. ACM Trans Inform Syst Secur TISSEC 12(1):61–627
14. Winsborough WH, Seamons KE, Jones VE (2000) Automated trust negotiation. DARPA Inform Surviv Conf Expo 1:88–102