# [Position Paper] Can we afford to remain apathetic towards security apathy?

Alexander G. Mirnig, Sandra Trösterer, Elke Beck, Manfred Tscheligi
ICT&S Center, University of Salzburg
Sigmund-Haffner-Gasse 18
5020 Salzburg, Austria
{alexander.mirnig, sandra.troesterer, elke.beck, manfred.tscheligi}@sbg.ac.at

## ABSTRACT

We argue that apathy towards security is a serious and, as of yet, underexplored issue in HCI. Secure and trustworthy design will have difficulty to ever really succeed if the user's priorities and intentions are contrary to these goals. The reasons for and different manifestations of security apathy have to be explored more thoroughly so that future design solutions can be evaluated not only on their success in general but also on how well they counteract varying degrees of security apathy. We want to push towards a more extensive approach towards security apathy, so that it will be possible to directly evaluate (both formatively and quantitatively), prevent and/or counteract security apathy on an application-specific as well as on a general level – an important milestone in IT-security. We are currently developing a questionnaire to elicit the degree of security apathy in users. With a way to measure the degree of security apathy we will be able to directly evaluate security feedback solutions in terms of how well they cope with apathetic attitudes and behavior.

## 1. POSITION

We argue that apathy towards security is a serious and, as of yet, underexplored issue in HCI. There is a plethora of literature regarding types of risk, risk perception and how it differs depending on the individual user type (e.g. [1, 3, 9]). Closely related to these types and the issue of real vs. perceived risk is the phenomenon of apathy towards security, i.e. a general disinterest in security measures and information. It is one thing to be aware of a risk and another to have a correct mental model of said risk [8]. An apathetic stance towards security is likely to have a negative impact on both levels, which makes this a problem that is certainly worth investigating. The issue of security apathy – although not always named as such – is certainly not a completely new one (cf. e.g. [4]) but we argue that it is in need of being treated as its own topic and discussed thusly (and not on an application-specific level only), since even the most well-thought-out design and security measures will have difficulties succeeding if the user is unwilling to employ them and/or actively working against them due to disinterest and resulting ignorance.

Such a closer look at the phenomenon of security apathy requires also looking into the reasons for it. On these quite a bit of research has been conducted in the past ([2, 5, 6 7] among others) which we could draw from. One of the reasons discovered is a certain dissonance between the security tools and the characteristics of security management done by users: According to Gross and Rosson [6] the reasons for the failure of current end-user security management tools and practices are that they are not goal oriented and that there is thus never a point at which the user can consider a goal to be satisfied. This can lead to a feeling of necessity of never-ending vigilance and a resulting impression of futility regarding security systems. Then there is the issue of users not feeling responsible for securing IT: In a study of Gross and Rosson [6] most people saw security as the responsibility of dedicated IT staff (technical perspective) or of the organization and its leaders (organizational perspective). Participants who expressed a social perspective, i.e. the end users include themselves as visible players in the security management, seemed to be more interested in security issues and were prepared to take a more active role in managing their own security. Another factor are differences in Internet experience and knowledge. Karvonen [7] argues that understanding the consequences of one's actions (and the risk associated with them) is a difficult task for most users. Gross and Rosson [6] similarly discovered a general disinterest in technical details as well as inaccurate, incomplete and/or outdated knowledge of security and privacy among users. Bellman et al. [2] found that online privacy concerns fall the more Internet users there are and the higher the average level of experience rises. Another big factor are differences in risk perception due to cultural differences: According to Karvonen [7] the perception of what constitutes a risk is not always the same among users. In a global survey about information privacy, Bellman et al. [2] discovered that privacy concerns are different between cultures, e.g. cultures with a high level of individualism are comfortable with higher levels of disclosure of private information when compared to cultures with lower individualism.

What these findings show us is that there is a certain discrepancy between users (and their preferences) and security management and we suspect this to be one of the main contributors to security apathy. These discrepancies manifest themselves in different ways and permeate a wide variety of user types. This also indirectly explains why security apathy is still such an unexplored area as it seems very difficult to grasp on a general and comprehensive level. It is therefore likely that different types of security apathy will have to be defined and differentiated from each other further down the line. But in order to arrive at the final goal, first steps

