International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 3, Issue 2, 2016, PP 29-34
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
http://dx.doi.org/10.20431/2349-4859.0302005
www.arcjournals.org

E-Government Information Security Trust Assessment Model

Yadigar Imamverdiyev

Institute of Information Technology of Azerbaijan National Academy of Sciences
9, B. Vahabzade Street, Baku AZ1141, Azerbaijan
yadigar@lan.ab.az

Abstract: *The establishment of trust in e-government information security is of prominent importance for the full use of the actual potential of e-government. In this article, the trust creation mechanism to e-government information security is analyzed, and the model for the assessment of trust is suggested. The model is based on integration of reputation values calculated according to trust data collected from different sources by taking into consideration the weight coefficients.*

Keywords: *E-government; information security; trust; information security trust; trust factors.*

1. INTRODUCTION

E-government considers the establishment of specific communicative infrastructures enabling the realization of mutual relationships of government bodies and citizens by using information and communication technologies. The key goal of e-government is the provision of improvement in coordination among government entities (government to government, G2G), the introduction of high-quality services to citizens by government entities (government to citizens, G2C), the improvement of effectiveness of mutual relationships between government entities and business sector (government to business, G2B), the regulation of relations between the government and non-government organizations in decision-making (government to non-government organizations, G2N), mutual relationship among the government and science, technology, innovation sectors (government to knowledge, G2K)[1].

However, the level of use of e-government services by citizens lags behind the desired level[2]. The absence of trust in e-government systems is one of the impediments on the expansion of e-government services[2,3]. The impediments to trust in online environment emanates from the absence of identifiers and personal characteristics, and the environment of indefiniteness. The trust is directly related to risk and considered during decision-making. The decision of the use of e-government services depends on their trust level in e-government information security. Hence, the trust issue of information security comes to the front, while using e-government services.

In this paper, the problems existing in trust shaping and assessment on e-government information security are analyzed. Different approaches to the content of trust definition in information security are analyzed, and the mutual relations of information security and trust are clarified. Thereafter, the components of trust in information security are specified, and the e-government information security trust assessment model is suggested.

2. THE DEFINITION OF TRUST

The trust is an essential human behavior. It is usually called as a connection of the society. The life of the society depends on trust among its citizens very much. The trust is considered as the basis of the social institutions of all sorts. The trust is an important factor of the mutual relations between social groups and organizations.

The trust plays a prominent role in all fields of humanities (sociology, psychology, economics, and political sciences) and technical sciences[4]. It is hard to define the trust, while there are different kinds of trust, and they depend on the specific context.

The psychologists study the trust as mental relations and investigate the processes when the person trusts or distrusts (cognitive trust models). Sociologists study the trust as a relationship among the

people. The social context of the trust is widely used in multi-agent systems. The economists study the trust in terms of utility. Theory of games is one of the most popular methods for studying the construction of trust by applying different strategies.

By using all those achievements, the researchers in computer sciences study the role of trust in fields of e-commerce, p2p networks, greed computing, semantic web, web services, and mobile networks[5].

In this paper the term of trust is defined as following.

Two parties act during the establishment of trust relations – *truster* (the subject of trust) and *trustee* (the object of trust).

The trust is a subjective probability introduced by subject A, the aim of the probability is to forecast whether the subject B has performed a specific activity.

By trust, it is comprehended as reliability, the subjectivity of the trust is underlined, the dependence (the external impact on actions) and the factors of profit (the actor tries to maximize his profit) are indicated. It is assumed that the relationship among agents is reiterable.

Although the trust is studied from various aspects in different fields of science and by different researchers, some general characteristics can be specified:

- The trust can play a role when the environment is ambiguous and risky.
- Specific decisions are made based on the trust.
- The trust is constructed on previous knowledge and experience.
- The trust is a subjective notion based on individual opinion and values.
- The trust is altered by new knowledge and time, but the experience has a dominating impact on old trust.
- The trust depends on the context.
- The trust is multi-branched (multi-aspect).

The trust can be static and dynamic. The value of the static trust does not alter by the time. The value of the dynamic trust can alter by the time. The trust depends on the circumstances. For instance, the subject can alter the boundary values depending on the circumstances in trust-based decision.

There are different sorts of trust relations, such as direct trust, recommended trust, and reputation-based trust.

3. TRUST AND INFORMATION SECURITY

The trust issue is not a novelty for information technologies. The models of trust are used in one way or another for the trustworthiness of distributed systems, multi-agent systems, and decision-making in ambiguous environment. The realization of authentication, electron signature, authorization as functions of the provision of information security in distributed systems is based on trust relationships.

