Using Adaptive Decision Making based on Incomplete Trust in Electronic Commerce

Petri Puhakainen*, Catharina Candolin**, Hannu H. Kari**
(*)Laurea Polytechnic
Lehtimäentie 1 C, FIN-02600 Espoo, Finland
petri.puhakainen@laurea.fi
(**)Laboratory for Theoretical Computer Science
Helsinki University of Technology
P.B. 5400, FIN-02015 HUT
FINLAND
{catharina.candolin,hannu.kari}@hut.fi

Abstract: - In electronic commerce, a transaction typically occurs between a seller and a buyer. To execute such transactions securely, a trust relationship has to be built between the parties. In this paper, we present a framework for making decisions regarding electronic transactions based on incomplete trust relationships. The buyer performs a trust evaluation of the seller prior to executing the transaction. The trust evaluation is made based on previous experience of the seller as well as on the experience other buyers have had with the seller. After the transaction, the buyer updates its trust level of the seller for possible future use.

Keywords: - incomplete trust, e-commerce, electronic transaction, trust evaluation, risk analysis

1 Introduction

An *electronic transaction* is the exchange or transfer of funds, information, or services from one principal to another by electronic means. The principal may be either a human or a computer. In electronic commerce, a transaction typically occurs between a seller and a buyer. In many cases, the buyer is a human using a computer, whereas the seller is represented by a computer system.

In order to execute electronic transactions securely, the buyer and seller need to establish a trust relationship. In this paper, we mainly focus on the trust that the buyer has in the seller.

Establishing trust can be difficult, since the seller and buyer may be completely unknown to each other. Therefore, the buyer can use recommendors to help it evaluate the level of trust in the seller. For example, the buyer can query other buyers, such as friends or relatives, for their opinions, or rely on the statements made by a trusted authority. As the buyer makes transactions with the seller, it can gradually build its own notion of trust. However, the buyer may still continue to query other principals for their opinions.

In this paper, we present a framework for making decisions regarding electronic transactions based on incomplete trust relationships. The algorithm used is adaptive, that is, it takes previous experience into consideration when evaluating the level of trust in the other party.

2 Electronic trust

The concept of trust has been widely studied in the computer security literature [1][2][3][4][5][6][7].

In [4], trust in a principal is defined to be *a belief that the principal, when asked to perform an action, will act according to a predefined description.* This belief implies that the principal will not attempt to harm the requestor, regardless of how it carries out the request. Trust is always expressed in relation to a principal and to an action.

The different types of beliefs that a principal may have in another principal can be categorized as follows:

- **Benevolence:** the belief that the principal cares about the welfare of the requestor.
- **Honesty:** the belief that the principal makes agreements in good faith.
- **Competence:** the belief that a principal has the ability to perform a particular task.
- **Predictability:** the belief that the actions of a principal are consistent, and that the requestor thus can predict the behavior of the principal.

Trust is not necessarily transitive, that is, even if `A` trusts `B` and `B` trusts `C`, `A` does not necessarily trust `C`. Furthermore, trust need not be symmetric. The fact that `A` trusts `B` does not imply that `B` trusts `A`.

Decision making has traditionally been done based on the existence of trust, that is, the requestor either trusts the principal or lacks trust in the principal. In the former case, the transaction is executed, whereas in the latter case it is not.

2.1 Incomplete trust

To model the real world trust relationships more accurately, it must be realized that trust is incomplete. For the purpose of this paper, we define *incomplete trust* to be *a belief that the principal, when asked to perform an action, will, with probability* `p`*, act according to a predefined description.* Incomplete trust is always expressed in a relation to a principal, an action, and the probability that the action will be performed as agreed.

Incomplete trust has the same properties as complete trust, but the transitivity of trust changes. For example, if `A` trusts that `B` behaves as agreed with probability 0.8, and `B` trusts `C` to behave as agreed with probability 0.5., then `A` can calculate its trust in `C` by using the trust levels from itself to `B` and from `B` to `C`.

