Journal of Theoretical and Applied Information Technology
31st January 2012. Vol. 35 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT TRUST ESTABLISHMENT MECHANISMS

[1]S.DELIGHT MARY, [2]K.S.RAVICHANDRAN

[1]Asst Prof., Department of Computer Applications, SASTRA University, Thanjavur, Tamil Nadu, India

[2]Assoc. Dean, Department of Information and Communication Technology, SASTRA University, Thanjavur, Tamil Nadu, India

E-mail: sdmmca@yahoo.com , raviks@it.sastra.edu

ABSTRACT

The extensive use of the Internet, for exchanging information, requesting and offering services make us to interact with unknown entities. Human use trust to facilitate interaction and accept the risk, when complete information is unavailable. In such situations, trust establishment mechanisms enable establishment of trust between unknown entities. Trust is a complex concept to define stringently due to its multifaceted nature. This paper presents the characteristics of trust observed from various views and types of trust the automated trust establishment mechanisms need to model for the future. The confidence in the identity of the entity and the trust in that entity are the facilitator of trust for the proposed trust establishment mechanism. Finally, the objectives of the trust model, to be used by the future trust establishment mechanism are highlighted.

Keywords: *Trust, Trust Establishment, Continuum Of Trust, Identity, Credential, Negotiation, Attributes Of Identity/Credential, Trust Model, Privacy*

1. INTRODUCTION

Trust is a basic fact of human life. Trust is a social good to be safeguarded as much as air and water. When it is damaged the community as a whole suffers; and when it is destroyed, societies falter and collapse [1].

We all make trusting decisions, every day of our lives and trust has become a vital part of our life. All the actions we perform have some trust factor in them and this is particularly true in case of interaction with someone or anything. The decision to trust is based on evidence to believe, or confidence in, someone or something's good intentions towards us [1]. The difficulty of collecting evidence, confiding unknown entities and the role of trust in online interactions has resulted in a research discipline "trust in open computer networks" in the intersection of sociology, psychology, philosophy, commerce, law, computer science… .

The objectives of this paper are, assessing the potential and increasing the quality of online trust establishment for the current and future real-world scenarios. This paper starts with the survey of the meaning and the need for trust, analyses the views and types of trust, subsequently lists the features of trust that need to be modeled by the trust establishment mechanisms. Then the requirements of automated trust establishment process, the role of confidence in the identity, attributes of identity in trust establishment and how to retain privacy while profiling are highlighted. Finally, the objectives of trust models to be used by the proposed trust establishment mechanism are identified. The paper concludes with the implications of the observations made and the future work.

1.1 What is trust?

Trust is a complex concept that is difficult to define stringently [2]. Depending on the author's viewpoint or the context in which it is examined, various definitions of trust have been offered. Due to trust's multifaceted nature, it is difficult to form a unified definition [3, 4, 5]. The dictionary definitions are on the notions of confidence, belief, faith, hope, expectation, dependence, reliance on the integrity, ability, character of a person or thing... .

1.2. The Need for Trust

Trust is required when another party/entity can cause harm [4]. The stability of a community depends on the right balance of trust and distrust [6]. Without trust, we would suffer from a loss of efficiency and dynamism. If trust is present, we benefit with better accomplishments, healthier personal development, and the ability to cooperate [1].

Modern communication media are increasingly making us to get rid of the familiar styles of interacting and doing business. With the recent development of networking technologies, we exchange information, request and offer services. This makes us to communicate with faceless/unknown entities (people or electronic devices). In such situations, we face the difficulty of making decisions involving risk. When complete information is unavailable, human use trust to facilitate interaction and accept risk [2, 17]. The components and entities of trust in Internet infrastructures and computer assisted interactions include, network hardware, telecommunication network protocols, operating systems, authentication, cryptographic and other security mechanisms, network service providers and their staff, the organization's technical and business staff, business partners, vendors, customers, software distribution mechanisms, application software, various servers, database management software … .

1.3 Diversity of Trust

As trust is studied in diverse fields, there are many views and types of trust. The main thrust of work on trust in the past has come from three main areas sociology, (social) psychology, and philosophy [1]. Within these fields, contributions and views of Diego Gambetta, Morton Deutsch, and Bernard Barber are of particular interest in this paper.

