TYPE AND SCOPE OF TRUST RELATIONSHIPS IN COLLABORATIVE INTERACTIONS IN DISTRIBUTED ENVIRONMENTS

Weiliang Zhao [†] Vijay Varadharajan [†] [‡] George Bryan [†]
[†] *School of Computing and Information technology*
University of Western Sydney
NSW 1797, Australia

[‡] *Department of Computing*
Macquarie University
NSW 2109, Australia

Keywords: Trust Relationship, Classification of Trust, Trust Direction, Trust Symmetry, Trust Scope.

Abstract: In this paper, we consider the modelling of trust relationships in distributed systems based on a formal mathematical structure. We discuss different forms of trust. In particular, we address the base level authentication trust at the lower layer with a hierarchy of trust relationships at a higher level. Then we define and discuss trust direction and symmetric characteristics of trust for collaborative interactions in distributed environments. We define the trust scope label in order to describe the scope and diversity of trust relationship under our taxonomy framework. We illustrate the proposed definitions and properties of the trust relationships using example scenarios. The discussed trust types and properties will form part of an overall trust taxonomy framework and they can be used in the overall methodology of life cycle of trust relationships in distributed information systems that is currently in the process of development.

1 INTRODUCTION

Trust is a very important concept in today's distributed systems. In the security world, trust was first used in trusted systems (TCSEC, 1985) and trusted computing (Landauer et al., 1989). Marsh (Marsh, 1994) has tried to formalize trust as a computational concept. In reputation-based systems (Wang and Vassileva, 2003; Xiong and Liu, 2003), the community-based reputation is used to evaluate trust and predict the future behaviors of involved peers. Recently there have been several pieces of work on trust negotiations (Huhns and Buell, 2002; Winsborough et al., 2000; Winslett et al., 2002). The main concern of trust negotiations is how to establish trust between entities in different security domains by means of cryptographically signed credentials. Another issue that has been addressed over the recent years is trust management. Several automated trust management systems have been proposed and implemented. Typical trust management systems include PolicyMaker (Blaze et al., 1996), KeyNote (Blaze et al., 1999) and REFEREE (Chu et al., 1997). For XML based web services, two versions of WS-Trust have been proposed (Della-Libera and et al, 2002; Anderson and et al, 2004).

Our main objective is to develop a sound understanding of trust relationships and to create a powerful set of tools to model the trust relationships for collaboration in distributed systems. In our earlier work (Zhao et al., 2004), we have outlined a formal definition of trust relationship and a set of definitions for modelling trust relationships. Our previous research only provides a starting point for the analysis and design of trust relationships. The classification of trust has not been addressed and the properties of trust have not been discussed. In this paper, we describe different forms of trust relationships under the taxonomy framework. We categorize the trust types into two layers and discuss the hierarchy of trust relationships under the taxonomy framework. We provide several definitions about properties of trust direction and symmetry between involved entities. In order to describe and analyze the scope and diversity of trust relationships, we provide a definition of trust scope label. The definitions in this paper provide new elements of the whole taxonomy framework. We believe that our definitions of the properties of trust relationships can provide the accurate terminologies and can be used in scenarios where the trust relationships are analyzed and modelled.

Zhao W., Varadharajan V. and Bryan G. (2005).
TYPE AND SCOPE OF TRUST RELATIONSHIPS IN COLLABORATIVE INTERACTIONS IN DISTRIBUTED ENVIRONMENTS.
In *Proceedings of the Seventh International Conference on Enterprise Information Systems*, pages 331-336
DOI: 10.5220/0002520003310336

The remainder of the paper is organized as follows. In section 2, we provide the definition of trust relationship. In section 3, we discuss different forms of trust and the hierarchy of trust relationships under our taxonomy framework. In section 4, we provide a set of definitions for trust direction and symmetric properties of trust relationships. We employee the Microsoft's domain trust as a regressive scenario example to illustrate the definitions in this section. In section 5, the scope and diversity of trust relationships are discussed. The definition of trust scope label and comparison rules between trust scope labels are proposed and a scenario example is provided. Finally section 6 provides some concluding remarks.

