ISSN : 0974 - 7435 Volume 8 Issue 1

BioTechnology
An Indian Journal

FULL PAPER

BTAIJ, 8(1), 2013 [62-66]

Study of implementation of trust

Jiang He
Department of Mathematics, Henan Institute of Science and Technology, Xinxiang, 453003, (R.CHINA)

ABSTRACT

This research developed a system of trusted agents and user nodes that cooperated to exchange behavior reports and establish a record of each node's behavior history. This history, based on reports and observations, was expressed as a reputation index (RI). The RI, with evidence in the form of signed FIs, provided an expectation of their partner's behavior before entering into or dissolving an association. By providing an indication of each other's trustworthiness, nodes avoided misbehaving nodes.

KEYWORDS

Implementing trust;
Security architecture;
Trust management system.

INTRODUCTION

Trust, and more importantly decisions on trustworthiness, is omnipresent in life. Luhmann's sociological approach[1] considered trust as "a means for reducing the complexity in society." This complexity was created as individuals interacted using their own perceptions, motivations, and goals. Solomon and Flores[2] contended that "trust forms the foundation, or the dynamic precondition, for any free enterprise society." They pointed out that what constituted freedom was the right to make promises and, more importantly, the responsibility for fulfilling them. Trust, therefore, was the basic underpinning of a cooperative environment. Trust was not an inherited trait but was learned as a member of the environment interacted with others. Another applicable definition of trust was provided by Gambetta[3]

"…trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action."

Humans usually based the decision to trust on historical evidence that led them to predict another person or entities' future behavior[4]. When this prediction was shown to be incorrect, the other person was trusted less, if at all. Rather than accept a philosophical betrayal, because "trust can only concern that which one person can rightly demand of another"[5], humans acknowledged the presence of selfishness in their environment[6] and took steps to avoid being victimized by self-centered peers. Any declaration of another's selfishness was dependent on establishing the context of the trust evaluation.

Time and context were two characteristics of the multi-dimensional nature of trust. The time aspect showed that trust was dynamic; a disreputable person could redeem himself through honest actions and a trusted person could become less reputable if he demonstrated deceit. Context was the situation in which trust was being considered. An example of context was that

Alice may trust Bob to order wine at dinner but wouldn't trust him to fix her car.

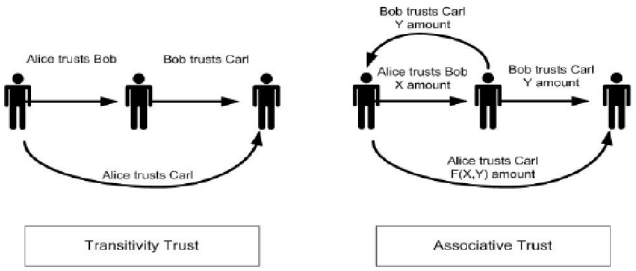

Figure 1 : Transitive and associative trust

Trust could be transitive, as shown in Figure 1. If Alice trusted Bob to pick wine and Bob trusted Charles to pick wine, Alice might reasonably trust Charles in wine selection if she were applying transitive trust. Alice could also constrain this trust by context. The constraint meant that, although Bob might trust Charles to split the bill fairly, Alice might have been willing to risk Charles' wine choice but might not be expected to trust the way he divided the check.

Alice might choose to constrain her trust through association, illustrated on the right side of Figure 1. This type of trust required Alice to gauge the extent she trusted Bob before asking his opinion on Carl's trustworthiness. Bob would reply with a qualified expression of his estimate of Carl's trustworthiness. Once she had established her trust in Bob and his trust in Carl, Alice combined both trust levels to create her own initial impression of Carl's trustworthiness. Alice's guarded trust or cynicism allowed trust to be expressed in a continuous, rather than discrete, manner as it was in sociological settings.