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

have to be made and we decided to do so by looking at the user attitudes and characteristics that induce apathetic behavior and what causes them. As a starting point, we decided to base our research on the findings of Dourish et al. [5] who identified three major neutral to negative attitude types that users display towards security measures, messages and technology. These three attitude types are (a) Frustration: Security appears as an obstacle and is rarely a primary concern for end users. Persistent security software and having to deal with security warnings and configurations is often seen as a hindrance and only secondary to a user's actual activity. This ranges from users being dissatisfied with security configurations and then adjusting or circumventing them manually to users who intentionally never turn off their phones due to them not wanting to having to remember their passwords. (b) Pragmatism: This attitude seems to be more common among the younger users. They adapt their behaviour to their perceived security needs (e.g. a pragmatist would have no qualms about knowingly using insecure technologies if they felt the risk was justified. These users see security as a balancing act between immediate needs and potential dangers. In order to achieve this balance, they need systems with a sufficient degree of both flexibility and translucency. (c) Futility: This attitude comprises of both an overall sense of futility in user's encounters with technology as well as the impressions that Hackers, cybercriminals, etc. will always be one step ahead of even the most sophisticated security software, meaning that there will always be new threats and attacks to adjust to. This feeling of having to always be vigilant and the unattainability of a (much desired) state of absolutely impenetrable security lead to an overall impression of futility as far as security is concerned. While it is doubtful that these three attitudes would be the only ones relevant for security apathy, they describe many factors one would associate with an apathetic stance towards security and are empirically well grounded, thus lending themselves very well to being a basis for a security apathy questionnaire. We do not claim that concentrating on these three attitudes alone is sufficient for capturing every type of security apathy there is. We *do*, however, consider it to be a very good starting point for a more comprehensive approach towards capturing security apathy and apathy-prevention driven design evaluation.

We have begun developing a questionnaire for eliciting the degree of security apathy in users by measuring the three aforementioned attitude types, with the scope of capturing more factors (additional relevant attitude types, behaviors) that lead to security apathy as the questionnaire develops. Such a questionnaire will allow us to divide users into more or less clear-cut categories regarding type and degree of security apathy. By analyzing design solutions not only on their own merits but also with regards to how well they work for user groups with different degrees of security apathy, i.e. it will be possible to directly evaluate (both formatively and quantitatively) design to prevent and/or counteract security apathy on an application-specific as well as on a general level – an important milestone in IT-security. Much research is needed until such a lofty goal will be in reach and we therefore want to use this opportunity to discuss several important aspects regarding security apathy-related risk assessment with the workshop participants. For one, an important question is whether security apathy is more of a personality trait (which are difficult to influence and therefore need to be catered to in many cases) or induced by other, non-personality dependent factors (which could be more easily influenced through e.g. clever design). If the latter is the case, then it would be interesting to know whether there are already any designs that encourage security apathetic users to be more security aware and how those websites were designed to work that way. Another interesting question is the interrelation between risk perception [10] and security apathy and how they influence each other (Could a certain kind of risk perception induce security apathy? What exactly are the influences of security apathy on a user's perception of risks?). We hope to draw from the experience and expertise of the workshop participants and have a fruitful discussion, which might shed some light on these questions as well as spark some interest in broader issue of security apathy as a whole and encourage further research.

## 2. REFERENCES

[1] Ackerman, M.S., Cranor, L.F. and Reagle, J. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*, ACM Press, New York, NY, 1-8.

[2] Bellman, S., Debray, E.J., Kobrin, S.J. and Lohse, G.L. 2004. International differences in information privacy concerns: A global survey of customers. *The Information Society*, 20(5), 313-324.

[3] Berendt, B., Günther, O. And Spiekermann, S. 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*, 48(4), 101-106.

[4] DeWitt, A.J. and Kulis, J. 2006. Aligning usability and security: a usability study of Polaris. In *SOUPS '06 Proceedings of the second symposium on Usable privacy and security*, ACM Press, New York, NY, 1-7.

[5] Dourish, P., Grintner, R.E., De La Flor, J.D. and Joseph, M. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401.

[6] Gross, J.B. and Rosson, M.B. 2007. Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 Symposium on Computer Human Interaction For the Management of Information Technology*. ACM Press, New York, NY, 10.

[7] Karvonen, K. 2007. Users and trust: the new threats, the new possibilities. In Universal Access in Human-Computer Interaction. *Applications and Services*. Springer, 893-902.

[8] Raja, F., Hawkey, K., Hsu, S. and Wang, K.-L.C. 2011. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *SOUPS '11 Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM Press, New York, NY.

[9] Sheehan, K.B. 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society*, 18(1), 21-32.

[10] Slovic, P., Fischhoff, B. and Lichtenstein, S. 1980. Facts and Fears: Understanding Perceived Risks. In *Societal Risk Assessment: How Safe is Safe Enough?*, Schwing, R.C. and Albers, W.A., Eds. Plenum Press, New York, NY.