2 DEFINITION OF TRUST RELATIONSHIP

In our previous work (Zhao et al., 2004), we have provided a formal definition of trust relationship with a strict mathematical structure. This definition of trust relationship is the cornerstone of our trust notion and the trust taxonomy framework. In this section, we will provide the details of the definition of trust relationship. The definition of trust relationship is expressed as:

Definition 1 *A trust relationship is a four-tuple* $T =< R,\ E,\ C,\ P >$ *where:*

- R *is the set of trusters. It contains all the involved trusters. It is a non empty set.*
- E *is the set of trustees. It contains all the involved trustees. It is a non-empty set.*
- C *is the set of conditions. It contains all conditions (requirements) for the current trust relationship. Normally, a trust relationship has some specified conditions. If there is no condition, the condition set is empty.*
- P *is the set of properties. The property set describes the actions or attributes of the trustees. It is a non-empty set. The property set can be divided into two sub sets:*
  - *Action set: the set of actions that the trusters trust that trustees will and can perform.*
  - *Attribute set: the set of attributes that trusters trust that trustees have.*

The above formal definition of trust relationship has a strict mathematical structure and a broad expressive power. It can reflect the commonly used notions of trust and provides a taxonomy framework. When trust relationships are used, the full syntax (four-tuple $< R,\ E,\ C,\ P >$ must be followed. Trust relationship T means that under the condition set C, truster set R trust that trustee set E have the properties in set P.

The above definition of the trust relationship is the basis of all properties of trust discussed in this paper. In our previous work (Zhao et al., 2004), there are more definitions, propositions and operations for modelling and analyzing of trust relationships in distributed systems.

3 CLASSIFICATION OF TRUST

Grandison et al (Grandison and Sloman, 2000) have given a bottom-up classification and used the terms as resources access trust, service provision trust, certification trust, delegation trust and infrastructure trust. We will illustrate them using our definition of trust relationship. Under our taxonomy framework, we categorize these trust relationships into two layers and provide the hierarchy of trust relationships.

- **Resources Access Trust**: Resources access trust relationship is a kind of trust relationship for the purpose of accessing resources. The access control has been the central concern of security for many decades. The trust relationship can be refined into authorization policies that specify actions the trustee can perform on the truster's resources and constraints that apply, such as the time periods for which the access is permitted. With the syntax of formal definition of trust relationship, resource access trust will be like "the trusters trust trustees under some conditions that trustees have the right to get access to some of trusters' resources".
- **Services Provision Trust**: services provision trust describes trusters' trust in provided services or resources of trustees. It is related to protection from maliciously or unreliably provided services or resources. With the syntax of formal definition of the trust relationship, service provision trust will be like "the trusters trust trustees under some conditions that trustees will provide the claimed services".
- **Certification Trust**: Certification trust is based on certification of the trustworthiness of the trustee by a third party. Certification trust is related to a special form of service provision trust. Certification authority is in fact providing a trust certification service. With the syntax of formal definition of trust relationship, certification trust will be like that "trusters trust trustees if trustees can provide certificates that trustees have a set of attributes or can do a set of actions according the certificates". The related service provision trust of certification trust will be like that "trusters trust certification authority under some conditions that the certification authority will only give certificates to suitable entities".

- **Delegation Trust**: Delegation trust is a special form of service provision trust. With the syntax of formal definition of trust relationship, delegation trust will be like that "trusters trust trustees under some conditions that trustees can make decisions on trusters' behalf, with respect to resources or services that the trusters own or control" (Ding and Petersen, 1995).
- **Infrastructure Trust**: Infrastructure trust is a kind of trust that trusters trust some base infrastructure under some conditions (Abrams, 1995; Abrams and Joyce, 1995). With the syntax of formal definition of trust relationship, infrastructure trust will be like that "trusters trust base infrastructure under some conditions for a set of properties of the infrastructure (some actions and attributes)".

