Towards a Decision Model Based on Trust and Security Risk Management

Baptiste Alcalde[1] **Eric Dubois**[2] **Sjouke Mauw**[1] **Nicolas Mayer**[2] **Saša Radomirović**[1]

[1] Université du Luxembourg
Faculté des Sciences, de la Technologie et de la Communication
6, rue Richard Coudenhove-Kalergi,
L-1359 Luxembourg, Luxembourg
Email: baptiste.alcalde@uni.lu, sjouke.mauw@uni.lu, sasa.radomirovic@uni.lu

[2] CRP-Henri Tudor - CITI
29, Av. John F. Kennedy, L-1855 Luxembourg, Luxembourg
Email: eric.dubois@tudor.lu, nicolas.mayer@tudor.lu

Abstract

From choosing the daily lunch menu to buying or selling stock options, decisions have to be made every day. In general, due to incomplete information, making a decision carries a risk. Typically, such risks are mitigated through risk management.

However, risk is not the only element involved in the decision process. When the decision to be made concerns an interaction between two entities, trust plays an important role. Trust, in such an interaction, is a prediction of one entity's reliance on the other entity to perform a certain action.

In this paper we formulate a trust reference model and take a first step towards a decision model by combining the trust model with an existing risk model. The decision model is illustrated by an example in the e-banking domain.
Keywords: Decision, Security Risk Management, Trust

1 Introduction

Heads or tails, chicken or beef, to buy or to sell – we have no choice but to make decisions all the time. Every decision carries a risk and we prefer, therefore, to base decisions on as complete and sound information as possible. Since frequently only partial information is available, one important part of the decision making process is risk management. Another, in everyday decisions equally important, part of decision making is *trust*. Trust is used as a prediction of reliance on an action, based on what one party, the *trustor*, knows about another party, the *trustee*. Relevant information in such a context could be the trustor's experience and reputation, a third-party's recommendation, and so forth.

In this paper, we initiate an investigation into decision making based on trust and risk management with a focus on security. In particular, we are using, say, the level of trust a client has in a service provider to the quality of the security risk management performed by the provider in order to facilitate a client's decision whether or not to engage in a transaction with the provider.

Trust and risk management are currently two very broad and active research topics. Nevertheless, a number of research questions are still to be addressed concerning the implications of trust and risk in the decision process. The specific research question addressed in this paper is *what are the concepts involved in a decision model based on trust and risk?* A modeling-based approach is used to identify the different concepts and explain their relationships. The benefits of the model are a clear ontology of concepts existing in the trust and risk domains and a formalization of these concepts which enables the next step toward automated support of the decision making process.

The paper is structured as follows. Section 2 introduces the risk management domain related to IS security and summarizes the risk management model. In Section 3, after an introduction to the notion of trust, the trust domain model is defined. The relation between the two models is discussed in Section 4, based on which a preliminary model is developed. An example is presented in Section 5 in order to illustrate the model through an instantiation. The paper ends with conclusions and an indication of open research questions in Section 6.

