Enhancing Trust Online

Kristiina Karvonen, Helsinki University of Technology, Department of Computer Science, P.O.Box 9700, FIN-02015 HUT, Espoo, Finland. Phone: +358 9 451 5785 Fax: +358 451 5351 E-mail: karvonen@tcm.hut.fi

Keywords: trust, trustworthiness, privacy, computer security, e-commerce

1. INTRODUCTION

Computer security and doing business online are issues that everyone is very anxious about at the moment, but the main interest is making money - not philosophy. At present, the untrustworthiness of the Web is one of the main obstacles for the developing of services there, as well as for their increased use. For example, the renowned usability expert Jacob Nielsen has written about the current climate of the Web as one of “disregard for customers who are traded like sheep" [1]. Nobody has really cared about the security of the users.

But things are beginning to change. For some, security is becoming a good business - there are serious problems out there, and people are looking for good security solutions. This means that people are likely to be willing to pay to protect their privacy as well as to secure their transactions online, be they of money or of private information. This

means business for security experts. But actually security is a good business for anyone wanting to do business in the Internet: there is likely to be an explosive growth of the amount of "e-customers" once the security issues are resolved, and a lot of money to be gained in the bargain. The e-commerce is growing already: according to a study committed by a Texan research Institute Center for Research on Electronic Commerce [2], the turnover of e-commerce in the world is expected to grow by 70 per cent this year compared to 1998. Once the customers' trust is won over, online trading is supposed to grow even more. Security is, thus, of interest to us all - in one way or the other.

What, then, is security? To effectively provide or use security services, we must know the objectives of the services and the effect they will have. Key security properties include privacy, integrity, authentication and access control, use of encryption for confidentiality, authentication and authority in handling information requests, and last but not least, creating of trust in the user towards the security of the system. We must raise the level of consciousness of both the user and provider of security services as regards what is trustworthy and what is not.

The goal of the TeSSA project [3], of which this study is a part, was to develop general-purpose security architecture for Internet-like networks based on strong cryptography. Providing the security through use of strong cryptography is a necessity, but it is not enough. The existence of such architecture must be communicated to the users in some way. In order to convince users that they can trust the service there must be a way to give proof of this trustworthiness. Through repeated user studies, we are trying to find a way to accomplish this. We try to find out, what are the makings of trust, and then intend to use the ingredients to create user interfaces that utilise these principles, in order to enhance trust towards the service in the user. We want the user to trust us - as service providers - to be trustworthy, secure and private [4].

It is, however, a good question whether this is the right thing to do - should the feeling of trust be so enhanced in the user, when so much is at stake? Can we really guarantee that we are trustworthy now and will be so in the future? And, once we find out what makes people trust us, is it ethical to use these means to promote the feeling of trust - is it the ethical thing to do? These are questions we try to go through in this paper.

The rest of the paper is organized as follows. To start with, we make a comment on using legislative means to provide security in section 2. Sections 3 and 4 provide short definitions on the concepts of privacy and security that we feel the concept of trust is built upon. In section 5 we concentrate on the issue of trusting itself. In section 6 we consider these issues from the ethical point of view, with a conclusion of the paper.

2. A SHORT NOTE ON LEGISLATION

The users in most studies on computer security would consider legislative intervention desirable. However, there are many difficulties with trying to enforce the security and privacy in the Internet through legislative means. Administration officials fear that regulation may not keep up with the emerging technologies, and it is not a good idea to have existing regulation or legislation that you cannot enforce. In fact, this would give the people wrong assurances about assumed security. The existence of a specific law would make people think that the matter of security has been taken care of, and would no longer worry about it. Yet there might not be any real reason to trust the service any more than if there were no law at all. In all, having a law over the matter is not the right solution to the problem – trustworthiness should be communicated to the user through design, not through legislative means. Legislation consists of definitions that apply fully only under ideal circumstances - what we are talking about is, however, the real world with real users, with real security needs and real security risks. Legislation is needed here as much as in any other area of human life, but making laws is just not enough. The core of the issue lies elsewhere, that is, in the mental structures of the human mind.

How, then, can we find about these mental structures? One way to accomplish this that has always been common in the history of western thought, is to look at the language and the meanings embedded in the terms relevant to our topic. Another way is to go to the individual beholders of these mental structures, and simply talk with them, or to observe them while performing tasks relevant to our enquiry, continuing work in the footsteps of cultural anthropology and ethnographic

research. Nowadays, this is usually called a "user study", and comes closest to the area of human psychology. In this paper, we intend to use both these ways to broaden our understanding of trusting, and try to find a bridge to combine the two approaches in some way. We will start by having a look at the words most commonly used in any discussions about computer security and trust.

3. SECURITY

What do we mean by security? A quick look in a Thesaurus tells us that security is linked with such concepts as “safe”, “reliable”, “stable”, “sure” or “riskless”. Looking at security from a more technical point of view, security seems to be made up of the ingredients of confidentiality, integrity and availability [5]. Confidentiality here means privacy: the information transmitted between two systems is revealed only to authorised individuals. Integrity, on the other hand, is protection of transmitted data from being transformed in any way. Availability is exactly what is appears to be: the data is available to authorised users whenever they need it [6].

It is clear that there can be almost as many definitions of security as there are users reported experiencing or lacking it. Whwn we talk about mental structures, security could be shortly described as a state of mind that constitutes of many different factors. In our usability studies, we took as our starting point the assumption that in any case, there are two concepts that are of utmost importance for any considerations of security, be it computer security or security in general. These two concepts are privacy and trust. Feeling secure means that there is trust, be it toward a person, an institution or a service on the Web. This trust includes the assumption of privacy – that any transaction performed will remain a private matter between the parties involved.

No matter how we define what we mean by security, at the core of the issues lies the problem that there might be a great difference between actual and perceived security. The users’ ideas about what is secure and what is not might not have anything to do with the actual level of security of, say, a service on the Web. The goal studying it is to

overcome this problem so that in the future, the actual and the perceived security of, say, a web-based service, would be the same. We want the alleged trustworthiness or untrustworthiness of any online service to be clearly and unanimonously visible to the user. This, in our opinion, would ensure the ethicality of that service. The question remains, is this ever possible in the full sense of the words?

4. PRIVACY

Privacy is one of the top priorities of consumers intending to use Internet-based services. It seems to be ahead of such qualities as ease-of-use or cost [7]. The use of Internet is threatening consumer privacy in new and extreme ways, and people are willing to take the time and effort to make sure that their privacy on the Net is being protected [8]. Privacy includes both the privacy of personal information supplied by the user for the service-provider as well as privacy of any transactions (that involve the use of money) performed by the user online in the Internet.

How, then, is one to describe the exact makings of the feeling of privacy? Another look in a Thesaurus tells us that privacy is "the quality or state of being apart from company or observation, that is, seclusion" (1 a), or "freedom from unauthorized intrusion, one's right to privacy" (1 b). In the archaic sense, privacy can also mean "a place of seclusion" (2). The third and last meaning given us by the Thesaurus links privacy with security through secrecy, depicting privacy as "secrecy" (3 a), or as "a private matter, secret" (3 b).

What about the mental world of the user, revealed through actions? In a study done at AT&T Labs-Research [9], it was found that the general attitudes of the users varied greatly, when it came to the question of what is considered to be private. The users were loosely grouped into three categories in their attitudes towards privacy. These were: 1) The privacy fundamentalists, who were extremely concerned about their privacy, 2) the pragmatists, who were also concerned about their privacy but were ready to trust the services if there was some sign of existing privacy protection, and 3) the marginally concerned, who were willing to give data web sites under almost any conditions. It is also likely that

there will be not just individual differences but also cultural ones what comes to the makings of privacy: The need for privacy and the requirements for experiencing when the standards for privacy are being met is likely to vary culturally as well.

5. TRUST

Finally, we are left with the concept of trust. What do we mean when we claim that we "trust someone"? How does the feeling of trust evolve, and how to enhance it? This is an area that has still remained largely untouched by scientific research – until now, there has been only one major study committed on the issue of trust as regards the use of the Internet as a marketplace [10] that we know of. In order to start with this, however, we need first to define trust.

Thesaurus provides us with the following answer: with trust we can mean "complete assurance and certitude regarding the character, ability, strength, or truth of someone or something ". As synonyms for trust, we get a list including concepts such as confidence, dependence, faith, hope, reliance, and stock. We also get a list of related words - these have something to do with the notion of trust. The list is made up of assurance, certainty, certitude, conviction; belief, credence, credit; positiveness, sureness; entrustment; overconfidence, and oversureness.

Philosophically, trust is to be separated from confidence and faith – both concepts with which the concept of trust seems to be at least partially overlapping [11]. Trust is related to all these concepts and must be set in context with them. Sociologically, trust could be defined as a sort of a header that describes the nature of transactions between two or more individuals, an individual and an institution or an authority, or between two institutions, to put it in a simple way [12]. Trust can be also viewed as a historically emergent property of human interaction that is tied to a specific form of social organization [13]. Modern forms of trust are, then, rooted in the rights, obligations, and liberties of citizenship [14].

No matter how we define trust, it is clear that we are talking of a complex phenomenon that has up-to-date not been analysed properly in

philosophical, sociological or technical sense of the word [4]. We are also talking about knowledge, or rather, the lack of it, whenever we bring forth the notion of trust: trust is needed exactly because of insufficient amount of information [15]. Without knowing for sure, we have to decide whether or not to trust the other party, be it another person, or, say, a service provider on the Web. This imbalance essentially creates the question of the ethicality of enhancing trust through perhaps artificial means. It also introduces us to the opposite of the concept of trust found in a Thesaurus - namely doubt, dubiety, dubiosity, skepticism, suspicion, and uncertainty. This imbalance also makes trusting seem unlikely or at least irrational. It might be more reasonable to *dis*trust instead.

6. THE ETHICS OF ENHANCING TRUST ONLINE

This question of imbalance in the amount of available information brings us back to the last items on the list of "related words" on the definition of trust, overconfidence and oversureness, when we start to consider the ethicality of enhancing trust online. If we succeed in our pursuit and indeed are able to identify the makings of trust and start using them, are we talking of a case of overconfidence? We may be sincere in our statement that we ourselves trust that we can provide secure, private and trustworthy services. We cannot, however, guarantee fully that a malicious third party is not intervening. It is common knowledge in the information business that most, if not indeed all, systems are breakable. Someone might hack their way into the system. We trust that it is not our system, but we do not know it beyond doubt. This being the case, should we enhance trust towards our system in the user or not?

It is a tricky question, but in our opinion, the answer is yes. The issue resolves itself to some extent, if we consider the opposite: of not enhancing trust. What will happen then? It seems that the current situation will continue as it is now: as one of untrustworthiness, of uncertainty and inequal information. The users often find they have no way of finding the right information, or are too busy to go and look for it [4]. By refraining from giving them any tools for deciding when it is reasonable to trust a service will not help but instead leaves more room for deceitful behaviour. The possibility of betrayal is an old one, and

arises whenever there is a transaction between two parties, regardless of the media it takes place in. It will not go away. The issue is, thus, to find the means to achieve the best possible solution in a real-world situation.

The best way to do this so far has been to use seals of approval [16]: a trust mark that shows that our security has been considered trustworthy by a third party. To do this convincingly, we need to find out, what the user finds convincing enough to trust us. "Every art and every inquiry, and similarly every action and pursuit, is thought to aim at some good; and for this reason the good has rightly been declared to be that at which all things aim", wrote Aristotle in the beginning of Nicomachaean Ethics [17]. Aiming for the good, in this case, means finding ways of communicating that we are concerned on the security issues, and we believe that we are trustworthy. Yes, we are dealing with probabilities here, not with absolute certainty. Yes, the possibility of fraud is there. In the long run, however, it is better to fight it than to let go.

7. REFERENCES

[1] Jakob Nielsen's Alertbox, March 7, 1999 at http://www.useit.com/alertbox/990307.htm

[2] Cf. http://cism.bus.utexas.edu/

[3] Telecommunications Software Security Architecture, a project at Telecommunications Software and Multimedia Laboratory at Helsinki University of Technology, http://www.tcm.hut.fi/Research/TeSSA/

[4] Karvonen, K: Creating Trust. Proceedings of the Fourth Nordic Workshop on Secure IT systems (Nordsec'99), November 1-2, 1999, Kista, Sweden, pp 21-36.

[5] White G.B, Fisch E.A, Pooch U.W.: Computer Systems and Network Security, CRC Press 1996, pp. 1-3

[6] Holmström, U: User-Centred Design of Security of Software. HFT Proceedings, Copenhagen, Denmark, May 4-7, 1999, pp. 49-57

[7] Cf. A poll on online insecurity conducted Feb. 18-23, 1998 for

Business Week by Louis Harris & Associates Inc. and Alan Westin, publisher of Privacy & American Business

[8] Hoffman, D.L., Novak, T.P., and Peralta, M.: Building Consumer Trust Online. Communications of the ACM, April 1999, Vol.42, No 4, pp. 80-85

[9] Cranor, I.F, Reagle, J. and Ackerman, M.S: Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. AT&T Labs-Research Technical Report TR 99.4.3, http://www.research.att.com/library/trs/TRs/99/99.4/99.4/

[10] ECommerce Trust Study. Joint Research Project by Cheskin Research and Studio Archetype/Sapient. January 1999. Http://www.studioarchetype.com/cheskin/)

[11] Seligman, A.B: The Problem of Trust. 1997 Princeton University Press, New Jersey, p. 16-17

[12] Giddens, A: Consequences of Modernity, Stanford: Stanford University Press, 1989, p.114

[13] Lewis, D. and Weigert, A.J: "Trust as Social Reality" in Social Forces 63, no. 4 (June 1985), p. 976

[14] Lewis, D. and Weigert, A.J: "Social Atomism, Holism, and Trust" in The Sociological Quarterly 26, no.4 (1985), pp. 455-71

[15] Cardholm, L.: Building Trust in an Electronic Environment, Proceedings of the Fourth Nordic Workshop on Secure IT systems (Nordsec'99), November 1-2, 1999, Kista, Sweden, pp. 5-20

[16] For information on seals of approval, see for example Benassi, Paola: TRUSTe: An Online Privacy Seal Program in Communications of the ACM, Feb.1999/Vol.42, No.2

[17] Aristotle, Nicomachaean Ethics, translated by W. D. Ross. Provided by The Internet Classics Archive available online at http://classics.mit.edu//Aristotle/nicomachaen.html