Chapter XXVI
Designing for Trust

Piotr Cofta
British Telecom, UK

ABSTRACT

Designing for trust is a methodology that attempts to design our perception of trust in information systems, in the long-term expectation that such systems will foster justified trust among people. The methodology contains several tools, but this chapter concentrates on a specific analytical tool that can be used to assess the compatibility between existing and required relationships of trust, in the context of information flow. While still under development, this methodology brings interesting results, identifying and addressing the strengths and weaknesses of incoming technical systems before they are actually deployed. This chapter discusses basic principles of designing for trust, presents the architectures of trust compatibility assessment tool and shows its applicability to citizen identity systems, using the proposed United Kingdom scheme as an example.

We become what we behold. We shape our tools and then our tools shape us.

—Marshall McLuhan

INTRODUCTION

Trust is one of the most pervasive yet least understood phenomena. While it has 17 different meanings and encompasses more than 30 constructs (McKnight & Chervany, 1996), the average person can intuitively and immediately determine the extent of trust in another person—as long as he can interact with such a person, preferably face to face. Unfortunately, digital systems negatively impact our ability to assess trust, thus reducing the benefits of modern information systems. Furthermore, they often become sources of distrust and distress, dis-connecting rather then connecting, as they allow criminals to alter the flow of information and deceive other participants.

All these negative consequences of a lack of trust in the operation and through the operation of digital systems leads to insufficient adoption of information systems, contributing to a surprisingly high failure rate of such systems (Clegg at al., 1997). The number of digital systems that have been deployed, only to be eventually scrapped as unaccepted (yet expensive) is quite large, and every system of this kind has contributed to a decline in the social trust of technology as such (Lacohee, Crane, & Phippen, 2006).

This undesirable situation has been noticed and several initiatives have been undertaken, such as Microsoft's Trustworthy Computing strategy (Charney, 2008). Designing for trust subscribes to the same stream, even though it addresses the problem of trust at earlier stages of the system lifetime, during the design phase of the information system. The methodology provides methods and tools that allow for the design of systems that reflect the extent of justified trust that one party has towards the other. As such, this methodology is less concerned with the trustworthiness of particular communicating agents or communication channels, as it concentrates on the ability to detect trusted and untrusted agents at the design stage, mostly to encourage further adoption of the system.

From the perspective of social trust and social acceptance, one of the most challenging projects of its kind is the deployment of citizen identity systems (known as identity card schemes) that are currently being pursued in several countries. While such schemes may be considered totalitarian by some, they can be of great benefit by improving and securing digital interaction, allowing for recognition of social norms and thus instilling trust. The prerequisite for them is social acceptance of such schemes (Cofta, 2004). However, current propositions are driven by technology efficiency (yet not always cost efficiency) and generally disregard the adoption factor and their impact on social trust.

It can be expected that by altering certain technical or operational aspects of such schemes, it is possible not only to build trust in systems and gain their social acceptance, but actually to turn the challenge into an opportunity by developing a platform where social trust can flourish, supported (rather then destroyed) by the technology.

This chapter starts from a general discussion of trust, then it drafts basic principles of 'Designing for Trust', to concentrate on a specific analytical tool and method, 'Architectures of Trust'), Finally, it shows the applicability of such a tool to the case of citizen identity systems, using an example of the proposed UK scheme.

TRUST

Trust is one of the most pervasive yet least understood phenomena. While it has 17 different meanings and encompasses 30 constructs (McKnight & Chervany, 1996), the average person can intuitively and immediately determine the extent of trust in another person—as long as he can interact with such a person, preferably face to face. The operational definition of trust that is used throughout the paper is derived from several typical constructs found in the literature (Mayer, Davis, & Schoorman, 1995).

The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party

It is generally accepted that trust can be expressed towards human intentional agents, but it can also be expressed towards technical or social agents that evoke an intentional stance (Dennett, 1989). Furthermore, trust can be expressed not only by humans, but also by technical agents, usually under direct or indirect instruction from humans. Within the methodology presented here, human (including social) and technical agents will receive similar treatment, even though their sources of trust (hence methods to determine it) may differ. While both humans and devices are nodes in the global communication networks, we attribute consciousness and cognition only to humans (Hodgson & Cofta, 2008). Trust between technical agents (such as computers) is therefore a reflection and representation of trust between human agents, not an emergent property of the technical system.