Evidence-Based Trust Reasoning

Jingwei Huang and David M. Nicol
Information Trust Institute, University of Illinois at Urbana-Champaign
1308 W. Main St., Urbana, IL 61801, USA
{jingwei,dmnicol}@illinois.edu

Keywords

Evidence-based trust, Trust model, Privacy

1. INTRODUCTION

Trust is a necessary component in cybersecurity. It is a common task for a system to make a decision about whether or not to trust the credential of an entity from another domain, issued by a third party. Generally, in the cyberspace, connected and interacting systems largely rely on each other with respect to security, privacy, and performance. In their interactions, one entity or system needs to trust others, and this "trust" frequently becomes a vulnerability of that system. Aiming at mitigating the vulnerability, we are developing a computational theory of trust, as a part of our efforts towards Science of Security. Previously, we developed a formal-semantics-based calculus of trust [3, 2], in which trust can be calculated based on a trustor's direct observation on the performance of the trustee, or based on a trust network. In this paper, we construct a framework for making trust reasoning based on the observed evidence. We take privacy in cloud computing as a driving application case [5].

2. WHAT IS TRUST?

Trust is a complex social phenomenon. Based on social studies of trust e.g. [6][1], we have the following view of trust [4]: *Trust is a mental state comprising: (1)* ***expectancy*** *- the trustor expects a specific behavior from the trustee (such as providing valid information or effectively performing cooperative actions); (2)* ***belief*** *- the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; (3)* ***willingness to take risk*** *- the trustor is willing to take risk for that belief.*

For developing evidence-based trust reasoning, we select the following three categories of relatively observable evidence, called CIA triad of trust evidence, in parallel to security CIA triad. **Consistency**(C), is about the trustee's compliance with some acceptable policies and industrial standards, and also include the historical performance of the trustee with respect to the trustor's expectation. We use "consistency" to reflect the broader concept of "integrity". The latter concept refers to that trustee adheres to the principles acceptable to trustee [6], in general context of societies, cultures, and religions. **Intention**(I), is about the trustee's motivation, goals, and plans. Intention is subsumed by goodwill; the latter is broader, including invisible moral responsibility to trustor and positive orientation toward the trustor or the representative group of the trustor; **Ability**(A), is about a trustee's technical and organizational competence with respect to fulfill a specific expectation.

HotSoS '14, April 8-9, 2014, Raleigh, NC, USA
ACM 978-1-4503-2907-1/14/04.
http://dx.doi.org/10.1145/2600176.2600193

3. EXPECTATION SPACE

Borrowing Solove's taxonomy of privacy [8] and extending it in the context of cloud computing, we organize cloud service providers' activities, which may lead to privacy violation, into the following categories: *data collection*, *data usage*, *data guarding*, *data situation informing*, *data dissemination*, and *data termination and disposal*. These categories of activities form cloud users' expectation space. A user's expectation is typical a subset of the actions (in the above categories) positively towards users.

4. EVIDENCE SPACE

The evidence space of trust judgment consists of two groups of facts: (1) what a service provider presents and/or performs to gain trust; (2) what was observed by users and third party professionals. From our study of trust mechanisms in cloud computing [4], the first group of evidence may include: (a) service provider's promise in the form of policy coverage of a specific expectation; (b) the extent of control allowing users to make decision about their data; (c) the transparency regarding how to handle users' data; (d) the accountability of the service provider's operations on users' data. The second group of evidence for trust judgment includes: reputation, brand name, business scale, major incidents reported, the number of users' complaints, certificates and audit reports issued by third party professional organizations, such as "Norton Secured" and "TRUSTe" seals.

5. EVIDENCE-BASED REASONING

We present the overall framework of the proposed evidence-based trust reasoning as follows. First of all, the entity making trust decision (trustor) identifies their specific expectation, referring to the expectation space; secondly, identifies evidence relevant to the expectation, referring to the evidence space and the CIA triad of trust evidence; thirdly,

constructs a Belief Network [7] for each expected item of privacy protection, using the CIA triad of trust evidence as intermediate level to connect the nodes in the evidence space to nodes in the expectation space. A Belief Network (BN) is a probabilistic model expressed as a DAG, with the assumption that given its parent nodes, each node is conditionally independent with all of the non-parent nodes.

Since evidence is typically incomplete, it is necessary to represent the uncertainty due to incomplete information. For this reason, we use an extended Belief Network model, in which each variable (a node) represents a proposition, which has one of three truth values – true, false, and unknown. The well known belief triple $< \alpha, \beta, \gamma >$ is used to represent the probability distribution over those three truth values. The belief triple can be interpreted equivalently as the probability of a belief being true is uncertain and within an interval between α and $\alpha + \gamma$ [3]. In this way, this extended BN allows to represent and reasoning with uncertain probabilities. If the probability distribution over the truth value unknown of every node remains as 0, the extended BN returns to the standard BN model. In this extended BN, trust is measured in the same form with the same semantics as in our trust calculus [3, 2]; this paradigm of evidence-based trust reasoning with belief networks is a natural extension to our calculus of trust, to allow inferring trust from observed evidence.

