

# On Security Sharing

**Kristiina Karvonen**

Helsinki Institute for Information Technology HIIT

19800 Aalto University

00076-AALTO, Finland

+358 9 470 28362

kristiina.karvonen@hiit.fi

## ABSTRACT

Security is tricky for most computer and online users besides the technical experts: Security is communicated through technical terms that do not mean much to most, and having to take part in managing the security is not a top priority activity for most users to spend time on. To overcome these obstacles, many users are currently coping by relying on their peers and immediate family to get informed about and helped with dealing with security. In this workshop position paper, I am discussing the several incidents where I have run into users who have chosen to *rely on other people* as their first option when trying to manage their security. I am also describing our current efforts in trying to make use of this inclination to rely on the people, when technology gets in the way.

## Keywords

Security, sharing, user experience, usability, privacy, trust

## INTRODUCTION

We all have this “security expert” in our circles we go to and rely on when we are confronted with computer and Internet security. Isn’t it so? However, this person we rely on can, in reality, be far from a “real” security expert if judged from the outside, and not that knowledgeable about security at all. But it all depends on the choices available: if this person is the best we can get – the best in our circles – this person *de facto* becomes the security expert of our circles.

*Relying on someone you already know* is very desirable. It provides a resource and helps getting on with the daily life. And, if something goes wrong that person is still around: *Permanence* is important to be able to rely on the resource. Further, as humans are by nature social beings, sharing of problems is only natural and reinforces the feeling of being part of a group. Such sharing applies to security sharing as well. In this paper, I will present a number of cases where I have run such security sharing activities among family members and friends in order to manage security.

*NordiCHI 2010 workshop on Understanding Friend- and Family-based Security and Privacy issues, October 17, 2010, Reykjavik, Iceland.(NordiCHI’10, October 17–20, 2010, Reykjavik, Iceland)..*

## Case 1: Security management in the family with teenage children

*Description:* When we were trying to come up with more usable secure device pairing methods for creating secure Bluetooth connections between different devices, we run into an interesting phenomenon during the user study: as we were having families with teenage children test out the pairing procedures we had invented, we found out that not only did the children do best in the attack scenarios, being able to detect that someone was pulling their nose while their parents fell for it, but we also found out that in families, not only were computers often shared among the family, but that the family members were also trying to cope with the security together as well. [K2][K3][K4].

Additionally, in a study among security experts described later in more detail, we were running an online questionnaire among the security experts with an optional section on parental issues and security. Unlike in e.g. the Eurobarometer survey on safer internet where parents report they cannot really guard their children’s online security the way they’d want to, these users *do have* the technical know-how at least to enable such guarding. However, it turns out the *security is negotiated within the family* in pretty much the same way as in the non-expert families and *managed together*. [K1]

*Analysis:* Combining the *parents’ motivation* to keep things safe with the *children’s ability* to take in new information and willingness to learn new stuff every day is a fruitful combination for managing the family computer and Internet security. This was sometimes achieved even without any actual security products such as anti-virus purchased. In the families, security had become an area where *forces were joined and losses were grieved for together*. Further, the *children were* in some sense *more able* to cope with managing the security. In the expert families, security was handled with pretty much the same attitude, except for the security products, which were usually installed.

*Lesson learned:* Managing security can be a joining force across people already close.

## Case 2: Making trust decisions online

*Description:* Some 10 years ago, I was conducting user studies among non-experts to find out what is the basis of trust decisions online. What I found out was that at a time when online purchases were not yet abundant and social network tools were a far cry from where they are today, people were already *relying on their peers and utilizing their social networks* in pretty much the same fashion they do today, only now enabled by the new social networking tools. In the late 1990's and early 2000, when considering whether or not an online purchase was safe, what a person would do was give a call to their friends on the phone or go ask around for advice. [K5]

*Analysis:* No-one wanted to be a guinea-pig for trying out a new service for its trustworthiness (unless they were trying it out with the company credit card, of course). Before indulging in any transactions, users requested for good news on previous encounters and experiences from others with the service. *One would not enter the online world on one's own but accompanied by one's friends and their experiences and advice.*

*Lesson learned:* Online trust decisions have always been a group effort, long before the technology really allowed for or supported it.

## Case 3: What motivates security experts to share their knowledge?

*Description:* upon aiming to understand and analyse what motivates users to be active participants on an online security-blog offered by a major security vendor, we found out that besides professional development and the plain interest in security *per se*, the security experts who actively participated in commenting the blog writings were in fact partly motivated by their *willingness to help other users* to avoid security pitfalls and to be able to manage their security. [[K1]

*Analysis:* Participating in the security forum was inherently social, and the security experts were not online merely for a personal gain.

*Lesson learned:* Most people like and are willing to help others. The possibility for helping should be sought out and offered. Also noble causes such as "aiming the common good" should not be underestimated as a motivator for helpful behaviour.

## Case 4: Being informed about security in the urban environment through peers

*Description:* I am currently working on finding out *how we experience and talk about security*. The work is motivated by the observation that when moving about a city one is not familiar with, it might be helpful to get some indication on which areas of the city might not be safe to venture into. But how can one *get* such information, and, further, *trust* such information, even if available? Obviously, there may be political issues in a city officially advertising some of its

parts as officially insecure, so a more likely option for giving and getting such information could be *through peers*. The work is further motivated by the fact that I have not really been able to find existing body of work in this area – how people might *share (or not share) their experiences related to security*, and if they share, how do they do it? Further, do they actively seek the possibility to warn others, and would they appreciate such information if it was offered to them? The way I go about the work is during my work-related travelling, I randomly ask from 10 local people, which areas of the city are less safe than others – pretending to be mere tourist and armed with a map.