All the above trust types must build on a more basic trust relationship which is the authentication trust or identity trust. Authentication trust is "trusters trust trustees under some condition that trustees are what they are claimed". Authentication trust belongs to a separate layer and all other trust types belong to another layer above it. This is illustrated in Figure 1. Note that trust types of layer two may not be necessarily specified in terms of an identity. Anonymous authorization belongs to access trust and it is an example that there is no specified identity. Anonymous authorization can be implemented using certificates with capabilities. The real identity of the involved trustee will not be revealed. For example, a customer has a certificate for accessing some resources on the Internet. The customer's behaviors of accessing the resources can be recorded. If it is desirable that the customer cannot be identified, the related access trust is a kind of anonymous access trust. Particularly for the resource access trust and service provision trust, the anonymous authentication is desirable in some cases. In such a situation, the layer of authentication still needs to provide a mechanism to deal with the same entity as the trustee in the whole scope of the trust process. Normally, there is a temporary and dynamic identification which will be uniquely connected with the involved trustee in the scope of the trust process. At layer two, trust relationships can be classified in different ways. In the following, we will give another kind of classification which is different from the bottom-up classification of Grandison et al. Based on strict definition of trust relationship, trust relationships at layer two can be classified according to the nature of the trustees in trust relationship $< R, E, C, P >$. If E is an infrastructure, the trust relationship belongs to infrastructure trust. If E is not an infrastructure, the trust relationship belongs to non-infrastructure trust. Non-infrastructure trust relationships can be classified based on the ownership of the property set. If the trusters have the ownership of the property set, the trust relationship belongs to access trust. If the trustees have the ownership of the property set, the trust relationship belongs to provision trust. If some properties are owned by trustees and some other properties are owned by trusters, then the trust relationship belongs to mixture (A&P) trust. The hierarchy of trust relationships at layer two is illustrated in Figure 2. In such a classification, delegation trust and certification trust are not independent types. As we have discussed, the delegation trust is a special form of provision trust, trustees are the providers of delegated decisions on behalves of trusters. A certification trust can be any subtype of non-infrastructure trust based on the nature of its property set.

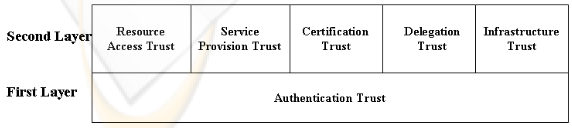

Figure 1: Trust Layers

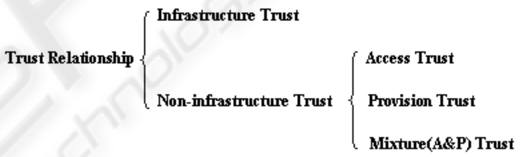

Figure 2: Trust Hierarchy

4 TRUST DIRECTION AND TRUST SYMMETRY

The properties of trust direction and trust symmetry play an important role in the collaborative interactions between involved entities in distributed information systems. In this section, we will provide a general description of the properties of trust direction and trust symmetry by a set of definitions and an scenario example. We believe that these definitions can cover most situations in the real world and can be used as standard scenarios for analyzing and modelling direction and symmetric characteristics of trust. The set of definitions about trust direction and trust symmetry are related to each other and they should be cooperatively used to analyze and model the properties of direction and symmetry of trust in distributed environments. One-way trust relationship, two-way trust relationship and reflexive trust relationship are defined for the properties of trust direction. For the properties of symmetry of trust relationships, definitions of symmetric trust relationships, symmetric two-way trust relationship, and the whole set of trust relationships are provided. The details of the definitions are described as follows.

Definition 2 *One-way trust relationship is the trust relationship with a unique trust direction from the trusters to trustees.*

One-way is the default feature of a trust relationship if there is no further description.

Two-way trust relationship can be defined and used in information systems such as Microsoft's domain trust. Actually, two-way trust relationship is the result of binding two one-way trust relationships together. We define two-way trust relationship as follows:

Definition 3 *Two-way trust relationship TT' is the binding of two one-way trust relationships $T =< R,\ E,\ C,\ P >$ and $T' =< R',\ E',\ C',\ P' >$ with $R' = E$ and $E' = R$. T and T' are the reflective trust relationships with each other in the two-way trust relationship.*

In the above definition, "binding" is the key word. If there are two one-way trust relationships between R and E but they are not bound with each other, then they are only two one-way trust relationships and there is no two-way trust relationship. When two one-way trust relationships are bound together, there is a two-way trust relationship and these two one-way trust relationships can be called reflective trust relationships with each other.

