A Study based on the Trust Management

Lakshmi
M.Tech Student (CSE)
Lovely Professional University, Phagwara, India

Pushpendra Kumar Pateriya
Assistant Professor (CSE)
Lovely Professional University, Phagwara, India

Saurabh Sharma
M.Tech Student (CSE)
Lovely Professional University, Phagwara, India

ABSTRACT

Trust plays a vital role in human life. It is the key to the door of other people's minds. It cannot be judge easily. The user may trust on an insecure channel for communication of sensitive information which may get leaked. In multimedia the authentication and authorization is related with Trust management. Applications where a more dynamic trust management is advantageous may have a quickly varying user base. It is important for user to deal with the uncertainty regarding the future and their interaction partners. The trust management system can be used for signature verification, semantic web, and for social networks. This paper discussed about different methods of trust management system.

Keywords

Trust management, emotional trust, logical trust, uncertainty

1. INTRODUCTION

In this era, electronic communication is one of the popular ways of communication. The data is transfer through internet which is considered as the fastest way of communication. Cryptographic techniques are used to provide the protection of data and information while transmission of data over the network [1]. Surfing the web is dangerous because the web contains lots of viruses, threats, hoaxes, etc and these can affect the system if downloaded content like software contain these. The spoofing of data can be done like eavesdroppers may listen in the credit card numbers or other sensitive information like passwords. Personal information may be collected legally but then used to violate one's privacy. Generally the dangerous program which contains suspicious code should be first checked through some software which can stop that code for execution. For example in case of the java applet interpreter it tries to give an execution environment in which programs are able to perform only "harmless" actions. The Proof Carrying Code (PCC) system requires mobile programs to provide evidence to potential hosts that they are "harmless" [2] [3]. Trust act an essential part in virtual organizations; respond to uncertainty caused by the business requirement for frankness. A user wants to have proof of harmlessness, but fragile forms of evidence may also be enough. An advice from a friend may encourage someone to trust that a piece of software is virus-free but that might be having a virus. People may trust on an insecure channel for communication of a bank transaction or transmission of the credit card number if the credit card company supposes liability for any false use of the number. As there is no central organization to supply support for traditional authentication for a fast changing actor base, making sensible authorization decisions about new, formerly unknown partners is difficult. The manual updating of the policy or access control settings quickly become painstaking, which force organizations into making only very wide decisions concerning large parts of the user base to evade the overly weighty process of personalizing the security settings. Trust is the key to the door of other people's minds. Robert Bruce Shaw (1997) in [4] defined trust as "Trust is a belief that those on whom we depend will meet our expectations on them."

Generally Trust is of two types:-

1. Emotional trust

2. Logical trust

1.1 Emotional trust

Emotional trust is that when one exposes his/her vulnerabilities to people, thinking that they will not take any advantage of his/her openness. There are some emotions that are associated with trust like faith, friendship, love, agreement, relaxation, comfort and loyalty, etc.

1.2 Logical trust

Logical trust is that when one have judged the probabilities of loss and gain, calculating expected utility based on hard performance data, and concluded that the person on whom we are trusting will behave in a predictable manner. There are some facts by which logical trust is determined like belief, behavioral trust, penalties, retaliation and replacement, honesty or trustworthiness of someone, etc.

In this paper, basically we focused on the Trust Management. This paper is organized as follows: in section 2, we have the Concepts for the Trust Management and in section 3; we have the Some Trust Management System video. In the end in section 4, is providing the conclusion over the discussion given in the paper.

2. CONCEPTS FOR TRUST MANAGEMENT

In the section, we consider trust as it is directed at self-governing actors. A service provider practicing electronic commerce on the Internet is called trustor whereas business partner or an individual requiring access to the trustor's services is called trustee. The trustees are self-governing actors because their actions are not directly controlled by outsiders like the trustor (service provider). Trust is important for people to deal with the uncertainty regarding the future and their interaction partners. The protection of law was considered by Stephen Marsh, a lack of options for feasible outcomes and other kinds of restrictions, dropping the above mentioned self-government of actors, as examples of factors dropping the need to trust [5]. In a more scientific environment, "trusted" hardware for monitoring [6] or cryptographically secure communications [7] also effort towards dropping uncertainty. A trust decision is binary means ‘0’ or ‘1’ and based on the equilibrium between risk and trust. When we consider a particular trustee in performing a certain action then it is made with a class of related situations in mind. The services which are provided by the trustor involve Actions. The effect of trust move toward to a risk: an authorization decision, reduced observation and resources allocated. The correlation of risk and trust is emphasized by many researchers, such as [5, 9, 10]. Reputation can be defined as an observation of a party creates through past actions about its objective and rules [8].