Sociologist Diego Gambetta [3] introduces trust as "a particular level of the subjective probability with which an agent assesses that another agent or a group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action".

Morton Deutsch [1] states, "Trusting behavior occurs when an individual perceives an ambiguous path, the result of which could be good or bad, and the occurrence of the good or bad result is contingent on the actions of another person." The use of the word 'perceives' in this definition implies that trust is subjective.

Barber [1] states that trust cannot be generalized over systems, but can be generalized between relationships, such that, in the same situation, the same actor can be trusted, to some extent, depending on his behavior towards others. For, example, the reputation of a doctor in a discipline can be generalized to other similar patients, but not necessarily to other discipline/roles.

The social psychologist Morton Deutsch identifies nine types of trust, where a choice to trust could be made in several different circumstances [1]. They are Trust as despair, Trust as social conformity, Trust as innocence, Trust as impulsiveness, Trust as virtue, Trust as masochism, Trust as faith, Trust as risk-taking [17] or gambling and Trust as confidence.

2. TRUST CHARACTERISTICS

From the above observations, it could be concluded that, the characteristics of trust influences the formation of trust. The important characteristics are:

- Trust is subjective- every individual decides whether to trust or not based on the evidence available, for personal evaluation. Even if two entities get the same data, they may not interpret it in the same way
- Trust is not symmetric- two individuals do not need to have similar trust in each other
- Trust is situation specific- trust in an environment cannot be directly transferred to another environment. A notion of context is necessary
- Trust is dynamic – trust evolves interaction after interaction. It increases if interactions are successful and decreases if they fail.
- Trust can be formalized – formal notations and methods can be used to represent and derive trust

Cahill [3] states that modeling trust's behavior is of greater use for the analysis than modeling trust itself, removing the need to adhere to specific definitions. Thus, it is sufficient that trust establishment mechanisms model trust's behaviors that are listed above.

3. TRUST ESTABLISHMENT

Trust establishment mechanism enhances trust, when an interaction demands to decide whether to trust an entity without knowing for sure. The establishment process has to specify admissible types of evidence, its generation, distribution, discovery and evaluation [8].

Traditionally trust establishment is being performed based on recommendations, letters of credit, background checks, reputation and so on. Similarly, for negotiation, agreement formation and fulfillment could be successfully completed via established roles such as notarization, record retention and business verification [9]. For on-line transactions, all these are required and some new requirements arise.

Adequate online substitutes and new information elements are being identified. Disclosure of protected resources/services is governed by access control policies. The policies specify, what credentials an entity needs to disclose in order to gain access. Each entity has to write its access control policies accordingly.

When the process of trust establishment is automated, trust is established incrementally, by exchanging credentials iteratively. This process is governed by trust negotiation protocol [11]. Trust negotiation is triggered, when an entity requests access to a resource owned/service provided by another entity. A trust negotiation strategy defines the ordering of messages (which credentials to disclose, when to disclose), the exact content of the messages, and when to terminate a negotiation. The goal of trust negotiation is to find a sequence of credentials (C_1, . . . ,C_k, R), where R is the resource/service to which access is requested. When credential C_i is disclosed, it proves policy has been satisfied by credentials disclosed earlier in the sequence [12].

Different negotiation strategies need to be developed based on relevance, tradeoffs between computational costs, the length of the negotiation process, the number of disclosures, the level of trust required…. Thus, considerable independence in the choice of negotiation strategy has to be allowed to the entities, while still providing guarantee that the chosen strategies will interact correctly during negotiation.

The entities participating in the negotiation have to manage the negotiation process. During the negotiation, the participant uses local negotiation policies to accept new disclosures from the other entity and to determine what local resources to disclose next [19].

If a need arises while trust is being established, it should also be able to export one's access control policies in a standard format that is interpretable by the entity trying to gain access to resources/services or credentials. For example, a buyer may need to know which credit cards are accepted by a merchant, and the merchant may need to know, the access control policies that he will have to satisfy before the buyer will disclose his/her specific card to the merchant. Thus, in the negotiation process credentials and/or access control policies are disclosed.

Trust establishment is more of a personal issue than being technical [10]. The generalization of trust establishment is not straightforward, as it involves one-to-one relationship between peer entities or many-to-many relationship between multiple organizations, having different security policies and security management systems. The verifier has to use his/her own judgment to assess the requestor's credentials and to conclude about trustworthiness of an entity after personal evaluation. Moreover, the methods of establishing trust depend on the purposes and context of trust. For instance, establishing trust for authorization services generally requires more information (credentials) in addition to a user's identity.

Thus, the objective of trust establishment mechanism is to wrap up these technologies and deliver services that would allow entities to achieve the trust levels they desire, with ease.

Once trust is sufficient, for disclosing a particular credential to the other entity, a policy must determine whether the credential is relevant to the current scenario.

3.1 Role Of Identity And Its Characteristics In Trust Establishment

Trust is, "strongly linked to confidence in, and overall optimism about, desirable events taking place" [1]. There is large support in the literature for the use of identity as a trust equivalent and traditionally trust relationships are being established based on identity [1, 13]. Identity trust (confidence in identity) can be seen as the base, on top of which each of the other trust is built. Thus, other trusts cannot exist without identity trust. However, different trusts demand different levels of identity trust requirements. Hence, identity trust and identity management are fundamental to all other trusts.

Identity is verified personally or through a trusted third party using shared secrets, public/private key, digital certificates.... James Couzens [4] disagrees with the concept, that identity proved by digital certificate is the key to trust and says the characteristics of the identity are more important to establish trust. The above concept clearly implies that, the characteristics associated with the identity are more important to establish trust. For example, knowing the reliability of authenticated parties is essential in provision trust and delegation trust.

3.2. Privacy Protection

An important issue in trust establishment mechanisms, which extracts characteristics, is lack privacy. As trust relies on profiling, trust establishment mechanisms are fuelled with information that aims at building more and more accurate profiles over time [18]. Accurate profile leads to a better guess to the likely behavior. If this information could trace to the real-world identity, it would become a sensitive issue. Thus, the process of trust establishment makes obvious the fact, “the privacy is at threat.” It should be remembered, privacy protection principle of “Collection limitation” [14] states, **“**Data collection should be proportional and not excessive compared to the purpose of the collection.”

To avoid this, the trust establishment mechanism has to retrieve the trustworthiness of the entities and not their real-world identity. Pseudonyms provide levels of indirection between trust and real-world identity [15]. Thus the mechanism, must dissociate the real-world identity of the entities from their actions while profiling. This aspect is different from anonymity.

Next, with current trust establishment mechanisms, an entity has to reveal all the attributes in a standard credential to the service provider for trust establishment whether necessary or not [7]. As not all interactions need the same degree of trust, the attributes disclosed should also need to vary.

Therefore, a trust establishment mechanism should reveal relevant and minimal number of attributes and/or credentials to acquire the desired service to protect privacy.

Thus the objectives of the proposed trust establishment mechanism are disclosing identity and the attributes incrementally and to retrieve the trustworthiness in the entity, not the real-world identity and to support the continuum of trust.

4. TRUST MODEL

The outcome of the trust establishment process is trust relation [9]. Trust modeling involves expressing trust relationships between entities [16]. The set of discrete trust relationships that are based on identity trust can be expressed formally as a continuum of trust relationships. Each relationship may have a different degree of trust involved in it. Many of the models used by the trust establishment mechanisms were studied from the perspective of establishing policies and security credentials and in determining whether credentials match policies [16, 18].

4.1 Bootstrapping Trust

An important issue of trust relationships in many of the current real world scenarios is that the trust needs to be established with minimal or no prior relationships/knowledge. That is ad-hoc trust relationships are established. In such scenarios bootstrapping trust or assigning an initial value to the trust is critical, as it assesses the efficiency of a trust model.