If the trusters and the trustees are the same, the trust relationship is reflexive. The reflexive trust relationship is defined as follows:

Definition 4 *Trust relationships $T =< R,\ E,\ C,\ P >$ is an reflexive trust relationship when $R = E$.*

The symmetry of two trust relationships could be an important concern in the analysis or modelling of trust relationships in distributed information systems. The symmetry of two trust relationships is defined as the follows:

Definition 5 *If there is trust relationship $T' =< R',\ E',\ C',\ P' >$ which is the result of swapping trusters and trustees in another trust relationship $T =< R,\ E,\ C,\ P >$ (the swapping includes all possible ownerships in condition set and property set), there is symmetry between T and T', T and T' are symmetric trust relationships with each other.*

In the above definition, the swapping of trusters and trustees includes all possible ownerships in condition set and property set. The two trust relationships have the same condition set and property set except the possible ownerships in them. The symmetric/asymmetric two-way trust relationship is defined as follows:

Definition 6 *A two-way trust relationship TT' is symmetric two-way trust relationship if there is symmetry between T and T'; otherwise TT' is an asymmetric two-way trust relationship.*

Sometimes it is necessary to discuss the symmetry of all trust relationships between a truster set and a trustee set, we have the following definition:

Definition 7 *WTR(R,E) is the whole set of trust relationships with same truster set R and trustee set E.*

Definition 8 *If every trust relationship in WTR(R,E) has a symmetric trust relationship in WTR(E,R) and every trust relationship in WTR(E,R) has a symmetric trust relationship in WTR(R,E), the trust between R and E are symmetric.*

Scenario Example : Here we use Microsoft's domain trust as a regressive scenario example to discuss the properties of trust direction and trust symmetry defined in this section. Domain trust allows users to authenticate to resources in another domain. Also, an administrator is able to administer user rights for users in the other domain. Our general definitions for the properties of direction and symmetry of trust relationships have general expressive power and can cover broad range of commonly used notations. The related concepts in domain trust can be viewed as specific cases of these general definitions. In the following, we will use our terms defined in this paper to review some concepts in domain trust.

- Based on **definition 1** in section 2, the domain trust can be expressed as "entities in domain A trust entities in domain B without any condition that entities in domain B have the right to get access of the set of resources in domain A".
- From our view point of trust classification in section 3, Microsoft's domain trust belongs to resources access trust. Domain trust binds the authentication and authorization together and has a standard two layer structure described in section 3.
- Microsoft's domain trust includes both one-way trust and two-way trust. In Microsoft's domain trust, one-way trust is defined as a unidirectional authentication path created between two domains. This means that in a one-way trust between domain A and domain B, users in domain A can access resources in domain B. However, users in domain B cannot access resources in domain A. Microsoft's one-way trust is an example of one-way trust relationship in **definition 2**. In a two-way domain trust, authentication requests can be passed between the two domains in both directions. Two-way trust is an example of two-way trust relationship in **definition 3**.
- The entities in same domain trust each other without any condition that entities have the right to get

access of the set of resources in the same domain. This is an example of reflexive trust relationship in **definition 4**.

- There is symmetry in the two-way domain trust. The two one-way trust relationships bound in the two-way trust relationship are "entities in domain A trust entities in domain B without any condition that entities in domain B have the right to get access of the set of resources in domain A" and "entities in domain B trust entities in domain A without any condition that entities in domain A have the right to get access of the set of resources in domain B". These two one-way trust relationships are symmetric trust relationships with each other in **definition 5**. Microsoft's two-way trust is symmetric two-way trust relationship in **definition 6**.
- In domain trust, the $WTR(A, B)$ based on **definition 7** has only one trust relationship from truster domain A to trustee domain B. For two-way domain trust, the trust between domain A and domain B is symmetric based on **definition 8**.

The properties of direction and symmetry of trust relationships play an important role in the modelling of the trust relationships in collaborative interactions in distributed environments. These definitions are new elements of the taxonomy framework about trust. We believe that they can cover most situations related with direction and symmetry of trust relationship in the real world.

5 SCOPE AND DIVERSITY OF TRUST RELATIONSHIP

Scope and diversity are two other aspects related to the trust relationship. The diversity of trust has been discussed by Jøsang (Jøsang, 1996) who expresses trust in three diversity dimensions. The first dimension represents trusters or trust originators, the second represents the trust purpose, and the third represents trustees. Jøsang uses the term trust purpose based on the observation that trust is relative to a domain of actions. In our formal definition of trust relationship, trusters and trustees are two tuples and they are similar to the terms of Jøsang. The origin diversity about trusters and target diversity about trustees are straightforward and have been described clearly by Jøsang (Jøsang, 1996). Jøsang's term of trust purpose is related to a domain of actions. In this section, we will define trust scope label to take the place of the trust purpose. The benefits of trust scope label will be discussed later in this section. The trust scope label is based on the four tuples of a trust relationship and it is the binding of the condition set and property set. The trust scope label is a new element of our taxonomy framework defined as follows:

Definition 9 *A trust scope label is a two-tuple $TSL =< C,\ P >$ where C is a set of conditions and P is a set of properties.*

The details of condition set C and property set P can be found in the formal definition of trust relationship in section 2. Actually, trust scope label provides a new layer of abstraction under the trust relationship and it defines the properties of the trust and its associated conditions. To compare two trust scope labels $TSL_1 =< C_1,\ P_1 >$ and $TSL_2 =< C_2,\ P_2 >$, we have the following rules:

1. $C_1 \subseteq C_2$ and $P_1 \supseteq P_2 \iff TSL_1 \geq TSL_2$;
2. $C_1 = C_2$ and $P_1 = P_2 \iff TSL_1 = TSL_2$;
3. $C_1 \supseteq C_2$ and $P_1 \subseteq P_2 \iff TSL_1 \leq TSL_2$.
4. In other cases, TSL_1 and TSL_2 can not be compared with each other.

The trust scope label is beyond the trust purpose in several aspects. Trust scope label composes of a subspace of trust relationships (two tuples out of four tuples) and describes the characteristics of the combination of condition set C and property set P. Trust scope labels could be treated as an independent subspace of trust relationships in the analysis and design of overall information systems. The property set in trust scope label covers not only actions but also attributes of trustees. Trust scope labels can be embedded in all the trust types described in section 3 and two trust scope labels could be compared with each other based on the rules given above.

Scenario Example: Consider an online software shop. We assume that anybody who wants to enter the online shop must register as a member of the online shop first. For describing the condition set and property set in possible trust relationships between the shop and possible customers, we use the following notations:

- $p1$ stands for that customers can read the documentation of the software.
- $p2$ stands for that customers can download the software.
- $c1$ stands for certificate of membership.
- $c2$ stands for the commitment of the payment for the software.
- $c3$ stands for the payment for the software.

We have the following trust scope labels:

1. $TSL1 =< \{c1\}, \{p1\} >$
2. $TSL2 =< \{c1, c2\}, \{p1, p2\} >$
3. $TSL3 =< \{c1, c2, c3\}, \{p1, p2\} >$

Based on the rules to compare two trust scope labels, we have

- $TSL1$ cannot be compared with $TSL2$ (or $TSL3$). There is no obvious relationship between $TSL1$ and $TSL2$ (or $TSL3$).
- $TSL2 > TSL3$. It means that the trust scope of $TSL2$ is less strict than that of $TSL3$.

In the analysis and modelling of trust relationships, the trust scope label may be quite complicated and the above comparison rules provide helpful tools in making judgements.

