Opinions classification in information security risk assessments with social networks analysis

Víctor Leonel Orozco López[1], **Raul Ceretta Nunes**[1]

[1]Centro de Tecnologia – Universidade Federal de Santa Maria (UFSM)
Av. Roraima 1000 – 97.105-900 – Santa Maria – RS – Brasil

vlopez@inf.ufsm.br, ceretta@inf.ufsm.br

Abstract. *Although there is a wide range of tested risk assessment methods, a common problem between these resides in the possibility of a bias in the data collection process. This occurs specially in contexts where a deterministic source of information is unavailable. To avoid this limitation, this work proposes a risk assessment process that classifies interview options based on trust quantification with social network analysis.*

1. Introduction

Risk assessment phase constitutes the basis of a successful risk management process, due to the information generated at this stage will conduct actions and investments to avoid risks in a organization operations. Thus it is becoming a key component of Enterprise Risk Management and related Application Guidance [PriceWaterhouseCoopers 2008].

Although there is a wide consensus about the effectiveness of the risk assessments for risks quantification, there are many methods to achieve it. Some of them are based on deterministic data sources and others on interviews with human beings. As showed in [Amaral et al. 2010], the interview based methods have a common inconvenience: the results of risk assessment could be biased by the subjective nature of the human beings opinions, affecting the final result and distorting the risks priority rankings.

By considering the interview based method a wide used method, this work explores the classification of interview opinions to reduce the bias of the risk assessment. Our proposal is to use trust as a parameter for qualification of the opinions about the possible risks. The key of our solution is that if we are able to measure the perception of trust in a human social network, we could use that quantification to assert if an opinion could be considered as good or bad.

The rest of the work is organized as follows. Section 2 reviews related literature and shows that there exist a direct relation between trust and risk. Section 3 explains the directions of how social networks can be used for trust quantification and section 4 proposes the usage of social networks within risk assessment phase. In the section 5 we explain the final considerations and future work.

2. Trust and risk

Risk in information security context is the likelihood that a threat could take advantage of a vulnerability associated to an information asset, causing adverse effects in various areas including economical and social scopes.

To avoid the negative effects of risks, the standard ISO/IEC 27005[ISO 2011] presents a series of steps conducted by a risk committee to identify, assess and address any risks through risk management process. These steps are: context definition, risk identification, risk estimation, risk evaluation, risk treatment, risk acceptance, risk communication and risk monitoring and review. The standard also emphasizes the importance of risk discovery by grouping the first three phases in a container phase called risk assessment, which is in charge of the risks definitions and prioritization.

[Amaral et al. 2010] states that although diverse risk assessment methods have the same objective and goals, some methods could derive in different results for the risk assessment. To fill the gaps between different methods on information security context -i.e. ISRAM, AURUM, ARIMA and FMEA-, they constructed a methodology that composes the results between the different methods.

However, the deviation is not only influenced by the method, but also by the information received as input when this information is subjective, like the ones collected on interviews with human beings.[Senik 2005] has highlighted the interviews, can provide some facts that are not available on deterministic data, where the only way to assume that a subjective data is well enough will depend on the trust levels of the source of information [Ko et al. 2005].

In this sense, [Lund et al. 2010] explicitly express that trust is inherently related to risk, and that an important part of managing trust is to comprehend the risks involved in trust-based interactions. In these interactions the positive and negative outcomes correspond to the trust measure opportunities and the build trust offers risks that should be evaluated.

3. Constructing a trust metric for risk assessment

Despite the many possibilities that are enabled by the trust, its quantification is usually a non-trivial process. It requires the creation of complex models to generate approximations to reality. Thus, to construct a trust quantification process, it must be defined which characteristics are desirable to get a meaningful trust quantification. A minimum set of desirable characteristics for a trust quantification process are [Lukas and Walgenbach]:

1. The quantification should take into account the presence of loss;
2. The quantification should avoid naivety; and
3. The quantification should evolve over time and increase in presence of non-opportunistic behavior.

3.1. Trust quantification methods

Trust quantification methods were commonly started with single-run evaluations in the organizational environment based on interviews and questionnaires, but it should not be considered a reliable trust metric because there is no evolution over time.

From [Manchala 2000] we know that trust could be built over time upon measurable variables in form of chains of trust between participants in a transaction to evaluate its risk. The e-commerce is a well known context that uses trust as basis to define deviations between possible good or bad experiences.

However, chains of trust are based on individual reputations of the participants that were constructed by reputation models, and many times those models present simple implementations and have a very intuitive understanding.

[Pinyol and Sabater-Mir 2011] stated, these quantification methods could present a lack of robustness, which has led to an increase in the research of the use of other trust determination methods where social network analysis is a promising approach.

3.2. Social networks

From [Cross et al. 2002], the construction of knowledge into an organization -like trust between colleagues- is a purely social process, and the speed for knowledge construction depends on how much easy is the communication between people. In this context it is also feasible to identify persons with important roles. Thus, it is possible to classify the importance of a human being within an organizational context.