Expressing trust in continuous terms qualified trust in terms of context (e.g., Alice trusted Bob's taste in wine) or acceptance of risk (e.g., since the bill was only $5, Alice was willing to see how Charles split the check). Individuals evaluated evidence of their peers' behavior, forming a perception of behavior through risking betrayal with each interaction. The means of determining trust was complicated by numerous definitions and applications of trust.

NODAL SYSTEM SECURITY ARCHITECTURE

Each member node contributed to the system security architecture, as shown in Figure 2. Each node executed a three-layered security agent that implemented this security construct. Some layers, like the KMS layer, contributed to the DCE at large, while others, like the Intrusion Detection System (IDS) layer, were focused more on the individual node. These agents were autonomous, in that the parameters were set by the operating node and not by network-wide security policies.

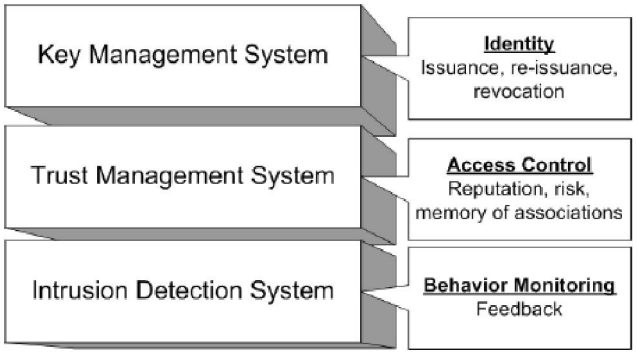

Figure 2 : System security architecture

An agent-based approach was selected because of its suitability to a mobile collaborative environment[7]. Each node possessed a complete security system and could operate independently based on peer nodes that were known to it or observations made first hand. A node could also join a coalition or collaborative group and take advantage of the group's information. The node retained this information when it chose to leave the coalition or the group's network area.

The KMS managed user identity certificates and established the rules for issuing, reissuing, and revoking certificates[8]. In a centralized network, this KMS relied on directory replication and certificate revocation lists (CRLs.) In a decentralized environment, the goal was to provide the KMS with access control decisions based on the trustworthiness of the perspective peer node.

The TMS was implemented as a central data-processing layer of the overall system security architecture. The TMS provided the KMS with a layer of abstraction of the overall trustworthiness of nodes, based on the activity of the nodes in the network. As the central layer, the TMS determined whether to trust or distrust its peers based on its individual trust thresholds. The trust management system then reported its trust decisions to the KMS for its consideration.

At the lowest layer, an IDS or network monitoring

FULL PAPER

scheme[9] provided periodic performance observations to the network. These observations were distributed throughout the system in a modified epidemic routing algorithm, similar to the selective dissemination scheme proposed by Datta[10]. The architecture's lowest level was simulated, as its specification and construction was beyond the scope of this paper.

The following sections develop the requirements for the trust management layer and detail the theoretical model underpinning its construction. First, we examine the requirements for building and using reputations in a virtual society or collaborative group. Then the TMS inputs and outputs are identified before the internal processes of the TMS are detailed.

IMPLEMENTING TRUST

Previous sections described how the KMS and the IDS layers of the system's security architecture provided reports and observations to the TMS in return for assessments or information. Within the TMS, the KMS-provided identity was used to anchor behavior information collected on an associate. The source of the information was included in the assessment of the associate's behavior, resulting in a reputation index that served as an expression of the associate's trustworthiness.

The TMS then applied the trustworthiness estimate to authorization decisions, whether we call these decisions access control or privilege management. Trust-based decisions were useable in distributed system security because traditional, centralized authorization mechanisms were perceived as inadequate[11]. A TMS gave the ability to identify misbehaving nodes that moved around in the network, with the intention of isolating them from the rest of the network. This isolation was achieved when the "good" nodes refused to interact with the "bad" nodes.

