Position Statement: Risk Perception and the Acceptance of New Security Technology

Marian Harbach, Sascha Fahl, Matthew Smith
Distributed Computing and Security Group, Leibniz University Hannover, Germany
{harbach,fahl,smith}@dcsec.uni-hannover.de

ABSTRACT

Risk perception and communication research in IT security has largely relied on studies addressing specific risks or threats and investigating how users assess or react to these. This approach offered valuable insights for the design of countermeasures against specific threats, such as phishing warnings or anti-virus protection. However, for the deployment of new and better IT security technology, the role of risk perception has not been properly analyzed yet. In previous studies, we found that users are interested in additional security measures, such as alternative authentication mechanisms or message encryption, but do not adopt them in everyday life. They showed little awareness of different sources of risks and therefore treated the Internet as a generally unsafe environment where nothing can be done to improve one's situation. In this position paper, we discuss why it is important to study and understand which and how risks are actually perceived by users during everyday Internet use without being asked about specific threats. We postulate that an understanding for the development of everyday risk perception will help to promote IT security technology.

1. INTRODUCTION

Existing work on risk perception analyzed users' common understanding [9] or how to incorporate them into security solutions [1] with respect to specific threats, such as phishing, hacking and malware. Additionally, researchers have looked at how to communicate a particular risk to a particular user group [4] or which factors influence the perception of specific risks [8, 3]. This important work allowed the usable security and privacy community to instill a certain amount of awareness for particular security and privacy measures in users (e. g. anti-phishing measures). However, we believe that we still do not fully understand which and how risks are perceived on the Internet if users are not prompted to think about specific threats. As we will outline below, this lack of understanding is especially evident in the unbroken prevalence of username and password and the, at best, slow adoption of email encryption in everyday Internet use. Users appear to perceive little to no risk in their daily Internet conduct and without perceiving specific threats or risks to be protected against, users are not ready to change their behavior. Additionally, understanding how risk perception can be changed or does change by itself will help to more effectively promote new security technology.

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

2. BACKGROUND

In the papers mentioned in the introduction, risk was assumed to arise from a specific threat, e. g. phishing, hackers, or malware. Thus, this threat was always *selected for* the users in the studies. However, we have repeatedly found that participants in our studies did not naturally differentiate threats or sources of risk at all. Consequently, they did not perceive much risk when no specific threat was mentioned. In our studies, several participants were confident with using only two different passwords across all their online accounts and saw no problems or risks arising from that practice. Yet, participants also often voiced concerns about virtually anything on the Internet being vulnerable to attack or "hacking". We believe that without being queried about a particular threat or risk, users will struggle to identify risks in general and consequently have little motivation to adopt new security practices. This attitude is mirrored in technology acceptance models discussed in business and information science (e. g. [2, 6]), where the appraisal of potential threats is an important precursor for the overall motivation to adopt a new security technology.

During focus groups we ran on a novel authentication technology [5], multiple participants expressed that they treat the Internet as a generally insecure medium and that they therefore, for example, do not use online banking at all. Among other comments, one participant believed that password managers "*surely could be hacked by someone*". Another participant said: "*I don't believe that there will ever be perfect security on the Internet. Whether you use [an alternative mechanism] or continue using passwords [. . .] there are vulnerabilities everywhere*". Many subjects believed that there will be a way to circumvent any security system at some point in time.

In a more general scenario, Hogarth et al. [7] investigated everyday risk perception. Participants recorded one risk and the most severe consequences involved in whatever they were doing when receiving a text message from the researchers three times per day on work days during 2 weeks. They found that the most frequently reported risks were the most salient ones as opposed to the most severe ones. Con-

sequently, they conclude that the risks consciously perceived are a subset of the risks actually faced. Many of the everyday risks commonly studied were also entirely absent from the risks reported by their participants. Additionally, retrospective assessments of the same risks were less severe than assessments collected simultaneously. They argue that real, emotionally charged risk assessments are therefore likely to be different from risk perceptions collected in surveys or laboratory settings.

