芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Toward Trust as Result: An Interdisciplinary Approach

Stefano De Paoli
National University of Ireland Maynooth, Ireland

GR Gangadharan
Novay, Netherlands

Aphra Kerr
National University of Ireland Maynooth, Ireland

Vincenzo D'Andrea
University of Trento, Italy

Martin Serrano
Waterford Institute of Technology, Ireland

Dmitri Botvich
Waterford Institute of Technology, Ireland

Abstract
This position paper introduces a holistic approach addressing the issue of trustworthy communications systems, their societal drivers and the requirements they place on the heterogeneous communications infrastructure for offering reliable services in the Future of the Internet. In particular, we outline some initial ideas that can be used to devise a "design-for-trust" framework for the Future of the Internet. We propose, in this approach, to support trust on three crucial interrelated concepts: 1) the concept of flat ontology 2) the concept of assemblage and 3) the concept of semantic annotations to compose the ontology.

Keywords: trust, future of the internet, interdisciplinary research, assemblage

Permanent URL: http://sprouts.aisnet.org/10-8

Reference: De Paoli, S., Gangadharan, G., Kerr, A., D'Andrea, V., Serrano, M., Botvich, D. (2010). "Toward Trust as Result: An Interdisciplinary Approach ," Proceedings > Proceedings of ALPIS . *Sprouts: Working Papers on Information Systems*, 10(8). http://sprouts.aisnet.org/10-8

TOWARD TRUST AS RESULT
AN INTERDISCIPLINARY APPROACH

Position Paper Prepared for ALPIS 2010

[1]Stefano De Paoli, [2]GR Gangadharan, [1]Aphra Kerr, [3]Vincenzo D'Andrea,
[4]Martin Serrano, [4]Dmitri Botvich

[1]National University of Ireland, Maynooth, Sociology Department, Maynooth, Ireland
{stefano.depaoli, aphra.kerr}@nuim.ie

[2]Novay, Enschede, The Netherlands
gr@novay.nl
[3]University of Trento, Department of Engineering and Computer Science, Trento, Italy
vincenzo.dandrea@unitn.it

[4]Waterford Institute of Technology, Telecommunications Software and Systems Group.
ArcLabs Ireland, West Campus, Waterford, Ireland
{jmserrano, dbotvich}@tssg.org

General Overview

Trust has emerged as one of the key challenges for the Future of the Internet and as a key theme of European research in the area of Information Society (RISEPTIS, 2009). We are convinced that an interdisciplinary approach in the formulation of Trust concepts and a tight collaboration between Social Sciences and Computer Science on this problem, are of paramount importance for devising sustainable Trust solutions for the (Future) Internet stakeholders[1].

This position paper introduces a holistic approach addressing the issue of trustworthy communications systems, their societal drivers and the requirements they place on the heterogeneous communications infrastructure for offering reliable services in the Future of the Internet[2]. In this paper, we outline some initial ideas that can be used to devise a "design-for-trust" framework for the Future of the Internet that: a) would allow the specification, validation, and enforcement of comprehensive Trust aspects; b) would ensure an emergent Trust for all the stakeholders involved and c) possesses adaptation capabilities hence allowing to cope with continuously changing situations.

The Problem

Social relations and societies more generally are strongly based on the Trust between people (Hardin, 2006). Computing and communications systems demand translation of particular aspects of sociological thinking to take advantage of concepts such as reputation and Trust to, for example, generate systems offering trustworthy and secure information services and networking applications (see for example Jøsang et al, 2007). In this way these systems can also be used to support diverse applications in other systems or sub-systems requiring certain security levels.

In computing, Trust management arise from the necessity to remotely execute operations, and has been adopted as a way to enable security for distributed systems in situations where risk taking management decisions exists (Blaze et al, 1996). Hence, Trust management

[1] See http://www.future-internet.eu/fileadmin/documents/bled_documents/security_pricacy_trust/080402_BO5-0-2_Issues_paper.pdf
[2] From FutureComm Website, description of the project http://futurecomm.tssg.org/

systems must offer certain guarantees to secure information, as well as processes that create, manage distribute, and govern information and services, in a reliable and efficient manner (Serrano et al. 2009-1).

In communications systems, reputation can act as control access mechanism providing certain level of Trust. Reputation mechanisms have been widely adopted in web services, where a high social-related level is required to satisfy end user demands (Serrano et al. 2009-2).