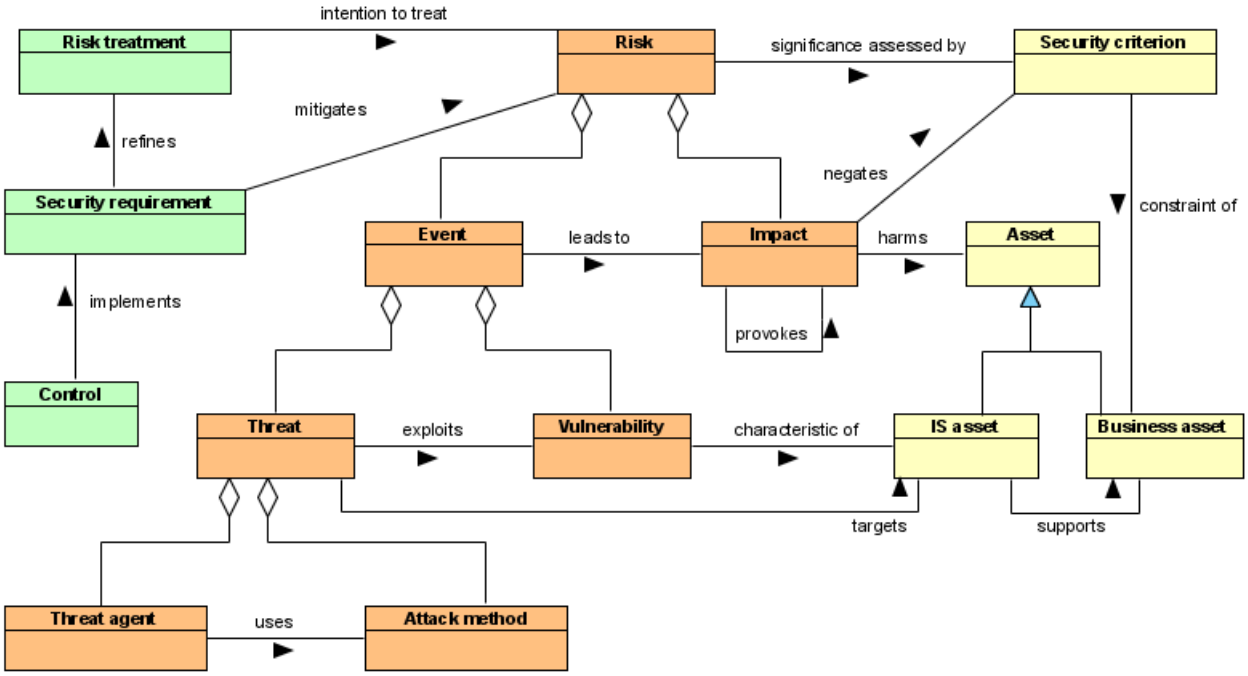

Figure 1: The ISSRM domain model

2 The Information System Security Risk Management Model

In this section the Information System Security Risk Management (ISSRM) domain and its reference model are summarized. This model has been established in previous research (Mayer et al., 2007) and has been applied to assess the support of some existing modeling languages with regards to the ISSRM domain (Matulevičius, Mayer and Heymans, 2008; Matulevičius, Mayer, Mouratidis, Dubois, Heymans and Genon, 2008).

ISSRM aims at protecting *assets* of an organization, from all harm to *IS security* which could arise accidentally or deliberately, by using a *Risk Management* approach.

Assets need to be secured because they are exposed to security risks when they are supported by an IS. In IS security, assets are to be protected in terms of the standard security criteria, i.e. confidentiality, integrity, and availability of information. Further properties such as authenticity, accountability, non-repudiation, and reliability may also be considered, depending on the context and objectives of the organization.

The ISSRM domain model shown in Fig. 1 has been obtained by identifying the core concepts in existing ISSRM literature and carefully analyzing the relationships between these concepts. The complete research methodology applied to arrive at this model has been described in (Mayer et al., 2007).

The core definitions of ISSRM concepts, are organized in three categories, asset-related concepts, risk-related concepts, and risk-treatment related concepts which are also color-coded in Fig. 1.

Asset-related concepts describe which assets are important to protect, and which criteria guarantee asset security. An *asset* is anything that has value to the organization and that is central in the achievement of its objectives (ISO, International Organisation for Standardisation, 2005). A *business asset* describes information, processes, capabilities, and skills inherent to the business of the organization. An *IS asset* is a component of the IS supporting business assets. *Security criterion* characterizes a property or constraint on business assets describing their security needs.

Risk-related concepts present how the risk itself is defined. A *risk* is the combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. An *impact* describes the potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or the cause of a risk) is accomplished. The *event*, in the frame of IS security, is the combination of a threat and one or more vulnerabilities. A *vulnerability* describes a characteristic of an IS asset or group of IS assets and that can constitute a weakness or a flaw in terms of IS security. A *threat* characterizes a potential attack or incident, which targets one or more IS assets that may lead to harm the assets. A

threat agent is an agent that can potentially cause harm to IS assets. An *attack method* is a standard means by which a threat agent carries out a threat.

Risk treatment-related concepts describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. A *risk treatment* is a decision of the intention to treat identified risks. A *security requirement* is the refinement of a risk treatment decision to mitigate the risk. *Controls* (countermeasures or safeguards) are means designed to improve security, specified by a security requirement, and implemented to comply with it.

3 The Trust Model

In the present section, we define the notion of trust we consider. We develop our trust model based on a similar methodology as the one used to arrive at the risk model presented in the previous section.

3.1 Definition of Trust

Trust lies at the intersection of several domains, including sociology, psychology, law, economics, ethics, and computer science. For instance, in (Riegelsberger et al., 2005; Grabner-Kräuter and Kaluscha, 2003; Corritore et al., 2003) the interplay of human and social sciences with computer science has lead to a new model of on-line trust.