3. RISK PERCEPTION IN EVERYDAY INTERNET USE

The findings of these previous studies motivate a new look at risk perception during everyday Internet use. It appears that when reasoning about online risks, users will resort to describing the Internet as a generally unsafe environment and therefore value protection mechanisms lower because nothing can be done to make them safer anyway. This view might stem from a lack of understanding that security consists of several independent parts that address specific risks and that increasing security for one of those parts can make them safer. They do not differentiate between security risks occurring because of, for example, insecure authentication mechanisms, lax privacy policies or missing transport security.

Alternatively, if users do understand at least some of the building blocks of IT security, they may be failing to see that there are different strengths of protection pertaining to particular security mechanisms. For example, because there were several incidents in the media where security mechanisms were circumvented, users may believe that guessing a weak password and breaking RSA are equally likely. It appears that, in the end, this is all simply attributed to the generally unsafe Internet instead of differentiating threats and risks by their true source.

While these theories of the perception of everyday online risks need to be confirmed by running appropriate studies, they are a possible explanation why many users have an almost apathetic attitude towards online security and privacy: If they think that the risk of any security mechanism being broken is equally likely and therefore their risk of having their information compromised is equal across mechanisms, the motivation to even consider additional or different measures is low. We believe that analyzing how and which risks are perceived during everyday Internet use is an important step towards finding ways to foster more security and privacy awareness in users and therefore helping us to motivate the adoption of novel security technology.

4. THE ROAD FORWARD

We suggest to run studies that investigate the perception of everyday online risks without prompting for specific threats. The results will allow the security community to facilitate the introduction of improvements, since trying to make users accept new security technology based on beneficial technical properties or dedicated communication of a few specific risks is an approach that has apparently failed.

Beyond analyzing the status quo, the question that arises is whether we can change users' current risk perception on the Internet through educational campaigns or training, whether this is a state of mind that we need to accept and work with, or can we do nothing but giving users time to adjust their risk perceptions by themselves to the modern ways of interaction and communication?

To the best of our knowledge, changes in risk perception in general with respect to risk exposure or familiarity with the risk generating activity have not been studied in detail. However, there are examples from other aspects of life where risk perceptions clearly change. For instance, the novice mountaineer will not know which dangers pertain to crossing a glacier, but, through repeated exposure to the risks, guidance and education, she will be able to assess the risks pertaining to that activity by herself. Yet, she will not only be able to assess the risks previously enumerated, but also gain an intuition for other potentially risky situations without being explicitly informed about these.

This example serves to argue that we may be able to train users' risk perception to a point where the user is able to actually have a more realistic view of potential risks and their sources and consequently make better risk-taking decisions. However, our mountaineer also has an intrinsic motivation to learn about the risks pertaining to the potentially hazardous environment: she wants to stay alive while enjoying the pleasures of being in the mountains. This is a fundamental difference compared to people using the Internet: people regularly die from avalanches or falling into crevasses but there currently is little potential for personal harm from using the Internet. The IT privacy and security community therefore needs to find ways to incentivize people to desire IT security and privacy. We believe that tackling this challenge is the most promising way to better protect users online and analyzing the current state of everyday risk perception a valid starting point.

5. REFERENCES

[1] J. Blythe and L. J. Camp. Implementing Mental Models. In *Proc. SPW*. IEEE, 2012.

[2] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science*, 35(8):982–1003, 1989.

[3] V. Garg and J. Camp. End User Perception of Online Risk under Uncertainty. In *Proc. HICSS*, 2012.

[4] V. Garg, L. Huber, L. J. Camp, and K. Connelly. Risk Communication Design for Older Adults. *Gerontechnology*, 11(2):166, 2012.

[5] M. Harbach, S. Fahl, M. Rieger, and M. Smith. On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In *Proc. PETS*. Springer, 2013.

[6] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao. Security Services as Coping Mechanisms: An Investigation Into User Intention to Adopt an Email Authentication Service. *Info Systems J.*, 2012.

[7] R. M. Hogarth, M. Portell, A. Cuxart, and G. I. Kolev. Emotion and Reason in Everyday Risk Perception. *Journal of Behavioral Decision Making*, 24(2):202–222, 2011.

[8] D.-L. Huang, P.-L. P. Rau, and G. Salvendy. Perception of Information Security. *Behaviour & Information Technology*, 29(3):221–232, 2010.

[9] R. Wash. Folk Models of Home Computer Security. In *Proc. SOUPS*. ACM, 2010.