Differences in Cross-Cultural and Individual Perception of Security and Privacy

Karoline Busse
University of Bonn
busse@cs.uni-bonn.de

Abstract

In the current academic discourse, security and privacy seem like a monolithic and rigid construct centered around best protection from the most powerful adversaries. From our own daily lives, we know that this theoretical image rarely matches the kind of security and privacy measures we implement in our daily communication. In the field of Usable Security and Privacy, we as researchers aim to incorporate the needs of users into our work. However, this research rarely encompasses individual needs or contexts in which security and privacy tools are used.

In this document I will outline the topic of my PhD thesis as well as published and planned research in the field of individual needs for security and privacy. Through qualitative as well as quantitative research, differences in security and privacy perception and behavior will be researched with emphasis on personal and cross-cultural contexts.

Are current research practices insufficient?

People are different, and so are their requirements and needs in regard to privacy and security [1]. A good example to illustrate the complexity of this problem is *threat modeling*, the first step in every security consultation: Who is the “attacker” against whom a person wants to protect their data and/or devices? Is it their younger sibling that might delete their savegames? Is it their ex-partner who can't let go? Is it a repressive government that would sanction or imprison the person if it found out about certain interests or features? Is it an internet-wide actor capable of mass surveillance and data aggregation? All these examples are equally valid adversaries, however, they are not equally addressed in today's research about (usable) security and privacy, where the emphasis is usually either on nation- or internet-wide adversaries.While defense against these powerful adversaries might be the "hardest" and has received a lot of attention by the research community [4, 12], many studies have shown that only a small fraction of end users actually regards these actors as a threat that requires actionable defense strategies [9, 17]. For most, these powerful adversaries remain too blurry to pose a real threat, which often leads to "nothing to hide" mentalities in the users' minds [10, 16].

In addition to these individual factors which vary from person to person, the user's cultural context plays another big role in determining requirements for usable security and privacy. Social sciences have since long found out that most research findings are only valid for the specific cultural and social context they were conducted with [14]. However, most research in our community focuses on US American or European sample groups and thus investigates the usability of the tools prominent in those regions. Meanwhile, there are huge populations in regions like East Asia, the Middle East, or Africa which are insufficiently considered in usable security and privacy research. It has been found out 15 years ago that it is not sufficient to simply apply study and experiment designs in a one to one fashion to these regions [8], instead we as researchers need to find out which cultural characteristics influence how people regard and interact with security and privacy enhancing tools in their respective cultural context. I argue that solely focusing on research in the US and Europe creates an imperialist view on Usable Security which is something we as a research community should actively avoid. Right now, regional practices and solutions to usable security problems are not considered actively in current research. Therefore, we need to work on our internalized imperialist and racist views and behaviour, we have to include non-western contexts (as well as researchers) in our everyday research procedures.

These examples of personal threat models and cultural context are only two out of many factors that shape an individual's perception of security and privacy. So far, these characteristics in security perception have rarely been researched, let alone in a cross-cultural context.

In my PhD thesis, I aim to improve this situation by performing studies about the perception of security and privacy in various contexts, where possible also in a cross-cultural fashion. My specific interest in this broad field is the gap between perceived and actual security resp. privacy. The main research questions that span my work are:

- Where are gaps between perceived and actual security resp. privacy and how do such gaps occur?
- To which extent do social and cultural factors lead to different perceptions of security and privacy?
- Are these gaps harmful for users, and if yes, how can we close them?

What work has been done before?

Perception of Security and Privacy

Gunson et al. as well as Weir et al. researched the trade-off between usability and security when it comes to banking or authentication [7, 18]. Another study conducted by Nilsson et al. shows that people have a distinct perception of security when they encounter various authentication methods [15]. Moreover, Chellappa et al. take a different path towards the perceived security in electronic commerce [5]. Four elements are presented: encryption, protection, verification, and authentication. Results show that perceived security has a relatively good effect on trust in electronic commerce, in comparison to reputation and financial liability. Kim et al. conducted a 219 participant survey in Korea, finding that perceived security and trust play a crucial role in the use of e-payment systems [11].

Security and Privacy in Non-Western Countries

In 2015, Alghamdi et al. published a study about banking practices and credential sharing in Saudi Arabia, a society where especially women have adapted in a unique fashion to their restricted mobility in public. In addition, the cultural value of family and the trust between family members leads to credential sharing within families, a habit that is rarely seen in typical Western societies and not even reflected in the terms and conditions of Saudi Arabian banks [2].

Another study by Lowry et al. investigated the effect of culture on privacy concerns within the application area of instant messaging. They conducted a study with participants from China and the United States and found out that cultural dimensions may act as predictors for privacy concerns [13].

These results indicate that a user's cultural and social context might shape their interaction and attitude towards security and privacy tools more than we currently acknowledge and need to be considered carefully when proposing new tools and mechanisms. What works well in a Western context might pose an impassable barrier or simply impractical for users in other cultural contexts [3].

What will I do to make it better?

My main directions of research can be summarized into two categories: Research about cross-cultural differences and similarities regarding security and privacy, and research about the gap between perceived and actual security resp. privacy. In this section, I will list my past and current research and give an outlook on planned next projects.