In the current trust models, during bootstrapping phase trust is assigned a value, based on third-party recommendations [20], as a default constant [22], as a constant representing the trustor’s initial disposition to trust [23], based on other trustor’s recommendations [6,22], close to trust in a similar/ known context [23], based on the trustor ’s trust value on the trustee in similar/ known contexts as well as trust value on other trustees in similar/ known contexts and the new context(direct trust)[21,23], as a constant representing the trustor’s initial disposition to trust based on security level/ close to trust on the in a similar context based on security level/ based on other trustor’s recommendations in the specific security level[24], based on its performance during an evaluation period [25].
During bootstrapping phase assigning a higher value of trust, may encourage malicious entities to reappear with a new identity. Assignment of very

low value may not encourage new entities or an existing entity in a new context. Moreover, the estimation of trust in the current models involves significant overhead. There is a tradeoff between computational costs and benefit in ubiquitous environment. In addition, the time and effort spent on cost/benefit analysis depends on the quantum of benefit in that situation. Hence, the concept of Sufficient Bootstrapping [26] can be applied.

5. IMPLICATIONS

To address the issues discussed in section 3 future mechanisms have to

- Develop broad classes of strategies
- Design a strategy-independent, language-independent trust negotiation protocol, that ensures the interoperability of these strategies across the trust negotiation architectures
- Use Zero-knowledge approach that reveals possession of a secret, without giving away the secret
- Use standard notations for expressing credential contents so that the contents can be interpreted unambiguously
- Support tools to help entities to write and update policies (what to disclose, what not to disclose and in which order to disclose)
- Enable automation of negotiation and trust establishment when it is required

The principles discussed in section 4 invite research in

- Information elements that are most suitable for deriving measures of trust
- Better notations for expressing the relationships
- Interpreting and using the information in decision making
- The role of the model, in improving the quality of online interactions
- Simple, still efficient computation of sufficient trust value during bootstrapping to suit the characteristics of mobile devices

6. CONCLUSION

The survey of the issues of trust, capabilities of current trust establishment mechanisms enable identification of the requirements of the trust establishment mechanisms, which have to establish trust in ad-hoc scenarios. The characteristics of trust, capabilities of trust establishment mechanism, and the nature of the proposed trust models are discussed. The future work includes construction of open strategies for ad-hoc scenarios, standard notations for representing credentials, trust relations and bootstrapping trust using the concepts of sufficient bootstrapping. Bootstrapping may be the often-performed activity in the world of pervasive computing.

REFERENCES:

[1] Stephen Marsh, “Formalising Trust as a Computational Concept”, PhD thesis, University of Stirling, Department of Computer Science and Mathematics, 1994

[2] Audun Josang, Elizabeth Gray, and Michael Kinateder, “Analysing Topologies of Transitive Trust”, In Proceedings of the Workshop on Formal Aspects of Security and Trust (FAST), September 2003

[3] Cahill.V et al., “Using Trust for Secure Collaboration in Uncertain Environments”, IEEE Pervasive Computing, Volume 2, July 2003

[4] James Couzens, “What is Trust?” available at “http://olt.qut.edu.au/it/itn584/gen/static/resources/01p-couzens.pdf”

[5] A. Josang, R. Ismail, and C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision”, Decision Support Systems, Volume 43, Issue 2, Pages 618-644, Elsevier, 2007

[6] A. Abdul-Rahman and S. Hailes, “Supporting Trust In Virtual Communities”, Proceedings of the 33rd Hawaii International Conference on System Sciences, Volume 6, Page 6007, IEEE Computer Society Press, January 2000

[7] Zhengping Wu, Alfred C. Weaver, “Dynamic Trust Establishment with Privacy Protection for Web Services”, IEEE International Conference on Web Services (ICWS'05), Orlando, FL, USA, July 2005

[8] George Theodorakopoulos, John S. Baras, “Trust Evaluation In Ad-Hoc Networks”, Proceedings of the ACM workshop on Wireless security 2004, Philadelphia, PA, USA, October 2004

[9] Adrian Baldwin, Yolanta Beres, Marco Casassa Mont, Simon Shiu, “Trust Services: A Trust Infrastructure for E-Commerce”, In HP Laboratories Technical Report, August 2001

[10] Albert Levi, M.Ufuk Caglayan, Cetin K. Koc, “Use of Nested Certificates for Efficient,