2.1 The Trust Management Model

Trust management in multimedia related to the authentication and authorization. In the situation of authentication, digital certificates establish the trust between two or more parties. The certificates are for identical proof or relationship in a cluster of good reputation. The trust related to the authentication is discussed in [7, 11]. Policy languages in [12, 13, 14], can be used to authorize the trustee with automated conclusion whether certain credentials are enough for performing a certain action. The language is included in Sultan trust management framework [15] for describing trust and recommendation affairs in the system. In case of authorization, the credentials are enough when the system is either having proof of the trustee’s identity or be familiar with a member of some satisfactorily trusted group. Trust is considered as monotonic in authentication level, the level of trust is based on proof of real behavior is not yet believed; the center of attention is on credentials matching policy. The behavior of the trustee should be measured as well to make trust more active. The intrusion detection systems in 2000 started the monitoring, but the information gained was not being considered to evolve reputation or trust. Not any of the existing systems then so far covered monitoring and re-evaluation of trust [16]. There has been seen a rapid change in the user base of those applications where a more active trust management is beneficial. Beginners create a difficulty for a trust management system based on behavior history only. The system must verify that the unknown persons should be trusted, even when the system does not know anything about them. The initial trust can be out of group while certification is provided; it may not be reasonable for some applications. In the same way, reputation systems are useful if the user has interacted with other systems assembling reputation before. A default level of trust must be considered for the fully unknown users. If the level is set too low, then the user might not be permissible to access the system at all, which make proving trustworthiness during one’s actions rather difficult [17]. Whereas if the default level of the trust is set very high then there might be necessity to limit the chance for users to “start over” by re-registration later than misbehaving.

2.2 The Trust Information Model

Existing trust models have been criticized for not building the relationship between trust and reputation clear and for treating them as independent of context or time [8]. Grandison and Sloman [15] find some of the logic-based frameworks which suffer from problems associated to applicability and limit themselves to a subsection of the trust management problem, the present solutions such as PolicyMaker [13], KeyNote [14], REFEREE [12] and Trust-Builder, a pledge architecture for sensitive credential exchange [11], just focus on certificates and access control, with no trust re-evaluation based on available information. Early structure of trust management, as corresponded to the abovementioned four systems, started by automating authentication and authorization decisions with the help of changeable sets of credentials. In this kind of situation, a level of trust is unchanged in relationship to passed credentials, and re-evaluation of trust is not based on experience information. Based on its environment the research on trust can be divided into three groups.

1. Infrastructure
2. Service
3. Community

The most fundamental level of trust is infrastructure. Early trust research has been concentrating on this level. As electronic trade has increase a grip and open systems become more common, trust forms a vital part on the service level also. There are still lots of problems to be solved on this level before research on the highest level the community. Mayer comes across for a differentiation between factors contributing to trust, trust itself and its result [9]. After two years Essin wrote a socio-technologically paying attention to the model for trust and policy, the goal behind that was to make them work efficiently in computer systems [18]. Gambetta in [19] sees trust as a subjective probability in the trustee doing a particular action. Jøsang clears about the target of trust in [20], a machine or a program (a rational entity) only implements the trust policy given by a human (a passionate entity) rather than trusting. Egger [21, 22] has come up with a model for trust-relevant factors from a customer’s point of view. The factors are appropriate for the perspective of a service provider as well, such as reputation, transference and propensity to trust.

3. SOME TRUST MANAGEMENT SYSTEM

In the section, we are discussing some trust management systems which are already in use.

3.1 REFEREE: Trust Management for Web Applications

REFEREE [12] stands for the Rule-controlled Environment For Evaluation of Rules, and Everything Else. It is a kind of an environment for evaluating conformity with policies or rules, but the evaluation procedure itself may engage dangerous actions and therefore is under policy control. The credentials refer to "Everything Else", who’s execution also requests to be under policy control. REFEREE is different from PolicyMaker which is the trust management system illustrated in [13]. In case of the PolicyMaker, it does not allow policies to control credential fetching or signature confirmation; it believes that the calling application has assembled all of the appropriate credentials and verified all digital signatures before calling the trust management system. REFEREE makes possible to write a policy that need signature verification, one that does not, or one that does only in certain circumstances. The Web will have advantage from a general platform for trust management, because different organizations will be able to build up component programs.