*Analysis:* This work is ongoing – currently the survey has been carried on in various cities in Europe (Finland, Denmark, Portugal, Spain). The initial findings are quite interesting. It seems it may be possible to *identify unsafe areas on the city map* that most respondents suggest as unsafe. This information is not currently available to the accidental tourist. Further, it seems *talking about security or insecurity is not common practice and can be intimidating to some*. Methodologically, it seems to me best results are gained by a combination of group work and individual interviews: the group talk *makes visible the differences in both the actual experiences and the attitudes* of the city dwellers, even when they know each other. The one-on-one talk offers *an outlet for the thoughts that were left unexpressed in the group situation*, for example due to social reasons: fear of standing out in a negative way among your peers.

*Lesson learned:* The people I've interviewed did seem to have an unexpressed view of their city's secure and insecure zones, and were sometimes surprised at other inhabitants' views and experiences and were interested in them. The peer-provided information on areas secure or insecure might have a ready audience, if possible to offer within the city. However, there are many issues that need resolving, such as how to make this information trustworthy, and so on.

## CONCLUSIONS

Security for non-experts is already a joint venture between family members, friends and trusted colleagues. The latest social networking tools and services only make more visible the innate social nature and behaviour of humans. As dealing with and managing information security related to computer use and the Internet is currently considered both difficult and undesirable, working on and pursuing the social aspects of this interaction can help make security management more *human*. The mentioned cases highlight some of the possibilities and existing habits in sharing on security; however, many other avenues on such sharing activities around security are probably just around the corner and should be further explored.

## THE TOP 10 REFERENCES

1. Caldeira, T. P. R. City of Walls: Crime, Segregation, and Citizenship in São Paulo. Berkeley: University of California Press, 2000. xi. 487pp.
2. Cheskin Trust Study. eCommerce Trust: Building Trust in Digital Environments. A joint study with Studio Archetype/Sapient and Cheskin, January 1999. [http://www.cheskin.com/view\\_articles.php?id=17](http://www.cheskin.com/view_articles.php?id=17)
3. Egelman, S., King, J., Miller, R. C., Ragouzis, N., and Shehan, E. 2007. Security user studies: methodologies and best practices. In *CHI '07 Extended Abstracts on Human Factors in Computing Systems* (San Jose, CA, USA, April 28 - May 03, 2007). CHI '07. ACM, New York, NY, 2833-2836
4. Goecks, J., Edwards, W. K., and Mynatt, E. D. 2009. Challenges in supporting end-user privacy and security management with social navigation. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, July 15 - 17, 2009). SOUPS '09. ACM, New York, NY, 1-12.
5. Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (Oxford, United Kingdom, September 08 - 11, 2009). NSPW '09. ACM, New York, NY, 133-144
6. Koskela, Hille (2002). Video surveillance, gender and the safety of public urban space: "Peeping Tom" goes high tech? *Urban Geography*, 23:3, 257-278.
7. Lindgaard, G., Fernandes, G., Dudek, C. & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression!, *Behaviour & Information Technology*. 25, 115-126
8. Mathiasen, N. R. and Bødker, S. 2008. Threats or threads: from usable security to secure experience? In *Proceedings of the 5th Nordic Conference on Human-Computer interaction: Building Bridges* (Lund, Sweden, October 20 - 22, 2008). NordiCHI '08, vol. 358. ACM, New York, NY, 283-289
9. Németh, J and Hollander, J. 2010. Security Zones and New York City's Shrinking Public Space, in:

International Journal of Urban and Regional Research, Blackwell Publishing, vol. 34(1), pages 20-34, 03. Nissenbaum, H. 2005. Where Computer Security Meets National Security. *Ethics and Inf. Technol.* 7, 2 (Jun. 2005), 61-73

10. Schechter, S, Dhamija, R, Ozment, A, Fischer, I. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies. *IEEE Security & Privacy*, 2007

## PUBLISHED WORK IN THIS AREA

[K1] Kaur, P, Immonen, O, Kirichenko, A, Karvonen, K: *Social Sharing of Security Expertise*, a poster to appear in IEEE Symposium on Security and Privacy 2010, Oakland, CA, USA. Also published in Symposium on Usable Privacy and Security (SOUPS 2010), Microsoft, Redmond, WA, US. July 14-16, 2010

[K2] Valkonen, J, Toivonen, A, Karvonen, K: [Usability Testing for Secure Device Pairing in Home Networks](#), in: Proceedings of IWSSI 2007, First International Workshop on Security for Spontaneous Interaction, 9th International Conference on Ubiquitous Computing (UbiComp 2007), September 16-19, 2007, Innsbruck, Austria

[K3] Uzun, E, Karvonen, K, Asokan, N: [Usability Analysis of Secure Pairing Methods](#), in: Proceedings of Usable Security (USEC'07), February 15-16, 2007, Trinidad&Tobago, a workshop co-located with The Eleventh Conference on Financial Cryptography and Data Security (FC'07), Springer-Verlag LNCS

[K4] Kostiainen, K, Rantapuska, O, Moloney, S, Roto, V, Holmström, U, Karvonen, K: [Usable Access Control inside Home Networks](#), in: Symposium proceedings of The Third IEEE International Workshop on Trust, Security, and Privacy for Ubiquitous Computing, June 18 2007, Helsinki, Finland

[K5] Karvonen, K: [The Beauty of Simplicity](#), in: Proceedings of the ACM Conference on Universal Usability (CUU 2000), November 16-17, 2000, Washington DC, USA, pp. 85-90, ACM Press