Trust has been defined in several different ways. The definition of trust adopted here, first formulated by Gambetta (Gambetta, 1988), is often referred to as "reliability trust". Thus, we define *trust* as the belief or subjective probability of the *trustor* that the *trustee* will adequately perform a certain action on which the trustor's welfare depends. We also refer to the trustor and trustee as agents, which may be humans or computer programs acting on the behalf of humans. Trust is hence a quantifiable relation between two agents.

3.2 The Consolidated Trust Model

In this section we discuss the concepts related to trust. Starting point of our discussion is a selection of papers representing the main views on the topic. Table 1 shows the various concepts used in the trust literature.

Previous work has shown that trust is affected by several subjective characteristics, such as social status, physical properties, and state of mind (Hassell, 2005; Hofstede et al., 2006; Marsh, 1994; Ziegler and Lausen, 2004; Vasalou and Pitt, 2005; Zak et al., 2004; Zak, Kurzban and Matzner, 2005; Zak, Borja, Kurzban and Matzner, 2005). These characteristics are commonly referred to as the *personality* of a human being. The characterization of the decision maker's personality naturally takes advantage of psycho-sociological contributions.

Another notion related to trust is *competence*. It refers to an objective measure of the abilities of the trustee to perform a given task. The competence value is increased for instance by the trustee's diplomas, certificates, years of experience, and so on.

Yet another factor influencing trust is formed by the *opinion* of other entities. To every interaction between two *agents*, the trustor can assign an opinion. The opinion can be any type of valuation, for instance a real value between 0 and 1, or a simple rating such as good or bad. The *reputation* of a trustee is a function of *third parties*' opinions from previous interactions with the trustee. A large number of papers on trust management systems includes reputation as a main concept (Resnick et al., 2000; Kamvar et al., 2003; Kinateder and Rothermel, 2003; Jøsang et al., 2003; Liu and Issarny, 2004; Nielsen and Krukow, 2004; Krukow et al., 2005; Shmatikov and Talcott, 2005; Traupman and Wilensky, 2006; Jøsang et al., 2007). If reputation systems allow a trustor to use third parties' opinions about a trustee, the trustor can also ask for third parties' recommendations (Jøsang et al., 2006; Gray et al., 2003; Seigneur et al., 2005). A *recommendation* from a trustor to a trustee is typically obtained when there is a chain of trusted entities from the trustor to the trustee.

Trust decisions are also defined to be dependent on the context. The *context* is information such as time, location, local norms and customs. For instance, healthcare advice in a hospital may be trusted differently than healthcare advice in the supermarket. Context denotes a set of elements that are independent of the trustor and the trustee.

To compute its trust, the trustor uses a *policy*, which is a function over reputation, recommendation, competence, and context as described above. The policy is the way the trustor weighs the various information in order to make a decision about a transaction and reflects the subjectivity in trust. For instance, if a trustor A weighs the recommendation more than the reputation, and a trustor's friend C tells that the trustee B is very bad, A can decide not to cooperate with B despite B's very good reputation.

Our *consolidated trust model* unifies the concepts we have studied above and the models based on them into one single model. The graphical representation of this model is displayed in Fig. 2.

4 The Decision Model

In this section we present a decision model which is based on an agent's trust in an action of a trustee as well as the risk in the trustee's IS in the sense defined in Section 2 and as assessed by an external party.

To arrive at our decision model, we investigate how risk and trust relate to each other in the decision process and identify the overlap between them.

4.1 The Decision Process

Given a problem, a decision process aims to resolve the problem by choosing one of several available options. This process can be decomposed into three phases, which are the information gathering phase, the information analysis phase, and the decision making phase.

Paper	Trustor	Trustee	Asset	Policy	Personality	Recommendation	Reputation	Third Party	Competence	Context
(Hassell, 2005)	×	×	×		×					
(Hofstede et al., 2006)	×	×	×		×					
(Carbone et al., 2003)	×	×	×	×		×				
(Agudo et al., 2005)	×	×	×							
(Jøsang et al., 2006)	×	×	×			×		×		
(Jøsang et al., 2005)	×	×	×			×	×	×		
(Ruohomaa and Kutvonen, 2005)	×	×	×				×	×		
(Essin, 1997)	×	×	×	×			×	×	×	×
(Viljanen, 2005)	×	×	×	×		×	×	×	×	×

Table 1: Various concepts in trust literature.

In the literature there are three approaches to making decisions. In the field of operations research, decision is an optimization problem which does not involve the decision maker nor the context of the decision. For H.A. Simon (Simon, 1947 (4th ed. 1997), the decision includes analysis of the decision maker's rationality but not the context. A third school of thought, which is adopted here and shared for instance by G.A. Klein (Klein and Zsambok, 1996), takes both the decision maker and the context into account.