There are three data types in REFEREE:

1. Programs
2. Statement lists, and
3. Tri-values,

A tri-value is that in which one of the value is true, false, or unknown. A statement list is a group of assertions expressed in some format.

An initial statement list is taken as input for each program and may also take additional arguments. A program may call up another program during its execution. Instinctively, a policy governing a particular action is a program that returns values true or false; that will depend on the available statements which are sufficient to infer compliance or non-compliance with a policy, or returns unknown if no conclusion can be made.

3.2 Trust Management Framework for Social Networks

Ping Zhang et al [23] proposed a new system of trust metrics which captures both its uncertainty and human trust level, while being intuitive and user friendly. They introduced two trust metrics: impression and confidence. They adapted measurement error propagation theory to compute confidence over a chain of trust. Including various types of social networks, this framework can be used in all the applications where human trust is involved. The experiments done on a real social network certify their framework and the enormous potential of their trust framework in various social network applications. In an experiment on real data the author(s) increased 2250 times the "trust view," while keeping the same level of confidence.

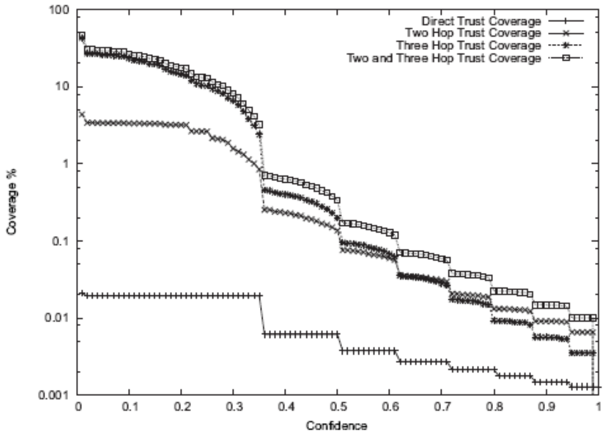

Fig. 1. Relation between desired confidence and trust coverage [23]

The trust coverage depending on confidence is evaluated. The trust coverage and desired confidence relation is shown in Fig. 1. The y axis representing coverage percentage scale is logarithmic because direct trust coverage is very low.

The two-hop and three-hop indirect trust coverage is calculated. The outcome showed that the two-hop only indirect trust coverage was two magnitudes higher than the direct one, and coverage of three-hop only trust was one magnitude more than two-hop coverage. Such results could be used by various applications on social networks to explore tradeoffs between trust coverage and its corresponding level of confidence.

3.3 Trust Management for the Semantic Web

The viewpoint behind the Semantic Web is the similar as that behind the World-Wide Web i.e. anyone can be an information provider or use anyone else's information. Matthew Richardson et al proposed a Trust Management for the Semantic Web [24]. One major complexity is that, the Semantic Web is a very large, uncensored system to which anyone may contribute. The author(s) handled the problem by employing a web of trust, in which every user keep trusts in a small number of other users. Then creation of these trusts into trust values for all other users. The result of computation is not a cluster "trustworthiness" of each user. In its place, every user receives a personalized set of trusts, which may differ widely from person to person. The properties are defined for combination functions which combine such trusts, and define a class of functions for which combining may be done locally while maintaining these properties. The experiments verify that the methods are robust to noise, and do not put unfair expectations on users. The Web is using algorithms like PageRank, which take benefit of the link structure of the Web. The experiments using data from the Epinions knowledge-sharing site, and from the BibServ site illustrated the potential of the approach, and the tradeoffs involved, they have set up for collecting and serving bibliographic references.

4. CONCLUSION

Through the overall discussion the paper describes the different concept of Trust Management System. Trust is considered as key to the door of other people's minds. The Trust cannot be judged easily. If the users are unknown than we have to set a default level for the trust. But there are problem with this too because if the value of the trust is set too low then the user cannot access the system and if the value of trust is very high then there are chances of misbehaving with the system. Trust management in case of the multimedia is having a relation with the authentication and authorization. The system REFEREE can be used to write a policy that needs signature verification. Including various types of social networks, the trust management framework can be used in all the applications where human trust is involved.