Dynamic, and Trust Preserving Public Key Infrastructure", ACM Transactions on Information and System Security (TISSEC) Volume 7, Issue 1, February 2004

[11] Ting Yu, Marianne Winslett, and Kent E. Seamons, "Supporting Structured Credentials and Sensitive Policies Through Interoperable Strategies for Automated Trust Negotiation", ACM Transactions on Information and System Security (TISSEC), Volume 6, no. 1, February 2003

[12] Wolfgang Nejdl, Daniel Olmedilla and Marianne Winslett, "Peer Trust: Automated Trust Negotiation for Peers on the Semantic Web", Proceedings of the Workshop on Secure Data Management in a Connected World (SDM '04), August/September 2004

[13] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications", IEEE Communications Surveys and Tutorials, Volume 3, 2000

[14] Marc Langheinrich, "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems", Proceedings of Ubicomp 2001, Ubiquitous Computing: LNCS 2201, Springer Verlag, Heidelberg, 2001

[15] Jean-Marc Seigneur and Christian Damsgaard Jensen, "Trust Enhanced Ubiquitous Payment without Too Much Privacy Loss", in Proceedings of Symposium on Applied Computing, ACM, 2004

[16] Narendar Shankar, William A. Arbaugh, "On Trust for Ubiquitous Computing", Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Gteborg, Sweden

[17] Ardion Beldad, Menno de Jong, Michaël Steehouder, "How Shall I Trust the Faceless and the Intangible? A Literature Review on the Antecedents of Online Trust", Computers in Human Behavior, Volume 26, Issue 5, Pages 857-869, September 2010

[18] Duen-Ren Liu, Chin-HuiLai, HsuanChiu, "Sequence-Based Trust in Collaborative Filtering for Document Recommendation", International Journal on Human-Computer Studies, Volume 69, Issue 9, Pages 587-601, August 2011

[19] Simin Hall, William McQuay, "Review of Trust Research from an Interdisciplinary Perspective - Psychology, Sociology, Economics, and Cyberspace", Aerospace and Electronics Conference (NAECON), Proceedings of the IEEE 2010, Pages 18 - 25, July 2010

[20] Kui Ren, Tieyan Li, Zhiguo Wan, Feng Bao, Robert H. Deng, Kwangjo Kim, "Highly Reliable Trust Establishment Scheme in Ad-Hoc Networks",
Eslevier, Computer Networks, Pages 687–699, Apr. 2004

[21] D. Quercia, S. Hailes, and L. Capra, "TRULLO – Local Trust Bootstrapping for Ubiquitous Devices", Proceedings of the 4th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Philadelphia, Pennsylvania, USA, 2007

[22] Munirul M. Haque, Sheikh I. Ahamed, "An Omnipresent Formal Trust Model (FTM) for Pervasive Computing Environment", Proceedings of the 31st Annual IEEE International Computer Software and Applications Conference (COMPSAC 2007), IEEE CS Press, Beijing, China, Vol. 1, Pages 49-56, 2007

[23] Sheikh I. Ahamed, Mehrab Monjur, Mohammad Saiful Islam, "CCTB: Context Correlation for Trust Bootstrapping in Pervasive Environment", Proceedings of the 6th Annual Conference on Privacy, Security, and Trust (PST 2008), Fredriction, NB, Pages 167–174, 2008

[24] Sheikh I. Ahamed, Munirul M. Haque, Md. Endadul Hoque, Farzana Rahman, Nilothpal Talukder, "Design, Analysis, And Deployment Of Omnipresent Formal Trust Model (FTM) With Trust Bootstrapping for Pervasive Environments", Journal of Systems and Software (JSS), Elsevier, Volume 83, Issue 2, Pages 253-270, February 2010

[25] Hamdi Yahyaoui, "A Trust-Based Game Theoretical Model for Web Services Collaboration", Accepted for Publication in Knowledge-Based Systems**,** October 2011

[26] Sarjinder Singh, Stephen A. Sedory "Sufficient Bootstrapping", Computational Statistics and Data Analysis, Volume 55, Number 4, Pages 1629–1637 April 2011