Although the notions of risk and trust are recognized as essential in the decision process, the relation between the two has not yet been formally stated. In the following section, we present this relation.

The resulting decision model has several advantages. Compared with existing decision models, the present one adds more granularity and sharpness to the notions of trust and risk, as well as to their relation in the decision process. Moreover, this model has the methodological advantage of providing a separation of concepts for the various elements considered in the decision process. This enables the entire model to benefit from improvements to any of its elements. Finally, the model is independent of decision metrics and algorithms. Thus, various metrics and algorithms can be used to evaluate decisions automatically. Furthermore, different metrics and algorithms could be compared to each other by plugging them into the model. This last aspect, however, will only be considered in future work.

4.2 Building the Decision Model

Several studies have shown a link between trust and risk in the decision process. Some authors believe that risk is an element of trust (Viljanen, 2005; Jøsang and Lo Presti, 2004; Brændeland and Stølen, 2004; Dimmock et al., 2005; Cvrcek and Moody, 2005), while it is our position (as follows from our definitions of trust and risk), shared by (English et al., 2004), that trust and risk are intimately related, but that neither comprises the other. Trust and risk are two important, partially overlapping components which are taken into account when an agent decides whether or not to engage in a transaction. Therefore, the question is how to join the trust and risk models, while taking the overlaps into consideration.

We take all components of both models into consideration and study the links and overlaps in these components in order to produce the decision model.

The central point of this decision model is the trustor, since he is the decision maker. The decision itself is not an object but an attribute of the trustor, since it is computed by him.

In order to make a decision, the trustor will assess the IS risks and evaluate the trust he has in the service provided by the trustee. The trustor will have to combine these two elements through a decision algorithm in order to know whether he decides to use the service. The decision algorithm depends on what metrics for risk and trust are used. As standard trust metrics are not defined to date and their development is left for future work, decision algorithms are consequently out of the scope of the current paper.

Another important link between the risk model and the trust model are the assets. The trustor's assets are at risk in the IS and entrusted to the trustee.

At a meta-model level, we haven't identified further overlaps of the trust and risk model in the decision model, but other views of the model can emerge when considering different objectives at a model level for example. Our decision model cannot represent such views without loosing generality. The consequence of taking another point of view could be the fusion of several components in the decision model. For instance, if we consider a setting where the trustee is malicious, then we can fuse the trustee and the threat agent, hence modifying the way risk is assessed. In another view, we could consider that some of the trustee's certificates can be seen as both an acknowledgment of risk treatment and a competence.

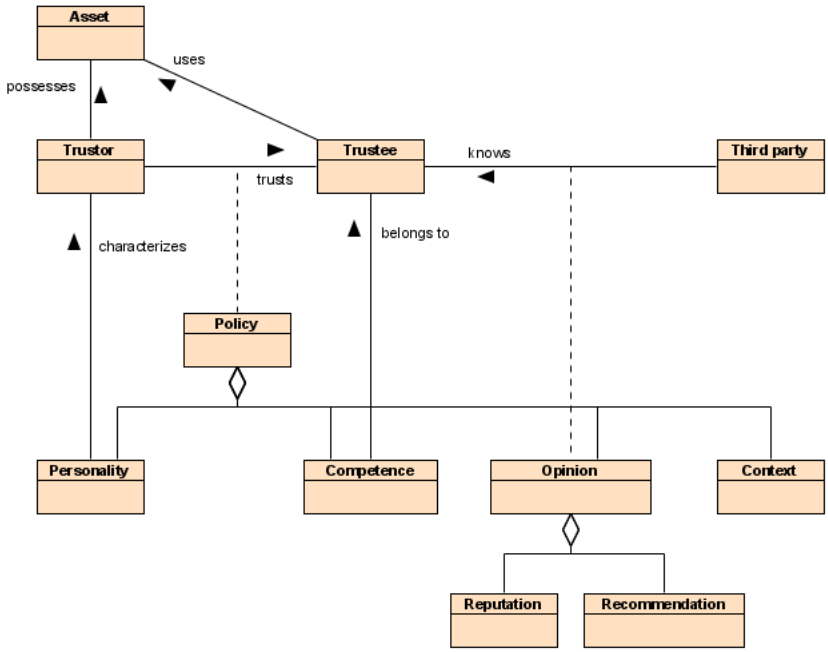

Figure 2: The Consolidated Trust Model

The resulting Decision Model is displayed in Fig. 3.

