Abstract

In our paper we argue that the building of trust in electronic commerce depends only partly on technical security and the knowledge of security gaps and ways of closing them. It is not only a technical system which is trusted but rather a socio-technical system, including users, business practices and related institutions. We will take a closer look at the concept of trust and its relation to knowledge, describe the current situation in electronic commerce, and analyse different technical approaches, that aim at providing security, and non-technical possibilities to enhance security and trust through institutions.

1 Introduction

Over the past few years the use of electronic commerce applications has spread at a rapid pace. Still, there are many who think that this process needs to be accelerated, or at least the present willingness to experiment needs to be encouraged even further. Initial euphoria about the newly developed technical and economic possibilities distracted from the discussion of potential obstacles to the continued spread of electronic commerce. Today, obstacles which were at first considered irrelevant are being discussed more intensively, for example the problem of security.

Developers of technology emphasise that they pay utmost attention to the security and reliability of products and systems. It is obvious, however, that concern for security and reliability alone does not guarantee the commercial success of electronic commerce applications. Thus, Müller points out that, in order to avoid expensive mistakes, trust also needs to be developed [Müller96]. Obviously, the opinion that trust is primarily built on technical reliability still exists, but there is also a growing understanding among technicians that commercial success implies a much wider array of factors. Trust may well be a crucial variable. Institutional and cultural factors are significant for the development of trust. The term trust is, in fact, increasingly used by those concerned with information security and electronic commerce. The most popular domain for its usage has been research regarding authentication and the infrastructure for public key technology in a networked environment.

For years social scientists have been dealing with the problem of risk. Beck even developed the notion of a ‘risk society’ [Beck92]. But very little has been written about trust in technical artefacts or systems. Wagner [Wagner94] says that talking about trust in a risk society will arouse the suspicion that one is being apologetic, although a risk society is actually a trust society and the daily use of a great number of different technologies is usually trustful. Our everyday use of technical artefacts and systems is, in fact, not usually based on a thorough knowledge of functional principles and related risks. With our superficial knowledge we expect technical products to work and that faults will be repaired rapidly or replacements found. We not only trust in technical systems, but also in their social context, i.e. the way we usually do business, the reputation of brand names and/or institutions, the due process of law, etc. It is not so much that we trust a specific technology, such as the telephone, but we rather trust socio-technical systems.

2 Trust and Ignorance

Trust is a risky investment. 1 The actor who trusts runs risks. He trusts that his expectations will be fulfilled. Although he has no certainty, whatsoever, he acts as if everything he expects and trusts in will, in

1 There are quite a number of definitions for the term trust. The Oxford English Dictionary mentions three. Each one involves a different understanding of trust. Insofar it seems essential to clarify what we mean by trust.
information and communication technology. Experts, plethora of scientific results concerning the security of knowledge and admit their ‘ignorance’. There is a means that actors are aware of the deficits in their technology. Acceptance of uncertainty in this context security is declining most obviously in science and in the continuous and cumulative improvement of certainties disappear without being replaced and faith society” [Beck92]. It seems that more and more knowledge is available within a society.

Based on an analytical distinction used by Beck [96: 300-305] we first of all distinguish between unacknowledged and acknowledged ignorance, arguing that trust is only relevant if actors are aware of their ignorance. Otherwise, they have no reason to feel uncertain and, hence, no need to develop trust. For our argument it is irrelevant whether the subjective feeling of security is justifiable, or not [Beck96: 290].

2.1 Unacknowledged Ignorance

Unacknowledged ignorance implies subjective security because from the actors point of view there is no doubt that his or her expectations will be fulfilled. As long as one is unaware of problems, there is no need to trust. In these cases there may be risks, but they do not matter to the actor because he is unaware of them.

2.2 Acknowledged Ignorance

In the case of acknowledged ignorance we differentiate between (a) acceptance of uncertainty and (b) rational ignorance. Acceptance of uncertainty (a) is an important characteristic of modern societies. Max Weber interpreted the development of modern societies as a process of constantly increasing domination of nature and a growing systemic ability to control the world. It is supposed that knowledge and control are, in essence, possible which implies that respective knowledge is available within a society.

It may be that this is no longer true of the “risk society” [Beck92]. It seems that more and more certainties disappear without being replaced and faith in the continuous and cumulative improvement of security is declining most obviously in science and technology. Acceptance of uncertainty in this context means that actors are aware of the deficits in their knowledge and admit their ‘ignorance’. There is a plethora of scientific results concerning the security of information and communication technology. Experts, however, restrict an assessment of the security of specific applications in two ways. First, they talk about relative security, pointing out that absolute security cannot be guaranteed. For the purposes of combating assaults on the security of a system it is only possible to recommend to establish a more or less viable relationship between protective mechanisms and reasonable expenditure. Secondly, they restrict their assessment with respect to the future validity of their statements, i.e. the pace and direction of the future development of technology cannot be anticipated and, therefore, they consider their statements to be linked to the present state of affairs and knowledge.

Technical development, the contexts of use, as well as the way applications are used, cannot be assessed precisely. Developers and operators try to take this into account and aim at developing error-tolerant systems. But it is impossible to anticipate all possible constellations. Various social science papers on the risks of technology show that the contingency of technical development is an insoluble problem [DierHof92; DieHoMa96]. It is no longer possible to rely on experts to develop and implement secure systems. When experts make their decisions they are aware of the fact that there are significant uncertainties.

The second kind (b) of acknowledged ignorance is rational ignorance which is an important mechanism for maintaining the ability to act in a complex and differentiated society. Regarding technical systems there is always the problem of maintaining the ability to act, despite the vast amount of information that is available but cannot be processed. We use many technical artefacts and systems although we do not, in fact, know how they work. We do not even bother to find out how they work. As long as technical systems work this is not a problem for the user. As early as 1913, Max Weber wrote that it is impossible to know everything about the functioning of technical systems under contemporary conditions because we all are dependent on using the achievements of complex systems in our daily lives, whether technical artefacts or social institutions [Weber88: 471-472]. Without trust in persons and in technical systems, as well as the related social systems, modern societies could hardly survive [Luhman89: 1; 7-8; Preise95: 270; Wagner94].

There is no uni-directional relationship between knowledge and the creation of trust. Especially the notion that more knowledge will create more trust is misleading. The relationship between knowledge and trust is ambivalent. Knowledge does not automatically create trust. It may also lead to mistrust, as “not only favorable aspects, but also dangers, require familiarity

2 Denning/Metcalfe [97] are very informative concerning the uncertainties of prognoses.

3 Compare examples discussed by Coleman [90: 175-196]
... to enable a trusting or mistrusting future experience" [Luhman89: 19-20]. Moreover, it must be taken into consideration that trust often means the refusal to collect additional information. In a complex environment, with an immense range of information, the ability to act is secured by trusting and not by being aware of all available information. Trust is an attempt to reduce social complexity.

In our opinion, the recommendation that every individual should know everything about the risks and threats of modern information technology is misleading. It implies that individuals must have at their disposal all the tools necessary to close the gaps in security according to the best existing knowledge, according to requirements and state-of-the-art technology [Dierst97: 59].

Our first conclusion is that it is improbable that trust in security can be achieved by a technical solution alone. Technology without any risks is an illusion. Risk management is what matters; a risk management which is guided by the consideration that we cannot have full knowledge about future developments. If trust is to develop in such a situation more than a seemingly perfect technical solution is necessary.

3 Trust, Security and Electronic Commerce

The role of trust can be evaluated further in light of the current discussion surrounding the spread of Electronic Commerce. Surveys show that at the moment there is little trust that electronic transactions are secure. In a survey among German consumers 60 % of those interviewed said they did not trust in the security of electronic transactions. The problem of security is of major importance for commercial users, too. The result of the Electronic Commerce Enquête reported the following items as the greatest hindrances to a further spread of electronic commerce: “a lack of general business methods” (71 %), “regulatory deficits in respect of electronically signed contracts” (70%), “unsolved legal aspects” (66.8 %) and “no secure payment in the WWW” (65.9 %) [MülSch99]. That is, the most important problems are not technical problems, but a lack of institutionalization, on the level of practices of action as well as official regulations. Regarding the obstacles to a more widespread use, other surveys on Electronic Commerce also show that (potential) users and suppliers consider regulatory and security aspects to be of great importance. In addition to an adequate IT-infrastructure, a suitable regulatory framework, an adequate supply of services, trust and acceptance by customers are mentioned as playing a crucial role. A comprehensive regulatory framework is necessary, but not necessarily sufficient to foster trust among consumers. Yet, without this trust, which is difficult to measure in objective terms, Electronic Commerce will be slow to gain wide acceptance. Trust is essential to any commercial transaction. Typically, it is generated through relationships between transacting parties, familiarity with procedures, or redress mechanisms.

In this context, it is interesting to note that higher security standards and expectations are demanded for electronic transactions than for traditional business practices. As a matter-of-fact, the security of a special technology is less significant than the trust in a new kind of business practice, i.e. trust in the functioning of a socio-technical system which replaces familiar and, in part, very insecure business methods. Referring to the hindrances mentioned above, an increase in security is obviously not the only solution to the problem. It is impossible for the individual user to assess all the technical details properly and he or she is no longer willing to accept simple affirmations such as “everything is secure”. This is especially true for electronic transactions as, to a great extent, they are no longer embedded in traditional contexts. There is no physical counterpart in the transaction. There may not even be real money and the transaction, as such, is being conducted within a computer network. The normal user, therefore, has to trust in the statements of experts and the functioning of institutions which confirm the trustworthiness of a socio-technical system.

With any new technical application, there must first be a learning process. If a person has little or no experience with a technology (or a new business practice), he or she has no direct “empirical” evidence, which could justify trust or distrust, neither concerning the direct effects as the success of transactions or indirect side effects as the unauthorized collection of personal data. It is evident that with the increasing complexity of a technology the possibilities for direct experience are reduced and indirect experience, usually conveyed by the media, will increase in importance. This creates problems which extend far beyond the technical aspects to the role of institutions acting as mediators of experience. The less experience there is the greater the influence of social communication on the trust becomes, which individuals as well as whole societies have in a technology. The experts we interviewed in a project dealing with security complained that users only take security measures seriously if the respective problems have been discussed in the press. This illustrates the prominent

---

4 http://www.nua.ie/surveys/?f=VS&art_id=905354587&rel=true
significance of this information channel and its role in communicating information about risk. Of course, social communication as well as social practices are culturally dependent and therefore culturally divergent. Differences may occur on different levels, between nations but also between relatively small social groups.

Trust, however, is clearly only one factor leading to greater acceptance. If there are no alternatives, using certain applications may become obligatory (as is often the case in the corporate context). Sometimes people are forced by rational calculation to use a system they actually do not trust in (e.g. aeroplanes for a significant proportion of people). There are also systematic differences between business-to-business and business-to-customer transactions. In the business-to-customer segment the barriers to a wider acceptance are higher and harder to overcome [Heiden98].

4 Technology and Institutions – Different Approaches to the Provision of Security and the Inspiring of Trust

It is, of course, necessary to deal with the technical aspects of trust in a technology and – if possible – minimise the risks of a technology. Yet developers have to avoid concentrating on technical problems alone, while endeavouring to achieve as much security as possible. Whether the communication technology will serve a certain purpose in a secure way not only depends on all technical components functioning reliably, but also on the behaviour of the actual user. Technicians often consider this phenomenon to be a disruptive factor. They complain about the “inappropriate behaviour” of the user regarding security problems. This is the case if, for example, users write down PINs and passwords or transmit them insecurely, or select PINs and passwords that can easily be decoded.

Regarding the reliance on technical security measures, a recurrent phenomenon also has to be remembered. If greater technical security actually leads to greater trust in a technical system, than very often the amount of risks people engage in also gets higher. More trust may lead to a less cautious use though, for example transactions in electronic commerce could become of a higher value, therefore the entire risk of the socio-technical system would remain more or less the same as before.

Institutional aspects have a great influence on the process of trust-building. We define institutions as generally applicable regulation patterns in which norms, habits, conventions and values are manifest, and also as governance arrangements, institutional sectors (e.g. systems of research) or formal organisations. Every technology is attached to a variety of such social institutions. It is for this reason that the use, as well as the further development of a technology, cannot be organised arbitrarily, but is embedded in a social context which is responsible for reducing abuse and for generating and confirming acceptance.

In the following we first want to show, that there is no simple and unambiguous relation between technical improvements and the enhancement of security or trust. Therefore we take a look at different and even seemingly contradictory technical approaches, that aim at providing security. Then we will turn to non-technical possibilities of enhancing security and trust through institutions.

4.1 Eliminating the technical potential for abuse

An important approach to creating security is to eliminate the technical potential for abuse and, thereby, to reduce the need for trust. However, this applies only to a certain perspective, which we refer to as the perspective of those who know. These may be technical experts, who know how the technical system works. Often it is also necessary to know some relevant details about the context in which the technical system is implemented and used. Unfortunately, this is not the perspective of most of the users of such a system, particularly everyday users. As mentioned above, it is not even necessarily the perspective of the experts. Due to the fact that the complexity of systems is continuously increasing, they usually have only limited knowledge of the relevant aspects and they are unable to anticipate all the technical developments of the future, or the way users will behave.

4.2 Creating technical potential for bargaining security levels

Research has not only focused on eliminating the potential for technical abuse in order to achieve security, but also on opening up technical opportunities, which offer different user groups the opportunity to negotiate their security requirements. In contrast to the situation described above, which is defined by the assumedly legitimate security interests

---

6 This is also mirrored in a policy statement by the OECD. Regarding the Internet it says: “Rightly or wrongly, a few well-publicised incidents have cast it as a Wild West of roaming bandits, immorality, little governance, and an unreliable infrastructure. While certainly an exaggeration, this image, if left to persist, is likely to mean that mainstream consumers and businesses will not widely adopt e-commerce.” [OECD98]

7 We refer to approaches, which were chosen in the research program "Multilateral Security in Communication" (MüRan99).
of one actor or group and the illegitimate interests of the attacker, this approach is based on the assumption that all relevant actors have equally justified interests, however contradictory they may be, for example the interest of accountability versus anonymity, and more or less the same power to apply their (own) rules of the game.

Evaluated from a sociological perspective this approach is very promising. Technologies are often not used in the same way developers imagined they would be and they are used in a variety of ways in a variety of different contexts and situations. Nevertheless, in the long run we expect the opening up of technical potential will result in fairly flexible and locally differentiated yet institutionalised usage patterns which determine the legitimate use of a technology under certain circumstances and the meaning of acts and messages. This can be interpreted as social closure.

Of course social closure is not restricted to the form of rules of action. Legislative and regulation authorities are examples of institutions, which take on the form of organisations.

4.3 Trust despite distrust

If we assume that distrust can never be dispelled completely, since it is impossible to close all security gaps and, thus, eliminate all possible causes of mistrust and we cannot expect users to have a comprehensive knowledge of what can be considered secure or insecure, then institutions play an important role. Just as there are different technical ways to foster trust in electronic transactions there is also a variety of institutions which can serve different functions, all of which could make trust in electronic commerce more likely.

Insurance, or the guarantees and warranties supplied by manufacturers, dealers, service providers or certification authorities, help to limit risks, since they assure, that in case, expectations are not fulfilled, the loss will be small. As a result, they are able to create trust even under the overall condition of distrust. A certain degree of institutionalised distrust in the form of controls may even strengthen trust in institutions.

Another possibility to reduce the probability that expectations are not fulfilled, is regulation. Legislative or regulatory authorities as well as (professional) associations regulate which actions are legitimate and who is permitted to offer certain services. People are likely to comply to the rules, because they take them as an unquestioned pattern of action, especially if the regulations are already established for some time, or because they calculate in a more rational way the advantages and disadvantages. Of course, regulations are usually underpinned by sanctions and the institutions which execute them.

Whereas sanctions come into play, if the question, whose expectations are justified, is already settled, institutions, which serve the purpose to regulate conflicts, are necessary, if contradictory expectations and claims arise.

4.4 Delegation of interests

Another important type of institutions acts in behalf of the interests of certain groups, for example users or consumers, who are not able to look after their interests themselves, at least not permanently. Usually these groups lack the necessary knowledge. The institutions may be self-organised or organised for example by the state, as for instance the Offices for Privacy Protection in Germany. Their tasks are describing and treating problems, lobbying and giving advice to the represented groups. All institutions, which are supposed to support the building of trust have to be trusted themselves. But this is especially crucial for consulting institutions, because those who recur to them have little or no possibilities to make a complaint, if they are deceived.

Obligatory control institutions or institutions for technical evaluation and certification perform a somewhat similar function. Users or consumers may consider them as exercising control or evaluation in their interest, if they have reason to believe that the criteria which guide the evaluation are in compliance with their interests.

4.5 Extrapolation of trust

As we already mentioned above, an important problem in the emerging field of electronic commerce, where a lot of new services and technologies are offered or even new institutions are founded, for instance new certification authorities, is the lack of experience as a basis for trust. A business partner or a new service provider or institution may be trusted by the others though, if it is part of an institution, that has already proofed to be trustworthy for other reasons.

It appears that the issue of fostering trust in electronic transactions may call for policy measures as a means of facilitating the development of institutions to provide information concerning the sellers and the development of certification schemes, which should be simple, widely recognised and easily understood. Whether such schemes will emerge through the intervention of public authorities, independent and collaborative efforts of consumer organisations, or the
initiatives of major financial institutions such as credit card agencies is of secondary importance at the moment and may differ between countries. Product liability, warranties and the right to annul sales are only a few of the components which need to be tackled.

5 Summary

The study of the development of trust in the security of electronic transactions is complex. We have shown that the need for trust to compensate for an unattainable level of knowledge is a characteristic trait of modern societies. This compensation cannot be achieved by technology alone, as this would require complete knowledge about the way it functions in a certain social context. The reactor incident in Tschernobyl shattered public trust in the reliability of statements concerning the security of technology and science. Moreover, trust does not focus on an isolated technical application, but on the social context in which it is embedded. Trust-building can be supported by institutions, but there is no easy way out. The building of trust can be a very lengthy process, the outcome of which is very hard to predict. The emergence of trust intermediaries, brokers, and third party services for electronic transactions is imminent. Trust will remain necessary, although precarious.

6 References