5. REFERENCES

[1] Saurabh Sharma, Pushpendra Kumar Pateriya, "A Study on different approaches of Selective Encryption Technique", International Journal of Computer Science & Communication Networks, Vol 2(6), 658-662

[2] G. Necula, "Proof-Carrying Code", to appear in Proceedings of the 1997 ACM Symposium on Principles of Programming Languages.

[3] G. Necula and P. Lee, "Safe Kernel Extensions without Run-time Checking", in Proceedings of the 1996 Usenix Symposium on Operating System Design and Implementation, pp. 229-243.

[4] Jim Rankin, "Building trust - the essential ingredient in partnering to improve business results".

[5] Marsh, S, "Formalising Trust as a Computational Concept", PhD thesis, University of Stirling, Department of Computer Science and Mathematics (1994)

[6] Baldwin, A., Shiu, S, "Hardware security appliances for trust", In: Trust Management:First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 28–30, 2003. Proceedings. Volume LNCS 2692/2003. (2003) 46–58

[7] Djordjevic, I., Dimitrakos, T.: Towards dynamic security perimeters for virtual collaborative networks. In: Trust

Management: Second International Conference, iTrust 2004, Oxford, UK, March 29–April 1, 2004. Proceedings. Volume LNCS 2995/2004. (2004) 191–205

[8] Mui, L., Mohtashemi, M., Halberstadt, A.: A computational model of trust and reputation. In: 35th Annual Hawaii International Conference on System Sciences (HICSS'02). Volume 7., IEEE Computer Society (2002)

[9] Mayer, R.C., Davis, J.H.: An integrative model of organizational trust. The Academy of Management Review **20** (1995) 709–734

[10] English, C., Terzis, S., Wagealla, W.: Engineering trust based collaborations in a global computing environment. In: Trust Management: Second International Conference, iTrust 2004, Oxford, UK, March 29–April 1, 2004. Proceedings. Volume LNCS 2995/2004. (2004) 120–134

[11] Winsborough, W.H., Seamons, K.E., Jones, V.E.: Automated trust negotiation.In: DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings. Volume 1., IEEE (2000) 88–102

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

[13] Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: Proceedings of the IEEE Symposium on Security and Privacy, IEEE (1996), 164- 173

[14] Blaze, M., Feigenbaum, J., Keromytis, A.D.: KeyNote: Trust management for public-key infrastructures (position paper). In: Security Protocols: 6th International Workshop, Cambridge, UK, April 1998. Proceedings. Volume LNCS 1550/1998., Springer-Verlag (1998) 59–63

[15] Grandison, T., Sloman, M.: Specifying and analysing trust for Internet applications. In: Proceedings of 2nd IFIP Conference on e-Commerce, e-Business, e-Government I3e2002, Lisbon, Portugal. (2002)

[16] Grandison, T., Sloman, M. "A survey of trust in Internet applications", IEEE Communications Surveys and Tutorials **3** (2000) 2–16

[17] Barber, K.S., Fullam, K., Kim, J. In: Challenges for Trust, Fraud and Deception Research in Multi-agent Systems. Volume 2631/2003 of Lecture Notes in Artificial Intelligence. Springer-Verlag (2003) 8–14

[18] Essin, D.J.: Patterns of trust and policy. In: Proceedings of 1997 New Security Paradigms Workshop, ACM Press (1997)

[19] Gambetta, D.: Can we trust trust? Trust: Making and Breaking Cooperative Relations (2000) 213–237 Electronic edition.

[20] Jøsang, A.: The right type of trust for computer networks. In: Proceedings of the ACM New Security Paradigms Workshop, ACM (1996)

[21] Egger, F.N.: From Interactions to Transactions: Designing the Trust Experience for Business-to-Consumer Electronic Commerce. PhD thesis, Eindhoven University of Technology (2003)

[22] Egger, F.N.: "Trust me, I'm an online vendor": Towards a model of trust for e-Commerce system design. In: Conference on Human Factors in Computing Systems, CHI'00 extended abstracts on Human factors in computing systems, ACM Press (2000)

[23] Ping Zhang, Arjan Durresi, "Trust Management Framework for Social Networks", IEEE ICC 2012 - Communication and Information Systems Security Symposium

[24] Matthew Richardson, Rakesh Agrawal, Pedro Domingos, "Trust Management For The Semantic Web", In Proceedings Of The Second International Semantic Web Conference