The level of trust may change over time due to the behavior of the principal. A principal that has behaved well in the past is assumed to be more trustworthy than a principal that is occasionally misbehaving. Furthermore, trust is likely to decrease faster than it increases since trust in a misbehaving principal will degrade immediately, whereas increasing trust happens gradually over time.

When making decisions based on incomplete trust, the level of trust is taken into consideration when performing the risk analysis. For example, if the risks are high and the trust level is low, then the transaction will not be executed. However, if the trust level is high or the risks are low, then the transaction will be executed.

3 Framework

When a buyer considers making a transaction with a seller, it starts by collecting information about the possible seller. The information can be based on its own experiences or the recommendations of others. Based on the gathered information, the buyer then evaluates the trust level it has in the seller. After that, the buyer performs a risk analysis, where it determines the possible consequences of performing or failing to perform the transaction. The risk analysis takes the level of trust into consideration. If the buyer makes the decision to execute the transaction, it will evaluate the success of the transaction and store the information for the future. The process of making a transaction is depicted in Figure 1.

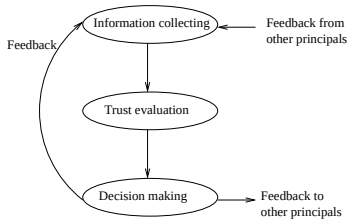

Figure 1: The process of making an electronic transaction

3.1 Collecting information

The principals considering to execute an electronic transaction need to gather information about each other in order to decide whether to execute the transaction in the first place.

Collecting information is done both locally and globally. Local information collecting is done by measuring the perceived success of executed transactions and is done by each principal individually. Global information collecting is done by querying

other principals for their perception of the trustworthiness of the other party.

The perceived success of transactions denote the *performance* of the other principal. This information is referred to as performance evaluation values (PE). The local PE is computed based on the transactions that the principal has made itself, whereas global PEs are based on the transactions made by others.

3.2 Evaluating trust

Before making the decision about whether to execute the transaction or not, the buyer needs to evaluate the trust it has in the seller. The level of trust is based on the local and global PEs. The local PE is assumed to be trusted 100%. However, when handling global PEs, the level of trust between the principals must be taken into consideration. The buyer may not trust a recommender completely, nor does the recommenders necessarily trust the principal that they obtain their recommendations from. Thus, a model based on managing incomplete trust relationships is applied when evaluating the trust between the buyer and the seller.

3.3 Decision making

Once the level of trust has been computed, a risk analysis must be performed in order to evaluate the possible risks related to an unsuccessful transaction and the possible consequences of not performing the transactions at all. Based on the outcome of the risk analysis as well as the level of trust, the decision regarding the execution of the transaction is made.

3.4 Feedback

After each electronic commerce transaction, the principals rate each other based on the perceived success of the transaction. The seller may be evaluated, for example, based on delivery time, promptness of delivery, and the quality of the delivered product. The buyer, on the other hand, may be evaluated based on payment time. The result of the rating is called a performance value (PV).

In large communities, where the number of transactions and sellers is large, it becomes infeasible to store all separate PVs. Therefore, only the n most recent PVs together with the time when the transaction was executed are stored. The PE of each seller is computed by a performance evaluation function, f_{PE}, which takes the PVs as input. The performance evaluation function gives more weight to more recent performance values in order to provide a better estimation of the current behavior of the seller.

The PEs are then stored for possible future use. The buyer can also act as a recommendor to another buyer.

4 Scenario

Let us assume that a buyer A has made a transaction with seller B. A now evaluates the success of the transaction, for example:

- X_1 = delivery time
- X_2 = promptness of delivery
- X_3 = quality of the product

Based on the measurements, A computes the performance value of the transaction:

$$PV = f_{PV}(X_1, X_2, \ldots, X_n) \quad (1)$$

A stores the PV of the transaction in its database as well as the time when the transaction was made. Due to storage restrictions, A may not be able to store all PVs it has made with B, but only the n most recent. If more than n PVs are stored, the oldest one is deleted.