In a social network this importance could be formally defined as centrality, a measure of power or influence of agents based on their importance into a network. The centrality can be calculated by measuring degree centrality (number of connections), closeness centrality (reach of the influence), betweenness centrality (bottlenecks constitutions) or using more elaborated algorithms [Tsvetovat and Kouznetsov 2011].

Our proposal is to take advantage of centrality (more specifically *trust centrality*) to classify the human opinions. The work hypothesis is that if it is possible to introduce the notion of trust into the risk assessment process, it is also possible to reduce the biases by giving priority to those opinions that are considered as more reliable. In practice we propose the introduction of TrustWebRank algorithm [Walter et al. 2009] into the risk assessment for information security context.

The motivations to choose TrustWebRank over other well-know social trust algorithms are enumerated following:

- TrustWebRank is not based only ratings over past experiences but also on trust that is present on the social network between agents.
- The evolution of trust perception is designed to map the natural trust evolution between human beings.
- By using TrustWebRank a direct relationship between all human-beings is not mandatory as long as they belong to the social network structure.

4. Trust aware risk assessment

4.1. Quantification with TrustWebRank

In its original definition, TrustWebRank is aimed to calculate the personalized trust for every one of the agents into a set of agents i that conform a social network, quantifying and classifying their *direct trust* perception -T_{ij}- over its neighborhood agents j where $T_{ij} \in (0, 1]$.

With $Tij = 0$ and degree $d = 0$ (number of connections), TrustWebRank introduces an *indirect trust* quantification based on feedback centrality over social networks relationships, where the indirect trust $\tilde{T}ij$ is defined by the equation 1 including three main characteristics: uniqueness of the solution, combination of direct and indirect

trust and normalization of trust. It also introduces a damping factor β which has a fixed value of 0.8 (determined as a product of their experiments) with an iterative variant -i.e. approximation- presented at the equation 2.

$$\tilde{T}_{ij} = S_{ij} + \beta \sum_{k \in N_i} S_{ij} \tilde{T}_{ij} \forall i, j \qquad (1) \qquad \tilde{T}_{ij}^{k+1} = S_{ij} + \beta \sum_{l \in N_i} S_{il} \tilde{T}_{lj}^{k} \forall i, j \qquad (2)$$

4.2. Introducing trust quantification into risk assessment

Given the diversity of methodologies available for risk assessments, and considering that [ISO 2011] only describes the general parameters of a risk analysis but not a specific implementation; in this work all considerations are made using [Amaral et al. 2010] as assessment method, with special focus on the impacts of trust centrality over the risk estimation.

In this method, risk identification is achieved with brainstorming between members of risk committee to get a consensus about assets, threats and vulnerabilities (selection of the members is discussed in a previous work [Primão et al. 2012]). Later, the risk committee defines qualification for every element and generates a list of risk with a *composite risk index* for every risk -i.e. risk estimation-. In the end that list is classified according to the context and risk acceptance policies -i.e. risk evaluation-.

In the risk estimation, every member of the security committee answers according to its knowledge, experience and competencies about p=probability, d=detection, o=occurrence, i=impact and s=severity of every risk. And, to standardize the input for the estimation, every participant choose only between qualitative adjectives with five possible values -i.e. very low, low, medium, high, very high- which are later converted to every method's scale.

Subsequently the original equations are normalized by multiplying the result of every assessment methods for different factors in order to get similar results as is presented on the equations at 3. The results of every equation are combined using an arithmetic average where the composite risk index CRI is defined as $CRI = \frac{\sum_{m \in M}}{n}$ where M = group of results, m = individual result, n = number of methods.

The trust quantification is then proposed by introducing a new factor t = trust, as show in weighted equations at 4. However, different to previous variables, this factor is not a product of interviews, it represents the centrality of the human beings.

$$\begin{aligned} Arima &= ((p \cap i) * 100)/5 \\ Isram &= ((p * i) * 100)/25 \\ Aurum &= ((p * i) * 100)/100 \\ Fmea &= ((s * o * d) * 100)/125 \end{aligned} \qquad (3) \qquad \begin{aligned} Arima &= ((p \cap i) * 100) * t/5 \\ Isram &= ((p * i) * 100) * t/25 \\ Aurum &= ((p * i) * 100) * t/100 \\ Fmea &= ((s * o * d) * 100) * t/125 \end{aligned} \qquad (4)$$

4.3. Analyzing trust influence with a model

To analyze the trust influence, we suppose an organization that conduct a risk management program in paralell to a trust management program, as suggested by [Lund et al. 2010]. From this we derive a graph with six agents a that have an initial estimated level of trust t.

We also assume a previous risk identification phase with six assets, twelve vulnerabilities and twelve threats, representing twelve potential risks from r_1 to r_{12}. Among the six agents, two have a higher coefficient of trust with range [0.7-0.9] and four have a medium coefficient of trust between [0.5-0.7). Additionally we also suppose that the risks r_3 and r_5, are in real life imminent risks that should be treated as soon as possible. But due the biased criteria, these risks are only considered in the range of [high - very high] by the reliable individuals and between [very low - high) for the rest.

Using the original risk assessment with random values between the previously described ranges, we got the results presented at the first half of Figure 1. Here it is evident that r_3 and r_5 do not reach higher priority because of the bias. Under those conditions these risks could not be considered for investment if the risk mitigation budget or the risk appetite does not cover the entire risk list.

Later, considering trust as a weighting factor, the bias is reduced as is presented in the second half of Figure 1. Here the introduction of trust as a weighting factor for the human opinions bias effectively reduced the bias using trust, where the risks considered as imminent $r3$ and $r5$ where ranked as top-middle risk, demonstrating that is feasible the introduction of trust with social networks into the risk assessment process.

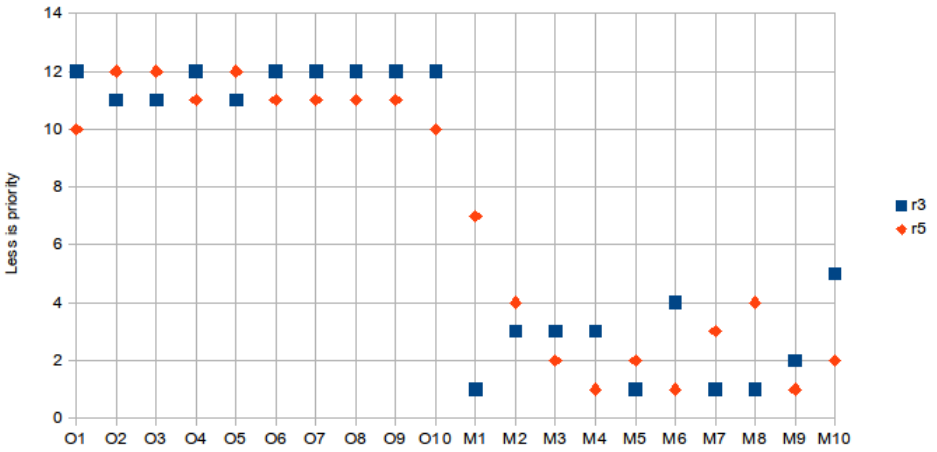

Figure 1. Original versus modified risk assessment

5. Final considerations

Throughout this work is evidenced the importance and the potential of the subjective data presenting inconveniences for risk assessments methods as described by [Amaral et al. 2010] where bad opinions could represent bad risk assessment results.

To counteract this problem this work explored the possibility of using trust as a metric to qualify human opinions, based on the affirmations of [Ko et al. 2005] and [Lund et al. 2010] about the properties of trust as a decision factor for good of bad opinions.

Based on the review of literature and modeling was possible to conclude that trust quantification through social network analysis is a feasible approach to reduce bias. At this time the trust-aware process is dependent on the availability of direct trust perceptions that are supposed to be a product of a parallel trust management program. In future works this relationship will be researched deeply, in order to integrate not only the metrics from social networks analysis but the whole process.

References

Amaral, E. H., Amaral, M. M., and Nunes, R. C. (2010). Metodologia para Cálculo do Risco por Composição de Métodos. In *Simpósio Brasileiro de Segurança de Informação e de Sistemas Computacionais*, pages 461–473.

Cross, R., Parker, A., and Borgatti, S. (2002). A bird's-eye view: Using social network analysis to improve knowledge creation and sharing. Technical report, IBM Institute for Business Value.

ISO (2011). *ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management*.

Ko, D., Kirsch, L., and King, W. (2005). Antecedents of knowledge transfer from consultants to clients in enterprise system implementations. *MIS quarterly*, 29(1):59–85.

Lukas, C. and Walgenbach, P. Trust me, it is High Trust: On Trust and its Measurement. Available at http://www.uni-konstanz.de/FuF/wiwi/workingpaperseries/WP_Lukas-Walgenbach-9-10.pdf.

Lund, M., Solhaug, B. r., and Stø len, K. (2010). Evolution in relation to risk and trust management. *Computer*, (May):49–55.

Manchala, D. W. (2000). E-commerce trust metrics and models. *Internet Computing, IEEE*, 4(April):36–44.

Pinyol, I. and Sabater-Mir, J. (2011). Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, pages 1–25.

PriceWaterhouseCoopers (2008). A practical guide to risk assessment*. Available at http://www.pwc.com/us/en/issues/enterprise-risk-management/publications/guide-to-risk-assessment-risk-management-from-pwc.jhtml.

Primão, A. P., Nunes, R. C., and López, V. L. O. (2012). Definição do Comitê de Análise/Avaliação de Riscos Baseado em Competências. In *XII SEPROSUL Semana de Engenharia de Produção Sulamericana*, pages 01–10, Assunción-Paraguay.

Senik, C. (2005). Income distribution and well-being: what can we learn from subjective data? *Journal of Economic Surveys*, 19(1):43–63.

Tsvetovat, M. and Kouznetsov, A. (2011). *Social Network Analysis for Startups: Finding Connections on the Social Web*, volume 3. O'Reilly Media, 1 edition.

Walter, F. E., Battiston, S., and Schweitzer, F. (2009). Personalised and dynamic trust in social networks. *Proceedings of the third ACM conference on Recommender systems - RecSys '09*, page 197.