Expressing Trust

Kristiina Karvonen **Ursula Holmström**
Department of Computer Science
Helsinki University of Technology
P.O.Box 9700 HUT
Finland
Tel. +358-9-451-57-85
{Kristiina.Karvonen, Ursula.Holmstrom}@hut.fi

1 INTRODUCTION

Quite recently, trust has become one of the hottest topics of study in computer security. There are several reasons for this. Firstly, trust is a problem for online transactions - lack of trust is considered to be one of the major obstacles for developing successful ecommerce enterprises (e.g.,[2], [4], [6]). Secondly, till today the technical representations of trust have not really had anything to do with the average person - trust was not an issue to be dealt with by the ordinary user, and all the security features were taken care of by technical experts [7]. However, through the rise of e-commerce and online transactions - not to mention a new consciousness of privacy issues - it has become necessary for non-technical users also to be able to handle their own security in a novel way – and especially to be able to manage, express and control their trust - who they trust online, in what situations and why, and to what extent. "Onlinetrust", then is a new concept for users that has to be made understandable and easy to handle. In order to accomplish this, we need to know, how and why people trust something or someone.

Not only users and use situations have changed, but there have been some major technological changes taking place. Distributed systems require a different way to handle the security of the system compared to single mainframe computers. The need to handle security in a unified way from (an often abstract) security policy to actual security mechanisms such as access control lists, has led to the introduction of trust management systems [1]. These trust management systems were designed for expert users and to be used in rather limited use situations e.g. system administration. Although other similar systems such as PGP [8] have been designed for applications closer to the end user (e.g. e-mail), they still do not cover the current plurality of users and use-situations. As it is, there are different technologies available for expressing trust in a technical sense, but none of these are usable for an average web user as such. What is needed is a way for computers to understand what "human trust "is made of.

To give an example of the problems we are dealing with, non-expert users do not think of the security system they are using in terms ofsubjects, objects and actions, but rather as means to an end, and theobjects they see while using the system are not directly mappable to network objects. This means that if a user trusts a bank, it is not obvious at all what the technical object it is that the trust in this case refers to. "Public key" might be a *good* answer, but is it the *best* answer?

2 HUMAN TRUST

What is trust from the user point of view? Existing studies show us that trust is formed through experience, and is a long-term proposition – hard to build and easy to lose [2], [6], [7]. In an often-cited study by Cheskin Research & StudioArchetype/Sapient [2], it was found that the *feeling of control* forms the basis for trust. On top of this, the study lists six fundamental ways to communicate trustworthiness. These are seals of approval, brand, navigation, fulfilment, presentation, and up-to-date technology.

2.1. Methods

Asking users directly on the topic is usually not a good idea. Users tend to give “school class answers” to such direct questions, instead of describing how they really behave. This is also why we have some doubts about using questionnaires to find out about security issues, even though such research exists also [3]. Instead, we have used qualitative structured interviews, going through mock-up UIs, or navigating through existing Web services for security features, and site reviews focusing on their apparent security, as judged by users [5], [7].

2.2. Research Questions

Our research agenda included the following problem areas, for which answers were clearly needed:

1. Sources of trust

- What are the sources of trust? Is it social networks (family, friends, colleagues), different mass media (television, radio, Internet, news papers, magazines), or other?

2. Definition of trust

- What do users mean when they state they trust someone or something?

3. How to express trust?

- What ways of visualising trust would be acceptable and understandable for the users?
- How can users express that they do trust a system? What ways can we provide them with, to enable such trust expressions?

4. Finding the right technology

- How can we map the users' expressions of trust with existing security technology, or
- Should we create a new set of security technologies "from a scratch" that would better take into account the novel uses and novel users?

2.3. Results

Our studies have given results very similar to the results of these other studies, with some notable exceptions. Firstly, we found that in Finland, even technically advanced users were quite unfamiliar with seals of approval, and suspicious of them. Secondly, even though the importance of brand name and reputation is important, there were differences in the amount of trust depending on what kind of a service was dealt with. Our study showed that there was more trust towards such online services with which trust has always been an issue, also in the real world. Banks are a perfect example of this. Trust towards a bank in the physical world stays more or less the same when using the bank's online services [7]. This means that trust in the real world i strongly transferable to online environments. Also, the sources of trust seem to vary - some trust the advice of a friend, some revert to a newspaper for information and so on.

3 DISCUSSION

The key question is, how to deal with the ccomplexity that security inevitably holds within. How could we guarantee that users can, at the same time, make a simple yet accurate decision about trust? Should we try to imitate the real-world trust between people or between people and banks, for example, or would some other approach be more fruitful? From the user point of view, the problem areas include the following:

- How can users find out if a service provider is trustworthy?
- How can users get information about security and trust issues?
- How can we motivate the users to care about their security in a positive way, and not to consider it as a burden?

4 REFERENCES

Blaze, M., Feigenbaum, J. and Lacy, J: "Decentralized Trust Management", in Proceeding of the 1996 IEEE Computer Security Symposium on Research in Security and Privacy, Oakland, CA, May 1996

ECommerce Trust Study. Cheskin Research and Sapient/Studio Archetype. 1999

Fogg, B.J. et. al.: Elements That Affect Web Credibility: Early Resultsfrom a Self-Report Study. Proceedings of CHI2000, Short talks, 2000.

Järvenpää, S.L., Tractinsky, N: Consumer Trust in an Internet Store: ACross-Cultural Validation. Jounal of Computer-Mediated Communication, Vol.5(2), December 1999.

Karvonen, K: Creating Trust. Proc. of Fourth Nordic Workshop on Secure ITSystems (Nordsec'99), November 1-2, 1999, Kista, Sweden

Nielsen, J: Trust or Bust: Communicating Trustworthiness in Web Design, http://www.useit.com/alertbox/

Nikander, P, Karvonen, K: Users and Trust in Cyberspace. Proceedings of theCambridge 2000 Workshop on Security Protocols, 2000

PGP Users Guide, http://www.pgpi.org/doc/guide/