This research developed a system of trusted agents and user nodes that cooperated to exchange behavior reports and establish a record of each node's behavior history. This history, based on reports and observations, was expressed as a reputation index (RI). The RI, with evidence in the form of signed FIs, provided an expectation of their partner's behavior before entering into or dissolving an association. By providing an indication of each other's trustworthiness, nodes avoided misbehaving nodes.

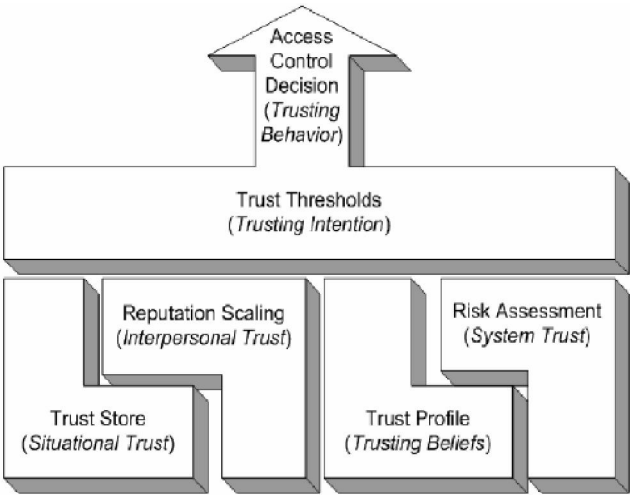

Figure 3 : Implementation of trust types and constructs

Starting with the theoretical work conducted by McKnight and Chervany[12], trust types and constructs were combined into modules and procedures, shown in Figure 3. These components were then linked through information flows to create the trust management system. The augmented trust construct diagram is shown in Figure 4.

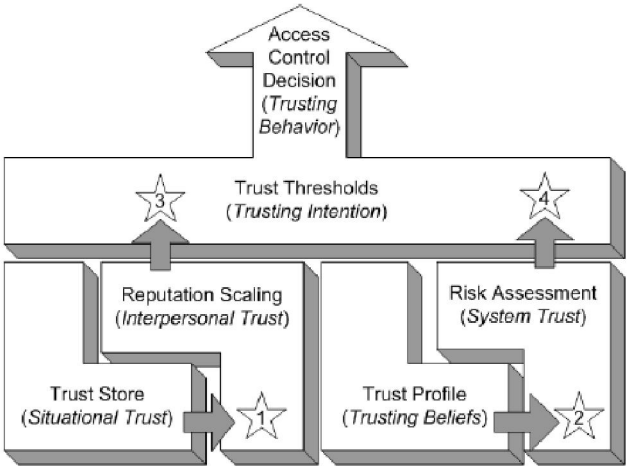

Figure 4 : Trust constructs with information flows

First, the trust store provided evidence to the reputation-scaling process in the same way that a situational trust construct provided the basis for the establishment of interpersonal trust. At the same time, the individual's innate tendency to extend trust guided the processing of global information to determine the current state of trust in the system or the surrounding the person found himself in. The information was processed and passed

to a higher-level process to assert the trust intention.

The trust intention was described as the current state of trustworthiness of an associate in the prevailing circumstances. Using interpersonal and system trust, the trust intention compared the associate's actions with the general risk state in the local area to produce a trust decision.

The transformation of the trust construct relationships to an operational system suitable for a mobile dynamic collaborative environment was fairly straightforward. Previous sections of this chapter discussed the quantitative mechanisms and the input/output relationships between the modules that represented the constructs. The system design, therefore, was the blueprint for the implementation of Chevarny and McKnight's hierarchy of trust.

Illustrated in Figure 5, this system design was centered on the trust management components that reside on each node of the network. The KMS and IDS were depicted at the top and bottom of the diagram, respectively. Arrows show how the modules exchanged information from these external entities. These flows were the same as discussed in Figure 4 but were described in terms of the information component rather than the conceptual element.