A then performs the performance evaluation to update the PE. The PE is based on the values of the PVs as well as the time when they were executed. For example, A may define a policy that states that transactions older than 6 months will not be taken into consideration, transactions older then 3 months but newer than 6 months have a weight of 0.5, and newer transactions have a weight of 1. The weight is denoted by c in the formula below:

$$PE = f_{PE}(c_1 * PV_1, c_2 * PV_2, \ldots, c_n * PV_n) \quad (2)$$

The next time A considers making a transaction with B, it needs to make a trust evaluation. For example, in Figure 2, A is about to execute a transaction with B and has collected the available PEs.

In this case, the value of the local PE is 0.8, i.e. 80%. A also queries X and U for their PEs. X does not have a PE of its own, so it queries Y, which responds with a PE of 0.5, i.e. 50%. Since A has a trust level of 90% with X, which in turn trusts Y with a level of 80%, A computes the value of the PE to be $0.9 * 0.8 * 0.5 = 0.36$, i.e. 36%. Similarly, the PE of the path via U, V, and W is computed to be 0.43, i.e. 43%.

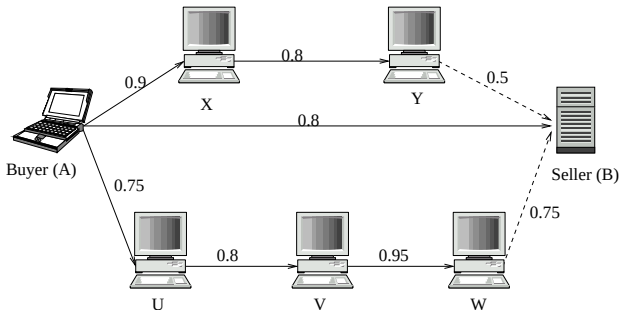

Figure 2: Evaluating the trust level between the buyer and the seller by using recommendors

Based on the values of the PEs, A computes the level of trust it has in B:

$$T = f_t(PE_1, PE_2, \ldots, PE_n) \quad (3)$$

The value of T is then taken into consideration in the decision making. If the transaction is executed, the process described above is executed again in a similar fashion.

5 Conclusion

Trust relationships between principals are seldom complete. Therefore, when making decisions about whether to execute an electronic transaction or not, the principals must take the level of trust they have in each other into consideration. If the level of trust is considered to be high enough with respect to the risks involved, the transaction may be executed. Upon execution of a transaction, the success needs to be measured for possible future use. That is, if the other principal followed the agreement made, the trust level will increase. However, if the other principal was misbehaving, the trust level will decrease.

The level of trust that a principal has in another can be distributed to other principals for trust evaluation. This means that a principal that has no prior experience with another principal can still make a reasonable decision about executing the transaction. Such webs of trust are typically built between friends or trusted authorities.

By learning from and distributing the experience, it is thus possible to enhance the security of the transactions, since misbehaving principals will not be able to continue their actions in the long run.

References

[1] T. Beth, M. Borcherding, and B. Klein. Valuation of trust in open networks. In *Proceedings of Computer Security–ESORICS'94*, November 1994.

[2] R. Fagin and J Halpern. I'm ok if you're ok: on the notion of trusting communication. In *Journal of Philosophical Logic*, 1988.

[3] A. Jösang. *Modelling Trust in Information Society.* PhD thesis, Norwegian University of Science and Technology, 1998.

[4] P. Nikander. *An Architecture for Authorization and Delegation in Distributed Object–Oriented Agent Systems.* PhD thesis, Helsinki University of Technology, 1999.

[5] G. Simmons and C. Meadows. The role of trust in information integrity protocols. In *Journal of Computer Security*, 1994.

[6] R. Yahalom, B. Klein, and T. Beth. Trust relationships in secure systems: a distributed authentication perspective. In *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, 1993.

[7] R. Yahalom, B. Klein, and T. Beth. Trust-based navigation in distributed systems. In *Computing Systems*, 1994.