5 An Illustrative Example

In this section we illustrate some of the details of the decision model through a simple example from the field of e-banking. We show how the various elements in the decision model get instantiated when trying to assess a client's decision to use a particular bank's e-service.

Our decision model applied to any e-service environment leads to a decision process involving a client as the decision maker and a service provider as the trustee. The decision process takes into account the client's trust in the service provider (to operate on the client's assets) as well as the risks existing in the provider's IS as assessed by an external party.

We consider the fictitious company *Superbank.com* as the service provider and the equally fictitious client *Mr. J. Hancock* as the client. Superbank.com has been in business for 5 years and has been issued an ISO/IEC 27001 certificate which boosts the banks *competence* score. A well-known rating company gives Superbank.com 8 out of 10 stars and Mrs. Hancock has been a satisfied customer for over a year. It can be expected that Mr. Hancock has some basic trust in e-banking services, since he's young and holds a Master's degree. The age, sex, and academic degree are examples of Mr. Hancock's *personality*. He understands some of the risks involved in using an e-banking service and understands enough about the auditing process to value the ISO/IEC 27001 certificate. Mr. Hancock cares about his wife's opinion, hence giving significant weight to her *recommendation*, but also to the bank's impeccable reputation for not selling customer's data to telemarketers. These factors all enter into Mr. Hancock's *policy* for evaluating his trust in Superbank.com. The assets Mr. Hancock is entrusting to the bank are his phone number, address, further personal details, and a certain amount of money.

The bank's security objectives with respect to their IS are to keep their customer's personal information confidential and to maintain the integrity of this information. An external, independent company has evaluated the bank's risks for these *security criteria*. The external company focused on assessing typical hacker attacks and evaluated the risks for phishing, SQL injections, and man-in-the-middle exploits. The external company used known probability distributions for these threats and took into account the known vulnerabilities the bank's system has. This allowed the company to compute the likelihood of an undesired event and the impact such an event has on the bank's assets which are comprised of their IS and their clients' personal information. The assessment considered the mitigating factors provided by the risk treatment the bank employs. Table 2 summarizes the data in this example.

Note that the purpose of the example is not to make a decision, but rather to explain the model. In order to make a decision based on the presented data, metrics will

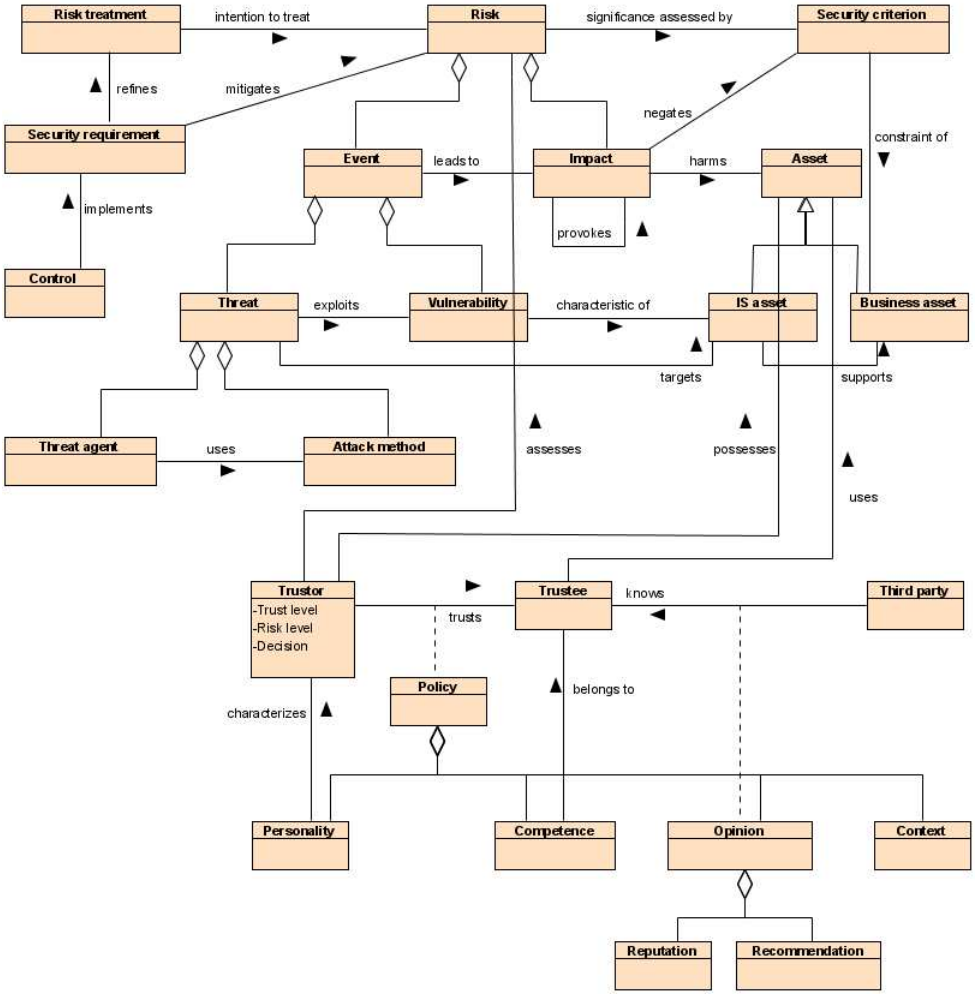

Figure 3: The decision model

need to be introduced into the model. This will be addressed in future work.

6 Conclusion and Future Work

We have made a first step towards a decision model which takes into account trust and IS security risks. We have arrived at this model by using an existing risk model and designing a new trust model. The trust model has been arrived at through the same research methodology that was applied in the creation of the risk model and presented in (Mayer et al., 2007). We have illustrated the model on a fictitious example from the e-banking domain.

Future work will naturally focus on the decision model's refinement, the introduction of metrics into the model, and the development of a modeling language. Furthermore, there are elements besides trust and risk which enter into a decision process. Two particular examples which will be addressed in future work are *conviviality* and *perceived usefulness*, but several further elements are conceivable.

Finally, other decision models based on trust and risk should be investigated. A particularly interesting model to consider would be one where the risk to be assessed is the trustor's risk resulting from the consequences of his decision, as opposed to the risk existing on the trustee's side which was considered in this paper.

References

Agudo, I., Lopez, J. and Montenegro, J. A. (2005), A representation model of trust relationships with dele-

Trustor	Mr. J. Hancock
Personality	*Age*: 25, *Sex*: M, *Education level*: Master
Policy	Insist on certification
	Reputation of bank $\geq 7/10$
	No negative recommendations
	Ignore context information
Third Parties	*1*: E-banking comparator
	2: Mrs. Hancock
Trustee	Superbank.com
Competence	*Experience*: 5 years, *Certification*: ISO/IEC 27001
Reputation	*Third party*: E-banking comparator, *Score*: 8/10
Recommendation	*Third party*: Mrs. Hancock, *Grade*: Good
Context	*Misc*: Good economical context
Business assets	Client data, Client's financial assets
IS assets	Customer database, Network
Security criteria	*Confidentiality of trustor's personal information*: 3/4
	Integrity of trustor's personal information: 4/4
Threat agent	Hacker
Attack method	Man in the middle
	SQL query
	Phishing
Threats	Hacker using man in the middle, *Likelihood*: 2/3
	Hacker using SQL query, *Likelihood*: 1/3
	Hacker using phishing, *Likelihood*: 3/3
Vulnerabilities	TCP/IP protocol weaknesses, *Level*: 2/3
	User unawareness, *Level*: 1/3
Events	Hacker using man in the middle exploiting TCP/IP protocol weaknesses, *Potentiality*: 3/5
	Hacker using SQL query exploiting TCP/IP protocol weaknesses, *Potentiality*: 2/5
	Hacker using phishing exploiting user unawareness, *Potentiality*: 3/5
Impact	Loss of personal information confidentiality, *Level*: 3/4
	Loss of personal information integrity, *Level*: 4/4
Risks	Hacker using man in the middle exploiting TCP/IP protocol weaknesses leading to loss of personal information confidentiality and integrity, *Level*: 12/20
	Hacker using SQL query exploiting TCP/IP protocol weaknesses leading to loss of personal information confidentiality and integrity, *Level*: 8/20
	Hacker using phishing exploiting user unawareness leading to exposure of user's login/password and then to loss of personal information confidentiality and integrity *Level*: 12/20
Risk treatment	Reduce risks with security measures on the IS
Security requirement	Perform security awareness
	Perform network filtering
Control	Define and follow a planning for security awareness training
	Install and configure a firewall and an IDS

Table 2: An example instantiation of the decision model.

gation extensions, *in* P. Herrmann et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 116–130.