Now, we briefly discuss how to calculate the complete conditional probability table (CPT) of a node, from the basic CPT, which is the CPT without considering truth value unknown. For a node x, we use X, $\neg X$, $?X$ to represent x having truth value of true, false, and unknown respectively; also use X^* to denote a known truth value of either X or $\neg X$. Assume that in a BN, node y has direct parents $x_1, \ldots x_n$; the basic CPT for y is known; without losing generality, assume that a row of the CPT for y corresponds to

$$pr(Y|X_1^*, \ldots, X_m^*, ?X_{m+1}, \ldots, ?X_n).$$

By the semantics of belief triple, we have

$$pr(Y|X_1^*, \ldots, X_m^*, ?X_{m+1}, \ldots, ?X_n) = \inf_{\substack{x_{m+1} \in \{X_{m+1}, \neg X_{m+1}\} \\ \cdots \\ x_n \in \{X_n, \neg X_n\}}} \{pr(Y|X_1^*, \ldots, X_m^*, x_{m+1}, \ldots, x_n)\}$$

similarly,

$$pr(\neg Y|X_1^*, \ldots, X_m^*, ?X_{m+1}, \ldots, ?X_n) = \inf_{\substack{x_{m+1} \in \{X_{m+1}, \neg X_{m+1}\} \\ \cdots \\ x_n \in \{X_n, \neg X_n\}}} \{pr(\neg Y|X_1^*, \ldots, X_m^*, x_{m+1}, \ldots, x_n)\}$$

and generally,

$$pr(?Y|X) = 1 - pr(Y|X) - pr(\neg Y|X).$$

After the CPT of each node in a BN is defined, the conditional probability of an expectation proposition being true, given a set of evidence, can be calculated as follows:

$$\begin{aligned} pr(S_k|E_1 \wedge E_2 \ldots \wedge E_m) = \sum_{c_k, i_k, a_k, e_{m+1}, \ldots, e_n} (& pr(S_k|c_k, i_k, a_k) \\ & \times pr(c_k|E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n) \\ & \times pr(i_k|E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n) \\ & \times pr(a_k|E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n) \\ & \times pr(E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n)), \end{aligned}$$

where S_k is an expectation proposition representing that the cloud service provider (trustee) behaves fulfilling the user's expected item k; variables c_k, i_k, and a_k represent CIA triad of trust evidence for expectation item k; $E_1, \ldots, E_m$ are a set of known evidence; $e_{m+1}, \ldots e_n$ are the set of potential evidence that the user does not know or just knows in a certain extent (thus having a probability distribution over the three truth values); each variable (in lowercase) may have one of the three its truth values, i.e. $x \in \{X, \neg X, ?X\}$; the last item, $pr(E_1 \wedge \ldots \wedge E_m, e_{m+1}, \ldots, e_n)$ calculates the joint probability distribution (JPD) of all potential evidence identified in the evidence space. Some evidence nodes may depend on other evidence nodes; a BN can be constructed to express the dependence, and used for calculating the JPD. For the nodes independent of each other, their probability distribution is used to calculate the JPD.

This application case of evidence-based trust judgment on privacy protection in cloud computing [5] is implemented with Netica (norsys.com/netica.html).

6. CONCLUDING REMARKS

Towards Science of Security, we are developing a computational theory of trust. This paper proposed a general framework for evidence-based trust reasoning, using an extended Belief Network model that enables BN to handle uncertainties due to not only the randomness of trustee's behaviour but also the incomplete information of trustor.

Acknowledgments

This material is based in part upon work supported by the Army Research Office under Award No. W911NF-13-1-0086, and upon research sponsored by the U.S. AFRL and AFSOR under agreement number FA8750-11-2-0084. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

7. REFERENCES

[1] K. Blomqvist. The Many Faces of Trust. *Scandinavian Journal of Management*, 13(3):271–286, 1997.

[2] J. Huang and D. Nicol. A Calculus of Trust and Its Application to PKI and Identity Management. In *Proceedings of IDTrust'09*. ACM, April 2009.

[3] J. Huang and D. Nicol. A formal-semantics-based calculus of trust. *IEEE Internet Computing*, 14(5):38–46, Sept. 2010.

[4] J. Huang and D. M. Nicol. Trust mechanisms for cloud computing. *Journal of Cloud Computing*, 2(1), 2013.

[5] J. Huang and D. M. Nicol. Evidence-based trust on privacy protection in cloud computing, 2014. Research Report of ITI, UIUC.

[6] R. Mayer, J. Davis, and F. Schoorman. An Integrative Model of Organizational Trust: Past, Present, and Future. *Academic of Management Review*, 20(3):709–734, 1995.

[7] J. Pearl. *Causality: Models, Reasoning, and Inference, 2nd Ed.* Cambridge University Press, New York, NY, USA, 2009.

[8] D. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477 – 560, Jan. 2006.