6 CONCLUDING REMARKS

Based on the formal definition of trust relationship with a strict mathematical structure proposed in our previous work, in this paper, we have focused on the modelling of trust relationships in collaborative interactions in distributed environments. We have discussed different forms of trust under the our proposed taxonomy framework. We believe that authentication constitutes layer one of trust and it plays a foundation role for other trust types on layer two. The hierarchy of layer two trust relationships proposed is based on the nature of the four tuples of a trust relationship. This hierarchy provides a bird's eye view of the purposes of trust relationships in the real world. The properties of trust direction and trust symmetry have been discussed and a set of definitions has been provided. In real implementations, these properties can be customized and configured based on the specific requirements. The trust scope label has been defined under our taxonomy framework and it could be used in the analysis of the scope and diversity of trust relationships.

The proposed properties of trust relationships and taxonomy framework are currently being used in the development of the overall methodology of life cycle of trust relationships in distributed information systems. We believe that the classification of trust are helpful for better understanding of the trust in distributed systems. We believe that the definitions about trust direction, trust symmetry and trust scope label provide suitable terms for the related properties and they can be used as tools for enabling the design and analysis of trust in collaboration of entities in real systems.

REFERENCES

Abrams, M. (1995). Trusted system concepts. In V., J. M., editor, *Computers and Security*, pages 45–56.

Abrams, M. and Joyce, M. (1995). Trusted computing update. *Computers and Security*, 14(1):57–68.

Anderson, S. and et al (2004). Web services trust language (ws-trust)(version 1.1). http://www-106.ibm.com/developerworks/library/ws-trust/.

Blaze, M., Feigenbaum, J., and Keromytis, A. (1999). KeyNote: Trust management for public-key infrastructures (position paper). *Lecture Notes in Computer Science*, 1550:59–63.

Blaze, M., Feigenbaum, J., and Lacy, J. (1996). Decentralized trust management. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 164–173.

Chu, Y. H., Feigenbaum, J., LaMacchia, B., Resnick, P., and Strauss, M. (1997). REFEREE: Trust management for Web applications. *Computer Networks and ISDN Systems*, 29(8–13):953–964.

Della-Libera, G. and et al (2002). Web services trust language (ws-trust) (version 1.0). http://www-106.ibm.com/developerworks/library/ws-trust/.

Ding, Y. and Petersen, H. (1995). A new approach for delegation using hierarchical delegation tokens. Technical report, University of Technology Chemnitz-Zwickau Department of Computer Science.

Grandison, T. and Sloman, M. (Fourth Quarter, 2000). A survey of trust in internet application. *IEEE Communications Surveys*.

Huhns, M. N. and Buell, D. A. (2002). Trusted autonomy. *Internet Computing, IEEE*, 6(3):92–95.

Jøsang, A. (1996). The right type of trust for distributed systems. In *Proceeding of the 1996 New Security Paradigms Workshop*. ACM.

Landauer, J., Redmond, T., and Benzel, T. (1989). Formal policies for trusted processes. In *Proceedings of the Computer Security Foundations Workshop II, 1989*, pages 31–40.

Marsh, S. (1994). *Formalising trust as a computational concept*. Phd thesis, University of Sterling.

TCSEC (1985). Trusted computer system evaluation criteria. Technical report, U.S.A National Computer Security Council. DOD standard 5200.28-STD.

Wang, Y. and Vassileva, J. (2003). Trust and reputation model in peer-to-peer networks. In *Proceedings of Third International Conference on Peer-to-Peer Computing*.

Winsborough, W. H., Seamons, K. E., and et al (2000). Automated trust negotiation. In *Proceedings of DARPA Information Survivability Conference and Exposition*.

Winslett, M., Yu, T., and et al (2002). Negotiating trust in the web. *IEEE Internet Computing*, 6(6):30–37.

Xiong, L. and Liu, L. (2003). A reputation-based trust model for peer-to-peer e commerce communities. In *IEEE International Conference on E-Commerce*.

Zhao, W., Varadharajan, V., and Bryan, G. (2004). Modelling trust relationships in distributed environments. In *Lecture Notes in Computer Science*, volume 3184, pages 40–49. Springer-Verlag.