In 2016, I collaborated in a research project that investigated the gap between perceived and real performance and robustness of key-fingerprint representations like numbers or hexadecimal digits. We were able to show not only that dictionary-encoded English language strings lead to the best performance and robustness, but also that participants perceived alphanumerically encoded key-fingerprints as more "trustworthy" compared to the other representations, albeit all approaches were providing the same level of security [6]. This indicates a gap between perceived and actual security, which I want to explore deeper with my current and future work.

In 2017, I presented an interview study about insecurity and power dynamics around the term "IT Security" and its meanings in a company context at the annual European Workshop on Usable Security. Based on sociological theory about language insecurities in the work context and the resulting power dynamics, five interviews were conducted in a small German company. Statements revealed that a zone of insecurity indeed exists around the term. While the initial hypothesis was that these might be harmful to the work climate, the interview results showed the contrary: The zone of language insecurity creates space for productive discussion and mutual education about new research and development in the field of IT security. I am currently expanding this study to include a broader sample.

I am currently working on a quantitative study about the usage and perception of different payment instruments in a cross-cultural context. This study draws participants from user groups in Europe, Asia, the Middle East, and North America. The study results indicate interesting cultural differences, for example that Chinese participants heavily use mobile payment and banking services. This might stem from the country's isolated software landscape which allows for focusing on cultural features and characteristics which in turn might be important for widespread adaption of new technology. A prominent example of such adaptation would be the feature to send *red envelopes* through payment apps, a typical form of money gifts between friends or family members in China. To reference work by Alghamdi et al., we could also observe high trust and credential sharing within families or among relationship partners in our Middle Eastern population.

In the near future, I plan to conduct research on privacy habits in the physical and virtual world as well as specific perception gaps in fields like biometric authentication or ad blocking, where possible in a cross-cultural context. IP-based location filters in common recruitment tools such as MTurk or Crowdflower allow for easy realization of such research.

Conclusion

In this position paper, I underline the need for security and privacy research based on end users' individual characteristics. The research community could gain crucial insights from including factors like the cultural context a tool is used in, or the gap between individual perceptions of security or privacy and the actual features a tool does or does not offer and would thus be able to tailor solutions better to the world's population. With my research, I aim to start closing this gap and to open up space for discussion and collaboration around the globe.

REFERENCES

1. Alessandro Acquisti and Jens Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3, 1 (2005), 26–33.
2. Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. *SOUPS '15: Proceedings of the Eleventh Symposium on Usable Privacy and Security* (2015), 297–308.
3. Khaled Baqer, Ross Anderson, Lorna Mutegi, Jeunese Adrienne Payne, and Joseph Sevilla. 2017. DigiTally: Piloting Offline Payments for Phones. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 131–143. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/baqer
4. Nikita Borisov, George Danezis, and Ian Goldberg. 2015. DP5: A Private Presence Service. *PoPETs* 2015, 2 (2015), 4–24. http://www.degruyter.com/view/j/popets.2015.2015.issue-2/popets-2015-0008/popets-2015-0008.xml
5. Ramnath K Chellappa and Paul A Pavlou. 2002. Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management* 15, 5/6 (2002), 358–368.
6. Sergej Dechand, Dominik Schürmann, Karoline Busse, Yasemin Acar, Sascha Fahl, and Matthew Smith. 2016. An Empirical Study of Textual Key-Fingerprint Representations. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 193–208. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/dechand
7. Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security* 30, 4 (2011), 208–220.
8. Janet A Harkness, Fons JR Van de Vijver, Peter Ph Mohler, and others. 2003. *Cross-cultural survey methods*. Vol. 325. Wiley-Interscience Hoboken, NJ.
9. Cormac Herley. 2009. *So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users*. Technical Report. https://www.microsoft.com/en-us/research/publication/so-long-and-no-thanks-for-the-externalities-the-rational-rejection-of-security-advice-by-users/
10. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium on Usable Privacy and Security*. USENIX Association, 39–52.
11. Changsu Kim, Wang Tao, Namchul Shin, and Ki-Soo Kim. 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications* 9, 1 (2010), 84–95.
12. Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. 2016. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 279–296. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kogias

13. Paul Benjamin Lowry, Jinwei Cao, and Andrea Everard. 2011. Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems* 27, 4 (2011), 163–200. DOI: http://dx.doi.org/10.2753/MIS0742-1222270406

14. W. Lawrence Neuman. 2013. *Social Research Methods: Qualitative and Quantitative Approaches*. Pearson Education.

15. Maria Nilsson, Anne Adams, and Simon Herd. 2005. Building security and trust in online banking. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems*. ACM, 1701–1704.

16. Daniel J. Solove. 2007. I've Got Nothing to Hide and Other Misunderstandings of Privacy 2007 Editor's Symposium. *San Diego Law Review* 44 (2007), 745.

17. Geordie Stewart and David Lacey. 2012. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security* 20, 1 (2012), 29–38. DOI: http://dx.doi.org/10.1108/09685221211219182

18. Catherine S Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security* 28, 1 (2009), 47–62.