Trusted and Trustworthy Information Technology

Piotr Cofta
Trusted Renewables Ltd, UK

Hazel Lacohée
BT Technology, Service & Operations, UK

INTRODUCTION

As we gradually entrust information technology with our accumulated knowledge, personal data and even our social networks, the question of trust in technology becomes one of the most important yet contentious subjects. There are those who demand that technology must be unconditionally trusted, and those who blindly accept such a demand. There are those who re-define the meaning of trust to fit underlying technology, and those who believe that technology itself makes people more trustworthy.

There are several conflicting definitions, standards and procedures describing what makes technology trustworthy and there are studies of what makes us deem technology to be trustworthy. While the discussion of trustworthy and trusted technology may not yet be (or ever) exhausted, it definitely deserves a structure, and that structure is what this article provides. A unique framework that combines social sciences and technology is introduced, allowing us to list, compare and discuss different meanings of trusted and trustworthy technology in a systematic way.

BACKGROUND

Considering that the construct of 'trust' suffers from very many different definitions (McKnight & Chervany, 1996), it is not surprising that 'trusted ICT' and 'trustworthy ICT' are not far behind in being ill-defined. While every discussion of the 'meaning of trust' (and trustworthiness) seems to quickly turn into a turf war regarding definition, an abbreviated list of the main views may be still beneficial.

This overview focuses on trust and trustworthiness in relation to technology, and does not address trustworthiness (or trust) in general; an extensive review of the various views of trust however, can be found e.g. in (Cofta, 2007). This overview starts with a brief historical engagement, progressing to the discussion of three important distinctions that define the modern approach to trust in ICT as well as to trustworthy ICT.

History

While discussions of trust can be traced back to antiquity, it is only recently that a role for technology has been forged in that context. Historically, an isolated but important reference to the technological artefact of a 'trusty sword' can be found in Shakespeare's A Midsummer Night's Dream (Act 5, Scene 1). However, a dependence on technology and the awareness of that dependence has only come about with the development of the industrial revolution.

Two conflicting views developed over time. First, technology has been attributed with certain Promethean features, those of improving the lives of the masses and delivering progress. This view has persisted through to recent times and is represented in works such as (Goklany, 2007). However, technology has also been treated with scepticism, doubt, and even fear, and that can be traced back probably to the legend of disobedient Golem or to the seemingly never-ending series of technology catastrophes. Luhmann (2005) reaffirms this view stating that the introduction of technology actually increases the overall risk, rather than eliminating it.

Microelectronics changed the dynamics of this discussion as it reinforced the intentional stance towards information technologies. The best (and the simplest) explanation was quite often in believing that ICT sys-

DOI: 10.4018/978-1-4666-5888-2.ch435

tems have intentions of their own. Trustworthiness of such man-made intentional systems naturally deserved consideration in the same way as trustworthiness of humans, re-using and re-purposing our natural ability to ascertain personal trustworthiness.

It is only recently that people generally started to realise their mistake in attributing intentionality to technology alone (Lacohée et al., 2008). This is due to an increased familiarisation with new technologies, active participation and education, combined with a series of breaches of social trust (Broersma, 2010). In combination this made people realise that behind every technology there is an organisation, and that the organisation - rather than the technology alone - should be an object of trustworthiness, thus leading to an approach that is inherently socio-technical.

Definition

The proper definition of trust and trustworthiness is both essential and particularly hard to achieve. When it comes to social trust, the authors subscribe to the behavioural definition of trust (Mayer, Davis, & Schoorman, 1995) that stresses the expectation of benevolent intentions that lead to the acceptance of vulnerability in the absence of compensating controls.

However, extending such a definition to technology is problematic, as technology is devoid of intentions; rendering trust in technology alone is quite unfounded. Consequently, technical trustworthiness has often been equated with other qualities, specifically with adaptability and reliability.

The authors have been using the notion of 'adaptive resilience' (Robinson, 2010) to describe the difference between systems that are reliable and systems that are trustworthy. Adaptive resilience is the capacity to remain true to core purpose and values whilst simultaneously absorbing disturbance and adapting with integrity in response to changing circumstances that make systems trustworthy. While the original concept of adaptive resilience is inspired by social sciences, it has been adopted by security research for critical national infrastructure.

The added value of trustworthiness over reliability and resilience is the ability to retain purpose while adapting functionality to changes in the environment. Therefore, a trustworthy system is a system that always performs best, considering the circumstances, not one that always does the same.

THE STRUCTURE OF CONFLICTS

The area of trusted and trustworthy technology is not only fragmented, it is sometimes antagonised by differences and liberal interpretation of both terms. Therefore it is probably best to describe it by defining, in a non-exhaustive manner, three core conflicts:

1. First, we have to make a distinction between technology that *has* to be trusted (even though it is not always trustworthy) and technology that *can* be trusted because it demonstrates a certain level of trustworthiness.
2. Second, we have to make a distinction between the elements of trust and trustworthiness that are attributed to objective technology, and the elements of trust and trustworthiness that are socio-technical, i.e. attributed to social systems that provide and deliver technology.
3. Finally, we have to make a distinction between technology that utilises existing trust (and trustworthiness) for the purpose of its function, and technology that facilities the creation of trust in response to trustworthiness.

These distinctions are orthogonal; hence attempts can be made to classify every research problem by all three. Thus, e.g. a problem of trusted routing is simultaneously a problem of (1) technology that can be trusted (2) attributable to objective technical agents and (3) that utilises existing trust.

In fact, most real-life problems (and the majority of research problems) related to technology and trust demonstrate a rather complex structure of trust and trustworthiness in themselves, so that examples of the classification provided here serve as an illustration rather than as an absolute reference.

First Distinction: Trusted Technology vs. Trustworthy Technology

Trusted Technology

The security (and often the functionality) of modern information systems are built on the premise of a single *trusted element* (known also as a security monitor) that enforces security policies on other components of the system.