There is a complicated relationship between information security and the trust. In online environment, the use of information security systems (for instance, cryptographic methods) enables the creation and increase of trust, at the same time, the cases of information security violation can damage the trust. The existence of legislation base, certification, monitoring and control systems helps to strengthen the trust in cyberspace. Moreover, as mentioned, the realization of several information security mechanisms (authentication, coding, e-signature and cryptographic protocols) in distributed systems is based on trust relationships between parties.

In online environment, the provision of information security is carried out with the centralized trust – the trust infrastructures or web of trust established by the third party. The centralized trust infrastructure can be established by creating the web certificate services centers based on public key infrastructures (KPI) in e-government environment. This network serves to the establishment of the sole government registry of e-signature certificates, the development of e-signature certificates for the users of state information systems, the provision of life cycle of certificates and the provision of sole trust space activity.

From the point of view of the relationships among the information security and the trust it is important to touch upon the notions of information security assurance[6].

4. MODELS OF TRUST

Several models of trust are suggested for the establishment of practical trust systems in distributed systems. In this section, some models of trust are briefly considered.

The trust can obtain binary (trust/distrust), discrete and continuous values. The trust in the interval [0, 1] may be 1 - the full confidence and 0 - uncertainty or 0 - complete lack of confidence, 0.5 - indefinitely and 1- complete confidences.

In several models, the trust is measured not with one value, but with several values (for example, the value of the trust, the value of distrust and the value of indefiniteness) or with intervals. In some models the trust is expressed with the range, probability, belief and fuzzy values.

The subjective logic-based trust model is an interesting approach for the evaluation of trust values in indefinite environment[7]. The opinion describes the satisfaction and is shown as a triplet: *b* (the measure of belief), *d* (the measure of disbelief) and *i* (the value of unawareness), here $b+d+i=1$. It is assumed that *b*, *d* and *i* values can take the continuous values in [0.1] interval. The strength of the model is its ability to opine regarding the opinions (on strict mathematical basis) and consensus, and recommendation developing operators. The weak sides are such that, it is impossible to assure the precise assignment of values by the users.

In the most cited dissertation, Steven March suggests the *formal model of trust*. In the model, he introduces the set of subjective variables and the method of combination of those for obtaining the values from full trust to full distrust in [-1;1] interval (March mentions that those extreme circumstances are not possible). Each of variables depends on the time and the context. In describes system the broader definition – an agent is used instead of human. March specifies three kinds of trust: *base trust* – for any context; *general trust* – for any context between two agents of their mutual relationship; *situation trust* – for the specific context between two agents.

Bayesian models of trust are based on Bayes rule and beta probability distribution models for reputation evaluation[9]. The posterior value of reputation is calculated as combination of prior values of new values (ratings). The value of reputation can be expressed as the expected value of the beta function given by α and β parameters, here α is the number of positive values and β is the negative values of the participant.

Reputation models are more widely spread for the evaluation of trust. The reputation is a public opinion shaped based on the characteristics, advantages and shortcoming of a specific subject. The value of the reputation is calculated as a sum of positive and negative reviews (for example, eBay). Although this method is primitive and the value of reputation is non-precise, its main advantage is the transparency and comprehensiveness for the user. Depending on the reputation, the time of assessment, distance, etc. the more complex schemes calculating the weights for the values are used in Epinions and Amazon.

CuboidTrust is the reputation-based global trust model based for peering networks. Three factors: the peer contribution to system, and feedback peer trust and quality of the resources are used as cuboids consisting of little cubes with (*x*, *y*, *z*) constructed coordinates (*z* is the quality of resource; y – the peer keeping the value and x – the peer rating the resource). The rating is binary, 1 indicates the authentic and (-1) the unauthentic or the absence of rating. The global trust for each peer is calculated with an appropriate value algorithm based on all values kept by the trust peers.

EigenTrust calculates the unique global trust value for each peer in p2p file sharing web based on previous download information of peers. The local trust value is calculated as $Sij = sat(i,j) - unsat(i,j)$, here $sat(i,j)$ is satisfactory downloads of *i* from *j* and $unsat(i,j)$ is unsatisfactory downloads of *i* from *j*. For each peer, the trust value is calculated with the appropriate value algorithm.

AntRep is an algorithm based on swarm intelligence; each peer contains the reputation tables similar to routing table of distance vectors. In reputation table, (i) each peer corresponds to one reputation content; (ii) the metrics for the next link is the probability of each neighbor to be chosen. For the evaluation and spreading of reputation values onward and backward marching ants are used. If there exists a neighbor with the highest reputation in reputation table, the ant is sent in this direction. In case

of no dominance, several ants are sent in all directions. After the required reputation information is obtained, backward marching ants are generated and this ant updates each reputation table on its way.

Semantic Web is a model for the evaluation of trust between two agents. All routes connecting those are calculated. The rating values assigned to till on each route are multiplied, all values on all routes are added for evaluation of final trust values.

TACS (*Trust Ant Colony System*) is based on behavior model of colony of ants. In this model while pheromone is determined according to the volume of trust of the peer to neighbor. The algorithm calculates and chooses the most trustworthy connection and most trustworthy route to the connection. By moving along each till, the ants try to find the most trustworthy route to servers with highest reputation. If the connection introducing the required service by the customers is detected and the pheromone marks exceed the specified level, the search is aborted; otherwise, they continue to search for the connections not yet visited[9].

TRUMMAR (*TRUst Model for Mobile Agent systems based on Reputation*) – the trust values are obtained from three kinds of agents – neighbors, friends and remote hosts. The neighbors trust the hosts in their webs under the same administrative management, the friends are other hosts under the trusted administrative control, and remote friends are hosts which are neither neighbors, nor friends, but voluntarily give information. The new value of the trust is calculated as a weighted sum of previous trust value and the collective trust values calculated by considering the reputation-based weights of neighbors, friends and remote hosts.

FIRE (created from lat. "**fi**des" ("trust") and "**re**putation" syllabics) integrates four different kinds of trust and reputation[10]:

Mutual relationship trust is obtained from direct mutual relationship experience in the past. The assessing target uses the previous mutual relationship experience to determine the trustworthiness of the agent.

Witness reputation is calculated based on witness information on the agent behavior. Hoping that the agents share their experiences, the assessing target can gather the opinions of other agents in mutual relationship with the agent. This information can be used for the assessment of the target agent trustworthiness based on witness opinions.

Role-based trust is determined with different relationships based on role among agents. Alongside with the previous behavior of the agent (the previous behavior is used in two cases) other information can be used for determining the trust. Those can be different relationships or knowledge field among the assessor and the target agent (for instance, norms or legislation system). For example, the agent owner can approve his trustworthiness or can trust other agent being member of the trusted group.

Approved reputation is established from references of the third party submitted by the agent. In previous cases the assessor must gather the target information himself. However, the assessing agent can try to gain the trust of the assessor by submitting the arguments on his trustworthiness.

5. TRUST FACTORS OF E-GOVERNMENT INFORMATION SECURITY

The trust in e-government information security is constructed based on following factors: privacy of private information; information security mechanisms; feedback between e-government and citizens; the convenience of information security use.

The privacy of private information plays a prominent role in the establishment of trust in information systems. At present, information systems easily gather individual information and provide the easy access to those. Hence, on purpose or accidental violation of the confidentiality of private information increases the risks and as a result, the trust in information systems security is reduced.

The violation of information confidentiality, integrity and the accessibility decreases the user's trust in information systems security. In all stages of life cycle the realization of all appropriate information security mechanisms is an important issue for the trust provision.

One of the significant elements of trust strengthening is the feedback between e-government and citizens. The information sharing with citizens regarding the e-government actions, the increase of awareness level regarding the conducted measures in information security field, the enlightenment of

the population in information technologies and information security fields play a prominent role in trust establishment.

Another attribute impacting the test is the usability of information security. The usability can be characterized as following:

- How easy it is for users to learn the interface;
- The effectiveness of the interface;
- How easily the users can memorize;
- The reduction of errors;
- Satisfaction of interface.

The research shows that the usability factors impact the trust of users in information systems, especially in web-sites, while those increase the comprehended opportunities. Moreover, the usability is necessary condition of the trust, while it is necessary that people would believe they use the software systems correctly.

6. TRUST ASSESSMENT MODEL FOR E-GOVERNMENT INFORMATION SECURITY

Trust index can be included in e-government information security. It is considered to carry out the survey including the questions such as "Do you trust in electron government information security?" and the answer such as "I trust", "I don't trust" and "I cannot say". The trust index is calculated as the ratio of the difference between trustees and non-trustees to the number of respondents. However, this approach is not able to answer the question of trust establishment.

In this paper, the model allowing the trust by taking into consideration the different information sources is suggested. The citizens collect the information regarding e-government information security based on their own experience, opinions of neighbors and friends and opinions expressed in mass media. The government entities can submit some evidence or take some liabilities for the provision of information security (for instance, the compliance certificates of information systems or used products with information security standards). Let's name those sources as model components and label them with *I, W, M* and *S* symbols accordingly.

For calculating the trust value, the relevant ratings must be gathered regarding the previous behavior of e-government. The gathered ratings set is used for the assessment of the future behavior of the state – the expected rating value in future feedback. The general method for calculating this value is the calculation of the average value of all ratings in the sets, however, those ratings are not relevant at same degree while calculating the expected rating value. For instance, some ratings can be older than others and may seem less important. Some ratings can emanate from more reliable sources, so that they must be trusted more in comparison with others. Thus, the rating weight function is included for each component. *K* index can be *I, W, M* and *S*; they indicate the direct experience, witness information, mass media tools and certificates respectively. The trust value is calculated as the weighted average of all accessible ratings:

$$T_K(a,c) = \frac{\sum_{r_i \in R_K(a,c)} w_K(r_i) \cdot v_i}{\sum_{r_i \in R_K(a,c)} w_K(r_i)}.$$

Here, $T_K(a,c)$ is the trust value in e-government information security by the agent *a* calculated based on *K* component with respect to *c* factor, $R_K(a,c)$ is the collected ratings set for evaluating the trust by *K* component.,$w_K(r_i)$ is the rating weight function for calculating the relevance (trustworthiness) level of r_i rating ($w_K(r_i) \geq 0$), and v_i is the rating weight value of r_i. Dividing by the sum of weights, the trust value is normalized to [-1, 1] interval. The rating weight functions $w_K(r_i)$ are determined separately for each component.

The general trust value is calculated as:

$$T(a,c) = \frac{\sum_{K \in \{I,W,M,S\}} W_K \cdot T_K(a,c)}{\sum_{K \in \{I,W,M,S\}} W_K}.$$

Here, W_K is the weight coefficients for each component. Those coefficients are selected according to the significance of each component for the considered case.

7. CONCLUSION

The investigation of the trust and its different options in the context of e-government is very important for both scientific research and practical applications. In this paper, the model is suggested for the assessment of the trust of citizens in e-government information security. The suggested model is based on the aggregation of information gathered from different information sources for the assessment of the trust, the significance (relevance) level of information sources are considered during the aggregation.

REFERENCES

[1] Alguliev R, Imamverdiyev Y, Yusifov F. Some conceptual views on information security of the society. J Comm Comp. 2012;9:644-648.

[2] Schwester R. Examining the barriers to e-government adoption. El J E-*Gov*. 2009;7(1):113-122.

[3] Colesca SE. Increasing e-trust: A solution to minimize risk in e government adoption. J Ap Quant Meth. 2009;4(1):31-44.

[4] Rousseau D, Sitkin S, Burt R, Camerer C. Not so different after all: a cross-discipline view of trust. Ac Manag Rev. 1998;23(3):393-404.

[5] Grandison T, Sloman M. A survey of trust in internet applications. IEEE Comm Surv Tutor. 2000;3(4):2-16.

[6] ISO/IEC TR 15443-1:2012 Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts. 2012.

[7] Jøsang A. Artificial reasoning with subjective logic. Proceedings of AWCR. 1997;48:1-17.

[8] Marsh S. Formalizing trust as a computational concept. PhD thesis. Stirling: University of Stirling; 1994.

[9] Firdhous M, Ghazali O, Hassan S. Trust management in cloud computing: a critical review. Int J Adv ICT Emerg Reg. 2011;4(2):24-36.

[10] Huynh TD, Jennings NR, Shadbolt NR. An integrated trust and reputation model for open multi-agent systems. Aut Ag Multi-Ag Sys. 2006;13(2):119-154.

AUTHOR'S BIOGRAPHY

Dr. Yadigar Imamverdiyev is a Head of Research Lab at Institute of Information Technology, Azerbaijan National Academy of Sciences. He received the M.Sc. degree in 1989 in Applied Mathematics at Azerbaijan State Oil Academy and Ph.D. degree in 2006 in Computer Science at Institute of Information Technology, Azerbaijan. He was a Postdoctoral Research Fellow in 2011.08 – 2012.08 at Biometric Engineering Research Center of Yonsei Univiversity, South Korea. He was a researcher in more than 10 International and Azerbaijani Research Projects. He has over 100 papers published in international journals and conferences. He is co-author of 6 books, and co-editor of 3 Proceedings Book.

Research Interests: Dr. Yadigar Imamverdiyev's research interests include biometrics, speaker recognition, information security, applied cryptography, risk management, and social network analysis.