Brændeland, G. and Stølen, K. (2004), Using risk analysis to assess user trust, *in* C. J. et al., ed., 'Trust Management, Second International Conference, iTrust 2004', Vol. 2995 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Oxford, UK, pp. 146–160.

Carbone, M., Nielsen, M. and Sassone, V. (2003), A formal model for trust in dynamic networks, *in* A. Cerone and P. Lindsay, eds, 'Proceedings of Int. Conf. on Software Engineering and Formal Methods, SEFM 2003', IEEE Computer Society, Brisbane, Australia, pp. 54–61.

Corritore, C. L., Kracher, B. and Wiedenbeck, S. (2003), 'On-line trust: concepts, evolving themes, a model', *International Journal Human-Computer Studies* **58**(6), 737–758.

Cvrcek, D. and Moody, K. (2005), Combining trust and risk to reduce the cost of attacks, *in* P. H. et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 372–383.

Dimmock, N., Bacon, J., Ingram, D. and Moody, K. (2005), Risk models for trust-based access control (tbac), *in* P. Herrmann et al., ed., 'Trust Management,

Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 364–371.

English, C., Terzis, S. and Wagealla, W. (2004), Engineering trust based collaborations in a global computing environment, *in* C.D. Jensen et al., ed., 'Trust Management, Second International Conference, iTrust 2004', Vol. 2995 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Oxford, UK, pp. 120–134.

Essin, D. J. (1997), Patterns of trust and policy, *in* 'NSPW '97: Proceedings of the 1997 workshop on New security paradigms', ACM, New York, NY, USA, pp. 38–47.

Gambetta, D., ed. (1988), *Trust: Making and breaking cooperative relations*, Department of Sociology, University of Oxford.

Grabner-Kräuter, S. and Kaluscha, E. A. (2003), 'Empirical research in on-line trust: a review and critical assessment', *International Journal on Human-Computer Studies* **58**(6), 783–812.

Gray, E., Seigneur, J.-M., Chen, Y. and Jensen, C. (2003), Trust propagation in small worlds, *in* P. Nixon and S. Terzis, eds, 'Trust Management, First International Conference, iTrust 2003', Vol. 2692 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Heraklion, Crete, Greece, pp. 239–254.

Hassell, L. (2005), Affect and trust, *in* P. Herrmann et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 131–145.

Hofstede, G. J., Jonker, C. M., Meijer, S. and Verwaart, T. (2006), Modelling trade and trust across cultures, *in* Ketil Stølen et al., ed., 'Trust Management, 4th International Conference, iTrust 2006', Vol. 3986 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Pisa, Italy, pp. 120–135.

ISO, International Organisation for Standardisation (2005), *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements*, International Organisation for Standardisation, Geneva, Switzerland.

Jøsang, A., Hird, S. and Faccer, E. (2003), Simulating the effect of reputation systems on e-markets, *in* P. Nixon and S. Terzis, eds, 'Trust Management, First International Conference, iTrust 2003', Vol. 2692 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Heraklion, Crete, Greece, pp. 179–194.

Jøsang, A., Ismail, R. and Boyd, C. (2007), A survey of trust and reputation systems for online service provision, *in* 'Decision Support Systems', Vol. 43/2, Elsevier Science B.V., pp. 618–644.

Jøsang, A., Keser, C., and Dimitrakos, T. (2005), Can we manage trust, *in* P. Herrmann et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 93–107.

Jøsang, A. and Lo Presti, S. (2004), Analysing the relationship between risk and trust, *in* C.D. Jensen et al., ed., 'Trust Management, Second International Conference, iTrust 2004', Vol. 2995 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Oxford, UK, pp. 135–145.

Jøsang, A., Marsh, S. and Pope, S. (2006), Exploring different types of trust propagation, *in* Ketil Stølen et al., ed., 'Trust Management, 4th International Conference, iTrust 2006', Vol. 3986 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Pisa, Italy, pp. 179–192.

Kamvar, S. D., Schlosser, M. T. and Garcia-Molina, H. (2003), The eigentrust algorithm for reputation management in p2p networks, *in* 'Proceedings of the 12th international conference on World Wide Web (WWW'03)', ACM press, New York, NY, USA, pp. 640–651.

Kinateder, M. and Rothermel, K. (2003), Architecture and algorithms for a distributed reputation system, *in* P. Nixon and S. Terzis, eds, 'Trust Management, First International Conference, iTrust 2003', Vol. 2692 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Heraklion, Crete, Greece, pp. 1–16.

