Editors: Vijay Varadharajan, vijay@ics.mq.edu.au
Fred Cohen, fc@all.net

Trust Management in the Pervasive Computing Era

Denis Trček
University of Ljubljana

Fide sed cui vide! (Trust, but see whom you are trusting!) Although this Latin saying goes back to the Roman Empire, it's becoming increasingly important for IT systems, which are leading us to the era of pervasive computing environments. These environments focus on cognitive communication by anticipating users' needs and trying to "understand" their lives in various contexts. Trust is certainly vital in this paradigm—if users are to rely on such environments or let those environments act on their behalf, they must trust pervasive computing solutions. The more sensitive the interaction in terms of security, privacy, or safety, the more trust there must be.

On a wider scale, these issues have clear economic implications, so it shouldn't be surprising that the highest EU officials, such as Viviane Reding, urge that more trust in the network is needed.[1] Furthermore, Andy Wyckoff of the Organisation for Economic Co-operation and Development notes that, as networks converge and the Internet becomes a key part of the economic infrastructure, concern is growing regarding how much trust we can place in the Internet.[2]

Here, I look more closely at what trust is, examine various quantitative methodologies for dealing with it, and argue for a more multidisciplinary approach to trust management for networks and pervasive computing.

Defining Trust

Looking back at the history of IT trust issues, one important past standard was the Trusted Computer System Evaluation Criteria, known as the Orange Book, which the US Department of Defense published in 1985. This standard was originally for military systems but became accepted for security classifications in the computer industry. What's most important is that the standard was about trusted computing systems. (Of course, the Orange Book paid no attention to certain points such as global networks, so it has little relevance today.) The question is, what do trusted computing systems and, primarily, trust, mean? Although the notion of trust seems intuitively clear, history shows that this hasn't been the case.

According to *Merriam-Webster's Collegiate Dictionary*, trust is "assured reliance on the character, ability, strength, or truth of someone or something." However, you can rarely treat trust in isolation, so its social dimension comes to the surface, as Dorothy Denning elegantly expressed in her definition of trust related to IT systems.[3] She stated that trust isn't a property of an entity or a system; it's an assessment. Such an assessment is driven by experience, shared through a network of interactions between people, and continually remade each time the system is used.

Now, which research domains should be involved in trust management issues in pervasive computing environments? We can obtain one relevant answer by looking at pervasive computing through the prism of the Internet and its main development directions:

- E-business appeared some 15 years ago and significantly affected many business processes. In this case, trusting "pervasive computing" was mainly about the security of businesses (in terms of prevented monetary loss and business continuation).
- Furthermore, the Internet is entering users' private domains, and new social phenomena are emerging. In this case, trusting pervasive computing exposes problems of users' personal integrity and privacy.
- Finally, sensor networks are emerging that will outgrow all other kinds of networks and extend the Internet into every corner of our lives. In this case, trusting pervasive computing adds safety problems.

So, the study of trust should be multidisciplinary. This primarily means including computing and information science on one hand, and psychology on the other. Although some research projects have employed multidisciplinary

1540-7993/11/$26.00 © 2011 IEEE

approaches, they've rarely included all the necessary ingredients. Furthermore, they often overlook the core of the trust phenomenon, as just defined. In addition, to complement current quantitative methodologies, we have to develop methodologies that support a quantitative treatment of trust by using qualitative assessments—some experiments done so far support this claim.

Some Main Approaches to Trust Management

Trust in IT environments is often treated mathematically, with Bayes' theorem as the starting point. The theorem states that the posterior probability of a hypothesis H after datum D is observed is $P(H|D) = P(D|H) * P(H)/P(D)$, where

- $P(H)$ is the prior probability of H before D is observed,
- $P(D|H)$ is the probability that D will be observed when H is true, and
- $P(D)$ is the unconditional probability of D.

Researchers have often used this theorem, mainly for naïve trust management.[4]

A more sophisticated approach, the Dempster-Shafer theory of evidence (ToE), is the basis for a subjective algebra that Audun Jøsang developed some 10 years ago.[5] This algebra starts with ToE and its set of possible states, a *frame of discernment* Θ. In Θ, exactly one state is assumed to be true at any time (for example, let Θ be given by atomic states x_1, x_2, x_3, x_4). Then, basic belief mass assignment is used to assign probabilities to the powerset of Θ that, in the case of, for example, $x_5 = \{x_1, x_2\}$, is interpreted as the belief that either x_1 or x_2 is true (an observer can't determine the exact substate that's true). The belief mass assignment is a basis for the *belief function*: for a subset $A \subseteq \Theta$, the belief function $bel(A)$ is defined as the sum of the beliefs committed to the possibilities in A. By analogously defining disbelief and uncertainty functions, a rigorous treatment on a mathematically sound basis is enabled.

Besides traditional logical operators, this subjective algebra introduces operators such as recommendation and consensus. It models trust ω with a triplet (b, d, u), where b is belief, d is disbelief, and u is uncertainty. Each of these elements obtains its continuous values from a closed interval [0, 1], such that $b + d + u = 1$.

These approaches' main problem is the complex mathematics, which users in pervasive computing environments would need to know. Considering that many users have problems with basic mathematical concepts such as probability, the need for complementary methods is clear.[6]

Some approaches deploy game theory, which might prove useful in certain contexts. But the main drawback is that, in the case of trust, the preference relation might not necessarily exist.[7] And when it exists, it is often not transitive. However, these requirements are the basis of game theory.

Furthermore, when trust is in question, many users aren't willing to let the computing environment decide for them; they prefer to make their own decisions. This further complicates the use of mechanisms requiring extensive mathematical knowledge. Finally, many users prefer qualitative expressions about trust over quantitative ones. Clearly, we need to go multidisciplinary, and we should first consider psychology.

Going Multidisciplinary

Jean Piaget's work can help us define the focus on the main characteristics and elements of reasoning and judgment processes.[8] According to Piaget, these elements (besides rationality) are, most notably, irrationality, temporal dynamics, and feedback dependence. Furthermore, Daniel Kahneman and his colleagues proved that people, when making decisions under uncertainty, can't analyze complex situations with uncertain consequences and therefore rely on various heuristics.[9] Although Piaget's and Kahneman's research didn't focus on trust, it's applicable to this domain. (Kahneman's research is also well recognized in the economics domain.)

In addition, Francis Fukuyama extensively studied trust in economics, exposing its importance as the main social virtue for the creation of the prosperity of societies. His research rests on the thesis that the future organization is the network organization, which will give an advantage to societies with a high degree of trust.[10]

Interestingly, in touching on the prosperity of network organizations from the IT perspective, this discussion comes full circle. Modern pervasive computing includes e-business, which is increasingly addressing the importance of (managing) virtual organizations. In addition, social networks are coming to the fore in our private lives, with notable examples such as Facebook, Twitter, and Second Life. This all implies the importance of support for qualitative assessments based on quantitative methodologies and the explicit inclusion of context for trust-related processes (and, consequently, the influence of a society that Denning emphasized in her definition of trust).

The Trust Management Landscape's Complexity

Trust in pervasive computing appears to be a difficult issue. First, it requires coordinated research by experts from various scientific fields. Second, because we aim to manage trust in computing environments,

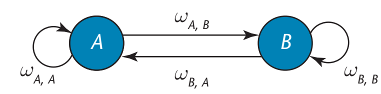

Figure 1. Trust relations. We can represent each society by a trust graph in which $\omega_{A,B}$ denotes the trust assessment (quantitative or qualitative) of entity *A* toward entity *B*.

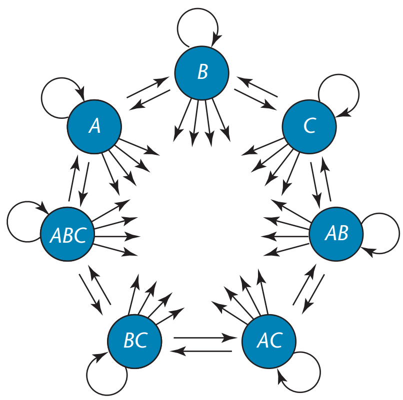

Figure 2. The complexity of trust relations. A society with three atomic entities requires computations on 49 relations.

we must formalize its treatment. The brief semiformal presentation in this section shows that trust is also computationally hard.[6]

We can view the entities in a trust relation as vertices connected by links, with each link representing a relation and having an associated attribute. This attribute can be not only quantitative but also qualitative, which distinguishes these graphs from ordinary graphs in discrete mathematics. As Figure 1 shows, we can represent each society by a trust graph in which $\omega_{A,B}$ denotes the trust assessment (quantitative or qualitative) of entity A toward entity B.

Trust generally isn't reflexive, symmetric, or transitive (the research previously mentioned supports this, but you can also make a simple mental experiment to see that this holds true). So, the question is, what's the total number of trust relations in a certain society? For n individual entities in a society, we have to evaluate the N trust relations:

$$N = \left(\sum_{m=1}^{n} \binom{n}{m} \right)^2 .$$

To understand this formula, consider a society with $n = 3$ (atomic) entities A, B, and C. The number of atomic entities is

$$\binom{3}{1} = 3.$$

The number of compound entities with two atomic elements is

$$\binom{3}{2} = 3 .$$

The number of compound entities with three atomic elements is

$$\binom{3}{3} = 1.$$

Thus, the total number of atomic and compound entities is $k = 7$, with $(k - 1) * k$ relations between them, to which we must add k reflexive relations. So, $N = 49$ (see Figure 2). Therefore, if the number of atomic entities is the input to our computational problem, computing all trust relations—that is, building a trust graph (which is the first step for further computations)—already initially requires the number of steps that is in EXP.

Considering aggregated trust on the level of a certain society, a new, related derivative emerges: reputation. Businesses already have a large interest in reputation systems. Owing to such systems' importance, the European Network and Information Security Agency published a position paper about their security in 2007.[11]

A Complementary Research Stream

Another stream of research on trust in IT systems exists. You could categorize the approaches mentioned earlier as computerized, with research apparatus resting on formal systems (with a grounding in mathematics and computer science). In contrast, this second stream comes from sociology and economics, and its research methodology is mainly statistics based. It focuses on trust in virtual environments—for example, online marketplaces.[12] It tries to identify factors facilitating business transactions in virtual worlds. So, it often researches IT-enabled (institutional) mechanisms that are crucial for trust, including feedback mechanisms, third-party escrow services, and credit card guarantees. This stream also builds on the well-known Technology Acceptance Model. Both streams are important because they represent complementary approaches to trust in IT-based environments.

Trust in pervasive computing environments will become the subject of increased multidisciplinary research. Because it is computationally hard, various heuristics will play an important role. In addition, simulations will constitute a valuable methodology for finding effective solutions. Finally, researchers should consider standardization in this area and should address trust phenomenon specifics. However, the challenges already mentioned are by no means the only ones.[13] The computing community will likely contribute significantly by combining "hard" trust (that is, security mechanisms) with "soft" trust (as defined in this article), thus reducing each stream's drawbacks while preserving its advantages.[14]

I probably haven't mentioned some important points in this article. But this can be expected with such a complex subject as trust, because the strongest links are the least visible. ☐

Acknowledgments

The Slovene Research Agency financed this research through research program P2-0359.

References

1. V. Reding, preface to *Report on the Int'l High Level Research Seminar on "Trust in the Net,"* EU Commission, 2006; ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/final-version-report-a4_en.pdf.
2. A. Wyckoff, "On Line Usages, Reshaping Economies and Societies," *Proc. Future of the Internet*, EU Communities, 2008, pp. 43–53; ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ch1-g940-280-future-internet-ld_en.pdf.
3. D. Denning, "A New Paradigm for Trusted Systems," *Proc. ACM SIGSAC New Security Paradigms Workshop*, ACM Press, 1993, pp. 36–41.
4. Y. Wang and J. Vassileva, "Trust and Reputation Model in Peer-to-Peer Networks," *Proc. 3rd Int'l Conf. Peer-to-Peer Computing* (P2P 03), IEEE CS Press, 2003, pp. 150–154.
5. A. Jøsang, "A Logic for Uncertain Probabilities," *Int'l J. Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 3, no. 9, 2001, pp. 279–311.
6. D. Trček, "A Formal Apparatus for Modeling Trust in Computing Environments," *Mathematical and Computer Modelling*, vol. 49, nos. 1–2, 2009, pp. 226–233.
7. M. Tennenholtz, "Game-Theoretic Recommendations: Some Progress in an Uphill Battle," *Proc. 7th Int'l Joint Conf. Autonomous Agents and Multiagent Systems* (Aamas 08), vol. 1, Int'l Foundation for Autonomous Agents and Multiagent Systems, 2008, pp. 10–16.
8. J. Piaget, *Judgment and Reasoning in the Child*, Routledge, 1999.
9. D. Kahneman, P. Slovic, and A. Tversky, eds., *Judgment under Uncertainty*, 22nd reprint, Cambridge Univ. Press, 2006.
10. F. Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1996.
11. E. Carrara and G. Hogbern, eds., *Reputation-Based Systems: A Security Analysis*, European Network and Information Security Agency, 2007.
12. P.A. Pavlou and D. Gefen, "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research*, vol. 15, no. 1, 2004, pp. 37–59.
13. V. Varadharajan, "Evolution and Challenges in Trust and Security in Information System Infrastructures," *Proc. 2nd Int'l Conf. Security of Information and Networks*, ACM Press, 2009, pp. 1–2.
14. V. Varadharajan, "A Note on Trust-Enhanced Security," *IEEE Security & Privacy*, vol. 7, no. 3, 2009, pp. 57–59.

__Denis Trček__ is with the University of Ljubljana's Faculty of Computer and Information Science, where he heads the Laboratory of E-media. He also collaborates with University of Primorska. Contact him at denis.trcek@fri.uni-lj.si.