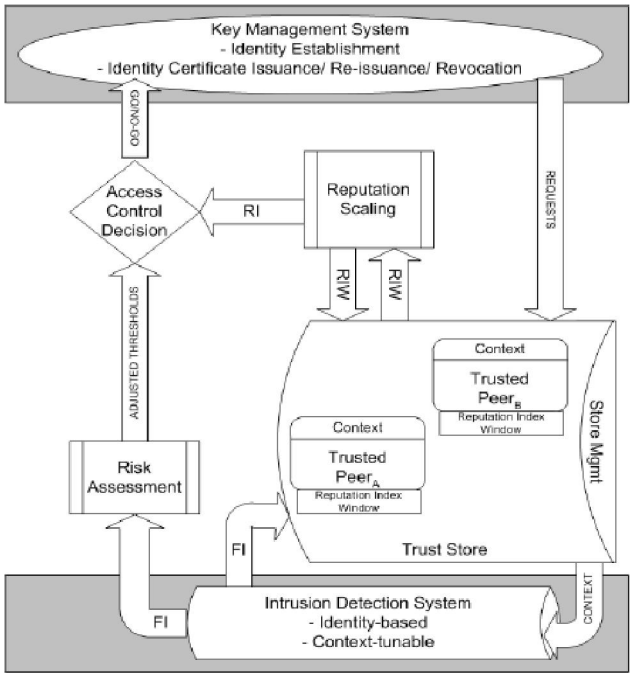

Figure 5 : Trust management system architecture

The center of the diagram shows how a node processed, evaluated, and stored the behavior information using the trust store (TS) and the reputation-scaling module (RSM). Risk assessment, a background process, continually adjusted trust thresholds based on current network conditions. When the KMS requested a trust decision, the prospective associate's reputation was compared to the current trust threshold. Once the evaluation was complete, the TMS forwarded an access control decision to the KMS. The remainder of this document concerns itself with the specification and simulation of the TMS operation.

REFERENCES

[1] N.Luhmann; Trust and Power, Wiley, **(1979)**.

[2] R.Solomon, F.Flores; Building Trust. New York, NY, Oxford University Press, **(2001)**.

[3] D.Gambetta; Can we trust trust? Trust, Making and breaking cooperative relations, electronic edition. D. Gambetta, Univ. of Oxford: Ch 13, 213-237 **(1988)**.

[4] K.Aberer, Z.Despotovic; Managing trust in a peer-2-peer information system. Proceedings of the 10th International Conference on Information and Knowledge Management, Atlanta, GA, 310-317 **(2001)**.

[5] L.Hertzberg; On the Attitude of Trust. Inquiry **31(3)**, 319 **(1988)**.

[6] P.Michiardi, R.Molva; Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. Proceedings of the European Wireless Conference (EW2002), Florence, IT, 1-6 **(2002b)**.

[7] L.Bartram, M.Blackstock; Designing Portable Collaborative Networks. Queue, **1(3)**, 40-49 **(2003)**.

[8] G.C.Hadjichristofi, W.J.Adams, et al.; A Framework for Key Management in a Mobile Ad-Hoc Network. International Journal of Information Technology, **11(2)**, 31-61 **(2005a)**.

[9] S.Buchegger, J.Y.Le Boudec; Nodes bearing drudges: towards routing security, fairness, and robustness in mobile ad hoc networks. Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, 2002., Canary Islands, 9-11, 403-410 Jan **(2002a)**.

[10] A.Datta, S.Quarteroni, et al.; Autonomous Gossiping: A self-organizing epidemic algorithm for selective information dissemination in mobile ad-hoc networks. Technical Report, Ecole Polytechnique Federal de Lausanne, June **(2004)**.

[11] M.Blaze, J.Feigenbaum, et al.; The Role of Trust

Management in Distributed Systems Security. Secure Internet Programming: Security Issues for Mobile and Distributed Objects. V. a. Jensen, Springer-Verlag, **(1999)**.

[12] D.McKnight, N.Chervany; The Meanings of Trust. Technical Report, Carlson School of Management, University of Minnesota, **(1996)**.