Klein, G. A. and Zsambok, C. E., eds (1996), *Naturalistic Decision Making*, Lawrence Erlbaum Associates.

Krukow, K., Nielsen, M. and Sassone, V. (2005), A framework for concrete reputation-systems with applications to history-based access control, *in* '12th ACM Conference on Computer and Communication Security CCS'05', ACM press, Alexandria, VA, U.S.A., pp. 260–269.

Liu, J. and Issarny, V. (2004), Enhanced reputation mechanism for mobile ad hoc networks, *in* C.D. Jensen et al., ed., 'Trust Management, Second International Conference, iTrust 2004', Vol. 2995 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Oxford, UK, pp. 48–62.

Marsh, S. (1994), Optimism and pessimism in trust, *in* J. Ramirez, ed., 'Proceedings of the Ibero-American Conference on Artificial Intellingence (IBERAMIA94/CNAISE'94)', McGraw-Hill, Caracas, Venezuela.

Matulevičius, R., Mayer, N. and Heymans, P. (2008), Alignment of misuse cases with security risk management, *in* 'Proc. 3rd Int. Conf. on Availability, Security

and Reliability (ARES '08), Symposium on Requirements Engineering for Information Security (SREIS '08)', IEEE Computer Society, pp. 1397–1404.

Matulevičius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P. and Genon, N. (2008), Adapting secure tropos for security risk management during early phases of the information systems development, *in* 'Proc. 20th Int. Conf. on Advanced Information Systems Engineering (CAiSE '08)', Springer.

Mayer, N., Heymans, P. and Matulevicius, R. (2007), Design of a modelling language for information system security risk managemen, *in* '1st Int. Conf. on Research Challenges in Information Science (RCIS 2007)', Ouarzazate, Morocco.

Nielsen, M. and Krukow, K. (2004), On the formal modelling of trust in reputation-based systems, *in* H. Maurer et al., ed., 'Theory is Forever', Vol. 3113 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, pp. 192–204.

Resnick, P., Kuwabara, K., Zeckhauser, R. and Friedman, E. (2000), 'Reputation systems', *Communication of the ACM* **43**(12), 45–48.

Riegelsberger, J., Sasse, M. A. and McCarthy, J. D. (2005), 'The mechanics of trust: A framework for research and design', *International Journal on Human-Computer Studies* **62**(3), 381–422.

Ruohomaa, S. and Kutvonen, L. (2005), Trust management survey, *in* P. Herrmann et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 77–92.

Seigneur, J.-M., Gray, A. and Jensen, C. D. (2005), Trust transfer: Encouraging self-recommendations without sybil attack, *in* P. Herrmann et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 321–337.

Shmatikov, V. and Talcott, C. (2005), 'Reputation-based trust management', *Journal of Computer Security* **13**(1), 167–190.

Simon, H. A. (1947 (4th ed. 1997)), *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*, The Free Press.

Traupman, J. and Wilensky, R. (2006), Robust reputations for peer-to-peer marketplaces, *in* Ketil Stølen et al., ed., 'Trust Management, 4th International Conference, iTrust 2006', Vol. 3986 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Pisa, Italy, pp. 382–396.

Vasalou, A. and Pitt, J. (2005), Reinventing forgiveness: A formal investigation of moral facilitation, *in* P. Herrmann et al., ed., 'Trust Management, Third International Conference, iTrust 2005', Vol. 3477 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Paris, France, pp. 146–160.

Viljanen, L. (2005), Towards an ontology of trust, *in* 'Trust, Privacy and Security in Digital Business', Vol. 3592 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, pp. 175–184.

Zak, P. J., Borja, K., Kurzban, R. and Matzner, W. T. (2005), 'The neuroeconomics of distrust: Physiologic and behavioral differences between men and women', *American Economic Review* **95**(2), 360–363.

Zak, P. J., Kurzban, R. and Matzner, W. T. (2004), The neurobiology of trust, *in* 'Annals of the New York Academy of Sciences', Vol. 1032, pp. 224–227.

Zak, P. J., Kurzban, R. and Matzner, W. T. (2005), Oxytocin is associated with human trustworthiness, *in* 'Hormones and Behavior', Vol. 48, pp. 522–527.

Ziegler, C.-N. and Lausen, G. (2004), Analyzing correlations between trust and user similarity in online communities, *in* C.D. Jensen et al., ed., 'Trust Management, Second International Conference, iTrust 2004', Vol. 2995 of *Lecture Notes in Computer Science*, Springer-Verlag Berlin Heidelberg, Oxford, UK, pp. 251–265.