One of the main challenges of this perspective of using Social Sciences to inform computer systems design is the mutual understanding and the reciprocal collaboration of Social Sciences and Computers Science. For example "*What is Trust for each of these disciplines?*" might be a legitimate question to ask. To simplify this, we can say that with the advent of distributed architectures we have witnessed a shift in the complexity of computer systems Trust: "the system access control policy", that rather than being a single statement enforced by the Operating system, "is more likely to be a composite of several constituent policies implemented in applications that create objects and enforce their unique access control policies" (Abrams and Joyce, 1995). This calls for a general complexity of Trust and Security based on dynamics creation of security policies and their enforcement. Social Sciences can provide a crucial contribution to tackle this complexity and the problem of dynamic creation and enforcement of policies.

Our Approach

The Internet and all the secure applications that run on it are an example of this complexity in the creation of Trust. Moreover, the need to plan and design not just for the Internet but for the Future of the Internet is perhaps an opportunity to challenge some of the taken for granted assumptions in this research area. We can indeed work towards new directions and solutions, and also challenge some of the established assumptions of Trust research.

For example a common approach of mainstream research is that "social Trust models" can be first extrapolated from social dynamics and contexts, second can be formalized as computer programs by using various forms of representations and finally can be executed on calculators, networks and applications with the goal of achieving Trust. But nothing ensures that this approach will necessarily bring Trust as result of this process, what it is secured is that a formalized social model of Trust is used as input in the design of trustworthy ICTs. We argue that more important than the formalization and the representation of Trust models is instead achieving Trust as the result or, in other words, that Trust should emerge as outcome of ICTs deployment.

We start with a different approach: our goal is to investigate how sociological approaches such as Assemblage Theory (DeLanda, 2002 and 2006; Lash, 2002) can facilitate the design of complex technical problems in the area of Trust. The Assemblage Theory is the study of how entities get shaped by their interrelations. We consider this a possible interesting avenue to explore for the dynamic design of policies and their enforcements in the management of the Future Internet and its services.

Our approach begins with simple problems: by analyzing some of the most relevant concepts in this area. In particular we begin with the concepts composing the systems we know as "Trusted Systems" (TSs): the security policy and the security mechanism. The security policy can be described as a rule/guideline on how, where, why, and when a subject can/cannot access a piece of information: in which context, at what time, for what purpose, and according to what laws, standards, organizational rules and so on. The policies therefore describe the conditions of possibility to obtain Trust (subject is trusted to access an object), and it can also prescribe outcomes if certain conditions are met. The control of the rule/policy is instead the enforcement of the rule which is imposed onto subjects (the machine imposes the prescriptions): this is the security mechanism. Subjects in this area are all active entities (computer programs, users or devices) in the system and Objects are passive entities such

as information.

The model of trusted systems we introduce seems to be based on a “judge” applying universal rules (even dynamically created) to particular elements (subjects and objects). However it is clear that different situations require different adaptability strategies and so the judge (System) should not be separated (from the entities), but rather it has to operate on the same plane of these entities (take decision on situations that keep changing). This means that rules should be created on the basis of situated knowledge on the local conditions of these entities, and not on an abstract representation of Trust.

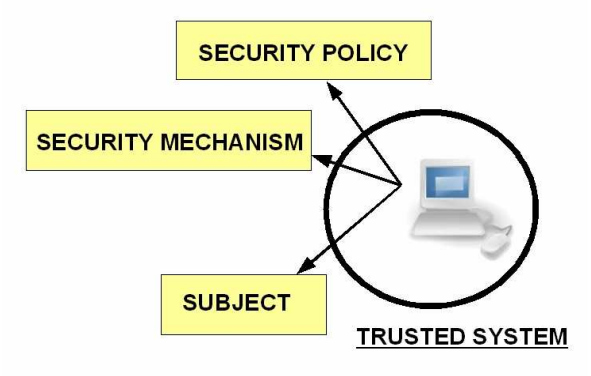

Figure 1: Concepts composing a Trusted System

We think that a good approach to conceptualizing Trust would in-fact be that of seeing it as an effect (a result) of the interrelations between elements in the form of an assemblage and not as an individual (pre)condition for interaction. This means that we will have to focus on at least two aspects of the design rationale of designing Trustworty ICT systems: building security policies and design reasoning (as artificial intelligence) security mechanisms as assemblages.

Since Trust is a collective socio-technical product, it has to be built together with the interrelation of various entities and not as its presupposition. Trust is not an essence, which explains order – but rather an outcome of the relations among entities. Hence, Trust cannot precede action (i.e. the enforcement of policies) but rather it emerges along with it. This perspective can lead perhaps to the design of a novel system that might support human production and understanding of Trust and mistrust in practice in different domains for the Future of the Internet.

Trust as Assemblage

A central problem here is to conceptualize the dynamic interrelation that can assess active entities as trustworthy or not on the basis of an “ontology”. We propose, in this approach, to support Trust on three crucial interrelated concepts: 1) the concept of *flat ontology* 2) the concept of *assemblage* and 3) the concept of *semantic annotations* to compose the ontology.

The idea of a *flat ontology* (DeLanda 2002 and 2006) is based on the argument that social entities should be characterized not on the basis of their essential property but instead on the basis of what they are capable of doing when they interact with one another. These capacities do depend on the entity properties but cannot be reduced to them since they involve an interrelation with other interacting entities. The concept of flat ontology induces processes and inter-relational dynamics encompassing changes according to the different roles of entities in different situations. One of the points of reflection here is whether we can rely on a flat ontology as a process to define dynamic security policies and their enforcement.

The key notion for grasping this dynamic is that of assemblage. The concept of 'assemblage' allows to think about the relations between a whole and the various parts that compose this whole. In the assemblage theory the relations among parts are conceptualized as follows: entities enter into the whole via contingent relations. In other words, the relations can change at any time and the parts can withdraw from one assemblage and enter into other assemblages even with different roles. We are of the opinion that the complexity of building Trust can be tackled by using this perspective. DeLanda clarifies that the relations among elements of an assemblage are not necessary, as in a 'system'. (DeLanda 2006). Indeed, differently from the concept of Assemblage, the concept of system, in both natural and social sciences, is also based on a conceptualization of the relations among elements that form a whole (the system). The relations among parts of a system are necessary and as a consequence the failure of one relation leads to the failure of the whole system.

Finally, semantic annotations are tags to instance data, with the objective of define relations known as mappings, between concepts and between ontology classes in form of formal descriptions. However by now it is not necessary to include details about the mentioned annotations, it is just important to mention they appear in this approach as result of research works about the social impact and semantics in computing systems.

Preliminary Conclusions

Our approach, although still very preliminary, is close to the emerging idea of a Socially Robust and Enduring Computing (SREC) (Hakken et al, 2009). The SREC seeks to combine methodological approaches used in computer science (such as creation of development tools) with those in social science, in the development of enduring technical solutions, especially in the area of software.
We are convinced that our interdisciplinary approach that combines the concepts of assemblage, flat ontology and semantic annotations constitutes an interesting avenue to explore, in a process of novelty designing of *Trust* in the area of Future Internet and its applications design. In this approach we seek to generate Trusted Systems as assemblages. We will apply this approach in communication systems for providing trusted decisions making processes, minimizing risk and increasing security, helping systems to detect malicious users and supporting creation/activation of services.

References

Abrams M. D. and Joyce M. V. (1995). “Trusted Computing Update”, *Computers and Security*, 1995, 14(1): p. 57 - 68.

Blaze, M., Feigenbaum, J., & Lacy, J. (1996). “Decentralized Trust Management”. In *Proc. of the 17th Symposium on Security and Privacy*, Los Alamitos: IEEE Computer Society Press, pp. 164–173.

DeLanda M. (2002). *Intensive Science and Virtual Philosophy.* London: Continuum.

DeLanda M. (2006). *A New Philosophy of Society: Assemblage Theory and Social Complexity*. London: Continuum.

Hakken D., Teli M., and D'Andrea V. (2009). “Intercalating the Social and the Technical: A Key Step in Coordinating Future Software Development”, Unpublished Manuscript submitted to *Transactions on Software Engineering*.

Hardin, R. (2006). *Trust.* Cambridge: Polity Press.

Jøsang, A., Ismail, R., and Boyd, C. (2007). “A Survey of Trust and Reputation Systems for Online Service Provision*”, Decision Support Systems*, 43(2), pp. 618-644.

Lash, S. (2002). *Critique of Information*. London: Sage.

RISEPTIS (2009). *Trust in the Information Society*. Available at http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html

Serrano M., van deer Meer S., Strassner J., De Paoli S., Kerr S., Storni C. (2009) "Trust and Reputation Policy-Based Mechanisms for Self-Protection in Autonomic Communications", IEEE Sixth International Conference on Autonomic and Trusted Computing (IEEE ATC-09), 7-9 July 2009, The University of Queensland, St Lucia, Brisbane, Australia.

Serrano, J. M., Serrat, J., Strassner, J. and Ó Foghlú, M. (2009). "Facilitating Information Interoperability in Network and Enterprise Management Systems", to appear in *International Transactions on Systems Science and Applications* (ITSSA), ISSN 1751-1461, 2009.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts